International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 09 | Sep-2016 www.irjet.net p-ISSN: 2395-0072

A Survey on Categorization of Steganography

Smitha.G.L[1], Dr.E.Baburaj[2]

[1] *Research Scholar, Dept of CSE, Sathyabama University, Chennai, Tamil Nadu, India.*
[2] *Professor, Dept of CSE, Narayanaguru College of Engineering,Manjalumoodu, Tamil Nadu, India.*

Abstract - *This paper elaborates the different types of steganography. There are two ways to categorize steganography: either based on the techniques that are used in the process of embedding secret data into the carrier or based on the cover type that holds the secret information. Then for each different carrier type some literature review was conducted to understand the works conducted in this area. It can be concluded that text as cover object are investigated by many researchers. Since no many redundancies exist in text, some changes to text can be obvious and easily detected by eavesdrop.*

Key Words: **Steganography**, **Text Steganography**, **Image Steganography, Audio Steganography, Video Steganography.**

1. INTRODUCTION

Nowadays individuals exchange information straightforwardly using the existing communication technologies such as a local area network, a wide area network or simply the Internet. This information can be very sensitive and need to be protected against any intruder who can intercept them during the communication phase. Therefore, transferring sensible information cannot be solely relied on the existing communication technologies channels. We need then a robust technique to protect the information and ensure that they cannot be detected by other parties.

Cryptography is used to encrypt information based on some mathematical formulas. It is widely used to protect information exchanged over the Internet. World Wide Web (WWW) and e-mail are both public channels for transferring information. However, both technologies are vulnerable to attacks [3] and exchanged information can be detected relatively easily. In cryptography the secret information is modified using some public and private keys and become unreadable (e.g., encryption). They are then sent over the public channels to the destination where the original information would be retrieved using the corresponding keys (e.g., decryption). This technique does not prevent against hacker's attacks that can intercept the decrypted information and apply their own techniques to retrieve the secret information. Therefore, it is necessary to find another methodology to protect the information exchanged safely over public channels without raising suspicions. This methodology is known as steganography and has become very popular in the last decade [4].

Steganography is the art of concealing sensible information into digital media (i.e., images, audio, text). It is a mechanism that completely differs from cryptography. In fact, in cryptography the information is modified but still can be seen in this unreadable format once sent over the networks, whereas in steganography the information is simply embedded into a digital support and cannot be noticed as long as the quality of the carrier is not deteriorated [5].

The steganography technique has been used many years ago to convey secret messages. For instance, a king in ancient Greece used to shave the slave's head and tattooed some secret information on it. When the hair was grown, the slave was sent to distribute the message. The receiver then shaved the hair and gets the secret message [6]. In modern life, steganography is employed for many purposes such as embedding copyright [6], embedding individual's detail in smart IDs and inserting patient detail in medical imaging system. There has been a rapid growth of interest on steganography particularly with intelligent service institutions. For instance the US Pentagon has recently allocated significant funds to conduct research in this area, as they believe that terrorists may use this methodology to exchange information [6].

Steganography hides information into a digital media called cover object which can be a video clip, a digital image, an audio file or simply a text. This digital media is called respectively a cover image, a cover audio, a cover video, and a cover text. Once the information is embedded in that cover it is called a stego-object. If the cover is an image or an audio file, then the result of embedding the information in the cover is referred to as stego-image or stego-audio respectively.

It is shown that images are excellent carriers to hide and exchange sensible information over networks [7]. Many algorithms have been proposed recently to hide information into images and preserve their quality. In this Master thesis we focus on image steganography algorithms. An image consists of light luminance or pixels represented as an array of values at different points. A pixel consists of one byte or

more. For example in 8-bit images each pixel consists of 1 byte (i.e., 8 bits). While each pixel in a 24-bit image is represented as three bytes representing the Red, Green and Blue (RGB) colors [6]. Any variation of the bits can lead to a different color.

In a good steganography algorithm, there are five vital features that should be considered [8]. The first one is the capacity payload which refers to the amount of secret information that a stego-cover can carry before the distortions become noticeable. The second feature is the un-detectability which means that the existence of the secret information should be undetectable whenever the stego-object is detected and analyzed. Other features that should be considered are: invisibility, security and robustness [7].

