A Survey on Steganography Techniques in Real Time Audio Signals and Evaluation

Article *in* International Journal of Computer Science Issues · January 2012

CITATIONS
31

READS
1,097

3 authors, including:

Azizah Abdul Manaf
Universiti Teknologi Malaysia
155 PUBLICATIONS **1,947** CITATIONS

SEE PROFILE

A Survey on Steganography Techniques in Real Time Audio Signals and Evaluation

Abdulaleem Z. Al-Othmani[1], Azizah Abdul Manaf[2] and Akram M. Zeki[3]

[1] Advanced Informatics School (AIS), Universiti Teknologi Malaysia (UTM)
Kuala Lumpur, Malaysia

[2] Advanced Informatics School (AIS), Universiti Teknologi Malaysia (UTM)
Kuala Lumpur, Malaysia

[3] Kulliyyah Information and Communication Technology, International Islamic University Malaysia (IIUM)
Kuala Lumpur, Malaysia

Abstract

Steganography has proven to be one of the practical ways of securing data. It is a new kind of secret communication used mainly to hide secret data inside other innocent digital mediums. Most of existing steganographic techniques use digital multimedia files as cover mediums to hide secret data. Audio files and signals make appropriate mediums for steganography due to the high data transmission rate and the high level of redundancy. Hiding data in real time communication audio signals is not a simple mission. Steganography requirements as well as real time communication requirements are supposed to be met in order to construct a useful and useful data hiding application. In this paper we will survey the general principles of hiding secret information using audio technology, and provide an overview of current functions and techniques. These techniques will be evaluated across both, steganography and real time communication requirements.

Keywords: *Real time communication, data hiding, LSB, audio steganography, signal processing.*

1. Introduction

Steganography has a long history of been used as a way to protect security and privacy of valuable information. While cryptography focuses on protecting the secret message by jumbling its content, steganography concerns on protecting the secret message by concealing its mere existence. The concealment of secret messages is achieved by embedding them into other seemingly-innocent host mediums [1], [2], [3]. Figure 1 below illustrates the basic idea of any steganography process.

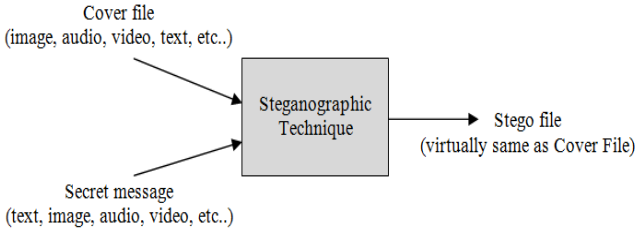

Fig. 1 Fundamental scheme of steganography process.

Steganographic application can hide different types of data within a cover medium. The resulting stego message contains the hidden information, even though it is seemingly identical to the cover medium. Steganography basically exploits human awareness and observation because human senses are not qualified to seek files that have information hidden inside them, while there are many third party programs can do what is called Steganalysis, which an art of inverse steganography aims to analyze and break a specific steganographic system. Normally, steganography is required where cryptography techniques are ineffective [4].

Generally, all digital mediums, signals, or files can be used in steganography process as cover media, but some formats are more suitable than others depending on the level of redundancy [5]. For instance, text steganography is believed to be the hardest type of steganography because of the low degree of redundancy in text as compared to image, audio or video. Redundancy can be described as the bits of a media, signal or file that offer accuracy more than needed for the object's use [6]. The redundant bits of an object may also be defined as those bits that can be easily altered without this change being

noticed easily [7]. Image, video and audio files in particular fulfill this requirement, while studies have also revealed other file formats that are suitable to be used for information hiding. Figure 2 illustrates the main categories of file formats or signals that can be efficiently used for steganography.

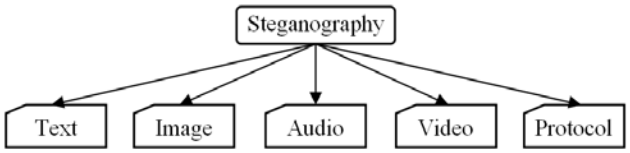

Fig. 2 Categories of steganographic cover mediums.

