ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 5, Issue 2, February 2018

Steganography Techniques: A Survey

[1] Dipak U. Chaudhari, [2] Dr. Sahebrao B. Bagal
[1]M.E. (E&Tc), [2] Principal
[1][2] Late G.N. Sapkal, C.O.E., Nashik, Maharashtra, India

Abstract: **-- Steganography means the study of invisible communication. In Steganography usually, hide the existence of the communicated data in such a way that it remains confidential & it maintains secrecy between two communicating parties. Data hiding techniques have the crucial role in the rapid growth of secret communications & intensive transfer of multimedia content. The art of hiding information in ways that prevent detection is used in Steganography. Secrecy is achieved by embedding data into cover image and generating a stego-image, in image Steganography. Different types of steganography techniques are present & each has their strengths and weaknesses. In this paper, we review the different data hiding & security techniques that are used to implement a steganography.**

Keywords— DCT, Frequency Domain, LSB method, PSNR, Steganography

I. INTRODUCTION

Now a day, the communication is the basic necessity of every growing area. The secrecy and safety of communicating data is very important in today's life. In daily life, we use many secure pathways like internet and/or telephone for transferring and sharing information, but it's not totally safe. The rise of the Internet is the most important Factor in networking is the security of information. To share the information in a concealed manner two techniques are used & that techniques are cryptography and steganography. In cryptography, we used encryption key, the message is modified in an encrypted form with the help of encryption key. The encryption key known to sender and receiver only. The message cannot be accessed by the hacker without using the encryption key. However, the transmission of encrypted message may easily arouse attacker's suspicion, and the encrypted message may be intercepted, attacked or decrypted violently. In order to overcome the drawbacks of cryptographic techniques, the another techniques have been developed which is steganography. It is the art and science of communicating in such a way that it hides the existence of the communication. Steganography is derived from the Greek words "stegos" which means "cover" and "grafia" means "writing"[6] defining it as "covered writing". Thus, steganography techniques hides the existence of data so that no one can detect its presence. In the image Steganography the information is hidden mostly in images. In steganography techniques the process of hiding information content inside any multimedia content like image , audio, video is referred as a "Embedding". If we combined both the techniques the confidentiality of communicating data may be increased.
The idea of information hiding has a long past. The Greek historian Herodotus writes of the Nobleman, Histaeus, who communicate with his son-in-law in Greece, has shaved the head of one of the most trusted slave and tattooed the message onto the slave's scalp. When the slave's hair grew back he sends slave with a hidden message and when slave reaches to the destination again he shaved his scalp and retrieve the message [7]. In the Second World War the Germans introduces new data hiding technique which is known as Microdot technique. In this the information, like images, was reduced in size until it was the size of a typed period. It was Extremely too difficult to detect a hidden information, a normal cover message was sent over the insecure channel with one of the periods on the paper containing hidden information [8]. Now a day's Steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Steganography intent is to hide the existence of the message, while cryptography scrambles a message in such a way that it can't be understood [11]. Steganography and cryptography are techniques used to protect data from unwanted parties but neither technology alone is perfect. Once the presence of hidden information is suspected, the reason of Steganography is partly affected. The strength of system is increases when Steganography combining with cryptography.

The Steganography has been divided into (i) Spatial domain Steganography: It includes LSB Steganography and Bit Plane Complexity Slicing (BPS) algorithm. Spatial domain is mostly used because of high capability of hidden information and easy realization. (ii) Transform domain Steganography: The secret information is embed in the transform coefficients of the cover image. The transform domain Steganography examples are Discrete Cosine Transform, Discrete Wavelet

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 5, Issue 2, February 2018

transform and Discrete Fourier Transform. Steganography used for wide range of applications such as defense organizations for safe circulation of secret data, intelligence agencies, in smart identity cards where personal details are embedded in the photograph itself for copyright control of materials, medical imaging where patient's details are embedded within image providing protection of information and reducing transmission time.

