IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A REVIEW OF MODERN STEGANOGRAPHY TECHNIQUES

Er. Parminder Singh*, Er.Parminder Singh Saini
*DIET, Kharar, Mohali, Punjab, India.
Asst. Professor DIET, Kharar, Mohali, Punjab, India.

ABSTRACT

Steganography is the art and science of hiding secret information using a cover object. It is a better way of covert communication than cryptography in that when using the cryptography, it raises a suspicion to unintended receiver that a secret communication is taking place whereas staganography hides the fact that a secret communication has taken place. Steganography has been in use since ancient times. Modern day steganography uses digital techniques involving digital media as cover objects like image, audio, video etc. Digital image has been a popular medium for steganography. This paper reviews the various techniques used for image steganography. Steganography techniques can be broadly categorized as Spatial domain and Transform domain. Popular spatial domain techniques are LSB substitution, Patchwork and Bit plane Complexity Segmentation (BPCS). The Transform domain techniques mainly consist of Discrete Cosine Transforms (DCT), Discrete Fourier Transforms (DFT) and Discrete Wavelet Transforms (DWT) based techniques. Steganography combined with cryptography can provide multilayer security and ruggedness in today’s scenario of unsecured public networks like internet.

KEYWORDS: Steganography, Cryptography, Least Significant Bit (LSB), Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Spatial Domain, Transform Domain.

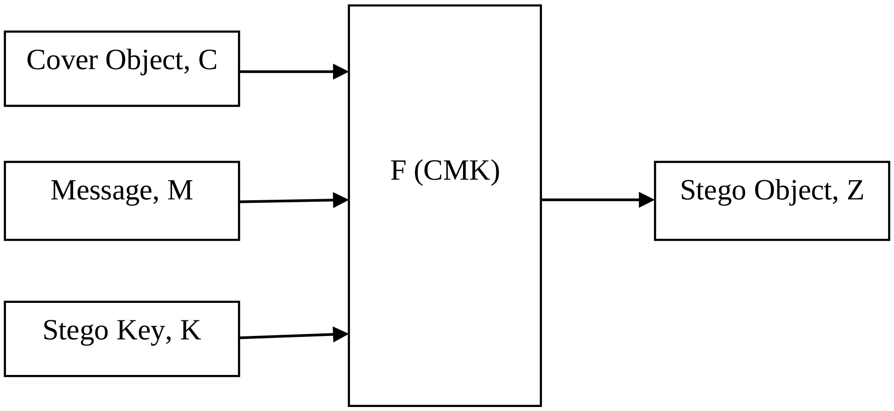
INTRODUCTION

Today, we are living in a digital world. With the rise of internet, digital TV, mobile data communication, our lifestyle has been affected and dependent on all these innovations. Users use large amount of data daily on these communication channels. Therefore there is enormous risk of data security and protection for sensitive data of the users. Apart from a common user, governments, security agencies, banking sector, corporate and industry sector need adequate means to secure sensitive data while communicating over internet. Over the years, many techniques of data security have evolved like encryption, steganography, coding etc. In encryption, the secret data is scrambled using security algorithms so that unintended recipient is unable to read the message. But in this process the eavesdropper comes to know that some secret data is being sent and there are ways & means to decrypt the data or even otherwise destroy the data. To overcome this problem, the role of steganography becomes important. Steganography is the technology for covert communication which hides the fact that a secret message is being communicated. With a good steganography technique, a user can send a secret message to the destination in such a way that an eavesdropper does not come to know that a secret communication has taken place. Steganography and cryptography differ from each other in the sense that cryptography aims at keeping the contents of a message secret whereas steganography aims at keeping the existence of the message a secret. Steganography and cryptography both are the ways for data security but neither of the technology is perfect and can be compromised. If the presence of hidden information is detected or even suspected, the purpose of steganography is partly defeated. The strength of steganography can be enhanced substantially by combining it with cryptography. Even if a secret message sent by steganography is separated, if it is in encrypted form with multilayer security algorithms, it is extremely difficult and tedious to decrypt the message. So in a way the secure steganography technique has its own importance in today’s scenario of hacking, intrusion, data theft, data destruction etc.

