Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.539 – 545

SURVEY ARTICLE

SURVEY ON SECURE AUDIO ENCRYPTION USING SILENCE PART OF THE SPEECH

V. Anusuya Devi[1], Dr. V. Kalaivani[2], T. Sam Pradeep Raj[3]

[1]Assistant Professor, [2]Associative Professor (SG), [3]Research Scholar

[1,2]Department of Computer Science and Engineering –PG

National Engineering College, Kovilpatti-628503, Tamilnadu, India

[3]Department of Computer Science and Engineering

Manonmaniam Sundaranar University, Tirunelvelli

[1] samanusuya23508@gmail.com, [2] kalai.nec@gmail.com, [3] sampradeepraj@gmail.com

Abstract— Embedding a secret message into a cover media without attracting any attention is known as steganography. Steganography is one of the methods used for hidden communication purposes. One of the cover media that can be used for audio steganography is speech. All the methods that we have found for audio steganography change the values of maximum number of samples from the audio signal. Usually change the sample values of the signal annoying the listener and reduce perceptual transparency. Hence the special methods are required for hiding the information in audio signal.

This survey proposes a new approach for steganography in speech signals. In this method, secret data are hidden in the silence part of the speech signal. The silence parts are identified by collaborative non voice detection algorithm. The secret data are hidden by reducing a small number of sample values from some samples of the silence part. The main feature of our method is to create the high perceptual transparent steganographic system with acceptable data hiding capacity. This method can hide information in a speech stream with very low processing time that makes our method as a real-time steganography method.

I. INTRODUCTION

Steganography is the art of covered writing. The purpose of steganography is covert communication to hide a message from a third party. This differs from cryptography, the art of secret writing which is intended to make a message unreadable by a third party. But does not hide very existence of the secret communication. While steganography is separate and distinct from cryptography. There are many analogies between the two and in fact some authors categorize steganography as a form of cryptography. Since hidden communication certainly is a form of secret writing. In ancient times messages were hidden on the back of wax writing tables and written on the stomachs of rabbits or tattooed on the scalp of slaves.

Steganography hides the covert message but not the fact that two parties are communicating with each other. The stego process generally involves placing a hidden message within some transport medium called the carrier. The secret message is embedded within the carrier to form the stego National Engineering College, Kovilpatti, Tamilnadu, India medium. The use of a stego key may be employed for encryption of the hidden message and for randomization within the stego scheme.

II. RELATED WORK

Fayfik Alnawok et al [6] proposed a new strategy for steganography to get the minimum effect on the images which is used to hide data into it. This is by dividing the original image into a number of segments these segment is achieved according to the number of characters included into the message which is going to be hided in the original image. In this approach the message will be coded by using the coding table. After the message has been coded it will be hidden into the image. The technique is to search segments in the image that corresponded to the coded character in this stage the technique is mark out the positions of each encoded character included in the original message. At last they try to test the new technique they found that the position of the character in image does not been affected besides the new technique is also hard to been beaked by uninterested user.

Chun-Shien et al [2] investigates a central problem in steganography that is: How much data can safely be hidden without being detected. To answer this question a formal definition of steganographic capacity is presented. Once this has been defined a general formula for the capacity is developed. The formula is applicable to a very broad spectrum of channels due to the use of an information spectrum approach. This approach allows for the analysis of arbitrary steganalyzers as well as non-stationary nonergodic encoder and attack channels. After the general formula is presented various simplifications are applied to gain insight into example hiding and detection methodologies. A framework for evaluating the capacity of steganographic channels under an active adversary has been introduced. The system considers a noise corrupting the signal before the detection function in order to model real world distortions such as compression, quantization etc. Constraints on the encoder dealing with distortion and a cover signal are not considered. Instead the focus is to develop the theory necessary to analyze the interplay between the channel and detection function that results in the steganographic capacity. The method uses an information spectrum approach that allows for the analysis of arbitrary detection functions and channels. This provides machinery necessary to analyze a very broad range of steganographic channels. In addition to offering insight into the limits of performance for steganographic algorithms this formulation of capacity can be used to analyze a different and fundamentally important fact of steganalysis. While false alarms and missed signals have rightfully dominated the steganalysis literature very little is known about the amount of information that can be sent past these algorithms. This paper presents a theory to shed light onto this important quantity called steganographic capacity.