The basic model for Steganography is shown on fig. (1). It shows basic process involved in Steganography which consists of Carrier, Message and Key. A carrier is also known as a cover-object, in which message is embeds and serves to hide the presence of the message. The different types of data (Ex. plain text, cipher text, different images) that the sender wants to remain confidential. Key is a stego-key, confirmed

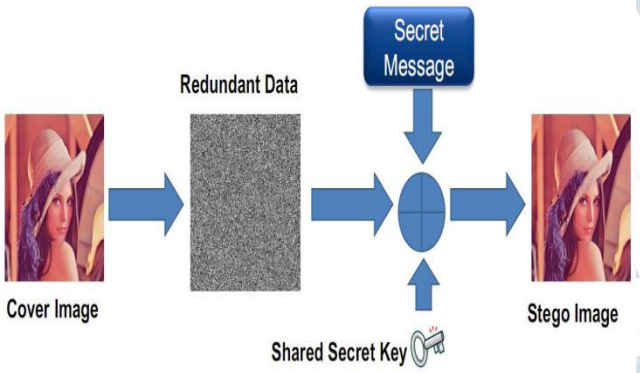

Fig. (1): Basic Model of Steganography

that only recipient who knows the key, related decoding key will be able to recover the message from a cover-object. The cover-object with the object secretly embedded message is then called as the stego-object [9]. Reconstruct the message from a stego-object requires the cover-object itself and a corresponding decoding key if a object stego-key was used during the information encoding process. The paper is organized in the following sections: Section II describes stenography principle. Section III describes types of Steganography. Section IV describes Image Steganography terminology. Section V describes Steganography techniques. Section VI explains factors affecting on Steganography method. Applications of Steganography are explained in section VII. Finally conclusion is presented in section VIII.

II. PRINCIPLE OF STEGANOGRAPHY

In Steganography the secret message is embedded inside the cover object in encrypted format by using hiding algorithm and it sent to a receiver over a network. At the receiver then decrypted the message by applying the reverse process on the cover data and reveals the secret data [9]. Fig. (2) shows the principle of Steganography. Steganography algorithm, tries to preserve the perceptive properties of original image. A suitable image, called as cover or carrier, is chosen. The secret message or information is then embedded into the cover using the Steganography algorithm, in a way that does not change the original image in a human noticeable way. The result image is new image, the stego-image, which is not looks different than original image.

Fig. (2): The principle of Steganography

III. TYPES OF STEGANOGRAPHY

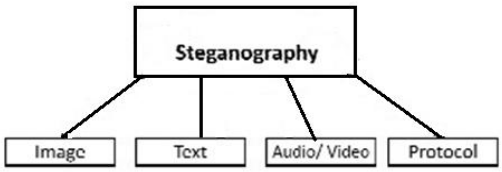

Fig (3): Types of Steganography

1. Steganography in Text: The Steganography consists of hiding information inside the text files. In this method, the secret information is hidden behind every nth letter of every words of text message. Numbers of methods are available for hiding information in text file. These methods are i) Format Based Method; ii) Random and Statistical Method; iii) Linguistics Method.

2. Steganography in Image: In this steganography hiding the information by taking the cover object as image. In image steganography pixel intensities are used to hide the information. In digital steganography, images are mostly used cover source because there are number of bits presents

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 5, Issue 2, February 2018

in digital representation of an image.

3. Steganography in Audio: In this steganography hiding data in audio files. In this method hides the information in WAV, AU and MP3 sound files. There are different types of audio steganography. They are i) Low Bit Encoding ii) Phase Coding iii) Spread Spectrum.

