A REVIEW AND COMPARISON OF STEGANOGRAPHY TECHNIQUES

STEGANOGRAFİ TEKNİKLERİ ÜZERİNE BİR İNCELEME VE KARŞILAŞTIRMA

Hüseyin Bilal MACİT
Mehmet Akif Ersoy University, Tefenni MYO, hbmacit@mehmetakif.edu.tr

Arif KOYUN
Süleyman Demirel University, arifkoyun@sdu.edu.tr

Orhan GÜNGÖR
Mehmet Akif Ersoy University, Tefenni MYO, orhangungor@mehmetakif.edu.tr

ABSTRACT: Speeding up communications and the Internet today facilitates the transfer of data from one end to the other. However, it has led to the emergence of the concept of information security. The most common method to provide information security is cryptography; which is encrypting the information. However, if an attacker seizes the data and finds a method to decrypt it, he gets confidential information. Besides, steganography is aimed at bringing information to an undoubted situation. Confidential data is embedded into an ordinary carrier data, and sent to peers suspiciously. This carrier data may be a protocol, audio, video, text, image, or any other digital object. If the attacker obtains the data, he will not doubt that the data is carrying another data. The security of the confidential data depends on the success of the embedding algorithm. In this study, different algorithms used in steganography based on carrier data are introduced, the performance of steganography algorithms are compared, together use of steganography and cryptography is investigated.

Keywords: Image steganography, audio steganography, video steganography, text steganography.

ÖZET: Internet ve iletişimin hızlandırılması ile günümüzde verilerin bir uçtan diğerine aktarılması kolaylaşmıştır. Ancak bu durum, bilgi güvenliği kavramının ortaya çıkmasına yol açmıştır. Bilgi güvenliği sağlamada en yaygın yöntem; bilgiyi şifreleme olarak bilinen kriptografidir. Ancak, bir saldırgan verileri ele geçirir ve şifresini çözmek için bir yöntem bulursa, gizli bilgiyi elde edebilir. Bunun yanında steganografi; bilgiyi şüphe çekmeyen bir duruma getirmeyi amaçlamaktadır. Gizli veriler sıradan bir taşıyıcı veriye gömülür ve şüphe çekmeden gönderilir. Bu taşıyıcı veri bir protokol, ses, video, metin, görüntü veya başka bir dijital nesne olabilir. Saldırgan veriyi elde etse bile, verilerin başka bir veri taşıdığından şüphe etmeyecektir. Gizli verilerin güvenliği, yerleştirme algoritmasının başarısına bağlıdır. Bu çalışmada, taşıyıcı verilere dayanarak steganografide kullanılan farklı algoritmalar tanıtılmış, steganografi algoritmalarının performansı karşılaştırılmış, steganografi ve kriptografinin birlikte kullanımı incelenmiştir.

Key words: Nesne steganografi, ses steganografi, video steganografi, metin steganografi

INTRODUCTION

As the possibilities of modern communication increase, the need for security tools also increases. Protecting data from unauthorized access and data integrity has become a major problem (Amin et al., 2003).Cryptography consists of advanced mathematical methods developed to provide data security. With these methods, the data can be encrypted and decrypted. The data is encrypted using a key, then sent to the recipient. Capturing the key by any third party greatly affects the security of the data (Tunçer and Karakuzu, 2016).The goal of cryptography is to make the data unreadable by a third party. The objective of steganography is to hide data from third parties (Doshi et al., 2012). A major disadvantage of cryptology is that the presence of the data can not be concealed. Encrypted data, although unreadable, is still present as data. If enough time is given, one can finally decrypt the data.

Steganography is a Greek word which means“hidden writing”. The word "steganos" means covered and "graphial" means writing (Kour and Verma, 2014). Steganography is the art and science of hiding the existence of data.The original cover data and the cover data carrying the hidden data are so similar that human perceptions

can not perceive. The process of hiding data inside a multimedia content which is called as cover media is called "Embedding".

Detection of confidential data is an important issue for researchers. In a suspicious situation, controlling hundreds or thousands of data with different algorithms is a time-consuming and high-transaction activity (Abboud et al., 2010). Some public institutions, individuals and companies where privacy is important, use steganography in addition to cryptography for safer data transmission. Steganography is a good way to hide and communicate confidential information without attracting others. Also, content producers and owners use steganographic methods to protect property rights of content they produce (Jayaram et al., 2011). This type of steganography which is called watermarking, is usually the job of placing hidden or visible information in the cover data for copy protection.