Protecting privacy for exchanging information through the media has been a topic researched by many people. Up to now cryptography has always had its ultimate role in protecting the secrecy between the sender and the intended receiver. However now a days steganography techniques are used increasingly besides cryptography to add more protective layer to the hidden data. Jing-Ming Guo et al [7] proposed a secret communication scheme is in which the data is doubly protected by both encryption stage and hiding stage. The message to be embedded is first processed by applying some encryption techniques. Here in the permutation algorithm that requires a pair of numbers as a key is employed to permute the original message. After the encryption stage the scrambled message is then embedded into a JPEG image by managing different quantization tables. The final result is a JPEG image containing some certain regions with different image quality. The recipient performs reverse steps to extract the information first extract the pattern of the scrambled message and then use the key which was shared previously to decipher the message. This scheme has its beauty because it is very plain clear, and highly practical. Another advantage is that it does not employ any traditional space such as plane or DCT domain. The proposed scheme works only by switching between the two different quality factors combining with an encryption procedure

to enhance the security thus in general it would be safe under some steganalysis schemes as shown in the experimental results. The strength of the scheme is based on the strength of the encryption key and the embedding technique using different QTs is to add a supplemental protective layer for the encrypted message by hiding it into a normal innocent JPEG image. Now a day most still images are compressed in JPEG format the simplicity of the proposed scheme would make it a very practical candidate for secret communication.

Robustness to compression is a basic requirement for any data hiding scheme. In this paper Kipper et al [1] concentrate on MP3 resistant oblivious data hiding. They propose three effective data hiding schemes where the message is embedded in amplitude DFT phase domain and noisy components respectively. In an amplitude modulation scheme a PN sequence is embedded in the original coefficients. Psychoacoustic model can be exploited to keep the distortion under the threshold. The second scheme hides the message in the DFT phase domain since it is believed the phase is less significant perceptually than amplitude. To design a compression-resistant hiding scheme, it is important to make use of the holes in the compression. In MP3 compression frequency resolution is the same in low and high frequency bands although it is often unnecessary at high frequency end. There exists some room to modify these high frequency coefficients without many artifacts. The third scheme noise substitution embeds the message in the high frequency coefficients. The spread spectrum modulation is extended in the audio case. Its advantage is psychoacoustic model can be used to control artifacts although it is not quite effective in host noise suppression. Phase modulation embeds the message in phase domain. It is effective in oblivious scenarios and can preserve quality at lower SNR than amplitude modulation. Taking advantage of MP3 compression we can also embed the message in high frequency coefficients. That corresponds to modification of noisy components. Simulations demonstrate the robustness to MP3 compression.

Masahiro Wakiyama et al [9] use audio steganography and propose that the new method of embedded secret data has high-capacity by improving the low-bit coding. When we embed the secret data in audio data it is important for the place of embedding data. It is meaningless that someone can detect the secret data at a glance as well as the image data. It is important to obtain big capacity without the variation in original data context. This paper describes an audio steganography using low bits coding. This approach is to replace the data of lower bit in a cover audio data by a secret data. They used wave file as an audio data. The wave file format is a subset of Microsoft's RIFF specification for the storage of multimedia files. We used 8 bits mono audio data. The secret data is a written text file. We propose two kinds of new methods of extended low bits coding. They improved the lowest bit coding and made a new method to increase embedded capacity. They used the audio data that the quantization bit rate is 8bit as experimental data. Therefore the range of audio data is from 0 to 255. The middle range of audio data is 128 and the sound of audio data is a silent sound. Therefore they don't use this range in audio data for embedding. If they embed the secret data in the silent sound, everyone notice the existence of the secret data. Therefore they don't embed the secret data into the middle range data. They make the middle range 128 to calculate the standard level of sound. They define the two thresholds 1 and 2 based on the standard level about middle range 128. They set the threshold 1 and 2 in experimental system. If the range of the amplitude is lower than boundary value 1 they don't embed the secret data. In this case they regard it small sound with noise. If the value of the audio data is between threshold 1 and 2 one bit is embedded in cover data. If the level of audio data is beyond threshold 2, two bits are used for the embedding. It is the method that uses the average amplitude data of surroundings audio data as threshold. They calculate the average about absolute value of amplitude regarding middle value 128 as value 0. The average of an amplitude level for audio data is calculated by 10 audio data about before and after 5 audio data except for own audio data about all sample data. If the level of the amplitude is bigger than that of the average value that is calculated by surroundings 10 pieces of audio data 2 binary digits are used for the embedding data. If not binary digits are not used for the embedding data. The level of the amplitude is very low and isn't suitable for the embedding data by the same reason such as the variable low bit coding. The numbers of embedding binary digits in this method are unified in two bits. They studied the audio steganography using wave file. They could embed the secret data by new extending method of low bit coding.