2. Structure of Steganography

Given the increased general attention over steganography technique and practices, some common terminology that most of the applications have in common have been discussed and determined [8]. The items agreed on are:

- **Emb (*m*):** Some information data or signal to be hidden, in other media.
- **Stego (*s*):** The output of the steganography process which is the signal, file or data that has the embedded message hidden in it.
- **Cover (*c*):** The input to the information hiding process which represents the innocent carrier signal or file.
- **Stegokey** or simply **key (*k*):** This is additional un-imbedded secret data which may be needed in the information hiding process. In particular, this key (or a related one) is typically needed to extract the embedded message again in the final destination.

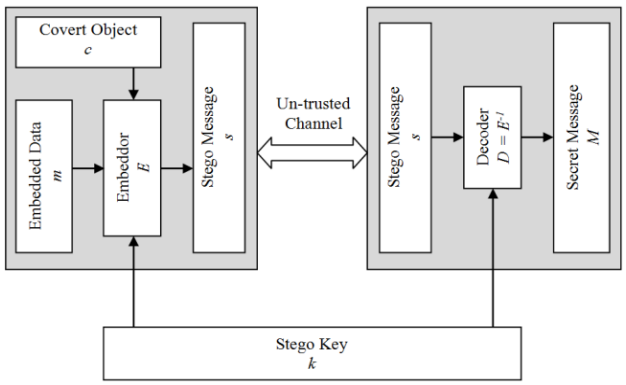

Fig. 3 Steganography terminology.

In general, steganographic system consists of embedding or encoding phase and extracting or decoding phase. As illustrated in Figure 3, the embedding process is accomplished by encoding or embedding the secret message into a covert innocent message using a stego key.

The result of this process is the stego message which contains both cover and secret messages combined according to the stego key. On the other hand, the decoding phase requires having the same stego key in order to be able to extract the embedded secret data from the stego message. In most steganography techniques, failing to have the stego key will make the process of extracting the secret message almost impossible.

3. Overview of Audio Steganography

Audio steganography is focused in hiding secret information in an innocent cover audio file or signal securely and robustly. Communication security and robustness are vital for transmitting important information to authorized entities while denying access to not permitted ones. By embedding secret information using an audio signal as a cover medium, the very existence of secret information is hidden away during communication. This is a serious and vital issue in some applications such as battlefield communications and banking transactions [9].

The secret message is concealed into the audio media by slightly changing the binary sequence of the audio file. Hiding secret information into digital audio media is generally more complicated than hiding secret information into other media, such as digital images. In order to hide secret information successfully, a range of techniques for inserting information into digital audio have been introduced. These techniques vary from simple ones that embed information as signal noises to more powerful ones that take advantage of complicated signal processing techniques to embed the secret message

3.1 Digital Audio Signal

Digital audio signals are different from other traditional analogue sounds in the fact that they are discrete signal rather than continuous ones. Discrete signals are produced by sampling continuous analogue signals at specific rates. For instance, the typical sampling rate for CD digital audio is 44 kHz. Figure 4 below, shows a continuous analog audio signal wave being sampled to create digital audio signal wave.

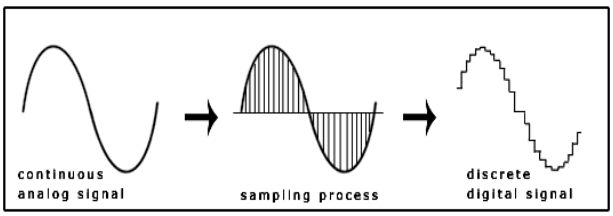

Fig. 4 Sampling of audio signal.

Figure 4 above emphasizes the discrete nature of digital audio signals. Nonetheless, typical sampling rate is generally set at a level in which the produced discrete signal is not imperceptibly distinguishable from the original continuous signal.

