International Journal of Advanced Trends in Computer Applications
www.ijatca.com

Art of Steganography

NazInder Kaur[1], Amanjot Kaur[2]
[1]Research Scholar, [2]Assistant Professor,
[1,2]Baba Banda Singh Bahadur Engineering College (Fatehgarh Sahib) India
[1]nazinderbhullar279@gmail.com, [2]amanjot.kaur@bbsbec.ac.in

Abstract: *Steganography is defined as study of imperceptible conversation. Steganography typically deals with approaches of hiding presence of communicated information in sort of manner that it stays confidential. It preserves secrecy among two communicating groups. In image steganography, secrecy is attained by means of embedding records into cover image and producing a stego- image. There are distinct kind of steganography strategies each have their strengths and weaknesses. In this paper, we review distinct security and data hiding approaches that are utilized to implement a steganography for instance LSB, ISB, and MLSB etc.*

I. INTRODUCTION

Nowadays, communication is primary necessity of every developing area. Everyone needs secrecy and protection in their communicating records. In our daily life, we utilize many secure pathways like internet or telephone for transferring and sharing information, but it's no longer secure at a certain stage. In order to share data in concealed manner two approaches could be utilized. These mechanisms are cryptography and steganography. In cryptography, message is changed in an encrypted form with assist of encryption key which is known to sender and receiver only. Message cannot be accessed by anyone without using encryption key. However, transmission of encrypted message may also easily stimulate attacker's suspicion, and encrypted message can also consequently be intercepted, attacked or decrypted violently. In order to overcome deficiencies of cryptographic approach, steganography strategies were developed. Steganography is art and science of communicating in this kind of manner that it hides existence of communication. Thus, steganography hides existence of information so that no one can discover its presence. In steganography procedure of hiding data content inside any multimedia content like image, audio, video is referred as an "Embedding". For enhancing confidentiality of communicating data both approaches may be combined. Remaining paper includes following section: II. Steganography III. Conclusion and Future Work.

II. STEGANOGRAPHY

Steganography is a Greek word which means concealed writing. Word "stegano" means "covered "and "graphical "means "writing". Thus, steganography isn't only art of hiding information however also hiding fact of transmission of secret information. Steganography hides secret data in some other file in such a way that only recipient knows existence of message. In historic time, information was protected by hiding it on back of wax, writing tables, and stomach of rabbits or at the scalp of slaves. But today's most of people convey information in form of text, images, video, and audio over medium. In order to safely transmission of confidential information, multimedia object like audio, video, images are utilized as a cover sources to hide facts

A. Types of Steganography

1. Text Steganography: It comprises of hiding data inside text documents. In this approach, secret information is hidden behind every nth letter of each words of text message. Numbers of approaches are available for hiding data in text file. These approaches are i) Format Based approach; ii) Random and Statistical approach; iii) Linguistics approach.

2. Image Steganography: Hiding information by taking cover object as image is denoted as image steganography. In image steganography pixel intensities are utilized to hide information. In digital steganography, images are extensively utilized cover source because there are number of bits presents in digital depiction of an image.

3. Audio Steganography: It involves hiding data in audio documents. This approach hides information in WAV, AU and MP3 sound documents. There are distinct approaches of audio steganography. These

approaches are i) Low Bit Encoding ii) Phase Coding iii) Spread Spectrum.

4. Video Steganography: It is a technique of hiding any type of document or data into digital video format. In this case video is utilized as carrier for hiding information. Generally DCT alter which is utilized to hide data in each of images in video, which is unnoticeable by human eye. H.264, Mp4, MPEG, AVI are formats utilized by video steganography.

5. Network or Protocol Steganography: It includes hiding data by taking network protocol for instance TCP, UDP, ICMP, IP etc., as cover object. In OSI layer network model there exist covert channels where steganography can be utilized.

B. Steganography Terminology

Steganography contain two terms that is message and cover image. Message is secret information that requireshiding and cover image is carrier that hides message in it.

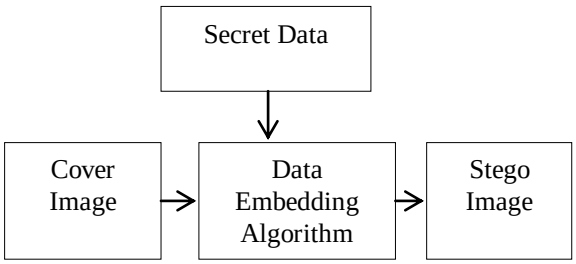

Fig 1: Steganography Diagram

C. Steganography Techniques

1. Spatial Domain Technique: in this Technique secret information is embedded directly in intensity of pixels. It means few pixel values of image are altered directly during hiding information. This is classified into following types: 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) Labelling or connectivity method vii) Pixel intensity based.

i) LSB: this Technique is most usually utilized for hiding information. In this technique inserting is done by exchanging least significant bits of image pixels with bits of secret information. Image gotten after embedding is almost similar to real image because change in LSB of image pixel does not bring too much difference in image.

ii) BPCP: In this segmentation of image are utilized by measuring its complexity. Complexity is used to determine the noisy block. In this method noisy blocks of bit plan are replaced by the binary patterns mapped from a secret data

iii) PVD: In this method, two consecutive pixels are selected for embedding data. Payload is determined by checking difference among two consecutive pixels and it serves as base for recognizing whether two pixels belong to an edge area or smooth area.