OVERVIEW OF STEGANOGRAPHY

The world steganography has been derived from the Greek Word “stegos” means “cover” and “graphia” means “writing”. Steganography is used to send secret message embedded in an innocent looking cover object in such a way that unintended recipients are not aware that a secret communication has taken place. The embedded information is “invisible” to an unaware observer. Steganography has been in use since ancient times. There are historical evidences which prove that ancient Greeks, Romans had been using steganography with the methods available at that time, like messages written on shaved heads of soldiers and growing the hair subsequently, wooden tablets with written messages and coated with wax. During world wars invisible inks, microdots and encrypted codes had been in use for communicating the secret messages.

The means of communications today mostly use digital technologies and the major part is shared by internet. There has been a lot of interest shown by researchers in digital steganography. The general model of steganography consists of a Cover object or Carrier, Message and Stego key as shown in figure below:

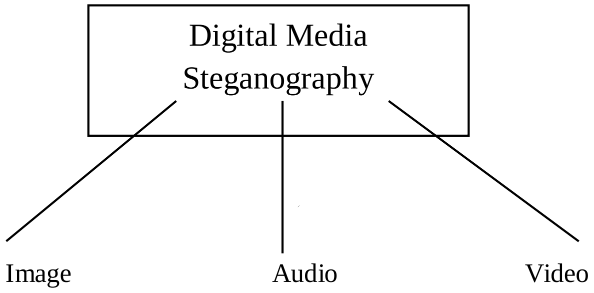


Message is the data that the sender wishes to remain it confidential. It can be plain text, ciphertext, other image, or anything that can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number. Password is known as *stego-key*, which ensures that only recipient who knows the corresponding decoding key will be able to extract the message from a *cover-object*. The *cover-object* with the secretly embedded message is then called the *Stego-object*. Recovering message from a *stego-object* requires the *cover-object* itself and a corresponding decoding key if a *stego-key* was used during the encoding process. The original image may or may not be required in most applications to extract the message.

CLASSIFICATION OF STEGANOGRAPHY

Modern steganography techniques utilize computers and networking. The digital steganography techniques can be classified as below:

- Digital Media Steganography
- Text/Linguistic Steganography
- File System Steganography
- Network Steganography



Digital media steganography generally use Digital Image, Audio or Video as the cover objects. Digital Image steganography is most popular as there is frequent use and communication of digital images on internet today. **Text and linguistic steganography** uses written text as carrier. Text steganography can involve anything from changing the formatting of an existing text, to changing words within a text, to generating random character sequences or using context-free grammars to generate readable texts. With any of these methods, the common denominator is that hidden messages are embedded in character-based text. **Steganographic file systems** are a kind of file system first proposed by Ross Anderson, Roger Needham, and Adi Shamir. Their paper proposed two main methods of hiding data: in a series of fixed size files originally consisting of random bits on top of which 'vectors' could be superimposed in such a way as to allow levels of security to decrypt all lower levels but not even know of the existence of any higher levels, or an entire partition is filled with random bits and files hidden in it. In a steganographic file system using the second scheme, files are not merely stored, nor stored encrypted, but the entire partition is randomized - encrypted files strongly resemble randomized sections of the partition, and so when files are stored on the partition, there is no easy way to discern between meaningless gibberish and the actual encrypted files. **Network steganography** exploits the protocols belonging to OSI reference model such as TCP/IP. The secret data bits are substituted with the redundant bits of protocol headers. Furthermore the communication channel is not perfect – errors are a natural phenomenon and thus it is possible to embed information in a pattern mimicking an ordinary distribution of damaged protocol data units. Digital Image steganography is elaborated in this paper.

DIGITAL IMAGE STEGANOGRAPHY

The digital image can be used to hide a secret message. In order to hide a message without changing its visual appearance, the image can be altered in “noisy” areas with many color variations. These modifications will be so minute that they will not be visible to the naked eye. On the basis of embedding domain, image steganography can be categorized as

a) Spatial Domain Techniques
b) Transform Domain Techniques

Spatial Domain Techniques

In spatial domain technique, the digital cover image is subdivided into bit planes. The secret bits are embedded directly by replacing the bits of the cover image. The popular spatial domain techniques are:

a) Least Significant Bit (LSB) substitution
b) Patchwork
c) Bit plane complexity Segmentation (BPCS)

Least Significant Bit Substitution

Digital images often have a large amount of redundant data. Therefore the secret message data can be hidden in an image by replacing the redundant data. A digital image is a collection of pixels and each pixel have a value representing the intensity levels. A color digital image pixels have Red, Green and Blue (R,G,B) pixels values and for a 24 bit color image R,G,B values are represented by 8 bit data for each color. The least significant bits of each color value contribute very little to the image. Even if last 1, 2 or 3 LSB’s are modified the human visual system have limitations to distinguish the changes in the image.