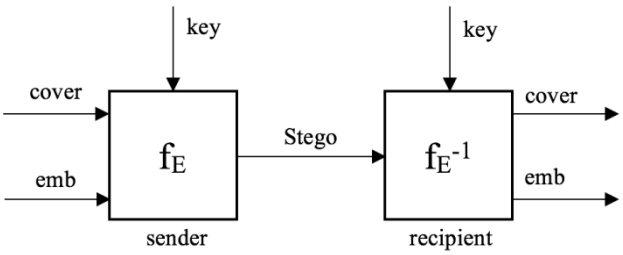

Figure 1. The general Steganography System (Jayaram et al., 2011).

Steganography consists of two terms, the secret message and the cover object (Kour and Verma, 2014).A general steganography system has been given in Figure 1(Fridrich, 2010). These terms in Figure 1 are;

- emb: The data to be embedded.
- cover: Carrier cover data
- stego: Embedded data bearing cover data
- key: Additional data that is used for embedding and required for extraction, hence the recipient should know
- f_E: The steganographic method that creates the stego data with the cover, the data to be embedded and the key.
- F_E^{-1}: The method which seperates stego data tocover media and hidden data using a key. In other words, the opposite of embedding.

When embedding a data, the following criteria must be considered;

- Embedded data should be as perceptible as possible.
- Embedded data must be embedded in the cover data itself. Embedding the data in a section such as the title of the cover means losing it during a format change.
- The stego data must be resistant to attack such as filtering, rotating, sampling.
- Corruption during attacks should be understandable and repairable using verification codes such as parity.
- A part of embedded data must be extractable even if a part of the cover file reaches the recipient (Rabah, 2004).

The effectiveness of a steganographic method can be determined by comparing the stego-image with the cover image. There are several factors that define the effectiveness of a technique. These factors are;

- **Robustness:** The embedded data shouldn't be corrupted when stego data is exposed to attacks such aslinear and nonlinear filtering, sharpening or blurring, random noise insertion, rotation and scaling, cropping or breaking, compression, and etc.
- **Imperceptibility:**Stego data should be just like an ordinary data. No user or software should be doubts that the stego file carries any other data.
- **Payload capacity:**It represents the amount of confidential information that can be stored in the cover data. Steganographic method aims to carry the maximum amount of confidential data with minimum change in cover data.
- **Peak Signal to Noise Ratio (PSNR):**This rate measures the quality between the original and the stego data. The higher the PSNR value means the more successful steganographic method.
- **Mean Square Error (MSE):**It is defined as the average difference between a reference image and a modified image. The smaller the MSE means the more efficient steganography technique.

- **Signal to Noise Ratio (SNR):**It is the ratio between signal strength and noise power. It compares the level of the desired signal with the background noise level.

Detecting a hidden data inside a cover data is called steganalysis. The steganalysis method attempts to identify the steganography by examining the captured data with various parameters. If there is a defined steganographic method and confidential data, the second purpose is to extract this data correctly. Steganalist is a person who develops and applies the methods of steganalysis.

Steganography Types

The type of cover data is also the type of steganography. Today, steganography is examined as text, image, audio, video and protocol steganography (Amirtharajan and Rayappan, 2013).

Text Steganography

Confidental data is hidden in text files. Different methods can be used to hide the data in the text file. These methods include;

- **Format Based Method:** Confidential data is hidden inside cover data with methods such as adding text spaces, deliberate typing errors, sizes of writing types.This method is easily detectable by a computer software, hence, it is a less preferred method.
- **Random and Statistical Method:** Hidden data is stored inside character strings. Places where confidential data are hidden must be reported to the extracter.
- **Linguistics Method:** Hidden data is stored in the syntactic structure.

Image Steganography

It is the method of hiding data inside a an image file as cover data. In image steganography, pixel densities are used to hide the data. Most commonly used image formats as cover data are; BMP, PNG, JPEG, TIFF and GIF (Kamble et al., 2013). Image steganography uses the weaknesses of the human visual system (HVS). Most commonly used methods in image steganography;

- Least Significant Bit (LSB)
- Spread spectrum
- F5
- Palette embedding
- Wavelet transform
- Data masking

Audio Steganography

This method hides data inside sound files. In this method, audio file formats such as WAV, AU and MP3 are used as cover data. Audio steganography has different methods (Rakhi and Gawande, 2013). These methods include;

- Least Significant Bit (LSB)
- Parity coding
- Phase coding
- Spread spectrum
- Echo hiding

Video Steganography

It is the technique of hiding any kind of file or data inside a digital video format file. Video steganography generally uses H.264, Mp4, MPEG and AVI video formats as cover data. A video file is a simultaneous combination of audio and video. So almost all of the steganography techniques that can be applied on image and audio files can be applied on video files. Video steganography provides less perceptibility because video is the fast flow of images and sounds (Kamble et al., 2013). Due to the large size of video files, payload capacities of video steganography is quite large (Doshi et al., 2012).

