International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

ROLE OF STEGANOGRAPHY IN SECURITY ISSUES

[1]Sabyasachi Pramanik, [2]Dr. R.P. Singh

[1]Research Scholar, Sri Satya Sai University of Technology and Medical Sciences, (India)

ABSTRACT

With the ever increasing amount and variety of data to be stored and transmitted in various mediums, the specification of security which has to be established at various levels of medium access and the accompanying issues of authentication and authorization has become a critical factor. Various stenographic, watermarking and data-embedding algorithms have usually manipulated the actual data in order to either hide any coveted information or to provide some level of access control over the medium. The mediums are usually images, video, audio etc., wherein specific portions or the overall space is usually 'corrupted' with 'significant' data. This paper is an attempt to bring out the significance of the steganographic techniques that are employed in information processing algorithms for data security. It deals with the problem of data security, focusing mainly on images, and tries to state the various properties and characteristics that the steganographic algorithms should possess.

I INTRODUCTION

The growing use of the Internet has led to a continuous increase in the amount of data that is being exchanged and storage in various digital media. This has led to some unexpected cases involving both benevolent and malevolent usage of digital data. Security and authentication techniques like digital watermarks; stenographic methods and other data embedding algorithms have contributed much to enhance the various security features and to preserve the intellectual property. In this respect, stenographic techniques have been the most successful in supporting hiding of critical information in ways that prevent the detection of hidden messages**.** While cryptography scrambles the message so that it cannot be understood, steganography hides the data so that it cannot be observed. Different types of steganographic techniques employ color composition, luminance, unusual sorting of color palettes, exaggerated noise, relationship between color indices etc. The framework for steganography can be given in terms of the prisoners' problem. The main objectives of the security or steganographic algorithms should be such as to provide confidentiality, data integrity and authentication. Applications for such a data-hiding scheme include in-band captioning, covert communication, image tamper proofing, authentication, embedded control and revision tracking. As data security is proving to be one of the foremost concerns of any system administrator, let it be a LAN or across the Internet, any distribution system must provide.

A short overview in this field can be divided into three parts and they are Past, Present and Future.

Past

The word "Steganography" technically means "covered or hidden writing". Its ancient origins can be traced back to 440 BC. Although the term steganography was only coined at the end of the 15th century, the use of steganography dates back several millennia. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been in use for centuries—for fun by children and students and for serious espionage by spies and terrorists. Cryptography became very common place in the middle ages. Secret writing was employed by the Catholic Church in its various struggles down the ages and by the major governments of the time. Steganography was normally used in conjunction with cryptography to further hide secret information.

Present

The majority of today's stenographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication.

Future

In today's world, we often listen a popular term "Hacking". Hacking is nothing but an unauthorized access of data which can be collected at the time of data transmission. With respect to steganography this problem is often taken as Steganalysis. Steganalysis is a process in which a steganalyzer cracks the cover object to get the hidden data.

