ISSN No-2031-5063 Vol.1,Issue.VI/Dec 2011pp.1-4

Research Paper

Steganography: To preserve the document security

Mr.Navin D. Jambhekar
Department of Computer Science
S.S.S.K.R.Innani Mahavidyalaya Karanja (Lad) Dist. Washim (MS)

ABSTRACT

The rapid expansion of the Internet has increased the availability of digital data such as audio, images and videos to the public. The digital data transmission is easiest for every one user, but if the data is theft or stolen then it will be more dangerous or unwanted. Protecting multimedia information becomes more and more important from illegal use.

Steganography, as defined by Kahn [C. Cachin, 1998], is "the art and science of communicating in a way which hides the existence of the communication". Steganography allows secret information to be embedded into a cover message without significantly damaging the content of the cover message. The message usually will be an image and the secret information which is to be embedded is called the stego message. This paper give the framework to use the steganography for securing the document from the malicious use.

Keywords: Steganography, Stego medium, secrete message.

1. Introduction

The Internet as a whole does not use secure links, thus information transmission is mostly prone to malicious use. Cryptography "the science of writing in secret codes" addresses all of the elements necessary for secure communication over an insecure. But cryptography does not always provide safe communication. The protection process is known as encryption and goes through a certain process of encryption. The process requires the original plaintext, the key needed for encryption, the algorithm; containing the blueprint of encryption process and finally it produces the ciphertext i.e. the material from the plaintext, unable to read by the unauthorized user. Original message is called as the plaintext. The disguised message is called as the ciphertext.

The plaintext message: Hello Friends
Key: rot3
The ciphertext message: Uryyb Sevraqf

Here with simple guess, anyone can predict the key to extract the original message.

The more secure method having none or very low hacking ratio is the Steganographic method.

2. Methodology

2.1 The Steganographic Method

Steganography is the art of concealing information in ways that prevent the detection of hidden messages. Steganography provides the way with which secret communication message will be hidden under the other image or medium which cannot be discover by any one without sender or receiver. The word steganography comes from the Greek Steganos, which mean covered or secret and –graphy mean writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding information such that its presence cannot be detected [P.Moulin & J.A. O'Sullivan,2001] and a communication is happening. A secret information is encoding in a manner such that the very existence of the information is concealed. Paired with existing communication methods, steganography can be used to carry out hidden exchanges. The basic model of steganography consists of covere object, Message and key. Where the cover object is the medium that embedded and serves to hide the presence of the message.

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. The Key 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. Least significant bit (LSB) insertion is a common and simple approach to embed information in a cover file: it overwrites the LSB of a pixel with anM's bit. If we choose a 24-bit image as cover, we can store 3 bits in each pixel. To the human eye, the resulting stego image will look identical to the cover image (Johnson and Jajodia, 1998).

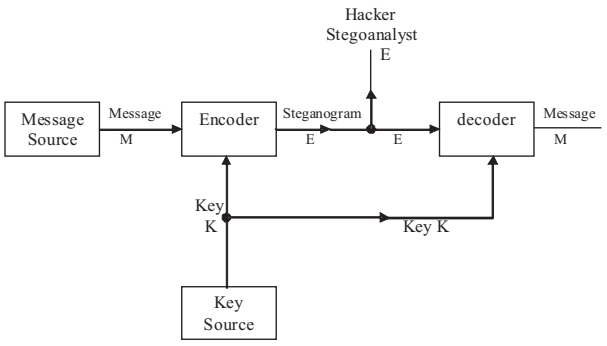
Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects have been proposed [N.F. Johnson & S. Jajodia, april 1998]. There have been many techniques for hiding information or messages in images in such a manner that the alterations made to the image are perceptually indiscernible. Common approaches are [N.F. Johnson & S. Jajodia,1998]:

(i) Least significant bit insertion (LSB)
(ii) Masking and filtering
(iii) Transform techniques

Least significant bits (LSB) insertion is a simple approach to embedding information in image file. The simplest steganographic techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible

difference because the amplitude of the change is small.
Masking and filtering techniques, usually restricted to 24 bits and gray scale images, hide information by marking an image, in a manner similar to paper watermarks. The techniques performs analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the noise level.
Transform techniques embed the message by modulating coefficients in a transform domain, such as the Discrete Cosine Transform (DCT) used in JPEG compression, Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover-image, which make them more robust to attack. Transformations can be applied over the entire image, to block through out the image, or other variants.