Digital audio files are stored in computers as a series of 0's and 1's. With a correct tool, it is possible to change the bits that structure a digital audio file. Such accurate controls permit changes to be performed to the binary bits that are not perceptible to the human sense

3.2 Methods of Audio Steganography

There are many steganographic techniques for hiding secret data or messages in audio in a way that the modifications made to the audio file are perceptually indiscernible. Several recent methods necessitate previous familiarity with signal processing techniques, Fourier transform, and other high level mathematics areas. Common techniques include [10] – [16]:

A) Least Significant Bit (LSB) Coding

Least significant bit (LSB) coding is the easiest and simplest method to hide secret data in a digital audio media. By replacing the least significant bit of each sample words with a bit of the secret data, LSB coding permits a big size of secret data to be embedded. LSB audio steganography techniques have the same previously discussed advantages and disadvantages of common LSB steganography techniques on other cover media.

In computing, the least significant bit (LSB) is the bit in the right most position of a binary number, which also determines whether the number is even or odd. It is equivalent to the least significant digit of a decimal number, which is the digit in the ones (right-most) position.

1	0	1	1	0	1	0	1

Fig. 5 Binary representation of decimal 181.

Figure 6 illustrates how the message “Hi” is encoded in a 16-bit quality audio sample using the LSB method. Here the secret information is “Hi” and the cover file is an audio file. “Hi” is to be embedded inside the audio file. First the secret information “Hi” and the audio file are converted into bit stream. The least significant column of the audio file is replaced by the bit stream of secret information “Hi”. The resulting file after embedding secret information “Hi” is called Stego-file.

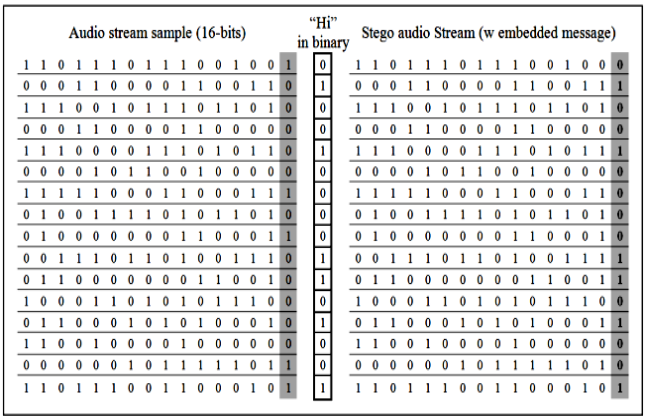

Fig. 6 LSB audio coding example.

In LSB coding, the idyllic secret data communication rate is 1 kbps for 1 kHz. In some variations of LSB coding, however, the two least significant bits of a sample word are use to hide two bits secret message data. This increases the capacity of embedded data but also increases the nose and therefore increases risk of being perceptible and eventually breakable.

Using LSB is possible, as modifications will typically not create perceptible changes to the sounds. Another method involves taking advantage of human sound system limitations. It is possible to encode messages using frequencies that are inaudible to the human ear. Using any frequencies above 20.000 Hz, messages can be hidden inside sound files and will not be detected by human checks [14].

B) Parity Coding

In parity coding, audio signal is broken down into separate areas of samples and hide the secret message in the parity bit of each sample area. If the parity bit of a sample area does not match the secret message bit to be embedded, the LSB of one of the samples in the area is inverted. Therefore, this will give a wider range of choices on where to hide the secret bit, and will keep the change in the signal more unobservable [17].

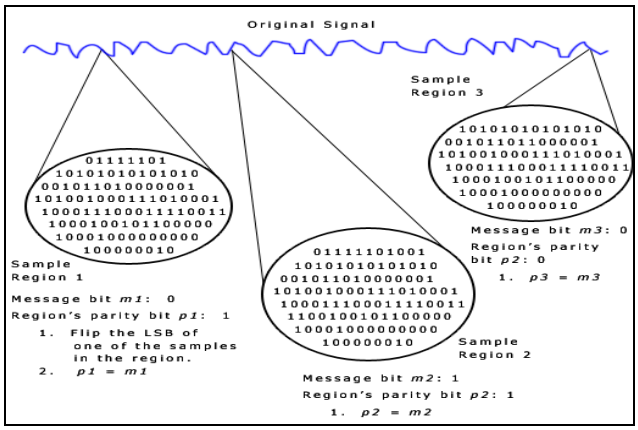

Fig. 7 Parity coding procedure.

