Volume 6, Issue 2, February 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Steganography Techniques - Data Security Using Audio and Video

Hilal Almara'beh
King Saud Bin Abdul-Aziz University for Health Sciences, College of Sciences and Health Profession
Riyadh, Kingdom of Saudi Arabia

Abstract: ***Due to the evolution of computer technologies and the internet, the security of information considers as the most challenges in communication to protect information. A large variety of stenographic techniques exists for hiding information in an appropriate carrier such as text, image, audio, video, and protocol, and can be sent to a receiver secretly. The techniques of audio and video steganography can be used to hide secret information by using another mechanismsuch as audio and video files. This paper presents a general review of steganography and a critical study of research papers in various techniques used in audio and video steganography.***

Keywords: ***Steganography, Digital Carrier, Audio-Steganography, Video-Steganography, Cryptography, Digital Watermarking***

I. INTRODUCTION

The term steganography is defined as a process of writing hidden messagesby using some techniques that no one else knows the existence of the message. Computer-based steganography allows changes to be made to what are known as digital carriers such as text, images, audio, video, or protocol, the changes represent the hidden message, but result if successful in no discernible change to the carrier. In steganography, before the hiding process, the sender must select an appropriate message carrier, the hidden message, and the secret key also; the sender could send the hidden message to the receiver by using any of the computerized communication techniques and steganography algorithms that must be able to encrypt the message more effectively. In the other side, after receiving the message the receiver decrypts the hidden message using the extraction algorithm and a secret key [1]. Figure.1 below shows a general steganography framework.

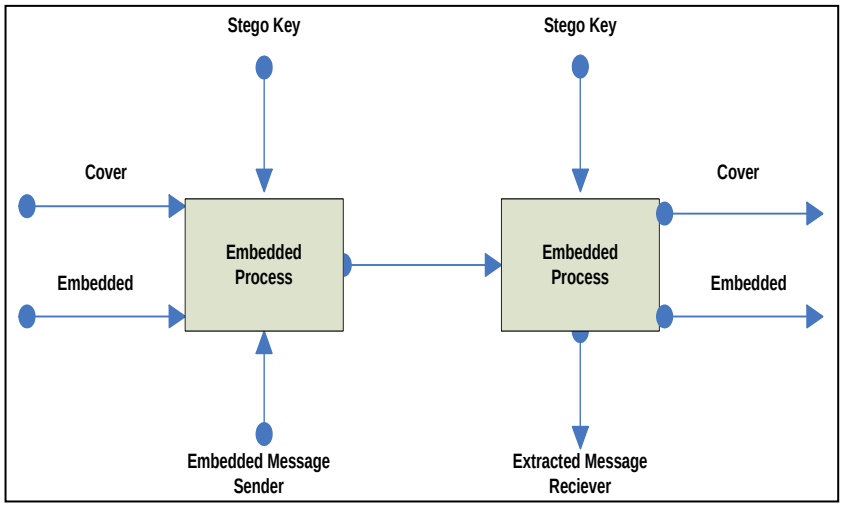

Fig.1 General Steganography Framework

The main objective of steganography is to avoid drawing attention to the transmission of hidden information to achieve the security of the secret message, meanwhile, if the hackers noticed any change in the sent message then this observer will try to know the hidden information inside the message [2],[3].This paper presents a study of steganography in (section1). Describes various techniques inaudio steganography and comprehensive review papers (section 2), also explains a various techniques inaudio steganography and comprehensive review papers in (section 3), and finally the conclusion in (section 4).

II. STEGANOGRAPHY

2.1 Difference between Steganography and Cryptography

Users on the internet have to send, share or receiveconfidential data most of the time [4]. Cryptography renders message unintelligible whichfocuses on message encryption but it is easy to find encrypted message through communication. In order to overcome the shortcomings of cryptographic techniques, steganography considers as

important techniques of hiding information but the communication is invisible from intruders.Both steganographic and cryptographic systems provide secret communications but different in terms of system breaking, if the intruder can read the message in cryptographic then it is broken but steganographic is considered broken once the intruders detect the existence of the secret message [5]. Steganography system is more fragile than cryptography systems in terms of system failure and this is because if the communication is detected even without decoding the message, a steganography system is considered a failure [6].

2.2 Types of Digital Carriers

There exist two types of materials in steganography: message and carrier. The message is the secret data that should be hidden and the carrier is the material that takes the message in its [7].Steganography hides the secret data in another file in such a way that only the recipient knows the existence of the message. In the old time, the data was protected by hiding it on the back of wax, or on the scalp of the slaves. But today's data is transmitted in the form of text, images, video, protocol, and audio over the medium, and in order to have a safe transmission of confidential data, the multimedia object such as text, image, audio, video, network protocol are used as a cover sources to hide the data, Figure.2 below shows the different multimedia objects that can be used for steganography techniques.