2. CATEGORIZATION BASED ON ALGORITHMS TECHNIQUES

The three major types of steganography techniques are: injection, substitution and generation [9]. We will briefly discuss them in this section.

2.1 Injection-based Technique

This technique is known as 'insertion'. It consists of injecting the secret message into the cover object. The secret message is hidden in an invisible part of the cover- object. In other words, the data is embedded in areas that are ignored by the processing application. For instance, some cover-objects consist of end-of-file flags that tell the processing application to stop when reaching such flags. Therefore the secret message can be inserted after that flags. In such case eavesdrops may not realize that some information are hidden in this cover-object.

The disadvantage of using this approach is that the stego-object size increases according to the amount of the embedded information. Therefore, the stego-object can be suspicious due to its large size once detected and compared to its original.

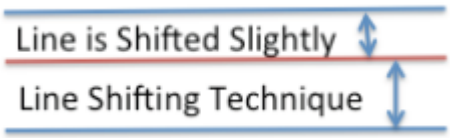

Figure -1: Line Shifting

2.2 Substitution-based Technique

The substitution-based technique is very popular. It overcomes the size enlargement problem of the cover image related to the injection technique. This technique consists of modifying the data of the cover-object and replacing it with the data of the secret message. For example messages can be hidden in byte of images by altering each bit. The substitution-based techniques gain is that the cover object size does not increase after embedding the hidden information. However, it may cause some distortion to the cover object. The degradation of the quality of the cover-object depends on the cover and algorithmic technique used.be used.

2.3 Generation-based Technique

This technique is different from the injection-based and substation-based techniques. It doesn't require having a specific cover-object. It generates the cover-object for the reason of hiding the secret information based on some information structure. One benefit of this technique is that the stego-object and the original-object cannot be compared together. Thus we cannot discover the existence of hidden message in the stego-object due to the uniqueness of the carrier.

Kipper [10] has suggested six classes of steganography techniques which are the following: explicitly substitution system, spread-spectrum techniques, transforms domain techniques, statistical method, distortion techniques and cover generation methods. These techniques can fall into the three general steganography techniques as shown in Table 1. For each technique, a brief explanation is given.

Table -1: Steganography Technique Categories

Techniques	General Technique	Description
Substitution system	Substitution-based	Redundant bits of cover-object are substituted with bits of secret message.
Spread-spectrum techniques	Substitution-based	Secret messages are hidden as noises and spread across the frequency spectrum.
Transform domain techniques	Substitution-based	Secret message is hidden after mathematical transformation is conducted on the cover-object.
Statistical method	Substitution-based	Cover objects statistical properties are changed for embedding purpose.
Distortion techniques	Injection-based	Changes to cover-object are made to hide message. Then measure the deviation from the original cover in the decoding phase.
Cover generation methods	Generation-based	Cover object is created for the reason of hiding message.

Table 1 shows that the most common techniques used in steganography are the substitution-based techniques as they consist of changing the cover object bytes only. They don't require additional information into the cover-object and the size of stego- object is the same as the size of cover object. This will eliminate the case where the size of the stego-object becomes very high although the content of the object looks small. If comparison is conducted then it can straightforwardly detect the presence of hidden information. On the other hand, changing cover object can cause distortion, which leads to easy detection of existence of hidden information. Hence, the cover object changes should

be selected and conducted carefully. In our work, we focus mainly on the substitution-based techniques.

3. CATEGORIZATION BASED ON CARRIER TYPE

The simplest way to categorize steganography is by classifying according to well- known types of cover-object used to carry hidden information that are text, image, audio and video.

3.1 Text Steganography

Embedding secret message into text is one of the oldest approaches to communicate secretly as mentioned previously in the history of steganography section. The secret message is hidden in another message that can be detected or extracted only by the targeted recipient. Recently different techniques exist for text steganography.