Suppose we want to hide letter “A” in the 8 bytes of the image pixels. The letter “A” is converted into ASCII form which is 65 or binary 01000001. The 3 pixel values of a 24bit color image can be represented by 9 bytes. Let the values are given as following:

00100111	11101001	11001000
00100111	11001000	11101001
11001000	00100111	11101001

After replacing each LSB (1 bit) of each byte with bits of character “A”, the value becomes:

0010011**1**	1110100**0**	1100100**0**
0010011**0**	1100100**0**	1110100**0**
1100100**1**	0010011**0**	11101001

The advantage of LSB based steganography is that it is simple to embed the bits of the message directly into the LSB plane of the image. The LSB modifications have very little effect on the image quality and thus the stego image looks identical to the cover image.

Patchwork

Patchwork is a data hiding technique developed by Bender et al. This technique is based on a pseudorandom, statistical model. It works by invisibly embedding a specific statistic, with Gaussian distribution into the host image. Two sets of pixel or patches, of the image are chosen, the first A and second B. Then the algorithm is applied which slightly brightens points in A while darkening by same factor in B. To determine the points of the image, which have to be modified, a pseudorandom number generator is used, fed with a secret key, which is shared by both the transmitter and receiver. The advantage of this technique is that the secret message is spread over the whole cover image, even if one patch is damaged, the other will persist. The disadvantage of this method is that it has low embedding capacity.

Bit Plane Complexity Segmentation (BPCS)

Bit plane complexity segmentation is a new steganographic technique which has large information hiding capacity. It is based upon the property that the replacement of the complex regions in each bit plane of a color image with random binary patterns is invisible to the human eye. In this method, the secret file to be embedded is segmented into a series of blocks having 8 bytes of data each. These blocks are regarded as 8x8 image patterns. Such blocks are called secret blocks. The color image is transformed from Pure Binary Coding System (PBC) to a Canonical Gray Coding System (CGC), because bit slicing is better in CGC than PBC. Each bit plane of the cover image is segmented into informative and noise-like regions by using a threshold value. The secret blocks are embedded into noise-like regions of the bit planes. If the secret block is less complex, it is conjugated to make it more complex. The cover image is converted back from CGC to PBC. The decoding algorithm is just the reverse procedure of the embedding steps.

Transform Domain Techniques

In spatial domain techniques, the processing is done on the image pixel values directly. The advantage of spatial domain techniques is their simplicity. In transform domain techniques, the cover image is converted into frequency domain using DCT (Discrete Cosine Transforms), DFT (Discrete Fourier Transforms) or DWT (Discrete Wavelet Transforms). Then the transformed coefficients are processed to embed the secret information. The changed coefficients are transformed back into the spatial domain to get stego image. The advantage of transform domain technique is that it can hide a large amount of data and provide high security but computationally they are more complex and involve lot of processing.

DCT based techniques

DCT (Discrete Cosine Transform) is widely used in JPEG and MPEG file formats for data compression. The use of DCT technique for steganography in digital media was introduced by Koch & Zhao (1995) and Cox et. al.(1997). DCT domain techniques provide better PSNR, small BER, good information integrity. In DCT technique, cover image is divided into blocks of 8x8 pixels and the two dimensional DCT is applied on each block. Each pixel block is transformed into 64 DCT coefficients. Altering any single DCT coefficient will affect all 64 image pixels in that block. The DCT coefficients of the transformed cover image are quantized. The DCT splits the image into high, middle and low frequency chosen to embed the secret information.