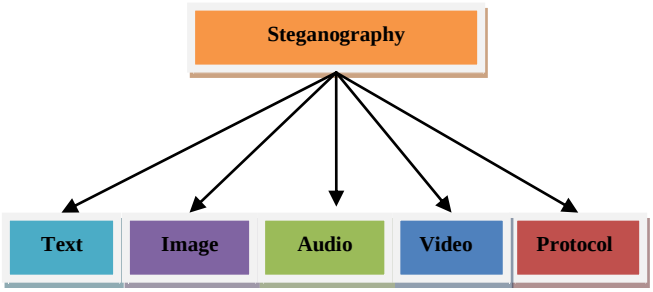

Fig. 2 Steganography Multimedia Objects

The different multimedia objects that used for hiding data in steganography techniques depend on its method. Text steganography is the first computerized method used to hide information inside the text files, and this method relies on to hide the secret data behind every nth letter of every word of the text message. There are a lot of methods for hiding data in the text file such as format based method, random method, statistical method, and linguistics method.

Imagesteganographyis widely used as a cover source because there are a number of bits presents in a digital representation of an image. It hiding the data by taking the cover object as an image, and it relies on pixel intensities to hide the data. Many methods available for hiding data in the image such as a spatial domain method, transform domain method, and masking and filtering method.

Audio steganography depends on hiding data in audio files by using WAV, AU, and MP3 sound files, and different methods are available of audio steganography such as low-bit coding method, phase coding method, spread spectrum method, and echo hiding method.

Video steganography used to hide any kind of files or data by using Mp4, MPEG, and AVIdigital video formats and different methods are available such as discrete cosine transform method, least significant bit method, and spread spectrum method. Finally, network or protocol steganography it is the latest technique for hiding the information, and it relies on network protocol such as TCP, UDP, ICMP, IP etc., as cover.

2.3 The Applications of Steganography

The main object of steganography is hiding data, and there are a lot of applications that use this technique for hiding data such as digital watermarking, secret communication, terrorists, copyright protection, and feature tagging, this sub-section introduces a brief description of each mentioned application.

Digital watermarking considers as one of the most important applications of steganographyand may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It basically embeds a digital watermark into an image.In secret communication application, there are two parties can communicate secretly without anyone knowing about the communication. The application depends only on an encoding the message and on the other side hides the existence of the message in some cover media. The terroriststeganography application can be used in large scale, they hide their secret messages in innocent or needing for donating and they cover the main targets to spread terrorism across the region or a part of the world. The copyright protection application related to watermarking, for example,a secret message is embedded in the images which serve as the watermark and thus identify it as an intellectual property which belongs to a particular owner. Feature tagging application such as captions, annotations, and thename of the individuals in a photo or location in a map can be embedded in an image. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features [8].

2.4 The Effectiveness of Steganography Methods

Many factors are using to determine the effectiveness of any steganography method when creating a digital data hiding system, and these factors determine the robust, secure, embedding capacity, noise, quality, and efficient of the

used technique. The first factor is imperceptibility which provides invisibility in which a person should be unable to distinguish the original and the secret image. The second is robustness which refers to the degree of difficulty required to destroy secret data without destroying the cover image. The third is payload capacity which uses two parties to have secret communication, one needs to embed only a small amount of copyright information, whereas the other side needs only to hide the communication and, therefore, have sufficient embedding capacity. The fourth factor is the peak signal to noise ratio (PSNR) which means the expression of the ratio between the maximum possible power of the signal andthe power of distorting noise that affects the quality of its presentation. The higher value of PSNR represents the better quality of the compressed image. The fifth factor is the mean square error (MSE) which means the average squared difference between a reference image and a distorted image. The smallest value of the MSErepresents the efficiency of the image. The last factor is a signal to noise ratio (SNR) which means the expression of the ratio between the signal power and the noise power. It compares the level of the desired signal to the level of background noise.

III. AUDIO STEGANOGRAPHY

In this technique, the secret message is embedded into a digitized audio signal which resultsin the slight altering of the binary sequence of the corresponding audio file. This section describesdifferent methods of audio steganography and a review of research papers concentrate on audio steganography.

3.1 Audio steganography Techniques

Different audio steganography techniques are used for hiding data, and the factors that affect these techniques are data hiding techniques, strength, and weakness of the method.Table.1 below summarizes the methods using in audio steganography.

