International Journal of Computer and Communication Technology

Volume 8 | Issue 2 Article 10

April 2017

HIDING SECRET DATA THROUGH STEGANOGRAPHY IN VOIP

SHILPA SUNIL WANKHADE
Department of Information Technology, Terna Engineering College, Nerul,Navi Mumbai,India, shilpasunilwankhade@gmail.com

PROF. RAMESH V. SHAHABADE
Department of Computer Engineering, Terna Engineering College, Nerul, Navi Mumbai,India, rameshvshahabade@gmail.com

Recommended Citation
WANKHADE, SHILPA SUNIL and SHAHABADE, PROF. RAMESH V. (2017) "HIDING SECRET DATA THROUGH STEGANOGRAPHY IN VOIP," *International Journal of Computer and Communication Technology*: Vol. 8 : Iss. 2 , Article 10.
DOI: 10.47893/IJCCT.2017.1411
Available at: https://www.interscience.in/ijcct/vol8/iss2/10

HIDING SECRET DATA THROUGH STEGANOGRAPHY IN VOIP

SHILPA SUNIL WANKHADE[1], PROF. RAMESH V. SHAHABADE[2]

[1]Department of Information Technology, Terna Engineering College, Nerul,Navi Mumbai,India
[2]Department of Computer Engineering, Terna Engineering College, Nerul, Navi Mumbai,India

Abstract- Steganography is an effective way of hiding secret data, by this means of protecting the data from unauthorized or unwanted viewing. Using cryptography technique will encrypt and decrypt message to provide better security. Cryptography protects the message from being read by unauthorized parties, steganography lets the sender conceal the fact that he has even sent a message. One of the new and promising communication medium that can be used as steganography is the Voice over Internet Protocol. VOIP covers a wide range of information hiding techniques. The main idea is to use free unused fields of VOIP protocols like TCP, UDP etc. By hiding one secret text into the cover speech using steganography we can get a stego speech, which sounds indistinguishable from the original cover speech. So even if the Hackers/crackers catch the audio packets on network, they would not notice that there is some secret text hidden inside it. To develop a Voice Chat Tool, this can also enable us to send secret data hidden inside the voice packets at the same time. We used LSB method of steganography and for better security we provide encryption to the message to be sent. There is no restriction on the length of message as more the communicators talk larger the file is sent. Human auditory system (HAS) operates over a wide dynamic range. It is challenging to hide secret data inside audio.

Keywords- *real time communication, VOIP, steganography, information hiding, stego speech, protocol headers, LSB, HAS, cover speech.*

I. INTRODUCTION

Steganography is the process of hiding secret data inside other, normally transmitted data. In other words, steganography means hiding of secret message within an ordinary message during sending or transmission phases and its extraction at the destination point.

Steganography and cryptography are closely related. Cryptography scrambles messages so they cannot be understood. It is a common approach to protect the audio contents by an encryption algorithm, such as the Data Encryption Standard (DES) or the Advanced Encryption Standard (AES) [3]. However, there may be some potential problems for these approaches. Steganography on the other hand, will hide the message so there is no knowledge of the existence of the message in the first place. At present time Voice over Internet Protocol (VOIP) is one of the most popular services in the internet. It was introduced to the telecommunication market and since then, changed it completely and gradually. As it is used worldwide more freely, the traffic volume that it generates is still increasing. Because of its popularity, it is becoming a natural target for steganography. VoIP is a general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks. Voice-over-IP (VoIP) as a new field for applied steganography. The term “VoIP” describes the digitalization, compression and transmission of analogue audio signals (in the majority of cases speech) from a sender to a receiver using IP packets. The receiver applies the reverse process and gets the reconstructed audio signal. After that he can act as the sender. A detailed review of Steganography methods that may be applied during signalling phase of the call can be found in. A new approach in Network Data hiding is to hide the Secret Text and series of characters in actual voice packet while keeping the application of the system intact. Any malicious user who would try to intercept this data would find this data as important as original VOIP data. Steganography is a art and science of writing hidden messages in such a way that no one, apart from sender and intended receiver suspects the existence of messages, a form of security. Nowadays, the UDP streaming files are used as a cover medium for hiding data and the RTP protocol uses this medium for successful transmission of hidden messages. But these techniques failed to satisfy the conditions such that the UDP would change its features and affect the transmission. Due to this fact, the attackers can guess the hidden information and break the confidentiality. Hence a solution is to be proposed to send original data in voice packets file and send the streaming content over UDP protocol without changing its characteristics. VOIP steganography covers a wide range of information hiding techniques, including popular techniques based on IP or TCP or UDP and other protocols. The main idea is to use free, redundant or unused fields of these protocols. In this work the VOIP call will be limited to two hosts using point-to-point connection with static IP addresses. This is As a result different from the real life VOIP applications which use client server calls, the system will be based on LAN network which provides an environment with almost zero noise. This paper is organized as follows: section II deals with literature survey. In section III some methods of audio steganography are summarized.