NedeGko Cvejic et al [5] increased the capacity of the classic LSB insertion method by performing the embedding process in the wavelet domain. In this paper they propose a new audio information-hiding algorithm that satisfies the imposed requirements for perceptual transparency and high bit rate of the hidden information. The proposed algorithm uses perfect reconstruction filter bank and embeds additional information inside wavelet domain of audio signal by modifying LSB values of wavelet coefficients. Objective and subjective tests show large advantage of the proposed method over time insertion method. For the same SNR values, proposed algorithm outperforms classical LSB algorithm by 150-200 kbps of hidden data. Subjective experiments showed that wavelet domain information hiding scheme is acoustically more transparent as well. Listening tests and SNR values have showed very high transparency of watermarked audio, even for data rates of additional data equal to a few hundreds kbps. They propose a new high capacity data hiding algorithm for audio signals. The algorithm makes use of perfect reconstruction filter bank and embeds additional information inside wavelet domain of audio signal by modifying LSBs of DWT coefficients. Experiments have shown large advantage over time domain LSB algorithm regarding both SNR values and subjective evaluation

Permutation steganography hides information in the ordering of elements of a set. Given n elements assuming that can be rearranged into any order a message can be encoded as the difference between the arrangements of elements with respect to a known reference ordering. Information has been hided in a Gif picture by reordering the color palette. A standard permutation steganography algorithm can encode an optimal message capacity up to $\log_2 n!$ bits for the different n! orders. But the standard permutation algorithm has the high run time complexity of very large numbers. So the standard is inefficient for the large number of elements. Bogomjakov et al proposed permutation steganography algorithm. It can be applied to any data set. The run time efficiency of an algorithm is O (n). According to theoretical optimum the hiding capacity produced by the Bogomjakov et al algorithm is less than one bit per element. In this paper Nien-ching huang et al [11] proposed an effective algorithm that increases the capacity even nearer to optimal but which maintain the same runtime complexity with the Bogomjakov et al algorithm. A theoretical analysis indicates that the proposed algorithm achieves 99% of optimal when using 128 elements. But the Bogomjakov et al algorithm attains only 98.34% of optimal. They conducted an experiment using a 3D polygon dataset for comparison. The analysis and practical experiments demonstrate that our algorithm attains a capacity closer to the optimal. Apart from the standard permutation algorithm to the best of my knowledge the proposed method provides the nearest expected capacity to optimal in the literature of permutation steganography.

Sajad Shirali Shahreza et al [13] proposed a new approach for hiding information in speech signals. In this method the silence intervals of speech are found and the length of these intervals is changed to hide information. This method can be used simultaneously with other methods. Audio steganography methods reported in the literatures can be classified into two major groups: temporal methods and transform domain methods. In temporal methods the hiding process, such as least significant bit replacement is done in time domain, while in transform domain methods the hiding process is done in another domain such as wavelet domain. One of the problems of steganography in transform domains is their unhiding. All of the methods that we found for audio steganography change the values of signal samples but do not change the number of samples for example adding or removing some samples. In this paper they propose a new approach for steganography in speech signals. In this method according to the data they want to hide they remove a small number of signal samples while do not change the values of signal samples. A special feature of speech signals is silence interval. In speech signals there are intervals which the speaker is not speaking. In these intervals the value of signal is low. One of the problems of applying general audio steganography methods such as LSB method to speech signals is that they usually hide information in all parts of the signal including silence intervals. But changing the values of samples of silence intervals for example by replacing LSB bits usually increases the values of the samples which make it annoying for listener and reduce perceptual transparency. So the special methods for hiding information in speech signals are required.

Shirali Shahreza et al [8] proposed an improved version of method for hiding information in silence intervals of speech. They modify that silence intervals of speech method to make it robust to compression. The new method is robust to compression algorithms such as MP3. They do not assume any special feature of the compression algorithm. In contrast to other MP3 resistant methods this method is done entirely in the temporal domain which makes it quite fast. In addition, it can hide information in a speech stream, which means that it can be used when the speech signal is generated in real time and only requires a small buffer. All the methods that we have found for audio steganography change the values of signal samples but do not add or remove any sample which changes the number of samples. In the proposed method they propose a new approach for steganography in speech signals. In this method according to the data we want to hide we remove a small number of signal samples. A special feature of speech signals is their silence intervals. In speech signals there are intervals when the speaker is not speaking. This feature is used in speech compression algorithms. In these intervals the value of signal is low. In our method we remove a number of samples from these silence intervals to hide data. The main advantage of this method in comparison with other MP3 resistant methods this method is a temporal domain method whereas other methods are transform domain method. In addition this method requires low computations. This enables this method to be a real-time method for streaming speech signals. In the encoder it only multiplies the signal samples by a number to amplify non silence samples and weaken silence samples and removes a number of samples from silence intervals which only requires a small buffer and can be done in real time. In the decoder it only counts the length of the silence intervals to extract data and does not even require a small buffer.