A. *Low-bit encoding* it is a simple technique which converts an analog audio signal to digital binary sequence, but this method cannot protect the hidden message from small modifications that can arise as a result of format conversion or lossy compression. In this technique, LSB of the binary sequence of each sample of a digitized audio file is replaced with the binary equivalent of secret message.

B. *Phase coding* 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.

C. *Spread spectrum*coding has two approaches, the direct sequence spread spectrum (DSSS) which is a modulation technique used in telecommunication and frequency hopping spread spectrum (FHSS). 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, and this noise signal is a pseudorandom sequence of (1 and −1) values, at a frequency much higher than the original signal, that way spreading the energy of the original signal into a much wider band.

D. *Echo hiding*method is embedded the secret message into the cover audio signal as an echo. Three parameters of the echo of the cover signal exist,capacity, decay rate, and offset from the original signal that is varied to represent encoded the secret binary message.

Table1. Summary of Audio Steganography Methods

Methods	Data hiding techniques	Strength	Weakness
LSB	Each sample in the audio is substituted by one-bit of hidden data	Simple and easy	Easy to extract
Phase Coding	Modulate the phase of the cover signal	Robust against signal processing operation	Low capacity
Spread Spectrum	Spread the information overall signal frequencies	Provides better robustness and increase transparency	Vulnerable to time scale modification and occupies more bandwidth
Echo Hiding	Hides the information by introducing echo in the cover signal	Avoid problem with the adaptive noise	Low data security and low capacity

3.2 Comparison of Various Techniques Used in Audio Steganography

Various steganography techniques have been presented in audio to improve the robust, quality, and more secure of hiding data. Table.2 presents a critical study of research papers in various techniques used in audio.

Table2. Audio Steganography Research Papers

Title	Keywords	Year	Method	Factor
An efficient method to audio steganography based on modification of least significant bit techniques using random keys.[9]	Steganography, Cryptography, Audio Steganography, and Lifting Wavelet Transform	2015	Lifting wavelet transform (LWT), and modification of LSB with three random keys	AVG PSNR =105.4161, and AVG SNR = 85.78115 with 38632 embedded bytes
Genetic algorithm in audio	HAS, SecretData, Genetic	2015	Genetic algorithm	Decrease the

steganography[10]	Algorithm, Mutation, Chromosome			difference between sample bits and adjusting bits
A Novel Spread Spectrum Digital Audio Watermarking Technique[11]	Audio signals, spread-spectrum, audio watermarking, blind extraction.	2003	spread spectrum watermarking	SNR = 65.46 dB Sharing = 0.9917 LPF = 0.7642
Information Hiding Using Audio Steganography with Encrypted Data[12]	Audio Steganography, Cryptography, Embedding, Encryption, Information Hiding	2014	Symmetric-key algorithm for embedding message and the modified LSB for extracting	Frequency analysis
Security Enhancement in Audio Steganography by RSA Algorithm[13]	Steganography, LSB, Cover Data, Stego File, Text Embedding on Audio, RSA	2015	Novel approach RSA	5 audio files AVG 5.946 MB, AVG 10L SNR 80.69, 5L 61.178, 100 L 36.61
Sound watermarking utilizing spread spectrum[14]	Digital Signal Processing, Watermarking Process, Audio Watermark	2015	Proposed audio spread spectrum watermarking	Mp3 files are used Sound square8820 bits. WM-peak=2 compare to 5 Hz and can be modified for another frequencies
Robust Audio Steganography Technique using AES algorithm and MD5 hash[15]	Advanced encryption system, steganography, modulation, Human Auditory System	2014	LSB for embedding, AES for encrypting the message, and MD5 used to cover audio.	WAV format are used, PSNR for M-size (40 KB) =56.44 dB, and M-size (200 KB) = 49.39 db.

IV. VIDEO STEGANOGRAPHY

The separation of video into audio and images or frames results in the efficient method for data hiding. The use of video files as a carrier medium for steganography is more eligible as compared to other techniques. This section describesdifferent methods of video steganography and a review of research papers concentrate on video steganography.

4.1 Video steganography Techniques

Different video steganography techniques are used for hiding data, and there are some factors that affect these techniques such as secret message, imperceptible, robust, and capacity.

A. *Least Significant Bit method* (LBS) it's the first and simple method that can hide large data into least significant bits of the host video, but it might be lost the hiding data after transmission.
B. *Spread Spectrum*method satisfies the robustness criterion and the amount of hidden data lost after applying some geometric transformations is very little, also, the amount of hidden lost is little even though the file is compressed with low bit-rate.
C. *The discrete cosine Transform* (DCT) method is based on multi-dimensional lattice structure that enables a high rate of data embedding and robust to motion compensated coding or enable the high quantity of hidden data and high quantity of host data by varying the number of quantization levels for data embedding.