The definition of the two dimensional DCT for an image A and output image B is

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N} \qquad \begin{array}{l} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{array}$$

where $\alpha_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 0 \le p \le M-1 \end{cases}$

$$\alpha_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 0 \le q \le N-1 \end{cases}$$

M an N are the rows and columns of A respectively

Discrete Fourier Transforms

In this technique, the cover image is subjected to DFT. Embedding is done in the frequency domain. The human visual system is more sensitive to low frequency components than the high frequency components. The midband frequencies are best suited for embedding the secret data to obtain balance between imperceptibility and robustness. The DFT of spatial value f(x,y) for the image of size MxN is defined as:

$$F(u,v) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y)\, e^{-j2\pi(\frac{ux}{M}+\frac{vy}{N})} \quad \text{where } u = 0 \text{ to } M-1, \; v = 0 \text{ to } N-1$$

Inverse DFT is used to convert frequency components to spatial domain value and is defined as:

$$f(x,y) = \frac{1}{\sqrt{MN}} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u,v)\, e^{-j2\pi(\frac{ux}{M}+\frac{vy}{N})} \quad \text{where } u = 0 \text{ to } M-1, \; v = 0 \text{ to } N-1$$

Discrete Wavelet Transforms

The wavelet transform decompress the image into three spatial directions i.e. horizontal, vertical and diagonal. The use of wavelet transforms in steganography was proposed by Abdul Wahab et al. (2008). The research on human perception finds that the retina of the human eye splits an image into frequency channels of approximately equal bandwidth which are processed independently. This multi resolution property is expected to allow the independent processing of the resulting components without significant perceptible interaction between them. Lee et al. (2007) presented a data hiding scheme based on integer wavelet transform. First the original image is divided into non overlapping blocks and hides the secret information into high frequency integer wavelet coefficients of each block by using LSB substitution. This scheme reported higher embedding capacity and lower distortion than other existing techniques. Chan et al.(2009) proposed a Haar Digital Wavelet Transform (HDWT) based reversible data hiding scheme. Yeh et al.(2013) presented wavelet bit plane data hiding techniques for compressed image. They use bit planes of DWT coefficients for hiding secret data based on multistage encoding.

CONCLUSION

Different steganography techniques have been reviewed in the paper. The implementation of a technique may also depend upon the type of application. Spatial domain techniques like LSB substitution are simple to implement and combining them with encryption algorithms can provide robust and secure steganography solutions. Transform domain techniques involve complex processing but can also provide good results like image quality and high data embedding capacity. There has been lot of interest of researchers in the field of steganography. Newer and better steganography techniques are expected in near future.

REFERENCES

[1] C.P.Sumathi, T.Santanam and G.Umamaheswari, “A Study of Various Steganographic Techniques Used for Information Hiding”,International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013

[2] Shashikala Channalli, Ajay Jadhav, “Steganography An Art of Hiding Data”, International Journal on Computer Science and Engineering Vol.1(3), 2009

[3] T. Morkel , J.H.P. Eloff , M.S. Olivier, “AN OVERVIEW OF IMAGE STEGANOGRAPHY”, Information and Computer Security Architecture (ICSA) Research Group

[4] Elżbieta Zielińska, Wojciech Mazurczyk, Krzysztof Szczypiorski, “Development Trends in Steganography”, Warsaw University of Technology, Institute of Telecommunications Warsaw, Poland, 00-665, Nowowiejska 15/19

[5] Joseph Raphael, Dr. V. Sundaram, “ Cryptography and Steganography – A Survey”, Int. J. Comp. Tech. Appl.

[6] Krista Bennett, “Survey, Analysis, and Robustness Concerns for Hiding Information in Text”, Department of Linguistics Purdue University

[7] Shamim Ahmed Laskar and Kattamanchi Hemachandran, “High Capacity data hiding using LSB Steganography and Encryption”, International Journal of Database Management Systems (IJDMS) Vol.4, No.6, December 2012

[8] Eiji Kawaguchi and Richard O. Eason, “Principle and applications of BPCS-Steganography”, Kyushu Institute of Technology, Kitakyushu, Japan,University of Maine, Orono, Maine 04469-5708

[9] Inderjit Singh, Sunil Khullar , Dr. S.C. Laroiya, “DFT Based Image Enhancement and Steganography”, International Journal of Computer Science and Communication Engineering Volume 2 Issue 1 (February 2013 Issue)

[10] Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath, “A SECURE COLOR IMAGE STEGANOGRAPHY IN TRANSFORM DOMAIN”, International Journal on Cryptography and Information Security (IJCIS), Vol.3, No.1, March 2013

[11] Mukta Goel, Rohit Goel, “Comparative Analysis of Hybrid Transform Domain Image Steganography Embedding Techniques”, IJSR - INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

[12] Gurmeet Kaur and Aarti Kochhar, “Transform Domain Analysis of Image Steganography”,International Journal for Science and Emerging ISSN No. (Online):2250-3641 Technologies with Latest Trends 6(1): 29-37 (2013)