Section IV deals with proposed system. In section V experimental results are discussed. Finally section VI deals with conclusion and future scope.

II. LITERATURE SURVEY

Many of current audio and network steganography algorithms are theoretically applicable to VoIP streams but in practice only some of them are feasible or applicable to VoIP taking in mind available equipment and technology. Data hiding in audio signals is especially challenging, because the human auditory system (HAS) operates over a wide dynamic range. The HAS perceives over a range of power greater than one billion to one and a range of frequencies greater than one thousand to one. Kratzer et al. [16], suggested that messages to be encrypted prior to embedding to improve security. Later they proposed a scheme that introduces the cryptographies for embedded messages. However, the encryption operation must be carried out offline before the embedding operation, because the adopted cryptographies are often time-consuming and incur delays that may degrade the speech quality. Gopalan and Wenndt [19] presented a method of embedding covert data in a cover audio signal by inserting low power tones. Chungyi and Quincy [20], proposed a scheme for transmitting secret speeches based on information hiding in VoIP systems. Their hiding process consists of two steps: First compressing the secret speeches and then filling their binary bits directly into the LSBs of cover speech using G.711. Thomas Vogel and Christian Kraetze[18], summarize the design principles from the general approach and introduce extended experimental test results of a Voice-over-IP (VoIP) framework including a steganographic channel. Chungyi Wang[3], propose a scheme for speech hiding in a real-time communication system such as voice over Internet Protocol (VoIP). A novel design of real-time speech hiding for G.711 codec, which is widely supported by almost every VoIP device. Hui Tian[4], presents an adaptive steganography scheme for Voice over IP (VoIP). Differing from existing steganography techniques for VoIP, this scheme enhances the embedding transparency by taking into account the similarity between Least Significant Bits (LSBs) and embedded messages. Moreover, we introduce the notion of Partial Similarity Value (PSV). Ahmed[1], The functional and cost advantages if Internet telephony are evident. The hacker scene is constantly looking for new weak spots and developing ingenious methods of attack to gain access to confidential and penetrate further into network. One of the most security issues faced by VOIP is end-to-end user identity, responder identity and how to authenticate it. To guarantee the privacy and integrity of the response information is important. In this research some security issues about VOIP, the role of steganography in VOIP communication, and a proposed mechanism to secure VOIP based on steganography and one time password.Yong Feng Huang[6], his paper 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). Study reveals that, contrary to existing thought, the inactive frames of VoIP streams are more suitable for data embedding than the active frames of the streams; that is, steganography in the inactive audio frames attains a larger data embedding capacity than that in the active audio frames under the same imperceptibility. Mengyu, Q., A.H. Sung, and L. Qingzhong[12], In this paper, they propose a scheme for steganalysis of MP3Stego based on feature mining and pattern recognition techniques. We first extract the moment statistical features of GGD shape parameters of the MDCT sub-band coefficients, as well as the moment statistical features, neighbouring joint densities, and Markov transition features of the second order derivatives of the MDCT coefficients on MPEG-1 Audio Layer 3. Support vector machines (SVM) are applied to these features for detection. Experimental results show that our method can successfully discriminate the steganograms created by using MP3stego from their MP3 covers, even with fairly low embedding ratio.

III. METHODS OF AUDIO STEGANOGRAPHY

There are many steganographic techniques for hiding secret data or messages in audio. Major and common techniques include [9], [10], [11].

A. LSB coding

A very popular methodology is the LSB (Least Significant Bit) algorithm, which replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data. 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. 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.

B. Phase coding

Phase coding substitutes the phase of an initial audio segment with a reference phase that represents the hidden data. This can be thought of, as sort of an encryption for the audio signal by using what is known as Discrete Fourier Transform (DFT), which is nothing more than a transformation algorithm for the audio signal. Phase coding addresses the disadvantages of the noise-inducing methods of audio steganography. Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. Rather than introducing perturbations, the technique encodes the message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-perceived noise ratio.

C. 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.

D. 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.

E. Parity coding

The parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. Thus, the sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive fashion.

IV. PROPOSED SYSTEM

General architecture of the proposed VoIP steganography prototype is shown in Figure 1 below.

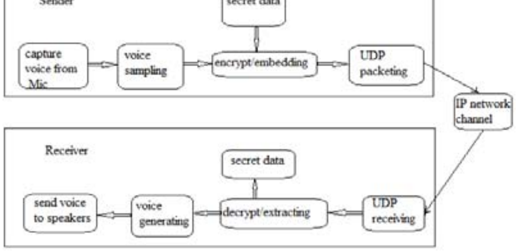

Figure1. Architecture of the proposed VOIP steganography prototype

The first step is to implement VoIP call by using either client server based or point-to-point based architecture. The VoIP call will be point-to-point based and consists of three steps: initializing call, performing the conversation, and ending the call.