4. Steganography in Video: In this technique hiding the information any kind of files or information into digital video format. In this case video (combination of pictures) is used as carrier for hiding the information. Generally discrete cosine transform (DCT) alter the values (e.g., 5.667 to 6) which is used to hide the information in each of the images in the video, which is unavoidable by the human eye. The formats used by video steganography are H.264, Mp4, MPEG, AVI.
5. Steganography in Network: The technique involves hiding the information by taking the network protocol such as TCP, UDP, ICMP, IP etc, as cover object. . In the OSI layer network model there is a existing covert channels used steganography.

IV. STEGANOGRAPHY TERMINOLOGY

Steganography consists of two terms that is message and cover image. Message is the secret data that needs to hide and cover image is the carrier that hides the message in it.

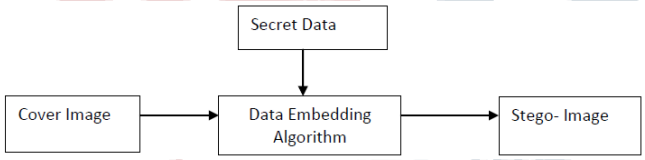

Fig 4: Steganography Diagram

V. STEGANOGRAPHY TECHNIQUES

Steganography in images are classified into two categories: 1.Spatial-domain based Steganography and 2. Transform domain based Steganography.

1. Spatial-Domain Method

In spatial domain based steganography the secret data is embedded directly in the intensity of pixels. It means some pixel values of image are changed directly during hiding data. Spatial domain techniques are classified into following categories: 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) Labeling or connectivity method vii) Pixel intensity based. In this method, the most common and simplest Steganography method is the least significant bits (LSB) insertion method. In LSB technique, least significant bits of the pixels are replaced by the message bits which are permuted before embedding [1].

1.1 Least Significant Bit Technique

The Least Significant Bit Technique is most commonly used for hiding data. In this technique the embedding is done by replacing the least significant bits of image pixels with the bits of secret data. The image obtained after embedding is almost similar to original image because the change in the Least Significant Bit of image pixel does not bring too much differences in the image. The Least significant bit (LSB) replacement is a common, simple approach to embedding information in a cover image. The least significant bit (8th bit) of some or all of the bytes inside an image is replaced with a bit of the hidden message. If we used a 24-bit image, a bit of each of the R, G and B color can be used, since they are each represented by a byte. i. e. one can store 3 bits in each pixel. The image of 800 X 600 pixel, therefore store a total amount of 1,440,000 bits or 180,000 bytes of embedded data[5].

For example, 3 pixels grid for the 24-bit image can be as follows:
(00101101 00011101 11011100)
(10100111 11000101 00001101)
(11010011 10101101 01100010)

When the number 300, which binary representation is 100101100, is embedded into the least significant bits of this part of the image. The resulting grid is as follows:
(00101101 00011100 11011100)
(10100111 11000100 00001101)
(11010011 10101100 01100010)

The number shown by above was embedded into the first 8 bytes of the grid, from these only the 3 underlined bits needed to be changed according to the message which is embedded. On average, only half of the bits in an image will need to be modified to hiding a secret message using the maximum cover size. Since there are total possible intensities of each primary color is 256, By changing the Least significant bit of a pixel results in small changes in the intensity of the colors. These changes cannot be detect by the human eye, thus the message is successfully hidden in image.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 5, Issue 2, February 2018

Fig 4: The cover image

Fig 5: The stego-image

1.2 Pixel Value Differencing (PVD): In PVD method, two consecutive pixels are selected for embedding the data. Payload is determined by checking the difference between two consecutive pixels and it serves as basis for identifying whether the two pixels belongs to an smooth area.

1.3 Hiding The Gray Images Using Blocks Technique

Now a day's internet is becoming very popular, channels for communication the security of digital media becomes a greater issue. By hiding of a message will reduce the possibility of detecting the secret message. In this method allows to hides gray image in one another and also the cover is divided into blocks of equal sizes and each block size is same as that size of the embedding image[9]. Compare the each pixel in embedding image with all the corresponding pixels in the blocks of the cover image that is pixel (i,j) in the embedding image is compared with the pixel (i,j) in all C blocks of cover image. Select a best pixel to embed. Best pixel is a pixel that gives minimum difference between it and the pixel to embed. For Example, if pixel (i,j) to embed has a value 250, and corresponding pixels values are: 248, 230, 249, 252, 255,260, 270, and 262 (assume cover is divided into 8 blocks). Then the pixel with value 249 will be selected to embed 250.