C) Phase Coding

Phase coding deals with the weaknesses of the previously discussed audio steganography techniques which induce noises to the medium. Phase coding is based on the reality that, unlike noises, audio phase components are imperceptible to the human ear. Rather than adding noises, this technique encodes the secret data bits to phase shifts in the phase spectrum of the audio signal, attaining inaudible encodings in terms of signal-to-noise ratio [14].

$$phase_{new} = \begin{cases} \frac{\pi}{2} & if\ message\ \ bit = 0 \\ -\frac{\pi}{2} & if\ message\ \ bit = 1 \end{cases} \quad (1)$$

In phase coding, the phase of an initial audio segment is substituted with a reference phase that represents the data. Following segments phase is modified back to maintain the relative phase between segments. Phase coding, when applicable, is one of the most efficient audio steganographic methods in terms of the signal to noise ratio (SNR). When the phase relation between each frequency component is dramatically changed, noticeable phase dispersion will occur. On the other hand, on condition that the alteration of the phase is small enough, an inaudible steganography can be accomplished [14], [15].

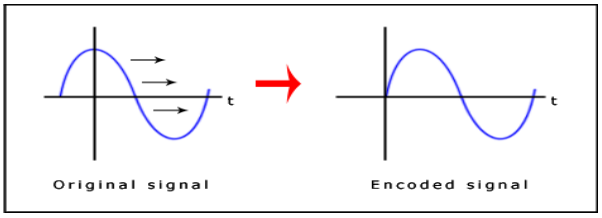

Fig. 8 The signals before and after Phase coding procedure.

D) Spread Spectrum

In the field of audio steganography, fundamental spread spectrum (SS) techniques attempts to distribute secret data throughout the frequency spectrum of the audio signal to the maximum possible level. This is equivalent to implementing LSB coding by spreading the secret data bits over the entire audio signal. However, different from LSB coding, the SS techniques spread the secret bits over the frequency spectrum of the audio media by using a code that is not reliant on the genuine signal. Consequently, the resultant signal will utilize a bandwidth wider than what is essentially needed for communication [15].

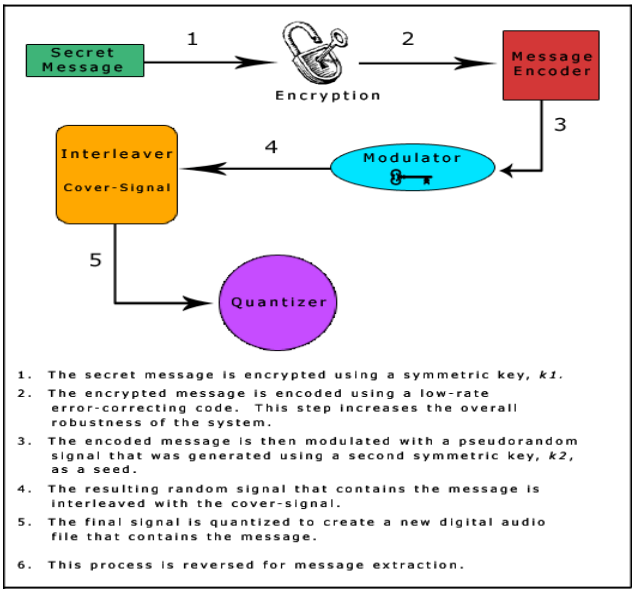

Fig. 9 Spread spectrum.

Two types of spread spectrum are utilizable in audio steganography: the direct sequence and frequency hopping schemes. In direct sequence spread spectrum, the secret data is distributed using a constant named the chip rate then adapted with a pseudorandom signal and then interleave with the cover signal. In frequency hopping spread spectrum, the frequency spectrum of the audio medium is changed so that it hops quickly among frequencies.

