ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

A Survey on Approaches and Communication in Spread Spectrum Image Steganography

K.Priyanka[1], Dr. Antony Selvadoss Thanamani[2]

M.Phil. Research Scholar, Dept. of Computer Science, NGM College, Pollachi, India [1]

Assistant Professor and Head, Dept. of Computer Science, NGM College, Pollachi, India[2]

ABSTRACT: In this paper, we have proposed a new image steganography scheme which is a Fuzzy based selection of wavelets. There are some attack forms to data and information. In consequence, today various efforts have been conducted to take care of data security and overcome attacks is previously already there is a way to take care of data security that is recognized by the name of cryptography. This system hides and recovers messages of substantial length within digital imagery while maintaining the original image size and dynamic range. The hidden messages can be recovered using appropriate keys without any knowledge of the original image. Image processing, error control coding, and spread-spectrum techniques utilized are described, and the performance of the technique is illustrated. Image restoration, error-control coding, and techniques similar to spread spectrum are described, and the performance of the system is illustrated. A message embedded by this method can be in the form of text, imagery, or any other digital signal.

KEYWORDS: Steganography; cryptography; substantial length; appropriate key; spread-spectrum.

I. INTRODUCTION

Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. Since nobody except the sender and the receiver knows the existence of the message, it does not attract unwanted attention. Steganography was used even in ancient times and these ancient methods are called Physical Steganography. Some examples for these methods are messages hidden in messages body, messages written in secret inks, messages written on envelopes in areas covered by stamps, etc. Modern Steganography methods are called Digital Steganography. These modern methods include hiding messages within noisy images, embedding a message within random data, embedding pictures with the message within video files, etc. Furthermore, Network Steganography is used in telecommunication networks. This includes techniques like Steganophony which hiding a message in Voice-over-IP conversations and WLAN Steganography the methods for transmitting Steganograms in Wireless Local Area Networks.

Some steganography techniques:

- Physical steganography
- Digital steganography
- Network steganography
- Printed steganography

II. RELATED WORK

A. Lease Significant Bit (LSB) approach:

The idea behind this scheme is to replace the LSB of the image pixels with the message bits. Most steganographic programs available today use some variation of LSB manipulation in order to hide messages in an image. The major advantage of the method is its quickness and easiness. Typically, it achieves high payload and low perceptibility. However, a too naive implementation may be susceptible to various visual and statistical attacks. The scheme also has a very low resistance to removal. For more details, please refer to the LSB examples subsection.

B. Injection approach:

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

In this approach, the source message is hidden in sections of the cover file that are ignored by the processing application. Therefore, avoid modifying those file bits that are relevant to an end-user leaving the cover file perfectly usable.

C. Substitution approach:

In this approach, the least significant meaningful content of the cover file is replaced with the source message in a way that causes the least amount of distortion to the cover file.

D. Generation approach:

It is unlike injection and substitution; it does not require an existing cover file but generates a cover file for the sole purpose of hiding the message.

III. PROPOSED METHODOLOGY AND DISCUSSION

A message is embedded in a digital image by the stegosystem encoder, which uses a key or password. The resulting stegoimage is transmitted over a channel to the receiver, where it is processed by the stegosystem decoder using the same key. During transmission, the stegoimage can be monitored by unintended viewers who will notice only the transmittal of the innocuous image without discovering the existence of the hidden message [1]. A casual observer won't be able even to detect the hidden communication, since it is under the noise level.

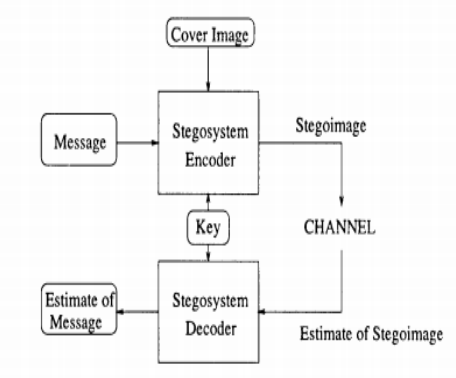

Fig 1: Process of stegosystem

The SSIS encoder adds more steps in order to push spread spectrum to its limits:

1. It optionally encrypts the message *m* to be embedded with *key1*, getting *e*
2. The data stream passes through a Low-Rate ECC (Error Correction Code) encoder, to acquire better robustness against destruction attacks and unwanted noise, becoming *c*.
3. Spread spectrum modulation, using a pseudorandom noise generator fed with *key2*, and get *s*
4. An interleaver and spatial spreader processes *s* using *key3* obtaining *i*
5. The output of the interleaver is added to the image *f*, getting *g*
6. A quantization process is used to preserve the initial dynamic range of the cover image. We'll call it still *g*