The initialization of VoIP calls start when one endpoint (the sender) sends an INVITE message to the other endpoint (the receiver) using receiver's IP address. If the receiver accepts the invitation, an OK message will be sent back to the sender. By receiving the OK message, the initialize step is done and both the parties will start the next (conversation).

A. Embedding Process

As the conversation session starts, voice signals are captured from microphone and sampled into PCM codes. The secret data will now be encrypted and then embedded using LSB technique. The stego voice signal will be packetized into UDP packets and sent to the receiver.

- Algorithm for embedding process

Step 1: Get secret data and convert it to an array of bits A1.
Step 2: Get a portion of voice data and save it into an array of bytes A2.
Step 3: Insert starting bytes (0,255,0,255,0) into voice data array.
Step 4: Insert 1 bit of secret data array into LSB of voice data array byte.
Step 5: Increment indexes of A1 and A2.
Step 6: repeat Step 4 and 5 until end of A1.
Step 7: Insert ending bytes (255,0,255,0,255) into voice data array

B. Extracting Process

Received UDP packets from the sender are extracted by the use of extracting function. The hidden data are then
extracted from the audio bits and converted back to its original form and displayed on the GUI of the receiver.

- Algorithm for extracting process

Step 1: Get the received voice signal and save it into an array of bytes A2.
Step 2: Search the received voice data for the starting bytes (0,255,0,255,0).
Step 3: Extract the LSB of one byte of voice data array and save it into an array of bits A1.
Step 4: Increment indexes of A1 and A2.
Step 5: Repeat Step 4 and 5 until finding the ending bytes (255,0,255,0,255).
Step 6: Recombine array A1 into array of characters.
Step 7: Display the result (the array of characters) on the GUI.

V. EXPERIMENTAL RESULTS

Results of VOIP call are presented below.

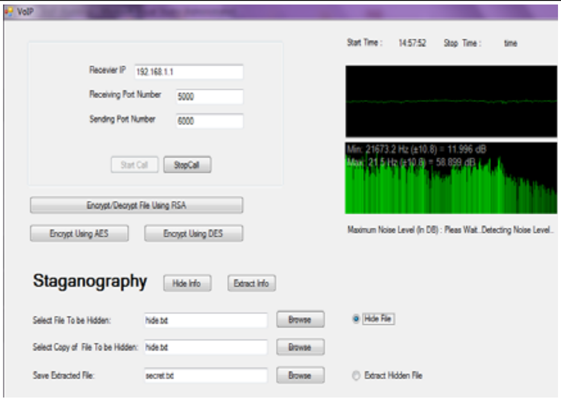

Figure2. VOIP call steganography GUI-1

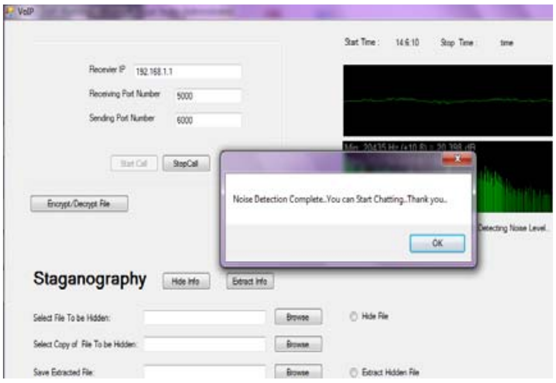

Figure3. VOIP call steganography GUI-2

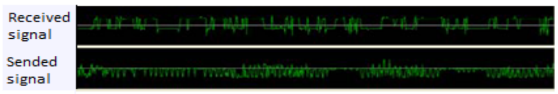

Figure4. VOIP call steganography results

Different secret data with different lengths are tested as shown in table below.

1) Results of hiding different sizes of secret data

TABLE 1

Measure	100 Bytes	1 KB	4 KB	8 KB
Time to extract data(sec)	3	238	1380	2908

2) Capacity- Capacity in data hiding indicates the total number of bits hidden and successfully recovered by the Stego system. The proposed system is highly capacitive.

3) No effect on voice quality- the ability of the embedded data to remain intact. The proposed system is secure and robust against noise.

4) VoIP lets the sender conceal the fact that he has ever sent a message; in this application there is no restriction on the length of message as more the communicators talk larger the file is sent.

