Steganography Techniques

SOURABH AGARWAL [1], MANOJ GUPTA [2]
[1,2]*Dept. of CSE, Poornima College of Engineering, Jaipur*

Abstract -- Steganography is defined as the study of invisible communication. Steganography usually deals with the ways of hiding the existence of the communicated data in such a way that it remains confidential. Steganography is the technique of hiding private or sensitive information within something that appears to be nothing out of the usual. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. It maintains secrecy between two communicating parties. In image steganography, secrecy is achieved by embedding data into cover image and generating a stego-image. There are different types of steganography techniques each have their strengths and weaknesses. In the Steganography is secret writing or hiding fact that communication taking place, by hiding secret information inside image. The scope of project is implementation of steganography tools for information includes any type of information file and image file and path where user want to retrieve the information file. For hiding information in image, their exist large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points

Indexed Terms -- Steganography, Cryptography, LSB, BPCP, PVD, DCT, PSNR

I. INTRODUCTION

In today's world, the communication is the basic necessity of every growing area. Everyone wants the secrecy and safety of their communicating data. In our daily life, we use many secure pathways like internet or telephone for transferring and sharing information, but it's not safe at a certain level. In order to share the information in a concealed manner two techniques could be used. These systems are cryptography and steganography. . In cryptography, the message is adjusted in an encoded shape with the assistance of encryption key which is known to sender and beneficiary as it were. The message can't be gotten to by anybody without utilizing the encryption key. Be that as it may, the transmission of scrambled message may effortlessly stimulate assailant's doubt, and the encoded message may along these lines be captured, assaulted or unscrambled viciously. With a specific end goal to beat the weaknesses of cryptographic systems, steganography strategies have been created. Steganography is the craftsmanship and art of conveying such that it conceals the presence of the correspondence. Along these lines, steganography shrouds the presence of information with the goal that nobody can identify its essence. In steganography the way toward concealing data content inside any sight and sound substance like picture, sound, video is alluded as an "Inserting". For expanding the privacy of conveying information both the procedures might be consolidated. The rest of the paper comprise of following segment: II. Steganography III. Conclusion and Future Work

II. STEGANOGRAPHY

Steganography is a Greek word which implies covered written work. "Steganos" signifies "secured" and "graphical" signifies "stating". In this way, steganography isn't just the specialty of concealing information yet in addition concealing the reality of transmission of mystery information. Steganography conceals the mystery information in another document such that lone the beneficiary knows the presence of message. In old time, the information was secured by concealing it on the back of wax, composing tables, stomach of rabbits or on the scalp of the slaves. In any case, the present a large portion of the general population transmit the information as content, pictures, video, and sound over the medium. Keeping in mind the end goal to securely transmission of classified information, the media question like sound, video, pictures are utilized as a cover sources to shroud the information.

a) Types of Steganography:

1. Text Steganography:

It consists of hiding information inside the text files. In this method, the secret data is hidden behind every

nth letter of every words of text message. Numbers of methods are available for hiding data in text file. These methods are i) Format Based Method; ii) Random and Statistical Method; iii) Linguistics Method.

2. Image Steganography:
Hiding the data by taking the cover object as image is referred as image steganography. In image steganography pixel intensities are used to hide the data. In digital steganography, images are widely used cover source because there are number of bits presents in digital representation of an image.

3. Audio Steganography:
It involves hiding data in audio files. This method hides the data in WAV, AU and MP3sound files. There are different methods of audio steganography. These methods are i) Low Bit Encoding ii) Phase Coding iii) Spread Spectrum.

4. Video Steganography:
It is a technique of hiding any kind of files or data into digital video format. In this case video (combination of pictures) is used as carrier for hiding the data. Generally discrete cosine transform (DCT) alter the values (e.g., 8.667 to 9) which is used to hide the data in each of the images in the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the formats used by video steganography.

5. Network or Protocol Steganography:
It 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 exist covert channels where steganography can be used.

b) 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.

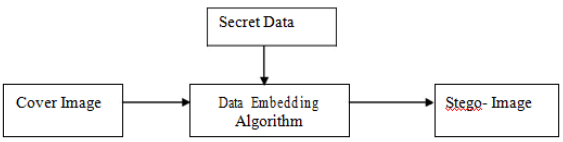

Fig. 1: - Steganography Diagram

c) Steganography Techniques:

1. Spatial Space Strategies:
In this strategy the mystery information is implanted straightforwardly in the force of pixels. It implies some pixel estimations of the picture are changed straightforwardly amid concealing information. Spatial area systems are grouped into following classifications: i)Least noteworthy piece (LSB) ii) Pixel esteem differencing (PVD) iii) Edges based information installing technique (EBE) iv) Arbitrary pixel inserting strategy (RPE) v)Mapping pixel to shrouded information technique vi) Naming or availability strategy vii) Pixel force based.

i) LSB: this technique is most ordinarily utilized for concealing information. In this strategy the installing is finished by supplanting the minimum critical bits of picture pixels with the bits of mystery information. The picture acquired in the wake of installing is relatively like unique picture in light of the fact that the adjustment in the LSB of picture pixel does not get excessively contrasts the picture.

ii) BPCP: In this division of picture are utilized by estimating its multifaceted nature. Intricacy is utilized to decide the loud square. In this technique loud squares of bit design are supplanted by the parallel examples mapped from a mystery information

iii) PVD: In this strategy, two successive pixels are chosen for inserting the information. Payload is dictated by checking the distinction between two successive pixels and it fills in as reason for distinguishing whether the two pixels has a place with an edge territory or smooth zone.