In the multibit assignment steganography the original palette is not changed and the colors in the palette are assigned to carry several bits. If a color possesses at least one neighbor color we say it is a gregarious color and we call a set containing a gregarious color and its all neighbors as a neighborhood set. Xinpeng Zhang et al [14] proposed a steganographic technique uses each gregarious color to represent a secret chip of several bits. For any pixel with a gregarious color one can always find a suitable color in the original color's neighborhood set and replace the original color with it to hide at least one secret bit. This way payload is increased or distortion is decreased when comparing with optimal parity assignment (OPA) method. On the other hand introducing a secret key in the multibit assignment procedure enhances security of the hidden information. In the OPA method the original color of a pixel is either kept unchanged or modified into its closest neighbor. Because the embedding rule is also known to the steganalyst having found the mapping relationship between the colors and their closest neighbors one can attempt to recover the original histogram in a reverse way of the data embedding. Since excessive operations can cause negative values in the recovered histogram the steganalyst is able to detect the presence of secret message and estimate the quantity of embedded bits. In contrast since the status of multibit assignment is determined by the secret key in the proposed scheme it is difficult to guess the modification relationship between the gregarious colors. That means the presence of secret message cannot be detected by the attempt of recovering the original histogram. In some steganographic techniques based on the human visual system, busy areas containing texture or edge contents are used to conceal more secret information since these areas can tolerate more changes. Clearly it will be beneficial to take into account the HVS in the multibit assignment mechanism. In future they will consider steganographic schemes that incorporate HVS characteristics in the multibit assignment mechanism to further improve the performance.

Yong Feng Huang et al [15] describes a novel high capacity steganography algorithm for embedding data in the inactive frames of low bit rate audio streams encoded by G.723.1 source codec, which is used extensively in Voice over Internet Protocol. VoIP are usually transmitted over low bit rate audio streams encoded by the source codec like ITU G.723.1 codec to save on network bandwidth. Low bit rate audio streams are less likely to be used as cover objects for steganography since they have fewer least significant bits than high bit rate audio streams. Little effort has been made to develop algorithms for embedding data in low bit rate audio streams. Huang et al proposed a steganography algorithm for embedding information in low bit rate audio streams. But these steganography algorithms have constrains on the data embedding capacity that is their data embedding rates are too low to have practical applications. Thus the main focus of this

study was to work out how to increase the data embedding capacity of steganography in low bit rate audio streams. The experimental results have shown that the proposed steganography algorithm can achieve a larger data embedding capacity with imperceptible distortion of the original speech compared with other algorithms. We have also demonstrated that the proposed steganography algorithm is more suitable for embedding data in inactive audio frames than in active audio frames. However, before the proposed algorithm comes into practical use in covert VoIP communications, it is necessary to explore how to assure the integrity of hidden messages in the case of packet loss.

Yu-Ming Cheng et al [16] presents a new steganographic approach designed to hide messages in HDR images. Our approach is based on spatial principles and doesn't consider robustness relative to the characteristics of steganography. To the best of my knowledge, this method is the first steganographic approach for HDR images. They use a two-sided method, modified from Chang and Tseng and developed their own L-sided method, inspired by Zhang and Wang to achieve greater adaptability and capacity. Unlike a common steganographic approach used for LDR images they start from the premise that the primary color channels have a different influence on image visualization. Thus at each channel the number of adaptive bits to be embedded on each pixel is determined by the weighted correlation between the values of neighboring pixels values. This adaptive scheme causes the steganographic HDR image to maintain good perceptual quality with respect to the human visual system. In addition this method also helps to preserve important image features such as contrast and luminance. This research indicates that the L-sided method provides a better approach to estimating pixel difference values and enables us to increase the capacity of a secret message while maintaining a similar visual appearance. Finally this scheme is self-extractable. That is the number of bits to be embedded can be calculated from the weighted correlation without extra overhead. Apart from considering adaptability they have dealt with the issue of authentication. They have found that it's advantageous to check the fidelity of the steganographic or stego HDR images before message extraction. Authentication ensures that the extracted message can be certified to determine its fidelity to the original secret message.