Many algorithms are used such as secured data transmission (SDT), hashed based LSB (HLSB), multiple LSB (MLSB), LSB polynomial equation algorithm (LSBPOLY), hybrid encryption and steganography (HES), LSB matching revised algorithm (LSBMR), and novel video steganography (NVS). Table3. Below shows steganography analysis features in different algorithms and all of them have imperceptibility.

Table3. Summary of Video Steganography Analysis Features

Algorithm / Factor	Robust	Capacity	Secure	Cover image	Secret image
Secured data transmission (SDT)	Robust	Better	Less secure	AVI	Image
Hybrid Encryption and Steganography (HES)	Robust	High	Secure	AVI	Text
LSB Polynomial Equation Algorithm (LSBPOLY)	Less robust	.Low	Less secure	AVI	Text
Hashed-based LSB (HLSB	Robust	Good	Less secure	AVI	Text

Multiple LSB (MLSB)	Robust	Good	Less secure	AVI	Text
LSB Matching Revised Algorithm (LSBMR)	Robust	High	Secure	AVI	Text
Novel Video Steganography (NVS)	Robust	High	High secure	AVI, MPEG, MOV, FLV	Text, image, audio, and video

4.2 Comparison of Various Techniques Used in Video Steganography

Various steganography techniques have been presented in the video to improve the robust, quality, and more secure of hiding data. Table.4 presents a critical study of research papers in various techniques used in the video.

Table4. Video Steganography Research Papers

Title	Keywords	Year	Method	Factor
Video Steganography by LSB Substitution Using Different Polynomial Equations [16]	least significant bit, steganography	2012	LSB Polynomial Equation Algorithm	180,000 bytes of embedded data, and AVI format for covering
Hashed-based least significant bit techniques for video steganography (HLSB) [17]	Steganography, video steganography, cover video, cover frame, secret message, LSB	2012	Hashed-based LSB (HLSB	AVG PNSR= 44.223, AVG MSE = 0.34, IF = 0.276, AVG Poly-load = 2.66
Improved protection in video steganography used compressed video bit streams [18]	Video steganography, real-time steganography, information hiding, compressed bit streams	2010	A new compressed video secure steganography(CVSS) algorithm, and DCT	MPEG-2 formats were used, and 42 m2v format compressed video streams were used.Correlation between 0.2 and 1.0
Enhancing data security using video steganography [19]	Steganography, cryptography, digital watermarking, LSB, encryption, AES.	2013	AES for encryption and SHA-1 for generating secret key	Varies block size 128, 192, and 256 bits, 10 rounds for 128 bit key,12 for 192 bit key and 14 for 256 bit key
Secure data hiding technique using video steganography and watermarking [20]	Steganography, digital watermarking, Least Significant Bit, Discrete Wavelet Transform, Discrete Cosine Transform	2014	LSB, inverse DWT, and inverse DCT	42 frames were used. PSNR <=52.71 and MSE<=0.353 of input frames
Video steganography through LSB based hybrid approach [21]	AES, LSB, Cryptography	2014	LSB, Hybrid Encryption and Steganography (HES), and AES	50 frames.PSNR for 1 bit LSB & AES <=50.PSNR for 2 bit LSB &AES <=43,PSNR for 3 bit LSB & AES<=30
Hybridization of motion detection technique in video steganography [22]	decryption, encryption, LSB, motion vector, Steganography	2015	hybrid motion detection and LSB	10 MPG cover video and 10 AVI Steg-video. AVG PSNR = 58.419.
Secure videosteganography based on discrete wavelet transform and Arnoldtransforms [23]	Alpha Blending, Arnold Transform DWT, PSNR, Video Steganography	2015	DWT, IDWT	5 cover videos, and 5 secret images 256*256. AVG PSNR = 98.516, MSE = 0.0, AVG NAE = 0.0075, AVG MD = 0.0086, and SC = 1.00335

V. CONCLUSION

This paper provides a literate review of audio and video steganography. As steganography becomes widely used in computing there aresome issues that need to be resolved in terms of hiding information to achieve better security. There are different factors that effective steganography methods such as PNSR, MSE, SNR, MD, and SC, also a wide variety of different techniques used with audio and video steganography such as LSB, DCT, DWT, phase coding, and echo hiding which helps to improve in security.

REFERENCES

[1] W, Peter. "*Disappearing Cryptography: Information Hiding: Steganography & Watermarking*", (second edition). San Francisco: Morgan Kaufmann. pp.192-213, march 1992.

