Steganography analysis techniques applied to audio and image files

Roshidi Din, Alaa Jabbar Qasim
School of Computing, College Arts and Sciences, Universiti Utara Malaysia, 06010 UUM Sintok, Kedah, Malaysia

Article Info

Article history:

Received Apr 30, 2019
Revised Jun 18, 2019
Accepted Jul 2, 2019

Keywords:

Audio
Image
LSB
Steganography
Video

ABSTRACT

The present work carries out a descriptive analysis of the main steganography techniques used in specific digital media such as audio and image files. For this purpose, a literary review of the domains, methods, and techniques as part of this set was carried out and their functioning, qualities, and weaknesses are identified. Hence, it is concluded that there is a wide relationship between audio and image steganography techniques in their implementation form. Nevertheless, it is determined that LSB is one of the weakest techniques, but the safest and the most robust technique within each type of the presented medium.

Corresponding Author:

Roshidi Din,
School of Computing College Art and Science,
06010 Universiti Utara Malaysia, Malaysia.
Email: roshidi@uum.edu.my

1. INTRODUCTION

Steganography has gained a lot of space in the computer field with the growth of the internet and access to digital media. However, this does not mean that it is a recent science as it has existed since ancient times. According to the historical review made [1, 2]. it was the Greeks who became the first to use the closest to steganography; having evidence of this even before 440 BC. Hence, it has its origin in the Greek language. In particular, steganography techniques have found their main application in the world of business including commercial brands, and in the music industry, in view of the need to maintain the trade design in secret, to protect copyright in digital media[3, 4], and mainly to prevent unauthorized personnels from knowing the existence of the hidden message. Similarly, steganography is used in illegal activities, such as terrorism, in a way that steganographic methods were used to plan the attacks of September 11, 2001. Because of these two factors, during the last decade, an intensive research in steganography and its detection methods are observed [5, 6].

Currently, there are various types of steganography, and the ability of computer applications that facilitate their function in the field of digital media in which above all, the image and audio files became stood out. They have been the most exploited due to the numerous methods created to hide information in these; and because in general, other types of digital files such as videos use the same techniques that are applied in audio[7, 8]. Additionally, it is emphasized that steganography is much more sophisticated in the digital media compared to other domains such as network channels since they consider that network-based steganography still needs to learn a lot from digital-based steganography [9, 10]. Based on the above discussion, it is evident that the level of research within steganography, in the field of digital media with audio and image files, is high. All this has led to having a large number of techniques applicable to these types of files that over time have evolved or newly generated. Therefore, it is necessary to carry out the present revision work that allows analyzing steganography techniques used in the image and audio files. In order to present an updated review of these main techniques with their strengths and weaknesses, different investigations have been carried out in this field.

2. STEGANOGRAPHY DEVELOPMENT

Steganography is often confused with cryptography, as both are part of the information protection processes. However, they are different in disciplines as both are implemented in having their own objectives. Meanwhile, cryptography is used to encrypt information in a way that is unintelligible to a probable intruder, despite knowledge of its existence [11, 12]. Steganography is the art of hiding information, through a steganographic system that embeds the hidden data in another means of normal communication without leaving any suspicion [13, 14]. Additionally, steganography is the science that is responsible for hiding the existence of certain communication [15, 16].

On the other hand, cryptography does not hide information but only encodes the data that makes them two complementary and orthogonal sciences, since it is possible to apply a cryptographic algorithm to the information before being hidden. In this way, if the hidden data is revealed, an additional security is maintained with these, simply because they would also be encrypted. [1, 17] also point out that the relevant requirements of steganography are to have a high degree of imperceptibility, to provide an algorithm without detectability, and the ability to survive normal compression by code [18].

3. STEGANOGRAPHY TECHNIQUES IN AUDIO FILES

Steganography in audio is more important than in other means of steganography (text, image, video), because it can carry more redundant information compared to other media. This is necessary to a means of covering as to hide the secret message. When joined together, they become the stegno-object as can be seen in Figure 1. In this area of audio steganography, the following classification, temporal domain, frequency domain, wavelet domain and Encoder domain are proposed.