We assume that the stego-image is sent through a noisy channel to the receiver and will become *g'*

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

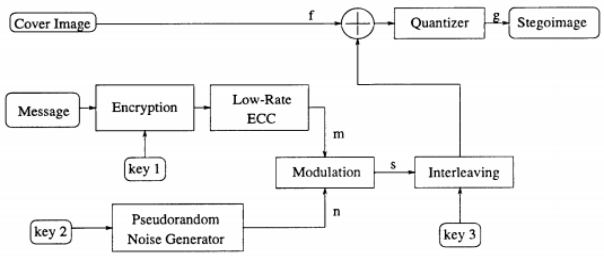

Fig 2: Encoding process

The decoding process fairly repeats the same steps backwards:

1. It gets an optimal approximation *f'* of the original image *f* using image restoration techniques
2. *f'* is subtracted from the stego image *g'* to reveal an estimate of the embedded data *i'*.
3. *i'* is fed into a keyed deinterleaver, that uses *key3* to construct an approximation of the hidden signal, *s'*.
4. *s'* is demodulated with *key2* to get an estimate of the encoded message, c'
5. c' is decoded through the low-rate ECC to get e'
6. if m was encrypted, then e' is decrypted with *key1* and this will give m'

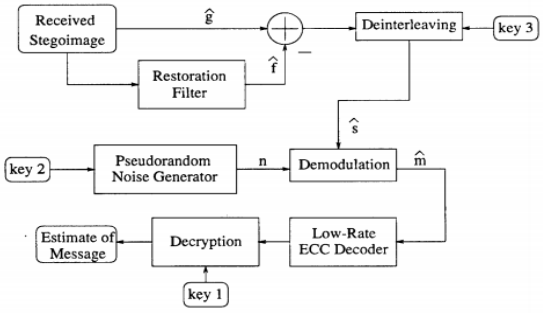

Fig 3: Decoding process steps backwards

The process of spreading the bandwidth of a narrowband signal across a wide band of frequencies. This can be accomplished by modulating the narrowband waveform with a wideband waveform, such as white noise. After spreading, the energy of the narrowband signal in any one frequency band is low and therefore difficult to detect. SSIS uses this technique to embed a message, typically a binary signal, within very low power white Gaussian noise. The resulting signal, perceived as noise, is then combined with the cover image to produce the stegoimage. Since the power of the embedded signal is low compared to the power of the cover image, the SNR is also low, thereby indicating low perceptibility and providing low probability of detection by an observer. Subsequently, an observer will be unable to visually distinguish the original image from the stegoimage. To construct the embedded signal, we incorporate the concept of a stored reference spread-spectrum communications system [2] to provide low probability of detection, either by computer or the HVS. The stored reference principle requires independent generation of identical pseudorandom wideband waveforms at both the transmitter and receiver. This can easily be accomplished by a private or public key [3] and identical pseudorandom waveform generators.

IV. EXPERIMENTAL RESULTS

Each byte of all these three matrices are encrypted using S-DES algorithm and an array of encrypted pixels is created. The dimension of so produced array will be for each of the three matrices and contains bits each. Each

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

element of the array is denoted in binary form and split into two parts. The first part contains the first four Most Significant Bits and the second contains the remaining four Least Significant Bits. In this method binary equivalent of the message is distributed among the LSBs of each pixel. For example we will try to hide the character 'A' into an 8-bit color image. We are taking eight consecutive pixels from top left corner of the image. The equivalent binary bit pattern of those pixels may be like this: 00100111 11101001 11001000 00100111 11001000 11101001 11001000 00100111 Then each bit of binary equivalence of letter 'A' i.e. 01100101 are copied serially to the LSB's of equivalent binary pattern of pixels, resulting the bit pattern will become like this: - 00100110 11101001 11001001 00100110 11001000 11101001 11001000 00100111 The only problem with this technique is that it is very vulnerable to attacks such as image compression and formatting[10].Image Steganography

A. *LSB technique*

The following steps are followed in this case: -

Step 1: The Image is broken into data units each of them consists of 8 x 8 block of pixels.

Step 2: Working from top-left to bottom-right of the cover image, DCT is applied to each pixel of each data unit.

Step 3: After applying DCT, one DCT Coefficient is generated for each pixel in data unit.

Step 4: Each DCT coefficient is then quantized against a reference quantization table.

Step 5: The LSB of binary equivalent the quantized DCT coefficient can be replaced by a bit from secret message.

Step 6: Encoding is then applied to each modified quantized DCT coefficient to produce compressed Stego Image.