E) Echo Hiding

In echo hiding techniques, secret data is inserted into an audio medium by introducing an echo into the discrete signal. Similar to SS technique, it also offers benefits as it allows high data communication rates and offers greater robustness compared to the earlier noise-inducing techniques.

In order to hide secret message effectively, three echo-related factors are involved and changed: amplitude, decay rate, and offset (delay time) from the genuine audio signal. All of those factors should be set lower than the human hearing threshold in order to keep the echo imperceptible. Additionally, offset values are changed corresponding to the binary secret data targeted. A specific offset value represents a binary one, and another offset value represents a binary zero. Figure 10 illustrates the echo hiding process

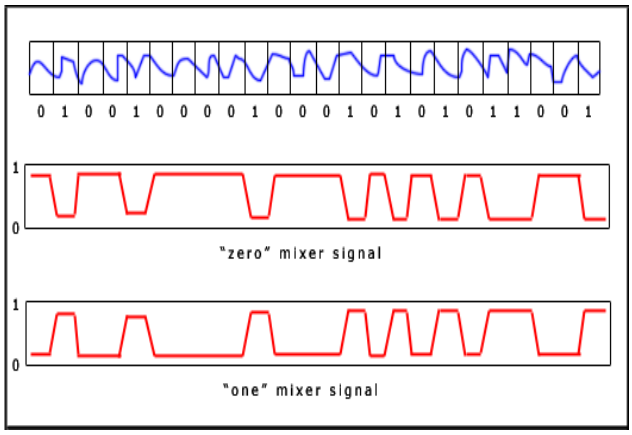

Fig. 10 Echo hiding.

3.3 Steganography in Real Time Audio Signals

Real-time communications (RTC) is any form of telecommunications in which information can be exchanged among the users instantly or with insignificant latency. RTC may occur in half-duplex or full-duplex approaches. Data can be transmitted in both directions on a single carrier simultaneously in full-duplex mode, while in half-duplex RTC data can be transmitted in both directions on a single carrier but not in the same time. Any type of communication, especially digital real-time one, needs to have one or more protocols to control and standardize the communication process among the clients. Generally, theses protocols used to rule the segmentation, framing, sampling, transmission, traffic controlling, receiving, and other main protocol tasks. The protocols used to send the sampled data using packets. Packet payloads are basically encoded multimedia data and they may contain any type of multimedia data.

Usually, protocol packets have some extra unused bits mainly for future use purposes as well as for some special situations. It is very useful and practical to hide secret information into these redundant bits allocated in the structure of every packet sent. This provides the ability to modify these bits to hide data without any perceptible change in the encoded multimedia contents. The sample word size, used by different multimedia encoding formats is an important aspect in finding out the maximum amount of available space in the cover medium for hiding the secret information. In general, least significant bits of each word value are probably usable to be modified with no perceptible change in the quality of the multimedia content. Thus, as an example, only half the amount of available space in a16-bit encoded audio cover medium will be available in comparison with a cover medium with an 8-bit word size.

The throughput of the real time communication system is another important factor used to define the performance of any proposed RTC steganography technique. As an example, utilizing the LSB of every sample in some kind of data compression protocol which has the packet size of 160 bytes, a suggested total of 20 bytes of secret data can be successfully embedded. If the throughput of this system is around 50 packets per second unidirectional, this results in approximately 1,000 bytes of full-duplex throughput of secret data within this covert communication channel

4. Test and Evaluation

All steganography techniques have to fulfill a few specific and essential requirements. A set of criteria has been proposed to further describe the quality of a steganography algorithm as illustrated in Figure 11 and discussed below.

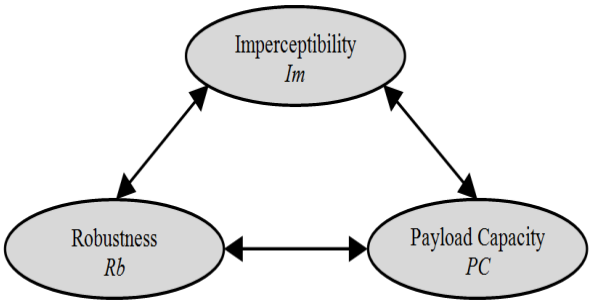

Fig. 11 Steganography requirements.