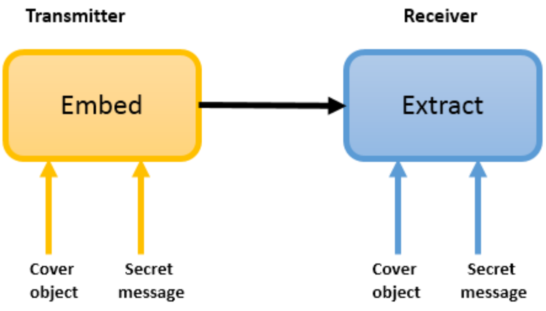

Figure 1. Block diagram for audio steganography

3.1 Temporal domain

This domain is mainly made up of the following techniques: Low bit encoding and Echo hiding. They are also known as spatial domain techniques[19].

a. Low Bit Encoding

This technique, also known as Least Significant Bit (LSB), is one of the first studied for the concealment of data in audio signals. The operation is based on selecting, by means of the watermark encoder LSB, a subset of audio samples chosen by a secret key, and in this subset of data the substitution of the bits to be hidden is made by the value of the bits original [20]. The main advantage of using LSB is the ease with which it can be applied to its application in a simple way, and being, at the same time, a great weakness with similar simplicity, since the hidden data are easily extracted by unauthorized people [11].

b. Echo Hiding

This is a technique that embeds information within an audio signal and bases its operation on finding "gaps" within the ranges of perception of the human auditory system, where data can be hidden, with the main objective that these have a minimum degradation with respect to the original data, which allows the change in the audio to be more difficult to perceive for the listener [21]. On the other hand, if there is only one echo in the original signal, only one bit can be encoded, in addition to offering advantages such as high data transmission rate and greater robustness than other methods [21].

3.2 Frequency domain

The main frequency domain techniques are Tone insertion, Phase Coding, Amplitude modification, and Spread spectrum. Each one of them will be described extensively in the following discussion.

a. Tone insertion

Tone Insertion is responsible for achieving the auditory imperceptibility of low power tones, within a larger spectrum. For this, the original audio is divided into segments of 16ms duration, in which the power of each frame is calculated and only a bit of the data is embedded in the original audio. Currently, Tone insertion is resistant to low-bass filter and truncated btis attacks. However, one limitation becomes the low capacity of data embedding, which allows the tones inserted are easy to detect [22].

b. Phase Coding

This technique is responsible for embedding information in the phase of the guest signal. What characterizes it is the good performance it has regarding the fidelity of the hidden data. However, one of its limitations is the low capacity of embedding since it embeds 16-32 bits of data in audio files of 1 second in duration [22, 23].

c. Amplitude Modification

This technique, a translation of the algorithm is carried out within the code, where the most relevant of said code is the ordering of the main amplitudes. Additionally, Amplitude modification can be embedded separately within each channel, using three sections of 512-frame, and achieving a very good compression, but with the risk of losing the data in mono compression. This method presents a great weakness in term of hearing but has a great potential if some volume is reduced, and the use of length segments of cryptographic variables are made [22, 23].

d. Spread Spectrum

It is stated that the two most common types of spread spectrum are frequency hopping, where the pseudo-noise code is used pseudo-randomly to help change frequency transmission periodically, and the direct sequence, where the pseudo-noise code is used to sequentially modulate the signal at a high rate. These authors emphasize that one of the advantages of this technique is the difficulty of transmission in being detected [22].

3.3. Wavelet domain

The Wavelet Domain has multi-resolution properties that make it appropriate for frequency analysis, in addition to working with coefficients of wavelet. In achieving that, when applying an inverse transformation, it is possible to reconstruct the stegano-signal**.** Additionally, a general method to work with Wavelet Domain is proposed, through the decomposition of the signal with the use of LSB when hiding the information, demonstrating that a great advantage of this technique has a greater transparency and hiding ability compared to other domains [19, 24].