Network or Protocol Steganography

It aims to hide confidental data inside a cover object which is aprotocol such as TCP, UDP, ICM and IP.There are hidden channels in the OSI layer networking model, where steganography can be used.

Steganography Techniques

Least Significant Bit (LSB)

It is the most commonly used steganographic method. It makes little change in the cover data that can not be perceived by human senses (Kour and Verma, 2014). The secret message is converted into a bit sequence. The cover data is divided into bit strings according to the data type as it is seen in figure 2 as an example. The last bit of each bit string is replaced by the next bit of the secret message. It is a very common method on picture and sound files. Theoretically, in an average LSB method, only 50% of the LSB's are changed (Kumar et al., 2017).

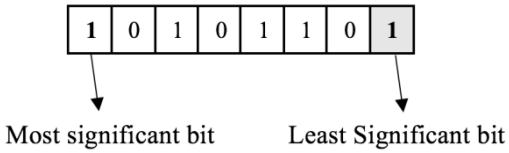

Figure 2. Least Significant Bit Of A 8 Bit Binary Array

In a 24bit image file; 8 bits of data representing colors; red, green and blue are kept for each pixel. Data can be hidden in the image or audio fileby replacing the last bit of each 8 bit data with the confidental data bit. This change will be so small that people can not be perceived by human senses. The process of embedding a 6-bit 110101 data in two pixels is shown in figure 3.

If it is considered as enlarged two pixels, the ones on the left side of the figure are the cover data. 6 bits of data are embedded in the RGB data of two pixels and the stego-data conversion of the cover data is shown in the right side. As itis clearly seen in figure 3, there is no visible change in the cover data.

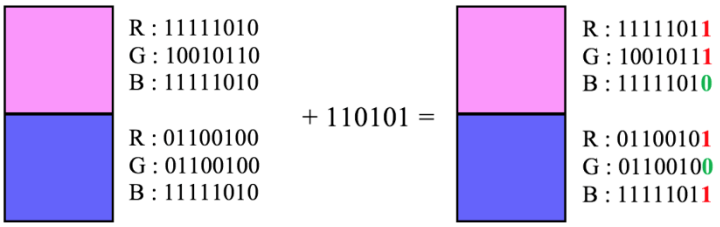

Figure 3. Embedding Data To An Image With Two Pixels

For LSB coding for audio steganography, the ideal rate is 1kbps for 1kHz (Adhiya and Patil, 2014). The cover audio data is sampled first and digital quantization is performed as shown in the figure 4 to find the digital value of each sample.

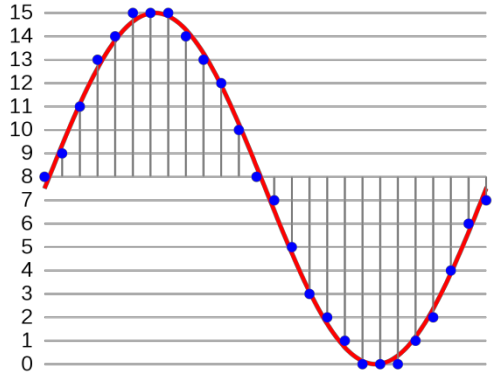

Figure 4. Sampling And Quantization Of A Sine Wave

A data can be embedded in the last bit of each of the obtained data arrays after quantization. When the acquired sequence is converted back to the analog signal, very small changes ocur in the amplitude values of the stego-sound data andthat can not be detected by the human ear.

Spread Spectrum

Spread spectrum concept is used in this technique. In this method, confidential data is spread over a wide frequency bandwidth. The ratio of signal to noise in each frequency band should be so small that it is difficult to determine the presence of the data. Even if the data fragments are removed from several frequency bands, there will still be enough hidden data in the other groups to recover. For this reason, it is difficult to completely remove the data without completely removing the cover. This is a very robust technique used mostly in military communications (Kour and Verma, 2014). There are different techniques used for the spread spectrum; Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS) and Time Hopping Spread Spectrum (THSS).

Statistical Technique

Technically, confidental data is embedded by changing various features of the cover. It involves dividing the cover into blocks and then placing a data bit on each block. The cover block is changed only when the value of nexthidden databit is '1', otherwise modification is not required.