II TYPES OF STEGANOGRAPHY

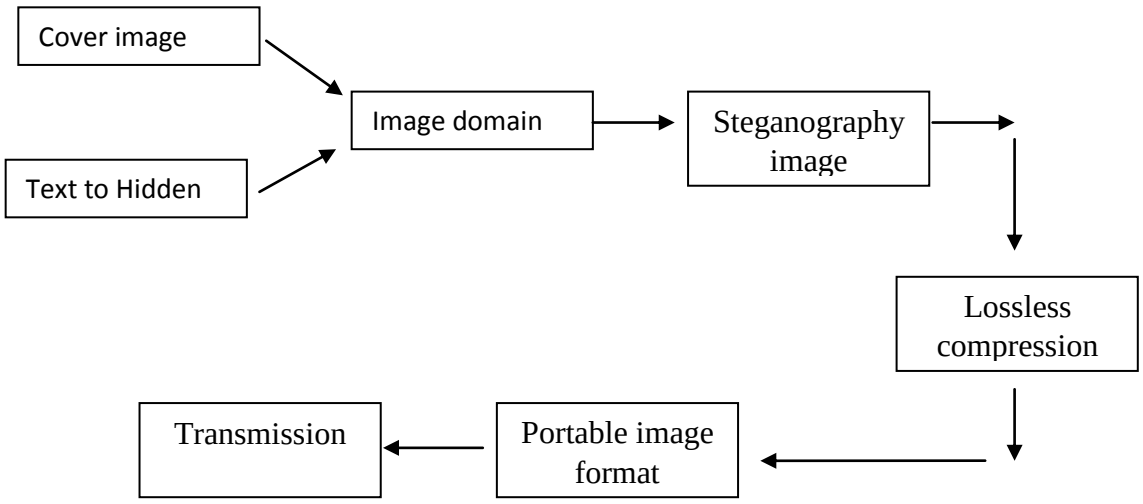
Steganography may be classified as pure, symmetric and asymmetric. While pure steganography does not need any exchange of information, symmetric and asymmetric need to exchange of keys prior sending the messages. Steganography is highly dependent on the type of media being used to hide the information. Medium being commonly used include text, images, audio files, and network protocols used in network transmissions. Image Steganography is generally more preferred media because of its harmlessness and attraction. Additionally exchange of greetings through digital means is on the increase through the increased use of the internet and ease of comfort and flexibility in sending them. Technology advancement in design of cameras and digital images being saved in cameras and then transfer to PCs has also enhanced many folds. Secondly, the text messages hidden in the images does not distort the image and there are techniques which only disturb only one bit of an image who's effects is

almost negligible on its quality. The major drawbacks of steganography are that one can hide very little information in the media selected. Some methods are following.

Encoding secret message in text/documents
Encoding secret message in audio
Encoding secret message in images

III TECHNIQUES

Given the proliferation of digital images, and given the high degree of redundancy present in a digital representation of an image (despite compression), there has been an increased interest in using digital images as cover-objects for the purpose of steganography. The simplest of such techniques essentially embed the message in a subset of the LSB (least significant bit) plane of the image, possibly after encryption. In this section the focus is on LSB embedding in digital images. When dealing with steganography in images it is important to choose an image carrier size and palette carefully since manipulation is more evident in small or well-known images. Based on the same premise, palettes with drastic changes in color are also unsuitable. It is recommended to use grey-scaled palettes, since there is no drastic change between shades. It has to be noted, that one of the more important weaknesses of the LSB is that it is vulnerable to lossy compression i.e. transforming an image to JPEG. However, as long as that compression is lossless, the medium maintains its state and there are no transformations in its behavior.



The techniques for hiding the text behind digital images are broadly classified into two categories:

(1) Image Domain Techniques - are entirely dependent upon the image's format (i.e. the way the pixels are arranged inside an image representation). Since pixels are represented by bits, bit manipulation is performed to 'invisibly' modify the color value of certain pixels. As a result, to the human eye the new image looks like the exact replica of the original image. Image domain techniques are generally applied to lossless formats.

(2) Transform or Frequency Domain Techniques - are independent on image formats and thus can be applied to lossy formats as well. They involve algorithms and tools that manipulate the image by applying transforms such as DCTs and Wavelet Transformations. They hide messages in more significant areas of the cover image and may manipulate image properties such as their luminance. Hence in these techniques we observe a trade-off between the amount of data to be hidden and the robustness of the image.

IV MEASURES

Security, embedding distortion and embedding rate can be used as schemes to evaluate the performance of the data hiding schemes.

Entropy

A steganographic system is perfectly secure when the statistics of the cover data and the stego data are identical, which means that the relative entropy between the cover data and the stego-data is zero. Entropy considers the information to be modeled as a probabilistic process that can be measured in a manner that agrees with intuition. The information theory approach to steganography holds the systems' capacity to be modeled as the ability to transfer information.

Mean Squared Error & SNR

The (weighted) mean squared error between the cover image and the stego-image (embedding distortion) can be used as one of the measures to assess the relative perceptibility of the embedded text. Imperceptibility takes advantage of human psycho visual redundancy, which is very difficult to quantify. Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR) can also be used as metrics to measure the degree of imperceptibility:

$$MSE= [\Sigma^{M}_{i=1} \Sigma^{N}_{j=1} (f_{ij} - g_{ij})^2]MN$$
$$PSNR = 10 \log_{10}(L^2 /MSE),$$

where M and N are the number of rows and number of columns respectively of the cover image, fij is the pixel value from the cover image , gij is the pixel value from the stego-image, and L is the peak signal value of the cover image (for 8-bit images, L=255). Signal to noise ratio quantifies the imperceptibility, by regarding the message as the signal and the message as the noise.