The following is the schematic diagram of the Steganographic system used to mix an image over the message for the security.



Here the Encocer performs the integration operation of the Message M with the Key K. Thus it produces the Steganogram E, thus
E = f (M,K)
Here the transformation of by the Encoder to message M produces the Steganogram E. It uses the particular key K where it is the key image file to be embedded over the message for security. Both the sender and receiver must use the uniform technique to extract the original message. Here if the hacker willing to predict the key, then it is impossible or even much harder to get the cover image used as the key K. No one cannot predict the key image and the insertion of which point in the Message image.

Here the Least significant bit insertion method (N.F. Johnson and S. Jajodia,1998) , is a common, simple approach to embedding information in a cover file. It is give some overheads of a slight image manipulation. Converting an image from a format like GIF or BMP, which reconstructs the original message exactly (lossless compression) to a JPEG, which does not (lossy compression), and then back could destroy the information hidden in the LSBs. To hide an image in the LSBs of each byte of a 24-bit image, you can store 3 bits in each pixel. A 1,024 ´ 768 image has the potential to hide a total of 2,359,296 bits (294,912 bytes) of information. If you compress the message to be hidden before you embed it, you can hide a large amount of information. To the human eye, the resulting stego-image will look identical to the cover image.

For example, the letter A can be hidden in three pixels (assuming no compression). The original raster data for 3 pixels (9 bytes) may be

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

The binary value for A is 10000011. Inserting the binary value for A in the three pixels would result in

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

The underlined bits are the only three actually changed in the 8 bytes used. On average, LSB requires that only half the bits in an image be changed. You can hide data in the least and second least significant bits and still the human eye would not be able to discern it.

2. Conclusion

As compared to other techniques of information security, the steganography is the powerful concept, that offer provable security have greatly enhanced our understanding of this important area of information security.

As privacy concerns continue to develop along with the digital communication domain, steganography will undoubtedly play a growing role in society. For this reason, it is important that we are aware of digital steganography technology and its implications.

3. Acknowledgement

The special thank goes to Dr. C.A. Dhawale for the valuable support for the work on every aspect of the research.

4. References

[1] C. Cachin, “An Information-Theoretic Model for Steganography”, in proceeding 2nd Information Hiding Workshop, vol. 1525, pp. 306-318, 1998.
[2] D. Artz, “Digital Steganography: Hiding Data within Data”, IEEE Internet Computing, pp. 75-80, May-Jun 2001.
[3] N.F. Johnson & S. Jajodia, “Steganalysis of Images Created Using Current Steganography
Software”, in Proceeding for the Second Information Hiding Workshop, Portland Oregon,
USA, April 1998, pp. 273-289.
[4] N.F. Johnson and S. Jajodia, “Exploring Steganography: Seeing the Unseen”, IEEE, pp. 26-34, 1998.
[5] S. Tanako, K. Tanaka and T. Sugimura, “Data Hiding via Steganographic Image
Transformation”, IEICE Trans. Fundamentals, vol. E83-A, pp. 311-319, February, 2000.
35Vot 71847 Information Hiding using Steganography Approach
[6] W. Bender, D. Gruhl, N. Morimoto and A. Lu, “Techniques for Data Hiding”, Systems
Journal, vol. 35, 1996.
[7] C. E. Shannon, “Communication theory of secrecy systems,” Bell Syst.
Tech. J., vol. 28, no. 4, pp. 656–715, 1949.