3.4. Encoder domain

It is stated that the Codebook modification and Bitstream hiding techniques are part of this domain, as both being used together to hide data in real-time communications through the use of voice codecs such as: SILK, ACELP or AMR. These techniques are the high robustness although their weakness lies in having a low rate of embedding [19, 24].

4. STEGANOGRAPHY TECHNIQUES IN IMAGE FILES

There are two ways to create digital images. First is through the computer, with drawing or design tools that generate diagrams, statistical graphs or others, and the second is with the sensors that generate digital images, which are the heart of devices such as scanners, digital cameras, and digital video cameras. Therefore, he affirms that this second type of images are the favorite for steganography, because they are the most used and therefore a better environment for the use of these has been developed. In this case, image techniques in steganography are classified in the following domains: spatial domain methods, transformation domain technique, distortion techniques and masking and filtering.

4.1. Spatial domain

There are several methods in the space domain, of which the following stand out the Least Significant Bit, RGB based steganography, Pixel Value Differencing (PVD), and Mapping based steganography. Each of these techniques is presented as follows:

a. Least Significant Bit

This is the most popular and simple when working with images since it has a low computational complexity and high embedding capacity. LSB hides the messages within an image by replacing the least significant bit of each pixel, that is, the bit of least value, by the data to be embedded. This technique is not safe since the stego-image contains spots in the places where the bits are hidden, and when applying attacks, such as the analysis of sample pairs, histogram analysis of image or others, the information can be easily obtained [25].

b. RGB Based Steganography

This technique is named in such a way because of the three primary colors in English, Red (R), Green (G) and Blue (B), in which one value for every three values describes a pixel. Each pixel is a combination of the components R, G and B in a 24-bit color scheme. A method using RGB image pixels as a means of coverage is proposed, through the use of a channel for the indication of secret data in the other channels, in which the indication channel changes from one pixel to another with natural random values that depend on the pixels of the image. The comparisons, made between this technique, are based on RGB and other LSB techniques, and it shows that it has more capacity with the same level of security[19, 24].

c. Pixel Value differencing

This method facilitates the incorporation of secret messages in an image, without major changes in the original file as its mechanism is based on embedding the secret data in an image of coverage. This is done by replacing the values of the difference of the blocks of two pixels of said image with the similar ones where bits of embedded data are included. In the same way, it points out that one of its characteristics is the use of the sensitivity of the human eye for the variations of gray values. Others point out that PVD can embed more data in pairs of pixels with larger differences. However, in these cases, PVD causes a considerable distortion that leads to degradation of the quality of the image.

d. Mapping Based Steganography

This technique can be called Pixel Mapping Method (PMM) as it is able to hide data within any grayscale image. This is done by selecting the embedding pixels by means of mathematical functions depending on the intensity of the seed pixel value. Before the embedding, a check is made that defines if the selected pixels or their neighbors are within the limits of the image or not, and then the data embedding is done with a mapping of every two or four bits of the secret message in each neighbor pixel. Within Table 1, this mapping of information for two-bit embedding is shown.

Table 1. PMM mapping technique for two-bit embedding

Bit couple	Intensity of pixel value	No of ones (Bin)
01	Pair	Pair
10	Odd	Odd
00	Pair	Odd
11	Odd	Pair

Some studies have developed an extended method of PMM, where the performance of PMM has been measured through various metric techniques such as Mean Square Error (MSE), Peak Signal-to-Noise Radio (PSNR), Root Mean Square Error (RMSE) and Structural Similarity Index (SSI), and a measurement has also been made with stegoanalysis techniques such as RS analysis, SP analysis and Chi-square analysis, resulting in a high safety measure and prove [5].

