Taking a Brief look at steganography: Methods and Approaches

Masoud Nosrati [*1], Ronak Karimi [2], Hamed Nosrati [3], Ali Nosrati [4]

[1, 2] Young Researchers Club, Kermanshah Branch, Islamic Azad University, Kermanshah, Iran.
[3, 4] Islamic Azad University, Kermanshah Branch, Kermanshah, Iran.
minibigs_m@yahoo.co.uk

Abstract: In this paper, we are going to introduce different types of steganography considering the cover data. As the first step, we will talk about text steganography and investigate its details. Then, image steganography and its techniques will be investigated. Some techniques including Least Significant Bits, Masking and filtering and Transformations will be subjected during image steganography. Finally, audio steganography which contains LSB Coding, Phase Coding, Spread Spectrum and Echo Hiding techniques will be described.
[Masoud Nosrati, Ronak Karimi, Hamed Nosrati, Ali Nosrati. Taking a Brief look at steganography: Methods and Approaches. Journal of American Science 2011;7(6):106-109]. (ISSN: 1545-1003). http://www.americanscience.org.

Keywords: Steganography; text steganography; image steganography; audio steganography.

1. Introduction

The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing” [1]. Steganography is one such pro-security innovation in which secret data is embedded in a cover [2]. The notion of data hiding or steganography was first introduced with the example of prisoners' secret message by Simmons in 1983 [3].

Steganography and cryptography are closely related. Cryptography scrambles messages so they cannot be understood. Steganography on the other hand, will hide the message so there is no knowledge of the existence of the message in the first place. In some situations, sending an encrypted message will arouse suspicion while an”invisible” message will not do so. Both sciences can be combined to produce better protection of the message. In this case, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques. [4]

There exist two types of materials in steganography: message and carrier. Message is the secret data that should be hidden and carrier is the material that takes the message in it [5].

There are many types of steganography methods. In this paper, we are going to take a short look at different steganography methods. Figure 1 in below shows the different categories of file formats that can be used for steganography techniques [6].

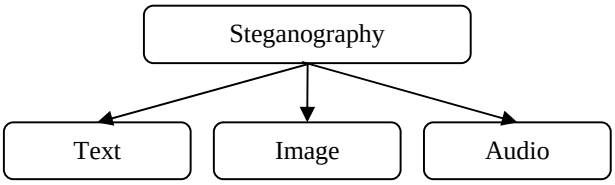

Figure 1. Steganography types diagram

In the second section, text steganography will be talked. Then we will get into images steganography principals in the third section. Finally audio steganography will be investigated.

2. Text steganography

Text steganography can be achieved by altering the text formatting, or by altering certain characteristics of textual elements (e.g., characters). The goal in the design of coding methods is to develop alterations that are reliably decodable (even in the presence of noise) yet largely indiscernible to the reader. These criteria, reliable decoding and minimum visible change, are somewhat conflicting; herein lies the challenge in designing document marking techniques. The document format file is a computer file describing the document content and page layout (or formatting), using standard format description languages such as PostScript2, TeX, @off, etc. It is from this format file that the image - what the reader sees - is generated.

The three coding techniques that we propose illustrate different approaches rather than form <an exhaustive list of document marking techniques. The techniques can be used either separately or jointly. Each technique enjoys certain advantages or applicability as we discuss below.

2.1. Line-Shift Coding

This is a method of altering a document by vertically shifting the locations of text lines to encode the document uniquely. This encoding may be applied either to the format file or to the bitmap of a page image. The embedded codeword may be extracted from the format file or bitmap. In certain cases this decoding can be accomplished without

need of the original image, since the original is known to have uniform line spacing between adjacent lines within a paragraph.

2.2. Word-Shift Coding

This is a method of altering a document by horizontally shifting the locations of words within text lines to encode the document uniquely. This encoding can be applied to either the format file or to the bitmap of a page image. Decoding may be performed from the format file or bitmap. The method is applicable only to documents with variable spacing between adjacent words. Variable spacing in text documents is commonly used to distribute white space when justifying text. Because of this variable spacing, decoding requires the original image - or more specifically, the spacing between words in the un-encoded document.

2.3. Feature Coding

This is a coding method that is applied either to a format file or to a bitmap image of a document. The image is examined for chosen text features, and those features are altered, or not altered, depending on the codeword. Decoding requires the original image, or more specifically, a specification of the change in pixels at a feature. There are many possible choices of text features; here, we choose to alter upward, vertical endlines - that is the tops of letters, b, d, h, etc. These endlines are altered by extending or shortening their lengths by one (or more) pixels, but otherwise not changing the endline feature [7].

There is another form of text steganography which is defined by Chapman et al. as the text steganography is a method of using written natural language to conceal a secret message [8].