Transform Domain Technique

The hidden message is embedded in the transform or frequency domain of the cover. This is a more complex way of concealing the transmission in the image. Different algorithms and transformations are used to hide the message in the cover. Conversion domain techniques consist of the following;

- Discrete Fourier Transformation (DFT)
- Discrete Cosine Transformation (DCT)
- Discrete Wavelet Transformation (DWT)
- Lossless or reversible method (DCT)
- Embedding in coefficient bits

Parity Coding

Parity is a bit-based method. Parity bit is a bit added behind a bit sequence depending on whether the sum of sequence is 0 or 1. For example; a 8-bit data sequence is obtained by addinga parity bit behind a 7-bit binary sequence. After the recipientside receives the data sequence, itsums the first 7 bits and compares it with the parity bit. If the result is incorrect, the message is corrupted on transmission and is requested again. In steganography parity coding, it divides a signal into sample regions instead of dividing into separate samples and codes each bit from the confidental message within the parity bit of each region as it is shown in figure 5. Thus, the sender has more options in embedding and the cover data can be changed in an imperceptible way.

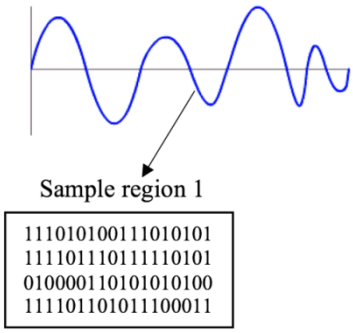

Figure 5. A Sample Region In Parity Coding

Phase Encoding

This method works on audio signals. The Human Auditory System (HAS) can not easily recognize the phase change and noise in an audio signal. This technique codes confidental signal bits as phase shifts in the phase spectrum of a digital signal and performs an unrecognized change in signal-to-noise ratio. In brief, this method divides the original audio stream or cover file into blocks and embeds the confidental message data sequence in the phase spectrum of the first block. Because the confidential data is only embedded in the first block, the load capacity is very low. However, since the confidential data does not spread to the cover file, it is resistant to attacks such as cutting and trimming. Working algorithm;

1. The header section of the cover data is removed.
2. The remaining data is divided into equal segments, which will be the same size as the confidental data.
3. Discrete Fourier Transform (DFT) is applied to each segment to form the matrix of the phases.
4. Confidential data is added to the phase vector of the first segment;

$$New\ phase = \begin{cases} Old\ phase + (\frac{\pi}{2}), & hidden\ message\ bit = 0 \\ Old\ phase - (\frac{\pi}{2}), & hidden\ message\ bit = 1 \end{cases}$$

5. A new phase matrix is created with the new phase value and the original phase matrix of the first segment.
6. The heading segment is added to the generated phase matrix.
7. By applying the inverse DFT, the audio signal is reconstructed (Kumar et al., 2012).

Echo Hiding

In echo hiding, confidental data is embedded in an audio file by adding an echo to the separate signal. It is done by adding delayed versions of the signal to cover signal (Tekeli ve Asliyan, 2017). Like the common spectrum method, it provides advantages because it allows a high data transmission rate and provides superior robustness. If only one echo is generated from the original signal, only one bit of information can be encoded. For this reason, the original signal is split into blocks before the encoding process starts as it is seen in figure 6 and 7. When the encoding is complete, the blocks are recombined to form the final signal.

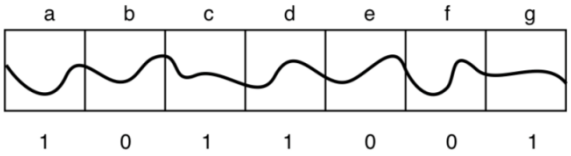

Figure 6. The Original Audio Signal Splitted Into Blocks Before Hiding The Echo

The number of blocks is equal to number of bits in the confidential message andeach block is equal in length.

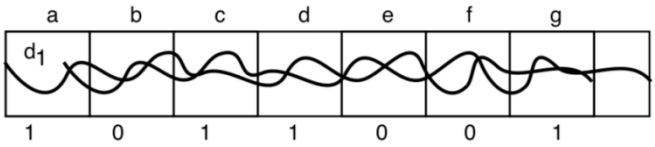

Figure 7. The Audio Signal In The Echo HiPing Process And The Bit Sequence Hidden In The Blocks

Cepstrum analysis method is used to extract a hidden data embedded with echo hiding method (Tekeli and Asliyan, 2017).

Masking and Filtering

This technique only uses grayscale images as cover data. Hidden data is stored in more important areas instead of being stored at the noise level. Since confidential data is more integrated into the image, detection and destruction is rather difficult (Kaur and Rani, 2016).