Multiple description coding has emerged as an attractive framework for robust transmission over unreliable networks. It can efficiently combat packet loss without any retransmission, thus satisfying the demand of real-time services and relieving the network congestion. In MD coding two or more bit streams called descriptions of the same image are generated which can be independently decoded. At the same time, the descriptions should carry correlated information. The correlated information is beneficial in the case of single-description reception in that it helps the estimation of the missing description from the received one. A minimum fidelity in the reconstruction can be obtained at the receiver when only one channel works For two-description image coding a conventional scheme is to partition an image into two parts and then to produce each description by alternatively concatenating a finely coded bit stream of one part and a coarsely coded bit stream of the other part. Zhiyuan Zhang et al [17] propose a novel two-description image coding scheme. As usual, each description of an image is constructed by a finely coded part and another coarsely coded part. The new scheme features that the coarse information is embedded into the fine information selectively using for example an LSB steganographic method. In this way coarse information can be carried on the fine information freely without allocating any more bit budget for the coarse information. A new idea for designing two descriptions coding with steganography has been presented. Instead of concatenating the two encoded parts to construct a description one coarsely coded part is embedded into the other finely coded part using the LSB steganographic method. A specific embedding based two description image coding scheme has been developed and tested to demonstrate the effectiveness of the proposed scheme with very encouraging results.

III. CONCLUSION

Based on the survey a new steganography method is proposed, for hiding secret data in speech signals. The proposed method hides data by changing the least number of samples in the non voice part of the speech signal. The proposed method has good perceptual transparency with acceptable high data hiding capacity. The main advantage of the

proposed method is a temporal domain. In addition, the proposed method requires low computations. This enables the proposed method to be a real-time method for streaming speech signals. In the encoder it modify a least number of samples from silence part which only requires a small buffer and can be done in real time. In the decoder, it only counts the non-zero sample in the silence part to extract data and does not even require a small buffer.

References

1. [Kipper04] Kipper, Gregory. Investigator's Guide to Steganography. Auerbach Publications: BocaRaton, 2005.
2. [Lu05] Lu, Chun-Shien. Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property. Idea Group Publishing, Hershey, 2005.
3. [Wiki09] "Steganograpy", http://en.wikipedia.org/wiki/Steganography, wikipedia page on steganography, includes links to many other sources.
4. Codr, Jessica. "A Java Application for Data Hiding in Image Files", Associated paper, Author's personal files and Appendix C.
5. Cvejic, "A wavelet domain LSB insertion algorithm for high capacity audio steganography" ,IEEE Transaction on Information Security, Oct 2002.
6. Fayik Alnawok, "Multi-Segment Steganography Technique", The International Arab Journal of IT, june 2008.
7. Jing-Ming Guo, "Secret Communication Using JPEG Double Compression", IEEE signal processing letter, OCTOBER 2010.
8. M.H. Shirali-Shahreza, "Real-time and MPEG-1 layer III compression resistant steganography in speech" , IET Information Security, 2010.
9. Masahiro wakiyama, "An audio steganography by a low-bit coding method with wave files", IEEE Conference on Information Hiding, January 2011.
10. Min-Wen Chao, "A High Capacity 3D Steganography Algorithm", IEEE transactions on visualization and computer graphics, June 2009.
11. Nien-Ching Huang, "Toward Optimal Embedding Capacity for Permutation Steganography", IEEE signal processing letter, VOL. 16, NO. 9, SEPT 2009.
12. Paulson, "Steganography Development Offers Promise", IEEE Computer, June 2010.
13. Sajad Shirali, "Steganography in silence interval of speech", IEEE Conference on Intelligent Information Hiding, April 2008.
14. Xinpeng Zhang etal, "Multibit Assignment Steganography in Palette Images", IEEE signal processing letter,2008.
15. Yong Feng Huang, "Steganography in Inactive Frames of VoIP Streams Encoded by Source Codec" ,IEEE Transaction on information security, JUNE 2011.
16. Yu-Ming Cheng, "A Novel Approach To Steganography in High-dynamic-range Images", IEEE Transaction on Information security, March 2009.
17. Zhiyuan Zhang, "Two Description Image Coding With Steganography", IEEE signal processing letter, VOL. 15, 2008.