The first ten bits are selected as the key to encrypt the red intensity pixel of payload image. The middle ten bits will be the key to encrypt the green intensity pixel of payload and finally the last ten bits is the key to encrypt blue intensity pixel of payload image. So the size of key image must be same as that of payload. If not, then the key image will get resized. Each pixel of the key image is split into three keys. This data is represented as an image [7].

The larger the cover message relative to the hidden message, the easier it is to hide the latter. For this reason, digital pictures which contain large amounts of data are used to hide messages on the Internet and on other communication media. It is not clear how common this actually is. For example: a 24-bit bitmapuses 8 bits to represent each of the three colour values at each pixel. The blue alone has 2^8 different levels of blue intensity. The difference between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye. Therefore, the least significant bit can be used more or less undetectably for something else other than color information. If this is repeated for the green and the red elements of each pixel as well, it is possible to encode one letter of ASCII text for every three pixels.

Stated somewhat more formally, the objective for making steganographic encoding difficult to detect is to ensure that the changes to the carrier the original signal due to the injection of the payload the signal to covertly embed are visually and negligible; that is to say, the changes are interchangeable from the noise floor of the carrier. Any medium can be a carrier, but media with a large amount of outmoded or compressible information are better suited.

From an information theoretical point of view, this means that the channel must have more capacity than the "surface" signal requires; that is, there must be redundancy. For a digital image, this may be noise from the imaging element; for digital audio, it may be noise from recording techniques or extension equipment. In general, electronics that digitize an analog signal suffer from several noise sources such as thermal noise, flicker noise, and shot noise. This noise provides enough variation in the captured digital information that it can be exploited as a noise cover for hidden

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

data. In addition, lossy compression schemes always introduce some error into the decompressed data; it is possible to exploit this for steganographic use as well.

V. CONCLUSION AND FUTURE WORK

All information hiding techniques that may be used to exchange steganograms in telecommunication networks can be classified under the general term of network steganography. The main weakness of steganography in malware is that the client software the part that looks for the data that being masked in unexpected places is public. Cybercriminals trying to spread their malware far and wide. Steganography helps the malware stay undetected until security researchers get a sample Steganography can be used for digital watermarking, where a message is hidden in an image so that its source can be tracked or verified or even just to identify an image.

REFERENCES

[1] Methodology of Spread-Spectrum Image Steganography byLisa M. Marvel, Charles T. Retter
[2] Simon, M. K., J. K. Omura, R. A. Scholtz, and B. K. Levitt. Spread Spectrum Communications, Volume I. Rockville, MD: Computer Science Press, 1985.
[3] Schneier, B. Applied Cryptography - Protocols, Algorithms, and Source Code in C. New York: John Wiley and Sons, Inc., 1996.
[4] Hartung, F., and B. Girod. "Fast Public-Key Watermarking of Compressed Video" Proceedings ofthe IEEE International Conference on Image Processing, Santa Barbara, CA, October 1997.
[5] Sujay Narayana and Gaurav Prasad "Two new approaches for secured image steganography using cryptographic techniques and type conversions" An International Journal Vol.1, No.2, December 2010
[6] C.-C. Chang, T. D. Kieu, and Y.-C. Chou, "A High Payload Steganographic Scheme Based on (7, 4) Hamming Code for Digital Images," Proc. of the 2008 International Symposium onElectronic Commerce and Security, pp.16-21, August 2008.
[7] Jiri Fridrich ,Du Dui, "Secure Steganographic Method for Palette Images," 3rd Int. Workshop on InformationHiding, pp.47-66, 1999. [17] R. Chandramouli, M. Kharrazi, N. Memon, "Image Steganography and Steganalysis: Concepts and Practice " , International Workshop on DigitalWatermarking, Seoul, October 2004.
[9] K. Kim, S. Park, and S. Lee, "Reconstruction of s2DES S–Boxes and their Immunity to DifferentialCryptanalysis," Proceedings of the 1993 Korea–Japan Workshop on Information Security and Cryptography, Seoul, Korea, 24–26 Oct 1993, pp. 282–291.
[10] "Steganography and Steganalysis: Different Approaches" Soumyendu Das, Subhendu Das, Sugata Sanyal.

BIOGRAPHY

Dr. Antony Selvadoss Thanamani has obtained his Ph.D in computer Science and currently he is working as Associate professor and HOD at NGM College, Pollachi. He has published more than 100 papers in international/national journals and conferences. His research interest include Data Mining, Cloud Computing, GRID Computing, Pervasive Computing, Nano Computing.

K.Priyanka has obtained his M.sc in Software System from Sri Krishna Arts and Science College at Coimbatore. Now she is doing her M.Phil in Computer Science at NGM College, Pollachi. Her research interest includes Networking's, Cryptography.