2. Transform Domain Method

In Transform domain technique; the secret message is embedded in the transform or frequency domain of the cover. The transform domain Steganography technique is used for hiding large amount of data and provides high security, good invisibility and no loss of secret message This is a more complex way of hiding the message in an image. Different algorithms and transformations are used on the image to hide the message in it. Transform domain techniques are broadly classified such as i) Discrete Fourier transformation technique (DFT) ii) Discrete cosine transformation technique (DCT) iii) Discrete Wavelet transformation technique (DWT) iv) Lossless or reversible method (DCT) iv)Embedding in coefficient bits. The 2-D DCT converts image blocks from spatial domain to a frequency domain. The cover image is divided into non overlapping blocks of size 8×8 and applies DCT on each of blocks of cover image using the forward DCT [2].

2.1 JPEG Image Steganography Technique

Steganography would not be possible to use with the JPEG images, since they use lossy compression which results in parts of the image information being altered. One of key characteristics of Steganography is the fact that information is hidden in the redundant bits of an object and since redundant bits are left out when using JPEG it was feared that the hidden message would be damaged. Even a one could somehow keep the message intact it would be difficult to embed the message without the changes being noticeable because of the harsh compression applied. Still, properties of a compression algorithm have been exploited in order to develop a steganography algorithm for JPEGs[5]. One of these properties of JPEG is exploited to make changes to the image unseen to the human eye. During the DCT transformation phase of compression algorithm, rounding errors occur in the coefficient data that are not noticeable and understandable. Although this property is what classifies the algorithm as being lossy, this property can also be used to hide messages. It is neither feasible nor possible to embed information in an image that uses the lossy compression, since the compression would destroy all information in the process. So, it is very important to recognize that the JPEG compression algorithm is actually divided into lossy and lossless stages. The quantization and DCT phase form part of the lossy stage, whereas the Huffman encoding used to further compress the data is lossless.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 5, Issue 2, February 2018

Steganography can take place between these two stages. Using the same principles of LSB insertion the message can be embedded into the LSB of the coefficients before applying the Huffman encoding. By embedding the information at this stage, in transform domain, it is extremely hard to detect, since it is not in the visual domain.

2.2 Spread Spectrum Image Steganography Technique

The concept of spread spectrum is used in this technique. In this technique the secret data is spread over a wide frequency bandwidth. The signal to noise ratio in every frequency band must be so small that it become difficult to detect the presence of data. Even if some parts of data are removed from several bands, there would be still enough information is present in other bands to recover the data. Thus it is difficult to remove the data completely without entirely destroying the cover. It is a very robust technique used in military communication. The spread spectrum image steganography of present invention is a data hiding or secret communication steganography system which uses digital imagery as a cover signal. Spread spectrum provides ability to hide a significant quantity of information bits within digital images while avoiding detection by an observer. The messages are recovered with lowest error probability due the use of error control coding. Spread spectrum image steganography payload , at a minimum, an order of magnitude greater than of existing watermarking techniques. Furthermore, the original images are not needed to extract the hidden messages. The proposed receiver needs only possess a key in order to reveal the secret messages. The existence of hidden information is virtually undetectable by human or computer analysis. at last, SSIS provides resiliency to transmission noise, like which found in the wireless environment and low levels of compression.

VI. FACTORS AFFECTING ON STEGANOGRAPHY METHOD

The effectiveness of any steganography method can be determined by comparing stego-image with cover Image. There are some factors that determines the efficiency of a technique. These factors are :

1. Invisibility : The invisibility means imperceptibility of Steganography algorithm and it is most important requirement. Strength of a Steganography lies in its ability to be unnoticed by human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised [3].