In this evaluation, since there are a number of sub layers, we think that it is better to measure each requirement separately.

4.1 Imperceptibility (*Im*)

The imperceptibility is the most important requirement of a steganography system, as the strength of steganography system depends on its ability to be unnoticed by the human senses (visually or acoustically). If it is noticed that

the cover medium has been altered, the steganography technique or system is not practical anymore [19]. The steganography system is said to be accurately imperceptible only if it is impossible to distinguish the covert data from the hidden secret information. It is sometimes enough that the alterations in the stego message be unobserved, on condition that the embedded message is not compared with the original covert message [20], [21].

4.2 Robustness (*Rb*)

Robustness defines how strong the used steganographic technique against changes. It measures the capability of the embedded secret data to endure different types of intentional and unintentional modifications. The hidden embedded message should be very hard to eliminate or modify without altering the quality of the covert medium [22], [23].

It is important for steganography techniques to be robust against both intentional and unintentional modifications to the message [19]. Many steganography techniques leave some kind of 'signature' when embedding the secret information. Typically, these signature data can be easily identified using statistical analysis. It is necessary that a steganography algorithm does not leave such a mark in the covert medium in order to be able to avoid and pass by such statistically analysis without being detected. In the communication of a stego message by reliable systems, the message may go through manipulations in an attempt to remove potential hidden information. Data manipulation, such as compression or rotating, might be applied to the message prior reaching its final destination. Depending on the manner in which the message is embedded, these manipulations may or may not destroy the hidden message depending on the method or technique used to hide the secret message

4.3 Payload Capacity (*PC*)

Payload capacity is the size of embedded data that can be hidden into a particular innocent cover medium relative to the size of this medium. The real challenge is how to hide as much secret data as possible while keeping the quality of the medium untouched and without infringe the imperceptibility requirement. Generally, increasing the embedding capacity makes the secret hidden information more conspicuous in viewing. To calculate the embedding capacity of a particular steganography system, the size of the embedded secret message is divided by the total size of the cover medium as shown in Equation 2.

$$Payload\ Capacity = \frac{Total\ number\ of\ bits\ of\ hidden\ data}{Total\ number\ of\ bits\ of\ cover\ file} \quad (2)$$

4.4 Real Time Suitability (*RTS*)

Steganography in real time audio signals involves additional requirements such as system complexity, throughput, bandwidth, delay, absence of duplications, failure recovery, and service setup time. These requirements directly affect the real time communication process, and hence, may have influences on the real time steganography processes [24], [25].

5. Discussion

Table 1 tabularizes the comparison of audio signal steganographic techniques based on the proposed evaluation criteria. The levels of technique fulfillment to the requirements have been defined as high, medium or low. A high indicates that the technique totally meets the requirement, while a low level indicates that the technique has some limitations or weaknesses relating to this requirement. A medium level indicates that the requirement is dependent on external factors [7], [19].

Table 1: Evaluation of steganography techniques in real time audio signals

Technique	***PC***	***Im***	***Rb***	***RTS***
LSB	High	Medium	Low	High
Parity Coding	Medium	Medium	Low	Low: Delay
Phase Coding	Low	High	High	Medium
Spread Spectrum	High	Low	High	Low: Bandwidth
Echo Hiding	High	Low	Medium	Medium

There are two major drawbacks related to the use of methods like parity coding. The human ear is sensitive and can often detect even the slightest bit of noise introduced into a sound signal, although the parity coding method almost makes the generated noise impossible to hear. Another drawback of using parity coding is the low robustness. Phase coding has the disadvantage of a low data transmission rate because the secret message is embedded in the first signal segment only. That is what makes phase coding method practical only when a small quantity of secret data needs to be transmitted. LSB coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded.