VI. CONCLUSION AND FUTURE SCOPE

Steganography is an effective method of hiding data which has been used throughout history. This software is very important for the people who wish to ensure security to data they are transmitting. This software provides the communication of secret messages inside a perfectly innocent carrier i.e. voice packets. The concept of Steganography in real time communication VoIP lets the sender conceal the fact that he has ever sent a message. In this application there is no restriction on the length of message because more the communicators talk larger the file is sent. LSB technique of VoIP steganography is tested and evaluated. Proposed system is robust against noise and is high capacitive.

Future Scope- The scope of project is very vast. We will try to build the project dynamic and flexible so that it can be adopted in any situations. Making the software accessible worldwide so that each and every individual can interact with our application whenever you are in need of it.

REFERENCES

[1] Ahmed, Mohamed Hashim, Abdel Fatah Hegazy, Bahaa Hasan, Steganography for VOIP , Proceedings of the 7th WSEAS International conference on information security and privacy,p.18-22.

[2] Bo Liu,Liang Xu, Ziling Wei, Baokang Zhao, Jinshu Su, Adaptive VOIP steganography for Information Hiding within Network Audio Streams , in Network based information system(NBiS) 2011 International conference on Digital Object Identifier,p.612-617

[3] Chungyi Wang and quincy Wu, Information hiding in Real time VOIP streams , 9th IEEE international sysmposium on multimedia 2007

[4] Hui Tian, Ke Zhou, Hong Jiang, Yongfeng Huang, Jin Liu, An adaptive steganography scheme for VOIP , IEEE International Symposium on Circuits and Systems, 2009. ISCAS 2009.

[5] Hegazy, A.F. Hasan B , Hashim M, Beyond steganography for VOIP , in Computer Engineering and Systems (ICCES) , 2010 International Conference ,p.46-51

[6] Yong Feng Huang, Steganography in inactive frames of VOIP Streams Encoded by Source Codec , IEEE Transactions on Information Forensics and Security , vol. 6, no. 2, p. 296-306, 2011

[7] 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.

[8] Hui, T., et al. An M‐Sequence Based Steganography Model for Voice over IP . in Communications, 2009. ICC 09. IEEE International Conference on. 2009.

[9] 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.

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

[11] 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.

[12] Mengyu, Q., A.H. Sung, and L. Qingzhong, Feature Mining and Intelligent Computing for MP3 Steganalysis. in Bioinformatics, Systems Biology and Intelligent Computing, 2009. IJCBS 09.International Joint Conference on. 2009.

[13] 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.

[14] Gopalan, K. Audio steganography using bit modification . In Multimedia and Expo, 2003. ICME 03. Proceedings. 2003 International Conference on. 2003.

[15] Schulzrinne, H. and J. Rosenberg, Internet Telephony:architecture and protocols – an IETF perspective . Computer Networks, 1999. 31(3): p. 237 - 255.

[16] Kratzer, C., et al. Design and evaluation of steganography for voiceover - IP . in Circuits and Systems, 2006. ISCAS 2006. Proceedings.2006 IEEE International Symposium on. 2006.

[17] Zamani, M., Manaf, A, Ahmad, R.B., Jaryani, F., Taherdoost H., Zeki, AM.,"A secure audio steganography approach", International Conference for Internet Technology and Secured Transactions 2009, Page(s):1 - 6.

[18] Thomas Vogel, Jana Dittmann, Reyk Hillert and Christian Kraetze, "Design and Evaluation of Steganography for Voice-over-IP", To appear in Sicherheit 2006 GI FB Sicherheit, GI Proceedings, Feb 2006,Magdeburg, Germany.

[19] Gopalan, K., S. Wenndt. “Audio Steganography For Covert Data Transmission By Imperceptible Tone Insertion”, Proc. The IASTED International Conference on Communication Systems and Applications, Banff, Canada, July 2004.

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

[21] Zhiwei Yu, Clark Thomborson, Chaokun Fu, Jianmin Wang, " A Security Model for VOIP steganography" international conference on multimedia information networking and security,2009.

[22] Zander, S., Armitage, G., Branch, P.: A Survey of Covert Channels and Countermeasures in Computer Network Protocols. IEEE Communications Surveys & Tutorials, 3rd Quarter 2007, Volume: 9, Issue: 3, pp. 44-57 (2007).

[23] Wojciech Mazurczyk, Zbigniew Kotulski - New VoIP traffic security scheme with digital watermarking - In Proceedings of SafeComp 2006, Lecture Notes in Computer Science 4166, pp. 170 - 181, Springer-Verlag, Heidelberg 2006

[24] Zamani, M., Manaf, A, Ahmad, R.B., Jaryani, F., Taherdoost H., Zeki, AM.,"A secure audio steganography approach", International Conference for Internet Technology and Secured Transactions 2009, Page(s):1 - 6.

[25] Andrew D. Ker, “Steganalysis of Embedding in Two Least-Significant Bits” 2007 IEEE transactions on information forensics and security, vol. 2, no. 1, march 2007.

◈◈◈