Shirali-Shahreza [11] proposed to substitute words of English text with other words that have the same meaning but with different spelling. Some words are spelled differently in British and American English. To embed the secret message, first the hidden message bit is checked and if it does not corresponds to the bit of the written word, and then substitution of the word is conducted. Semantic method is another similar way for embedding data where substitution is used to represent the binary bit pattern of zero or one corresponding to the bits of the hidden data. In this technique the word is substituted with its synonyms [11]. Line shifting and word shifting are two well-known techniques in text steganography. The first method hides information by shifting some lines [12] in a way to hold bits of information. The second method hides the secret information by adjusting the space between words to hide the bits. This work [12] proposed dynamic selection of some words to be substituted with their abbreviation. The information is hidden in short message service (SMS) messages and cryptographic technique is also applied.

An example of line shifting technique for text steganography is shown in Figure 1. The line is shifted slightly by some degree to correspond to the bit of the secret information.

Various techniques are suggested for text steganography that exploits the characteristic of some languages. For instance Shirali-Shahreza [13] proposed an algorithm that takes advantage of shape of the Arabic and Persian letters to embed the data as saved in Unicode Standard. Since the Arabic and Persian letters have four different shapes depending on their positions. In this method each word can hold one bit. Sun et al. [14] worked on Chinese text steganography and proposed a good substitution technique in which the simplified Chinese character and traditional chines character are used for substitution. They suggested Simple Substitution Method (SSM) applied on texts that are in only simplified forms. These characters are then substituted with traditional characters to hide information. For higher capacity Sun et al. [14] presented High Efficient Substitution Method (HESM). This method is the same as SSM except that the bits of hidden message are split into segments with same sizes. Therefore more bits are embedded each time a character is substituted. Changder et al. [15] proposed a novel approach for Indian text steganography. Their method involves hiding secret information by creating understandable sentences. Where the longest common subsequence is applied to find strings that forms sentences.

It is held that embedding covert information using text steganography is the hardest amongst all of steganography types. Because its lack of redundancy of the text and zero-overhead for hiding secret information [12].

3.2 Image Steganography

Recently, images have been widely used as a powerful digital support and are easy to exchange. It contain good amount of redundancy that makes them a good carrier for holding confidential messages. Consequently various methods for hiding information into images have been proposed. Figure 2 represents a stego-image that is embedded with secret text information composed of 3500 letters.

In image steganography, the secret messages are concealed in the pixels value. For example Pixel Pair Matching (PPM) uses two pixels to conceal digit SB in B-ary notational system. Adaptive Pixel Pair Matching (APPM) allows embedding digits in any notational system [8]. In this technique one pixel is chosen as a reference coordinate and the other pixel as a search coordinate. Rosaline et al. [8] suggested embedding audio files using APPM by first retrieving header content and then all fields are converted to bit stream. Where these bits are then embedded into the cover image.

One of recent algorithms is proposed by Chang et al. [16] which optimized a method based on Pixel-Value Differencing PVD. PVD technique uses block of 2 pixels for the purpose of

reference point and embedding secret bit. It depends on the difference between two consecutive pixels. From a range table we can compute how many bits a block can carry. Then secret bit is converted into decimal and added to its lower bound range. Finally the two consecutive pixels are changed due to this formula presented in [16]. Chang et al. [16] proposed the same technique as the explained previously but instead of using only one direction, three directions are used (2x2) block of pixel. This tri-way pixel-value differencing (TPVD) increases the embedding capacity. In addition, an optimal approach of selecting the reference point is proposed.

It is highly efficient to embed a ternary message to any pixel of an image in a steganography system. However it is required to convert the message bit from a binary format to a ternary format. Zhang et al. [17] suggested some improvement on binary covering function using Hamming code. The method proposed is based on hamming covering function C(R, n, k), where R is the maximum possible changes whenever k bits of messages (m_1,…,m_k) are embedded in the Least Significant Bit of n pixel gray values (b(x_1), …, b(x_n)). They proposed "Hamming+1" method, in which the block of pixels of the hamming covering function is expanded by one. Zhang et al. [42] purposed to minimize the average rate of embedding changes. Many other techniques exist to embed data into images.

3.3 Audio Steganography

Secret messages are possible to be covert into audio files. Low bit encoding, spread spectrum and echo data hiding are recognized techniques used to conduct audio steganography. The first method exploits the redundant bit of audio files to hold bits of secret information. The proceeding method involves injecting the secret messages into the audio file as noises and spreading the secret message across the frequency spectrum. The last method is about taking advantage of echoes in the sound files to hide information [18].