Regarding real time communication requirements, only LSB technique shows a high level of suitability in terms of delay, throughput, complexity, and reliability requirements of RTC. Parity coding technique requires the signal to be broken down into segments to apply the parity hiding on these segments and then transmits these segments to the destination. This introduces delays on the transmission process which severely affects the real time communication process. Spread spectrum coding expands the frequency bandwidth of the audio signal which in turn might not be available by the communication channel provider. Phase coding and echo hiding techniques have shown a high level of compatibility with real time requirements except some negative aspects related to system complexity, throughputs, and service setup time.

6. Conclusion

In this paper, several techniques are discussed as potential methods for embedding data in real time audio signals. While a degree of success has been achieved, each one of the proposed methods has its limitations. The ultimate goal of attaining protection of large amounts of secret data against deliberate attempts at removal may be still far from being obtained. The five techniques discussed above offer numerous choices and make this data hiding technology more obtainable and accessible. Prioritizing the importance of communication and security characteristics such as data rate, bandwidth, robustness, and noise audibility, must be done before choosing the steganographic technique which should completely fits the nature, environment and requirements of the application.

Although some data hiding techniques have been proposed by various researchers, the specific requirements of each data hiding technique vary from one application to another; with each of these techniques have some advantages and disadvantages. The flexible nature of audio formats, signals and files, is what makes them good and practical medium for steganography. Another aspect of audio steganography that makes it so attractive and promising is the ability to combine steganography techniques with existing cryptography technologies. We do not have to depend on one technique only. Secret data not only can be encrypted, they can be hidden and encrypted at the same time

References

[1] Mazurczyk, W. and K. Szczypiorski, "Covert Channels in SIP for VoIP Signalling", in Global E-Security, H. Jahankhani, K. Revett, and D. Palmer-Brown, Editors. 2008, Springer Berlin Heidelberg. p. 65-72.

[2] Hui, T., et al. "An M-Sequence Based Steganography Model for Voice over IP". in Communications, 2009. ICC '09. IEEE International Conference on. 2009.

[3] Tian, H., et al., "A Covert Communication Model Based on Least Significant Bits Steganography in Voice over IP", in Proceedings of the 2008 The 9th International Conference for Young Computer Scientists. 2008, IEEE Computer Society. p. 647-652.

[4] Nutzinger, M., C. Fabian, and M. Marschalek. Secure Hybrid Spread Spectrum System for Steganography in Auditive Media. in Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on. 2010.

[5] Petitcolas, F.A.P., R.J. Anderson, and M.G. Kuhn, Information hiding-a survey. Proceedings of the IEEE, 1999. 87(7): p. 1062-1078.

[6] Currie, D.L. and C.E. Irvine, 1996. Surmounting the effects of lossy compression on steganography. Proceedings of the 19th National Information Systems Security Conference, Oct. 22-25, Baltimore, Maryland, pp: 194-201

[7] Anderson, R.J. and F.A.P. Petitcolas, On the limits of steganography. Selected Areas in Communications, IEEE Journal on, 1998. 16(4): p. 474-481.

[8] Pfitzmann, B. (1996) (collected by): Information Hiding Terminology – Results of an informal plenary meeting and additional proposals; Information Hiding, LNCS 1174, Springer-Verlag, Berlin 1996, 347-350

[9] Gopalan, K. and S. Wenndt, Audio Steganography for Covert Data Transmission by imperceptible Tone Insertion. in Proc. the IASTED International Conference on Communication Systems and Application (CSA 2004), Banff, Canada, July 8-10, 2004, track 422-025.

[10] Shahreza, S.S. and M.T.M. Shalmani. High capacity error free wavelet Domain Speech Steganography. in Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on. 2008.

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

[12] Bhattacharyya, D., et al., Hiding Data in Audio Signal. Advanced Communication and Networking, C.-C. Chang, et al., Editors. 2010, Springer Berlin Heidelberg. p. 23-29.

[13] Chungyi, W. and W. Quincy. "Information Hiding in Real-Time VoIP Streams". in Multimedia, 2007. ISM 2007. Ninth IEEE International Symposium on. 2007.

