International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 6 | ISSN : 2456-3307

Audio Steganography

Sanju[1], Mamta Yadav[2]
[1]M.Tech Scholar CSE, M.D.U Rohtak,YCET Narnaul, Mahendergarh, Haryana, India
[2]Assistant Professor, CSE, M.D.U Rohtak,YCET Narnaul, Mahendergarh, Haryana, India

ABSTRACT

Audio steganography is the scheme of hiding the existence of secret information by concealing it into another medium such as audio file. In this paper we mainly discuss different types of audio steganographic methods, advantages and disadvantages. The rapid spread in digital data usage in many real life applications have urged new and effective ways to ensure their security. Efficient secrecy can be achieved, at least in part, by implementing steganograhy techniques. Novel and versatile audio steganographic methods have been proposed. The goal of steganographic systems is to obtain secure and robust way to conceal high rate of secret data. We focus in this paper on digital audio steganography, which has emerged as a prominent source of data hiding across novel telecommunication technologies such as covered voice-over-IP, audio conferencing, etc. The multitude of steganographic criteria has led to a great diversity in these system design techniques. In this paper, we review current digital audio steganographic techniques and we evaluate their performance based on robustness, security and hiding capacity indicators. Another contribution of this paper is the provision of a robustness-based classification of steganographic models depending on their occurrence in the embedding process.

I. INTRODUCTION

The word steganography comes from the Greek Steganos, which means covered or secret and graphy means writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding secret information in a cover file such that only sender and receiver can detect the existence of the secret information. A secret information is encoded in a manner such that the very existence of the information is concealed. The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data It is not only prevents others from knowing the hidden information, but it also prevents others from thinking that the information even exists. If a steganography method causes someone to suspect there is a secret information in a carrier medium, then the method has failed .The basic model of Audio steganography consists of Carrier Audio file Message and Password. Carrier is also known as a cover-file, which conceals the secret information. Basically, the model for steganography is shown in Fig 3. Message is the data that the sender wishes to remain it confidential. Message can be plain text, image, audio or any type of file. Password is known as a stego-key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file. The cover-file with the secret information is known as a stego-file. public key that corresponds to the private key that was used during the signing of the message. As a result, we obtain the original hash-value (the original message digests).

CSEIT18363 | Received : 01 July 2018 | Accepted : 08 July 2018 | July-August-2018 [3 (6) : 66-70]

In audio steganography, the basic spread spectrum (SS) method attempts to spread secret information across the frequency spectrum of the audio signal. This is similar to a system which uses an implementation of the LSB that spreads the message bits randomly over the entire sound file. However, unlike LSB coding, the Spread Spectrum method spreads the secret information over the frequency spectrum of the sound file using a code which is independent of the actual signal . As a result, the final signal occupies a bandwidth which is more than what is actually required for transmission.The Spread Spectrum method is capable of contributing a better performance in some areas compared to LSB coding, phase coding, and parity coding techniques in that it offers a moderate data transmission rate and high level of robustness against removal techniques.

The issue with changing the red qualities in our encode/translate steps, is that these regularly cause very obvious changes in the subsequent picture. This is particularly valid if the pixels that are being changed are a piece of a huge area of consistently hued pixels – the "spots" emerge and are recognizable. As an alternative, client can change just the lower request bits of every pixel shading (red, blue, and green). This will roll out inconspicuous improvements to every pixel's shading and won't be as clear. Keep in mind that every pixel has three bytes: one byte for red, blue and green hues. Every byte has 8 bits to encode a number somewhere around 0 and 255. When he swap out the red shading byte for a character, it is conceivable that he is changing the redness of that pixel by a considerable amount. For instance, he may have had a pixel with estimations of (225, 100, 100) which has loads of red, some green and some blue – this is fundamentally a ruddy pixel with a slight piece of pink shading to decimal number 97 so our new pixel gets to be (97, 100, 100). Presently he has equivalent amounts of each of the three hues to create a dim dark pixel. This dim is detectably not quite the same as the dull pink he had before; it will emerge in the picture particularly if the other close-by pixels are all dim pink.He needs an approach to encode our message without rolling out such uncommon improvements to the hues in the first picture. On the off chance that we just change the most minimal bits of every pixel, then the numeric qualities can just change by a little rate. For instance, assume he just change the last three bits (most minimal three bits) – these are the bits that decide the "ones place", the "twos spot" and the "fours spot". From the above proposed algorithm Data Integrity is upgraded utilizing a Digital Watermarking and Digital Signature. In this information is inserted with the picture and sent over the system where its respectability is checked by the examination of hash estimation of the first information or picture. The proposed work gives secure mystery correspondence among sender and collector, it guarantees that inserted information stays untouched and recoverable, watermarks the picture with fantastic visual quality without bringing on a discernible loss of value. It is valuable for copyright possession declaration purposes. The information which is covered up can't be effectively evacuated and oppose normal picture control strategies.