[2] Fabien A. P.Petitcolas, Ross J Anderson, Markus G. Kuhn,"*Attacks on Copyright*", University of Cambridge, April 1998.

[3] H. Wu, H. Wang, C. Tsai and C. Wang, "*Reversible image steganography scheme via predictive coding*". June (2010), ISSN: 01419382, pp. 35-43.

[4] Arvind Kumar and Km. Pooja,"*Steganography- A Data Hiding Technique*", International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.

[5] GunjanChugh, "*Image Steganography Techniques: A Review Article*", Bulletin of Engineering, Faculty of Engineering, Hunedoara, Romania, July-September 2013.

[6] Adel Almohammad, "*Steganography-Based Secret and Reliable Communications: Improving Steganographic Capacity and Imperceptibility*", A thesis submitted for the degree of Doctor of Philosophy, Department of Information Systems and Computing, Brunel University, August 2010.

[7] Christian Cachin, "*Digital Steganography*", Encyclopedia of Cryptography and Security, 2005.

[8] Rajkumar Yadav, "*Study of Information Hiding Techniques and their Counterattacks: A Review Article*", International Journal of Computer Science & Communication Networks, Vol 1(2), 142-164, Oct-Nov 2011

[9] Ali M. Meligy," *An Efficient Method to Audio Steganography based on Modification of Least Significant Bit Technique using Random Keys*", I. J. Computer Network and Information Security, pp. 24-29, June 2015.

[10] Manisha Rana andRohitTanwar, "*Genetic Algorithm in Audio Steganography*", International Journal of Engineering Trends and Technology (IJETT) – Volume 13 Number 1 – Jul 2014.

[11] Yekta Said Can, FatihAlagoz, and MelihEvrenBurus, "*A Novel Spread Spectrum Digital Audio Watermarking Technique*", Journal of Advances in Computer Networks, Vol. 2, No. 1, March 2014.

[12] R.Valarmathi, G.M.Kadhar, and Nawaz M.C.A,"*Information Hiding Using Audio Steganography with Encrypted Data*", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2014.

[13] Adeel Jawed andAtanuDas."*Security Enhancement in Audio Steganography by RSA Algorithm*", International Journal of Electronics & Communication Technology (IJECT) Vol. 6, Issue 1, Spl-1 Jan - March 2015.

[14] KomalGoswami andNitika Sharma, "*Sound Watermarking Utilizing Spread Spectrum*", International Journal of Computer Algorithm", pp.0975-8887, Vol.129, No.7, Nov 2015.

[15] Kamal Pradhan and ChinmayaBhoi," *Robust Audio Steganography Technique using AES algorithm and MD5 hash*", International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Vol.1 Issue 10 (November 2014).

[16] A. Swathi and S.A.K Jilani, "*Video Steganography by LSB Substitution Using Different Polynomial Equations*", International Journal of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5.

[17] KousikDasgupta, J.K. Mandal, and Paramartha Dutta, "*HASH BASED LEAST SIGNIFICANT BIT TECHNIQUE FOR VIDEO STEGANOGRAPHY(HLSB)*", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012.

[18] S. Suma Christal Mary M.E (Ph.D)," *IMPROVED PROTECTION IN VIDEO STEGANOGRAPHY USED COMPRESSED VIDEO BITSTREAMS*", (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, pp.764-766.

[19] VipulaMadhukarWajgad and Dr. Suresh Kumar," *Enhancing Data Security Using Video Steganography*", International Journal of Emerging Technology and Advanced Engineering, Vol.3, Issue 4, April 2013.

[20] Shivani Khosla and Paramjeet Kaur," *Secure Data Hiding Technique Using Video Steganography and Watermarking*", International Journal of Computer Applications (pp.0975 – 8887) Vol.95– No.20, June 2014.

[21] Hemant Gupta andSetuChaturvedi," *Video Steganography through LSB Based Hybrid Approach*", IJCSNS International Journal of Computer Science and Network Security, pp. 99-100, Vol.14, No.3, March 2014.

[22] Parwinder Singh and Navpreet Kaur, "*Hybridization of Motion Detection Technique in Video Steganography*", International Journal of Advanced Research in Computer Science and Software Engineering, pp.692-695, Vol.5, Issue 7, July 2015.

[23] Abhinav Thakur, Harbinder Singh, andShikha Sharda," *Secure Video Steganography based on Discrete Wavelet Transform and Arnold Transform*", International Journal of Computer Applications pp.0975 – 8887, Vol.123, No.11, August 2015.