2. Payload capacity : Payload capacity refers to the amount of secret information that can be hidden in the cover source. Watermarking usually embed only small amount of copyright information, whereas the steganography focus at hidden communication and therefore have sufficient embedding capacity. Watermarking, needs to embed only a small amount of copyright information. In other hand Steganography requires a sufficient embedding capacity [4].

3. Robustness against statistical attacks : Robustness refers to the ability of embedded data to remain intact if the stego image undergoes transformations, such as linear and non-linear filtering, sharpening/blurring, addition of random noise, rotations and scaling, cropping or decimation, lossy compression. Statistical Steg analysis is practice of detecting hidden information by applying statistical tests on image data. Many Steganography algorithms leave "signature" when embedding information that can be easily detected through statistical analysis.

4. Robustness against image manipulation : While being transmitted the image may undergo changes by an active attacker in an attempt to remove hidden data. Image manipulation, such as cropping or rotating, can be performed on a image. This may destroy a hidden message. It is required for Steganography algorithms to be robust against malicious changes the image.

5. Independent of file format : The most powerful Steganography algorithm thus possess the ability to embed information in any type of file.

6. Unsuspicious files : This requirement includes all characteristics of the Steganography algorithm that may result in images that are not used normally and may cause suspicion. Abnormal file size, for example, is one property of an image that can result in further investigation of the image by warden.

7. Peak Signal to Noise Ratio (PSNR) : The PSNR 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 compressed image. The higher value of PSNR represents the better quality of a compressed image.

8. Mean Square Error (MSE) : It is defined as the average squared difference between a reference image and distorted image. The smaller the MSE, more efficient the image steganography technique . MSE is computed pixel-by-pixel by adding up a squared differences of all the pixels and dividing by the total pixel count.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 5, Issue 2, February 2018

VII. APPLICATION OF STEGANOGRAPHY:

i) Database Systems Confidential Communication and Secret Data Storing
ii) Digital watermarking
iii) Access Control System for Digital Content Distribution
iv) E-Commerce
v) Media
vi) Systems Confidential Communication and Secret Data Storing
vii) Protection of Data Alteration

VIII. CONCLUSION

In this research paper we reviewed many papers on steganography techniques. These papers are very helpful and have wide future scope .By reviewing these papers we observed that most of the steganography work is done in the past years. Now, LSB is the most widely used technique for steganography. Some researchers have also used the techniques like spatial technique, water marking, distortion technique, ISB, MSB in their work and provided a strong means of secure information transmission. Different image file formats have different methods of data hiding messages, that having different strong and weak points respectively. For example, the patchwork approach has very high level of robustness against most type of attacks, but it can hides only very small amount of information. The LSB technique in both BMP and GIF makes up for this, but these both approaches result in suspicious files that increase the probability of detection when in the presence of a warden. Whereas one technique lacks in a payload capacity, while other lacks in robustness. Most of the papers that are discussed here are taken from IEEE Explore, IJCA, AICCSA, IJET, IJCSE etc. These papers provide a lot of help to the researcher for starting their work in this field. This review paper is more helpful for them to start their work in this field. The different security and data hiding techniques are used to implement steganography using ISB, LSB, MLSB .In next research we are going to use more advance schemes like steganography with some hybrid cryptographic algorithm for enhancing the data security.

REFERENCES

[1] Johnson, N.F and Jajodia, S., "Exploring Steganography:Seeing the Unseen", Computer Journal, February 2008.

[2] Blossom kaur1, Amandeep kaur2 and Jasdeep singh,"Steganographic approach for hiding image in dct domain" International Journal of Advances in Engineering & Technology, July 2011.

[3] R.Amirtharajan and R.Akila," A Comparative Analysisof Image Steganography;" International Journal of ComputerApplications (0975 – 8887) ,Volume 2 – No.3, May 2010.