[14] Kumar S. B., D. Bhattacharyya, P. Das, D. Ganguly and S. Mukherjee, “A tutorial review on Steganography”, International Conference on Contemporary Computing (IC3-2008), Noida, India, August 7-9, 2008, pp. 105-114.

[15] Bender, W., 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.

[16] Vapnik, V.N. “Statistical Learning Theory”. John Wiley and Sons, New York, USA, 1998.

[17] Dutta, P. Bhattacharyya, D. and Kim, T. (2009). Data Hiding in Audio Signal: A Review. International Journal of Database Theory and Application Vol. 2, No. 2, June 2009

[18] Kahn, D. “The History of Steganography”, Proc. of First Int. Workshop on Information Hiding, Cambridge,UK, May30-June1 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson (Ed.), pp.1-7

[19] Morkel, T., J.H.P. Eloff, and M.S. Olivier. An Overview of Image Steganography. In Proceedings of the ISSA 2005 New Knowledge Today Conference, Information Security South Africa (ISSA), pp 1-11 (CD).
[20] Setyawan, I. "Geometric Distortion in Image and Video Watermarking, Robustness and Perceptual Quality Impact". Ph.D. Thesis. University of Technology, Department of Electrical Engineering, Indonesia, 2004.
[21] Langelaar, G.C., I. Setyawan, and R.L. Lagendijk, Watermarking digital image and video data. A state-of-the-art overview. Signal Processing Magazine, IEEE, 2000. 17(5): p. 20-46.
[22] Chen, W.Y., A Comparative Study of Information Hiding Scheme Using Amplitude, Frequency and phase Embedding, PhD thesis. National Cheng Kung University, Tainan, Taiwan, 2003.
[23] Voyatzis, G. and I. Pitas, Protecting digital image copyrights: a framework. Computer Graphics and Applications, IEEE, 1999. 19(1): p. 18-24.
[24] Ferrari, D., Client requirements for real-time communication services. Communications Magazine, IEEE, 1990. 28(11): p. 65-72.
[25] Gaitonde, S.S., D. Jacobson, and A.V. Pohm, Bounding delay on a multifarious token ring network. Commun. ACM, 1990. 33(1): p. 20-28.

Abdulaleem Z. Al-Othmani is a Ph.D. student in Computer Science at University Technology Malaysia (UTM), KL. He received his Bachelor of Science in Computer Engineering in 2002 at Baghdad University, Iraq and a Master of Science in Computer Science in 2010 from the University of Technology Malaysia, Malaysia. In 2010, he started his Ph.D. in Computer Science at the Faculty of Computer Science and Information Systems, UTM. His research interests include audio signal processing, data hiding, cryptography, mobile steganography, and real time communication.

Azizah Abdul Manaf is a professor of image processing and Pattern Recognition from University Technology Malaysia (UTM). She graduated with B.Eng (Electrical) 1980, MSc. Computer Science (1985) and PhD (Image Processing) in 1995 from UTM. Her current areas of interest and research are image processing, watermarking, steganography and computer forensics and she has postgraduate students at the Master and PhD level to assist her in these research areas. She has written numerous articles in journals and presented an extensive amount of papers at national and international conferences on her research areas. Prof. Dr. Azizah has also held management positions at the university and faculty levels such as Head of Department, Deputy Dean, Deputy Director, and Academic Director. She is currently the Deputy Dean – Academic of Advance Informatics School (AIS) at UTM Second Author biography appears here. Degrees achieved followed by current employment are listed, plus any major academic achievements. Do not specify email address here.

Akram M. Zeki has obtained B.Sc. from University of Jordan, Amman, Jordan. And Master in Computer Graphics from Faculty of Computer Science and Information Technology at University Putra Malaysia. His PhD was from Faculty of Computer Science and Information System at University Technology Malaysia. Recently he is Assistant Professor at Kulliyyah of Information and Communication Technology, International Islamic University Malaysia. His research interest including: Watermarking, Steganography, Information Security and Image Processing.