4.2. Transformation domain

Transformation domain is classified into the following techniques: Discrete Fourier Transformation (DFT), Discrete Cosine Transformation (DCT), and Discrete Wavelet Transformation (DWT). He also states that the strongest steganography techniques nowadays, work in the transformation domain, since they have an advantage over spatial domain techniques, by hiding information in areas that are less exposed to compression, clipping and to image processing. The techniques of this domain are discussed below.

a. Discrete Fourier Transformation

DFT is a technique based on mathematical transformations that convert the pixels in such a way that it gives the effect of spreading the location of the values of the pixels over a part of the image. On the other hand, the advantages of image steganography with Fractional Fourier Transform (FrFT), which is a generalization of DFT, by its fractional order (α) achieves a domain optimal, given that in the performance tests with PSNR and MSE, one might get ideal results. Thus, FrFt with a fractional additional parameter (α) presents a greater security compared to other techniques of the transformation domain [5].

b. Discrete Cosine Transform

In steganography, embedding the secret message in the least significant bit of the discrete cosine is coefficient of a digital image. Also, these authors explain that its operation is based on breaking down the image into blocks of 8x8 pixels; from right to left and from top to bottom. DCT is applied to each block, until the message is finally embedded in the DCT coefficients. In addition, in an analysis made to DCT, it is concluded that it has an advantage compared to algorithms such as LSB and DWT since the results of PSNR are high with respect to the other two algorithms, although within the same results, the DCT robustness is medium [5].

c. Discrete Wavelet Transform

The technique is the decomposition of images based on the transformation of small waves, called wavelets, of different frequencies [5].

d. Distortion Techniques

The distortion techniques is about covering the original image during the decoding process in order to check if there are differences between the original image and the distorted image. On the contrary, the encoder adds as a sequence of modifications in the coverage image, creating a stego-object. This sequence of modifications is selected to match the message that is required to be sent. This technique limits certain advantages as it is necessary to send the coverage image, considering that steganography techniques should not use the coverage image more than once.

4.3. Masking and filtering

This technique has an effectiveness similar to the watermarks of documents by creating masks in an image. Although masking does change the properties of the image, it can be done in such a way that anomalies are not identified to the human eye. This author also highlights that masking and filtering have greater robustness than LSB with respect to compression, trimming, and image processing. In general, it is restricted to working with 24-bit images or images with gray scales, but it has a favour that the data is hidden in the visible part of the image and not on another level, which gives resistance to compression algorithms, in the case of JPEG formats.

5. CONCLUSION

At the end of the present analysis, it can be concluded that both steganography in audio and in image are closely related in terms of the way in which the techniques are implemented and the ability to hide a message in the end by keeping it imperceptible and undetectable to human’s sight and hearing. However, there are very weak techniques that have already been violated, such as LSB, which is one of the simplest to apply but offers very little security and robustness since the hidden data is easy to extract. On the other hand, made hiding and Spread Spectrum are among the safest methods for audio steganography; likewise, PMM and Discrete Cosine Transform have more security with respect to other techniques.

ACKNOWLEDGEMENTS

The author wish to thank the Ministry of Higher Education Malaysia in funding grant under the University Grant FRGS with S/O 13576, RIMC of Universiti Utara Malaysia, Kedah.

REFERENCES

[1] H. Abdulzahra, R. Ahmad, and N. M. Noor, "Combining cryptography and steganography for data hiding in images," *Applied Computational Science*, pp. 128-135, 2014.

[2] V. K. C.Gayathri "Study on Image Steganography Techniques " *International Journal of Engineering and Technology (IJET),* 2013.

[3] R. Amirtharajan and J. B. B. Rayappan, "Steganography-time to time: A review," *Res. J. Inform. Technol,* vol. 5, pp. 53-66, 2013.

[4] K. S. Babu, K. Raja, K. K. Kiran, T. M. Devi, K. Venugopal, and L. Patnaik, "Authentication of secret information in image steganography," in *TENCON 2008-2008 IEEE Region 10 Conference*, 2008, pp. 1-6.