Correlation

Correlation is one of the best known methods that evaluate the degree of closeness between two functions. This measure can be used to determine the extent to which the original image and the stego-image are close to each other, even after embedding data. Localization, that is detection of the presence of the hidden data relies on the use of cross correlation function R_{XY} of two images X and Y, defined as [8],

$$\mathbf{R_{XY}\ (\alpha,\beta\ )= \sum_i \sum_j X(i,y)\ Y(i-\alpha\ ,j-\ \beta)}$$

V CONCLUSION

Given the high degree of redundancy present in a digital representation of multimedia content, there has been an increased interest in using it for the purpose of steganography. Analyzing data in which information has been hidden is called steganalysis, and results of steganalysis can be used to change or improve embedding techniques. No technique of information hiding can ensure perfect secrecy; however, by combining steganography with other techniques, such as cryptography, a higher chance of success can be achieved. One should think of steganography, not as a replacement to cryptography but as a vital supplement to it.

REFERENCE

1. C. Cachin, "An Information-Theoretic Model for Steganography". In *Information Hiding:second international workshop, Preproceedings*; 15-17 April 1998; Portland, Oregon.
2. Gary C. Kessler. An Overview of Steganography forthe Computer Forensics Examiner.
3. Johnson, N. F. and Jajodia, S. (1998). Exploringsteganography: Seeing the unseen. Computer,31(2):26–34.
4. R. Chandramouli, Nassir Menon. Analysis of LSBbased Image Steganographic techniques.
5. Westfeld, A. (2001). F5-a steganographic algorithm:High capacity despite better steganalysis. In Proc. 4thInt'l Workshop Information Hiding, pages 289–302.
6. Ahsan, K. &Kundur, D., "Practical Data hiding inTCP/IP", Proceedings of the Workshop onMultimedia Security at ACM Multimedia, 2002.
7. Bender, W., Gruhl, D., Morimoto, N. & Lu, A.,"Techniques for data hiding", IBM Systems Journal,Vol 35, 1996.
8. M. Swanson, M. Kobayashi, and A. Tewfik,"Multimedia data embedding and watermarkingtechnologies," *Proceedings of the IEEE*, Vol. 86, No.6, pp. 1064-1087, 1998.
9. H. Berghel, L. O'Gorman, Protecting ownershiprights through digital Watermarking, IEEE ComputerMag., pp 101-103, 1996.
10. Ahmet M. Skicioglu, 'Protecting IntellectualProperty In Digital Multimedia', IEEE Computer,2003.

11. Bogdan J. Falkowski. Lossless binary imagecompression using logic functions and spectra.
12. N.F. Johnson, S. Jajodia, Exploring steganography: seeing the unseen, IEEE Computer 31 (2) (1998) 26–34.
13. F.A.P.Petitcolas, R.J.Anderson, M.G.Kuhn:"Information Hiding- A Survey", Process of IEEE, vol.87,no.7, pp.1062-1078, July, 1999.
14. Artz D (2001). "Digital steganography: hiding data within data" Internet Computing. IEEE, 5(3): 75-80
15. R. Chandramouli, Nassir Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE 2001.
16. K. Sullivan, Z. Bi, U. Madhow, S. Chandrasekaran, and B. S. Manjunath, Steganalysis of quantization index modulation data hiding, Proc. of 2004 IEEE International Conference on Image Processing, vol. 2, pp. 1165-1168, 2004.
17. Jar no Mielikainen, "LSB Matching Revisited", Signal Processing Letters, IEEE, Publication Date: May 2006 Volume : 13, Issue : 5, pp. 285- 287.
18. K. Gopalan. Audio steganography using bit modification. In Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '03), volume 2, pages 421–424, 6-10 April 2003.
19. Xuping Huang, Ryota Kawashima, NorihisaSegawa, Yoshihiko Abe. "The Real-Time Steganograph Based on Audio-o-Audio Data Bit Stream",Technical report of IEICE, ISEC, vol.106 pp.15-22, September 2006.