2. Spread Range Strategy:
The idea of spread range is utilized as a part of this procedure. In this strategy the mystery information is spread over a wide recurrence data transfer capacity. The proportion of flag to clamor in each recurrence band must be small to the point that it wind up hard to identify the nearness of information. Regardless of whether parts of information are expelled from a few

groups, there would be sufficiently still data is available in different groups to recuperate the information. Therefore it is hard to expel the information totally without annihilating the cover .It is an extremely hearty system for the most part utilized as a part of military correspondence.

3. Statistical Procedure:

In the system message is installed by changing a few properties of the cover. It includes the part of cover into pieces and after that implanting one message bit in each square. The cover piece is altered just when the span of message bit is one generally no change is required.

4. Transform Domain Technique:

In this technique; the secret message is embedded in the transform or frequency domain of the cover. This is a more complex way of hiding message in an image. Different algorithms and transformations are used on the image to hide 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

5. Distortion Techniques:

In this technique the secret message is stored by distorting the signal. A sequence of modification is applied to the cover by the encoder. The decoder measures the differences between the original cover and the distorted cover to detect the sequence of modifications and consequently recover the secret message.

6. Masking and Filtering:

These techniques hide information by marking an image. Steganography only hides the information whereas watermarks becomes a portion of the image. These techniques embed the information in the more significant areas rather than hiding it into the noise level. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image. This method is basically used for 24-bit and grey scale images.

d) Factors Affecting a Steganography Method:

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

1. Robustness:

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 or blurring, addition of random noise, rotations and scaling, cropping or decimation, lossy compression

2. Imperceptibility:

The imperceptibility means invisibility of a steganography algorithm. Because it is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye.

3. 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.

4. PSNR (Peak Signal to Noise Ratio):

It is defined as the ratio between the maximum possible powers 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.

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

6. SNR (Signal to Noise Ratio):

It is the ratio between the signal power and the noise power. It compares the level of adesired signal to the level of background noise.

e) Application of Steganeography:

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

III. CONCLUSION AND FUTURE WORK

In this exploration work we audited numerous papers on steganography systems. These papers are adequate and have wide future degree .By inspecting these papers we watched that a large portion of the steganography work is done in the year 2012 and 2013. In these years, LSB is the most generally utilized procedure for steganography. A few analysts have likewise utilized the strategies like water checking, twisting procedure, spatial strategy, ISB, MSB in their work and gave a solid method for secure data transmission. The majority of the papers that are talked about here are taken from IEEE Investigate, AICCSA, IJET, IJCSE, IJCA and so on. These papers give a considerable measure of assistance to the initiator for beginning their work in this field. This audit paper is sufficient for them to begin their work in this field. The diverse security and information concealing methods are utilized to actualize steganography utilizing LSB,ISB, MLSB .In additionally inquire about we will utilize more propel plans like steganography with some half breed cryptographic calculation for improving the information security.

REFERENCES

[1] 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 2015

[2] 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 2014

[3] 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 2012

[4] 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

[5] Shabir A. Parah, Javaid A. Sheikh, G.M. Bhat, *"Data Hiding in Intermediate Significant Bit Planes, A High Capacity BlindSteganographic Technique",* International Conference on Emerging Trends in Science, Engineering and Technology , pp.192-197, July 2016.

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

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

[8] 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, 2014.

[9] Adnan Gutub, Ayed Al-Qahtani, AbdulazizTabakh, "*Triple-A: Secure RGB Image Steganography Based on Randomization",* International Conference on Computer Systems and Applications (AICCSA-2009), pp: 400-403,10-13 May 2016.

[10] R.Amirtharajan, Sandeep Kumar Behera, MotamarriAbhilashSwarup, Mohamed Ashfaaq and John BoscoBalaguruRayappan*, "Colour Guided Colour Image Steganography*"

Universal Journal of Computer Science and Engineering Technology , 16-23, Oct. 2016, pp. 2219-2158.

[11] Anil Kumar , RohiniSharma,*"ASecure Image Steganography Based on RSA Algorithm and Hash-LSB Technique* ",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2017.

[12] Gutub, A., Al-Qahtani, A., and Tabakh, A., *"Triple-A: Secure RGB image steganography based onrandomization*", Computer Systems and Applications, AICCSA 2009, IEEE/ACS, pp. 400 –403, 2009..

[13] Dr. Fadhil Salman Abed "*A Proposed Method of Information Hiding Based on Hybrid Cryptography andSteganography* ", IJAIEM, Volume 2, Issue 4, April 2015

[14] K. S. Babu, K. B. Raja, K. Kiran Kumar, T. H. Manjula Devi, K. R. Venugopal and L. M. Pataki, *"Authenticationof secret information in image steganography"*, IEEE Region 10 Conference, TENCON-2008, (2008) November,pp. 1-6.

[15] M. Chaumont and W. Puech, *"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 byEURASIP, (2006) September 4-8.

[16] A. M. Hamid and M. L. M. Kiah, *"Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis*", International Journal of Engineering and Technology (IJET): 0975-4042, (2009).