3. Image steganography

Hiding information inside images is a popular technique nowadays. An image with a secret message inside can easily be spread over the World Wide Web or in newsgroups. The use of steganography in newsgroups has been researched by German steganographic expert Niels Provos, who created a scanning cluster which detects the presence of hidden messages inside images that were posted on the net. However, after checking one million images, no hidden messages were found, so the practical use of steganography still seems to be limited.

To hide a message inside an image without changing its visible properties, the cover source can be altered in ”noisy” areas with many color variations, so less attention will be drawn to the modifications. The most common methods to make these alterations involve the usage of the least-significant bit or LSB, masking, filtering and transformations on the cover image. These techniques can be used with varying degrees of success on different types of image files.

3.1. Least Significant Bits

A simple approach for embedding information in cover image is using Least Significant Bits (LSB). The simplest steganography 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 [9]. To hide a secret message inside an image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24-bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel. For example, the following grid can be considered as 3 pixels of a 24-bit color image, using 9 bytes of memory:

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

When the character A, which binary value equals 10000001, is inserted, the following grid results:

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

In this case, only three bits needed to be changed to insert the character successfully. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximal cover size. The result changes that are made to the least significant bits are too small to be recognized by the human visual system (HVS), so the message is effectively hidden [4].

As you see, the least significant bit of third color is remained without any changes. It can be used for checking the correctness of 8 bits which are embedded in these 3 pixels. In other words, it could be used as “parity bit”.

3.2. Masking and filtering

Masking and filtering techniques, usually restricted to 24 bits or grayscale images, take a different approach to hiding a message. These methods are effectively similar to paper watermarks,

creating markings in an image. This can be achieved for example by modifying the luminance of parts of the image. While masking does change the visible properties of an image, it can be done in such a way that the human eye will not notice the anomalies. Since masking uses visible aspects of the image, it is more robust than LSB modification with respect to compression, cropping and different kinds of image processing. The information is not hidden at the ”noise” level but is inside the visible part of the image, which makes it more suitable than LSB modifications in case a lossy compression algorithm like JPEG is being used [4].

3.3. Transformations

A more complex way of hiding a secret inside an image comes with the use and modifications of discrete cosine transformations. Discrete cosine transformations (DST)), are used by the JPEG compression algorithm to transform successive 8 x 8 pixel blocks of the image, into 64 DCT coefficients each. Each DCT coefficient F(u, v) of an 8 x 8 block of image pixels f(x, y) is given by:

$$F(u,v) = \frac{1}{4}C(u)C(v)\left[\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y) * \cos\frac{(2x+1)u\pi}{16}\cos\frac{(2y+1)v\pi}{16}\right]$$

, $C(x) = \begin{cases} \frac{1}{\sqrt{2}} & x = 0 \\ 1 & else. \end{cases}$

After calculating the coefficients, the following quantizing operation is performed:

$$F^{Q}(u,v) = \left\lfloor \frac{F(u,v)}{Q(u,v)} \right\rfloor$$

Where Q(u, v) is a 64-element quantization table. A simple pseudo-code algorithm to hide a message inside a JPEG image could look like this [4]:

```
Input: message, cover image
Output: steganographic image containing
message
   while data left to embed do
         get next DCT coefficient from cover
image
         if DCT 6= 0 and DCT 6= 1 then
                get next LSB from message
                replace DCT LSB with message
         bit
         end if
         insert DCT into steganographic image
   end while
```

4. Audio steganography

In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods are available for audio steganography. We are going to have a brief introduction on some of them.

LSB Coding

Sampling technique followed by Quantization converts analog audio signal to digital binary sequence. In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message.

Phase Coding

Human Auditory System (HAS) can’t recognize the phase change in audio signal as easy it can recognize noise in the signal. The phase coding method exploits this fact. This technique encodes the secret message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to- noise ratio.

Spread Spectrum

There are two approaches are used in this technique: the direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). Direct-sequence spread spectrum (DSSS) is a modulation technique used in telecommunication. As with other spread spectrum technologies, the transmitted signal takes up more bandwidth than the information signal that is being modulated. Direct-sequence spread-spectrum transmissions multiply the data being transmitted by a "noise" signal. This noise signal is a pseudorandom sequence of 1 and −1 values, at a frequency much higher than that of the original signal, thereby spreading the energy of the original signal into a much wider band.

The resulting signal resembles white noise. However, this noise-like signal can be used to exactly reconstruct the original data at the receiving end, by multiplying it by the same pseudorandom sequence (because 1 × 1 = 1, and −1 × −1 = 1). This process, known as "de-spreading", mathematically constitutes a correlation of the transmitted Pseudorandom Noise (PN) sequence with the receiver's assumed sequence. For de-spreading to work correctly, transmit and receive sequences must be synchronized. This requires the receiver to synchronize its sequence with the transmitter's sequence via some sort of timing search process. In contrast, frequency-hopping spread spectrum pseudo-randomly retunes the carrier, instead of adding pseudo-random noise to the data, which results in a uniform frequency distribution whose width is determined by the output range of the pseudo-random number generator [10].