Balgurgi et al. [19] introduced a method to combine two methods together to embed messages. The first method the Least Significant Bit is used with the second XORing method. The XOR operation is performed on the bit of the LSB and the bit next to it. If the secret message bit is 0 and the result of XORing is 1 then the LSB of cover audio is flipped and kept unchanged if are equal. In case the message bit is 1 and XORing is 0 then the LSB of cover audio is flipped otherwise it is not changed. The message is retrieved by XORing the LSB and the second LSB. After extracting every 16 bits, it is converted to the decimal corresponding value.

Speaker and speech recognition and speech analysis systems use cepstral domain feature. Gopalan [20] presented a method focused on speech spectrum where the messages are hidden in the cepstral domain. Cepstral is the inverse Fourier transform of logarithm of the spectrum of a signal and involves manipulation of statistical means. The proposed method first pair of masked frequencies is selected amongst the most frequently occurring. The selected pair is used as part of the key for embedding into the signal. Then given a cover speech, f1 and f2 are two chosen frequencies of a sinusoid cepstrum are obtained with the maximum amplitude. For each signal speech the message is embedded following modification of the complex cepstrum as illustrated in [20]. To extract the data, at each frame spectral magnitude ratio of f1 and f2 are computed. In [20] demonstrated how the ratio is computed. .

Many other various techniques exist to embed messages into audio files. We refer the reader to this work [21] to get a detailed view about the latest techniques and categories on audio steganography. In this survey, the use of audio files as a cover object to exchange secret information is investigated.

3.4 Video Steganography

Video files consist of frames of image and sounds. Therefore most steganography image and audio methods can be applied on video as well. Videos are good carrier for hiding large amount of information. The distortion in video files is not easily noticeable by human due to moving stream of frames and sounds. Few approaches that lately have been proposed are presented.

Figure 3 (a) shows a frame of a video that is used as cover-video. Figure 3 (b) is the stego-video where a text is embedded inside it [22]. The technique uses bit-wise operation where bits of the frame content are modified to hold information.

Some researchers proposed to work on the use of lazy lifting wavelet transform to transform the video into sub-bands. Then apply Least Significant Bit on the sub-band of the transformed video. This work [23] presented a technique to embed data into both the image and audio component. Where the lazy wavelet transformed is used to hide data in the coefficient of the image component. The length is then hidden using Least Significant Bit in the audio component. The extraction is conducted by reversing the process of embedding data in the video.

Alternative technique used for video steganography is non-uniform rectangular partition of frames to embed

messages. For instance, Hu et al. [24] proposed an algorithm that uses optimal quadratic approximation to determine the gray weights of sub-images with specified bivariate polynomial. If the estimated weight of sub-image with the bivariate polynomial reconstructs the original sub-image restricted by an error control, then the partition is stopped. Otherwise sub-image is split into four parts and the approximation calculation is conducted again. Those steps are repeated until the pixel of the sub-image become greater than or equal to the undetermined coefficients or the approximation requirement is satisfied. Where the code which consists of partition code and differences of gray values are embedded in the fourth bit of each gray byte. At the receiver side the codes are extracted from the image. Based on the extracted code, coefficients are computed and each sub-image is recovered which is important to recover the secret message. This was applied to video steganography by using the previous algorithm on each frame of video.

Figure -2: Image Containing Secret Information

(a)

(b)

Figure -3: (a) Cover-Video Fram (b) Stego-Video Frame

4. CONCLUSIONS

This paper presented the categories of steganography. Then for each different carrier type some literature review was conducted to understand the works conducted in this area. It can be concluded that text as cover object are investigated by many researchers. Since no many redundancies exist in text, some changes to text can be obvious and easily detected by eavesdrop. Therefore characteristic of languages are exploited to do manipulation to embed the secret data. Thus, some of the approaches suggested in this field are specific to languages. Audios are also used as cover object and they attract many interests by the steganography research community. However meaningful audio should be transmitted to make it less suspicious to eavesdrop. Audio requires higher audio file size compared to images. Finally because the sizes of video files are large too, it is not common to transmit and exchange videos by E-mail. Consequently, video steganography is not as popular as image steganography and not many research works are performed on video steganography.