CONCLUSION

Steganography is the art and method of hiding data into another data. This study describes different steganography methods according to the cover data type they are working on. Table 1shows the advantages and disadvantages of the methods that are described.

Table 1. Comparison Of Steganography Methods According To Some Criteria

Technique	Robustness	Imperceptibility	Payload capacity	Complexity
LSB	LOW	HIGH	HIGH	LOW
Spread Spectrum	MEDIUM	LOW	LOW	MEDIUM
Statistical Technique	MEDIUM	HIGH	LOW	MEDIUM
Transform domain	HIGH	HIGH	MEDIUM	HIGH
Parity coding	HIGH	HIGH	LOW	MEDIUM
Phase coding	HIGH	MEDIUM	LOW	MEDIUM
Echo hiding	HIGH	MEDIUM	MEDIUM	MEDIUM
Masking and filtering	LOW	MEDIUM	LOW	MEDIUM

Steganography is becoming increasingly common and secure with the methods currently being developed. The most appropriate steganography method can be selected by considering several variables such as the size of the data to be embedded, the security requirements, the environment which the data is goint to be sent. For higher security requirements, steganography and cryptography can be used together.

REFERENCES

Abboud, G., Marean, J., Yampolskiy, R.V. (2010). Steganography and Visual Cryptography in Computer Forensics, Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering, 25-32, DOI 10.1109/SADFE.2010.14

Adhiya, K.P., Patil, S.A. (2012).Hiding Text in Audio Using LSB Based Steganography, Information and Knowledge Management,(2)3, 8-15, ISSN 2224-5758.

Amin, M.M., Salleh, M., Ibrahim, S., Katmin, M.R., Shamsuddin, M.Z.I. (2003). Information Hiding using Steganography, 4th National ConferenceonTelecommunication Technology Proceedings, 21-25, Shah Alam, Malaysia.

Amirtharajan, R., Rayappan, J.B.B. (2013). Steganography - Time to Time A Review, Research Journal of Information Technology, (5)2, 53-66, ISSN:1815-7432, DOI:10.3923/rjit.2013.53.66

Doshi, R., Jain, P., Gupta, L. (2012). Steganography and Its Applications in Security, International Journal of Modern Engineering Research (IJMER), (2)6, 4634-4638, ISSN: 2249-6645

Fridrich, J. (2010). Stegaongraphy in Digital Media: Principles, Algorithms and Applications, Cambridge University Press, ISBN: 9780521190190, U.K.

Jayaram, P., Ranganatha, H.R., Anupama, H.S. (2011). Information Hiding Using Audio Steganography - A Survey, The International Journal of Multimedia & Its Applications (IJMA), (3)3, 86-96, DOI : 10.5121/ijma.2011.3308

Kamble, P.R., Waghamode, P.S., Gaikwad, V.S., Hogade, G.B. (2013). Steganography Techniques: A Review, International Journal of Engineering Research & Technology (IJERT), 2(10), 3784-3793, ISSN: 2278-0181

Kaur, H., Rani, J. (2016). A Survey on Different Techniques of Steganography, MATEC Web of Conferences 57, 1-6, DOI: 10.1051/matecconf/20165702003

Kour J., Verma, D. (2014). Steganography Techniques – A Review Paper, International Journal of Emerging Research in Management &Technology, 3(5), 132-135, ISSN: 2278-9359, India

Kumar, P.P., Bhagat, R., Suvarna, S. (2017). Steganography Using Visual Cryptography, Independently published, ISBN-10: 1520478364, ISBN-13: 978-1520478364, 20-76.

Kumar S., Bandyopadhyay, B., Banik, G. (2012). LSB Modification and Phase Encoding Technique of Audio Steganography Revisited, International Journal of Advanced Research in Computer and Communication Engineering, (1)4, 1-4, ISSN : 2278 – 1021.

Rabah, K. (2004). Steganography – The Art of Hiding Data, Information Technology Journal, 3(3), 245-269, ISSN:1682-6027.

Rakhi, P.G., Gawande, S. (2013). A Review on Steganography Methods, International Journal of Advanced Research in Electrical Electronics and Instrumentation Engineering, (2)10, 4635-4638, ISSN: 2320 – 3765.

Tekeli, K., Asliyan, R. (2017). A Comparison of Echo Hiding Methods, The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), (1), 397-403, ISSN: 2602-3199

Tunçer, S., Karakuzu, C. (2016). Veri Güvenliğini Artırmak Amacıyla Bilgiyi Şifreleme ve Steganografik Yöntemlerle Görüntüye Gizleme, EEB 2016 Elektrik-Elektronik ve Bilgisayar Sempozyumu ,183-187, Tokat, Turkey