Echo Hiding

In this method the secret message is embedded into cover audio signal as an echo. Three parameters of the echo of the cover signal namely amplitude, decay rate and offset from original signal are varied to represent encoded secret binary

message. They are set below to the threshold of Human Auditory System (HAS) so that echo can't be easily resolved.

Video files are generally consists of images and sounds, so most of the relevant techniques for hiding data into images and audio are also applicable to video media. In the case of Video steganography sender sends the secret message to the recipient using a video sequence as cover media. Optional secret key 'K' can also be used during embedding the secret message to the cover media to produce 'stego-video'. After that the stego-video is communicated over public channel to the receiver. At the receiving end, receiver uses the secret key along with the extracting algorithm to extract the secret message from the stego-object.

The original cover video consists of frames represented by Ck(m,n) where 1 £ k £ N. 'N' is the total number of frame and m,n are the row and column indices of the pixels, respectively. The binary secret message denoted by Mk(m, n) is embedded into the cover video media by modulating it into a signal. Mk(m, n) is defined over the same domain as the host Ck(m,n).The stego-video signal is represented by the equation:

$$Sk(m, n) = Ck(m, n)+ak (m, n) Mk(m, n) , k = 1, 2, 3 . . .N$$

Where $ak(m, n)$ is a scaling factor. For simplicity $ak(m, n)$ can be considered to be constant over all the pixels and frames. So the equation becomes [11]:

$$Sk(m, n) = Ck(m, n)+a (m, n) Mk(m, n) , k = 1, 2, 3 . . .N$$

5. Conclusion

In this paper, we talked about steganography and its types. First we had a look at text steganography and Line-Shift Coding, Word-Shift Coding and Feature Coding techniques as different methods of it. Then we got into image steganography and introduced LSB, Masking and filtering and Transformations. As the ending part, Audio steganography was talked and LSB Coding, Phase Coding, Spread Spectrum and Echo Hiding were investigated.

Corresponding Author
Masoud Nosrati
Department of Computer Engineering
Islamic Azad University, Kermanshah Branch, Young Researchers Club, Kermanshah, Iran.
E-mail: minibigs_m@yahoo.co.uk

5/7/2011

References

1. Sara Khosravi, Mashallah Abbasi Dezfoli, Mohammad Hossein Yektaie, A new steganography method based HIOP (Higher Intensity Of Pixel) algorithm and Strassen's matrix multiplication, Journal of Global Research in Computer Science, Vol. 2, No. 1, 2011.
2. S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.
3. G. J. Simmons, "The prisoners' problem and the subliminal channel" in Proc. Advances in Cryptology (CRYPTO '83), pp. 51-67.Berglund, J.F. and K.H. Hofmann, 1967. Compact semitopological semigroups and weakly almost periodic functions. Lecture Notes in Mathematics, No. 42, Springer-Verlag, Berlin-New York.
4. Robert Krenn, Steganography and steganalysis, Internet Publication, March 2004. Available at: http://www.krenn.nl/univ/cry/steg/article.pdf
5. Christian Cachin, Digital Steganography, Encyclopedia of Cryptography and Security, 2005.
6. Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal, Data Hiding Through Multi Level Steganography and SSCE, Journal of Global Research in Computer SciencJournal Science, ISSN: 2229-371x, Volume 2, No. 2, February 2011, pp. 38-47.
7. J.T. Brassil, S. Low, N.F. Maxemchuk, and L. O'Gorman, "Electronic Marking and Identification Techniques to Discourage Document Copying", IEEE Journal on Selected Areas in Communications, vol. 13, Issue. 8, October 1995, pp. 1495-1504.
8. M.Chapman, G. Davida, and M. Rennhard, "A Practical and Effective Approach to Large-Scale Automated Linguistic Steganography", Proceedings of the Information Security Conference, October 2001, pp. 156-165.
9. Mohamed Amin, Muhalim and Ibrahim, Subariah and Salleh, Mazleena and Katmin, Mohd Rozi (2003) Information hiding using steganography. Project Report. Available at: http://eprints.utm.my/4339/1/71847.pdf
10. Direct-sequence spread spectrum (DSSS), Frequency-hopping spread spectrum (FHSS) Wikipedia, the free encyclopedia, GNU Free Documentation License http://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum http://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum.
11. Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay and Sugata Sanyal, "Steganography and Steganalysis: Different Approaches", International Journal of Computers, Information Technology and Engineering (IJCITAE), Vol. 2, No 1, June, 2008, Serial Publications.