[5] C.-C. Chang and H.-W. Tseng, "A steganographic method for digital images using side match," *Pattern Recognition Letters,* vol. 25, pp. 1431-1437, 2004.

[6] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal processing,* vol. 90, pp. 727-752, 2010.

[7] S. Deepthi, A. Renuka, and S. Hemalatha, "Data hiding in audio signals using wavelet transform with enhanced security," *Computer Science & Information Technology (CS & IT).*pp137-146, 2013.

[8] R. Din and A. Samsudin, "Intelligent steganalytic system: application on natural language environment," *WSEAS Transactions on Systems and Control,* vol. 4, pp. 379-388, 2009.

[9] A. K. Jain and U. Uludag, "Hiding fingerprint minutiae in images," in *Proceedings of 3rd Workshop on Automatic Identification Advanced Technologies*, 2002, pp. 97-102.

[10] H. Jalab, A. Zaidan, and B. Zaidan, "Frame selected approach for hiding data within MPEG video using bit plane complexity segmentation," *arXiv preprint arXiv:0912.3986,* 2009.

[11] A. Febryan, T. W. Purboyo, and R. E. Saputra, "Steganography Methods on Text, Audio, Image and Video: A Survey," *International Journal of Applied Engineering Research,* vol. 12, pp. 10485-10490, 2017.

[12] T. Morkel, J. H. Eloff, and M. S. Olivier, "An overview of image steganography," in *ISSA*, 2005, pp. 1-11.

[13] K. Rabah, "Steganography-the art of hiding data," *Information Technology Journal,* vol. 3, pp. 245-269, 2004.

[14] N. Rani and J. Chaudhary, "Text steganography techniques: A review," *International Journal of Engineering Trends and Technology (IJETT),* vol. 4, pp. 3013-3015, 2013.

[15] S. Rastogi and A. Shakya, "An Analysis of Recently Used Steganography Techniques on Images." *International Journal of Computer Science Trends and Technology (IJCST)*. Volume 3 Issue 5, Sep-Oct 2015.

[16] P. C. Ritchey and V. J. Rego, "Hiding Secret Messages In Huffman Trees," in *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2012 Eighth International Conference on*, 2012, pp. 71-74.

[17] T. Amarunnishad and A. Nazeer, "Secured Reversible Data Hiding In Encrypted Images Using Hyper Chaos," *International Journal of Image Processing (IJIP),* vol. 8, p. 423, 2014.

[18] A. Khare, M. Kunari, and P. Khare, "Efficient algorithm for digital image steganography," *Journal of Information Science, Knowledge and Research in Computer Science and Application,* pp. 1-5, 2010.

[19] B. G. Banik and S. K. Bandyopadhyay, "Review on Steganography in Digital Media." *International Journal of Science and Research (IJSR).* February 2015; 4(2): 265-274.

[20] N. Cvejic and T. Seppänen, "Increasing Robustness of LSB Audio Steganography by Reduced Distortion LSB Coding," *J. UCS,* vol. 11, pp. 56-65, 2005.

[21] S. K. Bandyopadhyay, D. Bhattacharyya, D. Ganguly, S. Mukherjee, and P. Das, "A tutorial review on steganography," in *International conference on contemporary computing*, 2008.

[22] M. Nosrati, R. Karimi, and M. Hariri, "Audio steganography: a survey on recent approaches," *world applied programming,* vol. 2, pp. 202-205, 2012.

[23] S. Bhattacharyya, "A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier," *Journal of global research in computer science,* vol. 2, 2011.

[24] A. Almohammad, "Steganography-Based Secret and Reliable Communications: Improving Steganographic Capacity and Imperceptibility," Department of Information Systems and Computing Brunel University. Thesis. 2010.

[25] O. G. Roshidi Din, Alaa Jabbar Qasim, "Analytical Review on Graphical Formats Used in Image Steganographic Compression," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. Vol 12, No 2, pp. 441~446, 2018.