II. IMPLEMENTATION

There have been many techniques for hiding information or messages in audio in such a manner that the alterations made to the audio file are perceptually indiscemible. Common approaches include:-

2.1 LSB CODING:-

A very popular methodology is the LSB (Least Significant Bit) algorithm, which replaces theleast significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data. That's usually an effective technique in cases where the LSB substitution doesn't cause significant quality degradation, such as in 24-bit bitmaps. In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position.

of signer is denied. Procedure of verification must certify signer's identity. In some cases, May a valid signature is recognized as invalid and an invalid signature is recognized as valid. This is a bad feature for verification that its result always is not true.

Efficiency parameter defines which scheme is more effective and optimal for its applications. This is an approximation parameter that based on several conditions such as programmer's skill to implement mentioned algorithms, security of network and system designs, percentages of verification signatures, relations between choosing appropriate scheme and its applications and so on. As referred above, efficiency is calculated approximately and it's not enough for judgement among these schemes. This only provides an overview to select appropriate schemes according to our applications

The binary representation of decimal 149, with the LSB highlighted. The MSB in an 8-bit binary number represents a value of 128 decimal. The LSB represents a value of 1. For example, to hide the letter "a" (ASCII code 97, which

HASE CODING:-

The phase coding technique works by replacing the phase of an initial audio segment with a reference phase that represents the secret information. The remaining segments phase is adjusted in order to preserve the relative phase between segments. In terms of signal to noise ratio, Phase coding is one of the most effective coding methods. When there is a drastic change in the phase relation between each frequency component, noticeable phase dispersion will occur. However, as long as the modification of the phase is sufficiently small, an inaudible coding can be achieved

This method relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is.

Phase coding is explained in the following procedure:

a. Divide an original sound signal into smaller segments such that lengths are of the same size as the size of the message to be encoded.
b. Matrix of the phases is created by applying Discrete Fourier Transform (DFT).
c. Calculate the Phase differences between adjacent segments.
d. Phase shifts between adjacent segments are easily detectable. It means, we can change theabsolute phases of the segments but the relative phase differences between adjacent segments must be preserved. So the secret information is inserted only in the phase vector of the first signal segment as follows.
e. Using the new phase of the first segment a new phase matrix is created and the original phase differences.
f. The sound signal is reconstructed by applying the inverse Discrete Fourier Transform using the new phase matrix and original magnitude matrix and then concatenating the sound segments back together

DIGITAL SIGNATURE USES:

Avoiding communication in well-known forms greatly reduces the risk of information being leaked in transit.

- Another form of steganography, called watermarking is used primarily for identification and entails embedding a unique piece of information within a medium without noticeably altering the medium.

• Steganography can also enhance individual privacy. This is effective only if the hidden communication is not detected.The most private communication is the one that never existed Advantage This method is easy to implement but is very susceptible to data

Disadvantage This method can be used when only a small amount of data needs to be concealed. Jayaram P, Ranganatha H R, Anupama H S discuss different types of audio steganographic methods,. Advantage This paper concludes that audio data hiding techniques can be used for a number of purposes other than covert communication or deniable data storage, information tracing and finger printing tamper detection. R S RIDEVI, DR. A DAMODARAM and DR. SVL.NARASIMHAM gives basic idea behind to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safer manner.

Advantage This proposed system is to provide an efficient method of or hiding the data from hackers and sent to the destination in a safe manner and this system will not change the size of the file even after encoding and also suitable for any type of audio file format.

Disadvantage The quality of sound depends on the size of the audio which the user selects and length of the message. Samir Kumar Bandyopadhyay et. Al 2010] detects certain flaws in mostly substitution techniques of

steganography:

Having low robustness against attacks which try to reveal the hidden messag e. Since substitution techniques usually modify the bits of lower layers in the samples LSBs, it is easy to reveal the hidden message if the low transparency causes suspicious 2) Having low robu stness against distortions with high average power. Unin tentional attacks like transition distortions could destroy the hidden message if is embedded in the bits of lower layers in the samples LSBs[4]. Christine K. Mulunda,Peter W. Wagacha, Alfayo O. Adede worked with text as the cover medium with the aim of increasing robustness and capacity of hidden data. Elitism was used for the fitness function.