REFERENCES

[1] Mielikainen, J. (2006). LSB matching revisited. IEEE Signal Processing Letters, 13(5), pp. 285-287.

[2] Luo, W., Huang, F., & Huang, J. (2010). Edge adaptive image steganography based on LSB matching revisited. IEEE Transactions on Information Forensics and Security, 5(2), pp. 201-214.

[3] Leavitt, N. (2004). "Scob attack: a sign of bad things to come", Computer, 37(9), pp. 16-18.

[4] Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. Computer, 31(2), pp. 26-34.

[5] Anderson, R. J., & Petitcolas, F. A. (1998). On the limits of steganography. IEEE Journal on Selected Areas in Communications, 16(4), pp. 474-481.

[6] Caldwell, J. (2003). "Steganography", CROSSTALK The Journal of Defense Software Engineering, pp. 25-27.

[7] Rodrigues, J. M., Rios, J. R., & Puech, W. (2004). SSB-4 System of Steganography using bit 4. In 5th International Workshop on Image Analysis for Multimedia Interactive Services.

[8] Imaculate Rosaline, S., & Ashok Raj, M. (2013). Adaptive Pixel Pair Matching based Steganography for Audio files. In International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System, pp. 1-5.

[9] Ashok, J., Raju, Y., Munishankaraiah, S., & Srinivas, K. (2010). Steganography: An overview. International Journal of Engineering Science and Technology, 2(10), pp. 5985-5992.

[10] Kipper, G. (2004). Investigator's guide to steganography. CRC Press.

[11] Shirali-Shahreza, M. (2008). Text steganography by changing words spelling. In 10th International Conference on Advanced Communication Technology, Vol. 3, pp. 1912-1913.

[12] Rafat, K. F. (2009). Enhanced text steganography in SMS. In 2nd International Conference on Computer, Control and Communication, pp. 1-6.

[13] Shirali-Shahreza, M., & Shirali-Shahreza, S. (2008, September). Persian/Arabic Unicode Text Steganography. In Fourth International Conference on Information Assurance and Security, pp. 62-66.

[14] Sun, X., Meng, P., Ye, Y., & Hang, L. (2010). Steganography in Chinese text. In International Conference on Computer Application and System Modeling, Vol. 8, pp. V8- 651.

[15] Changder, S., Ghosh, D., & Debnath, N. C. (2010). LCS based text steganography through Indian Languages. In 3rd IEEE International Conference on Computer Science and Information Technology, Vol. 8, pp. 53-57.

[16] Chang, K. C., Chang, C. P., Huang, P. S., & Tu, T. M. (2008). A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing. Journal of Multimedia.

[17] Zhang, W., Wang, S., & Zhang, X. (2007). Improving embedding efficiency of covering codes for applications in steganography. IEEE Communications Letters, 11(8), pp. 680-682.

[18] Mangarae, A. (2006). Steganography FaQ. Zone-H. Org March 18th.

[19] Balgurgi, P. P., & Jagtap, S. K. (2012, October). Intelligent processing: An approach of audio steganography. In International Conference on Communication, Information & Computing Technology 2012, pp. 1-6.

[20] Gopalan, K. (2008). Audio steganography by modification of cepstrum at a pair of frequencies. In 9th International Conference on Signal Processing, pp. 2178-2181.

[21] Djebbar, F., Ayad, B., Hamam, H., & Abed-Meraim, K. (2011). A view on latest audio steganography techniques. In International Conference on Innovations in Information Technology, pp. 409-414.

[22] Swathi, A., & Jilani, S. A. K. Video Steganography by LSB Substitution Using Different Polynomial Equations. International Journal of Computational Engineering Research (ijceronline. com) Vol. 2, pp. 1620-1623.

[23] Patel, K., Rora, K. K., Singh, K., & Verma, S. (2013). Lazy Wavelet Transform Based Steganography in Video. In International Conference on, Communication Systems and Network Technologies, pp. 497-500.

[24] Hu, S., & KinTak, U., (2011). A Novel Video Steganography based on Non-uniform Rectangular Partition. In The 14th International Conference on Computational Science and Engineering , pp. 57-61.