2. Spread Spectrum Technique: Concept of spread spectrum is utilized in this approach. In this approach secret information is spread over a wide frequency bandwidth. Ratio of signal to noise in each frequency band must be so small that it becomes hard to detect presence of information. Even if portion of information are erased from numerous bands, there would be still sufficient data is exist in other bands to recover information. Thus it is hard to eliminate information totally without totally abolishing cover. It is a very strong approach mostly utilized in military communication.

3. Statistical Technique: In this approach message is embedded by changing numerous properties of cover. It contains splitting of cover into blocks and then embedding one message bit in every block. Cover block is altered only when size of message bit is one otherwise no modification is essential.

4. Transform Domain Technique: In this approach; secret message is embedded in transform or frequency domain of cover. This is a more complex way of hiding message in an image. Distinct algorithms and transformations are utilized on image to hide message in it. Transform domain approaches are generally classified such as i) Discrete Fourier transformation approach (DFT) ii) Discrete cosine transformation approach (DCT) iii) Discrete Wavelet transformation approach (DWT) iv) Lossless or reversible approach iv)Embedding in coefficient bits

5. Distortion Techniques: In this approach secret message is stored by distorting signal. A set of modification is applied to cover by encoder. Decoder measures differences among real cover and distorted cover to detect set of modifications and consequently recover secret message.

6. Masking and Filtering: These approaches hide data by marking an image. Steganography only hides data whereas watermarks become a portion of image. These approaches add data in more important areas rather than hiding it into noise level. Watermarking approaches can be applied without fear of image destruction due to lossy compression as they are more joined into image. This

approach is essentially utilized for 24-bit and grey scale images.

D. Factors Affecting a Steganographic Method

Effectiveness of any Steganographic approach can be determined by comparing stego-image with cover Image. There are few factors that determine efficiency of a technique. These factors are:

1) Robustness: It refers to capability of embedded information to remain intact if stego- image undergoes transformations, for instance linear and non-linear filtering, sharpening or blurring, addition of random noise, rotations and scaling, cropping or decimation, lossy compression.

2) Imperceptibility: It means invisibility of a Steganographic algorithm. Because it is first and foremost requirement, since strength of steganography lies in its capability to be unnoticed by human eye.

3) Payload Capacity: It refers to quantity of secret data that can be hidden in cover source. Watermarking typically embed only a small amount of copyright data, whereas, steganography focus at hidden communication and therefore have sufficient embedding capacity.

4) PSNR (Peak Signal to Noise Ratio): It is defined as ratio among maximum possible power of a signal and power of corrupting noise that affects the fidelity of its representation. This ratio measures the quality between theoriginal 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 average squared difference among a reference image and a distorted image. Smaller the MSE, more efficient the image steganography technique. MSE is calculated pixel-by-pixel by adding up squared differences of all pixels and dividing by total pixel count.

E. Application of Steganography

1. Confidential Communication and Secret Data Storing
2. Digital watermarking
3. E-Commerce
4. Protection of Data Alteration
5. Media
6. Database Systems
7. Access Control System for Digital Content Distribution

F. Limitations of Steganography

1. Steganography hides a message, but if somebody recognizes message is there, message can be read. To avoid this, cryptography joint with steganography is utilized. For instance, message could be encrypted before it is hidden. Consequently, even if message is found, it cannot be read.

2. If somebody accused that Steganography is being utilized, hidden message can be demolished. For instance, if information is hidden within an image, message is typically embedded into least important bits. Hence, if bit composition modifies even a little, message is destroyed.

3. Additional drawback is due to size of medium being utilized to hide information. Message should be hidden in such a manner that it needs least modifications in cover source in which it is embedded.

III.CONCLUSION

In this work we studied many papers on steganography methods. These papers are enough and have large future scope. By studying these papers we perceived that most of steganography work is done in year 2012 & 2013. In these years, LSB is most commonly utilized method for steganography. Few researchers have also utilized methods like water marking, distortion technique, spatial method, MSB in their work and provided a strong means of secure data transmission. With the help of Wavelet transform, an unintentional viewer will not be aware of very existence of secret-image. Distinct security and data hiding methods are utilized to implement steganography utilizing LSB, and MLSB. In advance research we are going to utilize more advance schemes like steganography with few hybrid cryptographic or wavelet algorithms for increasing data 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 2013.

[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 2013

[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 2013.

[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 Blind Steganographic Technique", International Conference on Emerging Trends in Science, Engineering and Technology , pp.192-197, July 2012.

[6] 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.

[7] 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.

[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, 2006.

[9] 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.

[10] R.Amirtharajan, Sandeep Kumar Behera, Motamarri Abhilash Swarup, Mohamed Ashfaaq and John Bosco Balaguru Rayappan , "Colour Guided Colour Image Steganography" Universal Journal of Computer Science and Engineering Technology , 16-23, Oct. 2010, pp. 2219-2158.

[11] Anil Kumar, Rohini Sharma,"A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7,July 2013.

[12] Gutub, A., Al-Qahtani, A., and Tabakh, A., "Triple-A: Secure RGB image steganography based on randomization", 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 and Steganography ", IJAIEM, Volume 2, Issue 4, April 2013

[14] K. S. Babu, K. B. Raja, K. Kiran Kumar, T. H. Manjula Devi, K. R. Venugopal and L. M. Pataki, "Authentication of 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 GreyLevel Image", 14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, copyright by EURASIP, (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).