III. REFERENCES

[1]. W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz, S. Pogreb, "Techniques for data hiding", IBM Systems Journal, Volume 39 , Issue 3-4, July 2000, pp. 547 – 568.

[2]. Samir Kumar Bandyopadhyay, Debnath Bhattacharyya, Poulami Das, Debashis Ganguly and Swarnendu Mukherjee, "A tutorial review on Steganography", International Conference on Contemporary Computing (IC3-2008), Noida, India, August 7-9, 2008, pp. 105-114.

[3]. Robert Krenn, "Steganography and steganalysis", An Article, January 2004.

[4]. Nedeljko Cvejic, Tapio Seppben "Increasing the capacity of LSB-based audio steganography " FIN90014 University of Oulu, Finland ,2002.

[5]. Sajad Shirali-Shahreza M.T. Manzuri-Shalmani "High capacity error free wavelet domain speech steganography" ICASSP 2008

[6]. Neil F.Johnson, Z.Duric and S.Jajodia. "Information Hiding Steganography and Watermarking-Attacks and Countermeasures",Kluwer Academic Publishers, 2001

[7]. F.A.P.Petitcolas, R.J.Anderson, M.G.Kuhn:"Information Hiding- A Survey", Process of IEEE, vol.87, no.7, pp.1062-1078, July, 1999.

[8]. Min Wu, Bede Liu. "Multimedia Data Hiding", Springer- Verlag New York, 2003.

[9]. N. Taraghi-Delgarm, "Speech Watermarking", M.Sc. Thesis, Comptuer Engineering

Department, Sharif University of Technology, Tehran, IRAN, May 2006.

[10]. M. Pooyan, A. Delforouzi, "LSB-based Audio Steganography Method Based on Lifting Wavelet Transform", in Proc. 7th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT'07), December 2007, Egypt.

[11]. R.A. Santosa and P. Bao, "Audio-to-image wavelet transform based audio steganography," Proc. of 47th Int. Symposium ELMAR, June 2005, pp. 209- 212.

[12]. Xuping Huang, Ryota Kawashima, Norihisa Segawa, Yoshihiko Abe. "The Real-Time Steganography Based on Audio-to-Audio Data Bit Stream",Technical report of IEICE, ISEC, vol.106 pp.15-22, September 2006.

[13]. Aoki, Naofumi. "A Band Widening Technique for VoIP Speech Using Steganography Technology", Report of IEICE, SP,106(333), pp.31-36, 2006.

[14]. Xuping Huang, Ryota Kawashima, Norihisa Segawa, Yoshihiko Abe International Conference on Intelligent "Information Hiding and Multimedia Signal Processing" © 2008 IEEE.

[15]. A. Delforouz, Mohammad Pooyan, "Adaptive Digital Audio Steganography Based on Integer wavelet transform ", IEEE Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2007, 26-28 Nov 2007, pp 283-286.

[16]. R. A. Santosa, P. Bao," Audio-to-Image Wavelet Transform based Audio Steganography", 47th International Symposium ELMAR-2005 , 08-10 June 2005, Zadar, Croatia, pp 209-212.

[17]. S. Shirali-Shahreza, M. T. Manzuri-Shalmani, "Adaptive Wavelet Domain Audio Steganography with High Capacity and Low Error Rate", IEEE International Conference on Information and Emerging Technologies, 2007, 06-07 July 2007 pp 1-5.

[18]. Yincheng Qi, Jianwen Fu, and Jinsha Yuan, "Wavelet domain audio steganalysis based on statistical moments of histogram", Journal of System Simulation, Vol 20, No. 7, pp. 1912-1914, April 2008.

[19]. Yin-cheng qi, liang ye, chong liu "Wavelet domain audio steganalysis for multiplicative embedding model" Proceedings of the 2009 International Conference on Wavelet Analysis and Pattern Recognition, Baoding, 12-15 July 2009.

[20]. V. Vapnik, "Statistical Learning Theory", John Wiley, 2008.

[21]. Mengyu Qiao, Andrew H. Sung , Qingzhong Liu "Feature Mining and Intelligent Computing for MP3 Steganalysis" International Joint Conference on Bioinformatics, Systems Biology and Intelligent Computing 2009.