[4] V. Nagaraj, Dr. V. Vijayalakshmi and Dr. G. Zayaraz, "Modulo based Image Steganography Technique against Statistical and Histogram Analysis", IJCA Special Issue on"Network Security and Cryptography" NSC, 2011.

[5] Dumitrescu, S., W. Xiaolin and Z. Wang, 2003. Detection of LSB steganography via sample pair analysis. In: LNCS, Vol. 2578, Springer-Verlag, New York, pp: 355 -372.

[6] T. Sharp, "An implementation of key-based digital signal Steganography", in Proc. Information Hiding Workshop,Springer LNCS 2137, pp. 13–26, 2001.

[7] Jarno Mielikainen, "LSB Matching Revisited", Signal Processing Letters, IEEE, Publication Date: May 2006Volume : 13, Issue : 5, pp. 285- 287.

[8] K..M. Singh, L.S. Singh, A.B. Singh and K.S. Devi,"Hiding Secret Message in Edges of the Images", Information and Communication Technology, 2007. ICICT '07, pp. 238-241.

[9] Jagvinder Kaur and Sanjeev Kumar, " Study and Analysis of Various Image Steganography Techniques" IJCST Vol.2, Issue 3, September 2011

[10] Lee, Y.K.; Chen, and L.H., "High capacity image Steganographic model", Visual Image Signal Processing, 147:03,June 2008

[11] Ahn, L.V. and N.J. Hopper, 2004. Public-key steganography. In Lecture Notes in Computer Science.Vol. 3027 /2004 of Advances in Cryptology - EUROCRYPT 2004, pp: 323–341. Springer-Verlag Heidelberg.

[12]Yang, Chunfang., Liu, Fenlin., Luo, Xiangyang., and Zeng, Ying., "Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, January 2013.

[13] Ishwarjot Singh ,J.P Raina," Advance Scheme for Secret Data Hiding System using Hop field & LSB" International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013.

[14] G. Manikandan, N. Sairam and M. Kamarasan "A Hybrid Approach for Security Enhancement by Compressed Crypto-Stegno Scheme ", Research Journal of Applied Sciences, Engineering and Technology 4(6): 608-614, 2012

[15] Shabir A. Parah, Javaid A. Sheikh, G.M. Bhat, "Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique", International Conference on Emerging Trends in Science, Engineering and Technology , pp.192-197, July 2012.

[16] Michel K. Kulhandjian, Dimitris A. Pados, Ming Li, Stella N. Batalama, and Michael J. Medley, "Extracting spread-spectrum hidden data from digital media ", IEEE transactions on information forensics and security, vol. 8, no. 7, july 2013.

[17] Chang, Chin-Chen., Lin, Iuan-Chang., and Yaun-Hui YU., " A new Steganographic method for color and gray scale image hiding", Computer Vision and Image Understanding, ELSEVIER, Vol. 107, No. 3, pp. 183-194,2007.

[18] Bailey, K., and Curran, K., "An Evaluation of Image Based Steganography Methods", Journal of Multimedia Tools and Applications, Vol. 30, No. 1, pp. 55-88, 2006.

[19] 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), pp: 400-403, 10-13 May 2009.

[20] Swati malik, Ajit "Securing Data by Using Cryptography with Steganography" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

Mr. Dipak U. Chaudhari from Late G. N. Sapkal College of Engineering, Nashik, Savitribai Phule University Pune. The area of interest is signal processing. Presently working at N.D.M.V.P.S's., College of Engineering, Nashik in the department of Electronics and Telecommunication Engineering.

Dr. Sahebrao B. Bagal has completed his M.E. in Electronics and Ph. D. in E&TC from S.R.T.M. University, Nanded. His area of interest is Signal Processing. Presently he is working as a Professor and Principal at Late G. N. Sapkal College of Engineering, Anjaneri, Nashik.