http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 8 (8): 1140-1149, 2009
ISSN 1812-5638

Realization of a Covert Communication System Over the Public Switching Telephone Network

[1]Jixin Liu and [2]Zheming Lu
[1]Harbin Institute of Technology Shenzhen Graduate School, Shenzhen, China
[2]School of Aeronautics and Astronautics, Zhejiang University, Hangzhou, China

Abstract: In this study, a covert communication applying the vector quantization based information hiding algorithm and the Public Switching Telephone Network (PSTN) is implemented. The system aims at offering good security of the secret binary image message and the real-time performance that is very important for the speech calling of the telephone service. Therefore, we adopt a simple and effective encryption method for the secret binary image message prior to the embedding process. The embedding position is also protected by using a secret key. By using these methods, the requirement of short-term protection in the bursting phone call communication for the secret binary image message and the real-time encryption are both fulfilled. Furthermore, an information hiding algorithm based on vector quantization is proposed and the advantage of it is discussed. We evaluate the system with the ITU-T G.729a standard speech codec in StegoPhone, which is our platform for research on covert communication technology via PSTN. The experimental results show that our method has negligible hearing effects on the conversation speech and meet the requirement of the real-time calling conversation communication via PSTN.

Key words: Covert communication, vector quantization, public switching telephone network, information hiding

INTRODUCTION

Everyday, lots of information, whether through internet or the traditional Public Switching Telephone Network (PSTN), whether in the form of digital or analog, are exchanged. Also, the rapid development and explosive growth of computer network and multimedia technology introduces a series of security problems for the sensitive information, leading to the increasingly importance and researching attention of the secure communication. For example, in military application circumstances, the transmission of crucial message should not be aware to the adversary, for he will attempt to extract the message. If he can not extract the message, he would attempt to obstruct the transmission or at least interfere with the normal transmission procedure. For another example, in common application condition, some important private information (such as user password and account, etc.) is very easy to be revealed during telephone conversation if there is eavesdropper on the line. To protect these kinds of sensitive and secret information and transmit them safely, there are many methods have been developed. These methods can be classified into three catalogues, the covert communication using signal processing techniques or spread spectrum technique to accomplish the Low Probability of Detection (LPD) and Low Probability of Interception (LPI) system (Danezis, 2005; Orr *et al*., 1993; Roy and Doherty, 2009; Narayanan and Chuang, 2007; Radhakrishnan *et al*., 2002) the secret communication system by using the cryptography technology (Tao and Chuo, 1996; Diez-Del-Rio *et al*., 1994) and the covert communication by applying the steganography or information hiding technology to embedding the secret and sensitive message into the carrier signal to cover the existence of transmission (Gopalan, 2003; Tavakoli *et al*., 2006; Xiong and Ming, 2006; Huang *et al*., 2008; Kirovski and Malvar, 2001; Tian *et al*., 2008).

The covert communication protocol and channel is accomplished by using the small amounts of shared state in many TCP/IP stacks, the Direct Sequence Spread Spectrum (DSSS) technique is used to guarantee that the communication is covert and resistant to noise. A prototype by using this method is demonstrated and a further discussion is made to a more secure LPD communication protocol through the use of TCP features (Danezis, 2005). The construction of wavelet-based LPD/LPI waveform having the key properties for avoiding detection and interception is demonstrated and the comparison to the transform domain technique and

Corresponding Author: Jixin Liu, Harbin Institute of Technology Shenzhen Graduate School, Shenzhen, China
Tel: +86-13732216189

filtered QPSK method is carried out (Orr *et al*., 1993). The spread spectrum technique using noise-modulated waveforms is proposed for covert communications in (Narayanan and Chuang, 2007). The covert communication is implemented based on the principle of signal overlay, the transmitter transmits the weak secret message simultaneously with a cover signal overlapping in time as well as frequency to render ordinary signal detection techniques inoperative in detecting the presence of the covert signal (Roy and Doherty, 2009). The covert receiver employs the Empirical Decomposition (EMD) technique to extract the secret message signal. Other technique such as frequency hopping is also used to make it harder for the intended receiver to detect and intercept the signal. This scheme shows its usefulness for covert voice communication applications and data transmission from being detected by unwanted and intended receivers and it is resistant to jamming attack. A new form of multimedia steganography called data masking is proposed by Radhakrishnan *et al*. (2002), the secret message signal is processed to make it appear like a multimedia object using an inverse Wiener filter to foil an eavesdropper. This method is also can be recognized as the first catalogue.

Cryptography and encryption are well studied and prevalently used methods for secure communication. But because of the noise like behavior of the encrypted secret message signal, it will draw great attention during its transmission, leading to the attacks from the adversary. The chaotic switching is extended to general chaotic parameter modulation and by applying the adaptive controller, synchronization between the transmitter and receiver is maintained and secret message signal is recovered (Tao and Chuo, 1996). A communication terminal called Tiche is described by Diez-Del-Rio *et al*. (1994), it can achieve privacy protection when fax or speech are transmitted over the PSTN and is cryptographic technique based equipment. The ciphering system is based on both public key and private key algorithms. This covert communication method is belonging to the second type of the secret communication catalog. The disadvantage of this method is that eavesdropper will obtain the noise signals during the secret communication process and this will arouse the attention of the eavesdropper, who can record the communication data for future cryptanalysis or just interfere with or disturb the communication process. To overcome these shortcomings, steganography (or information hiding), as one of the alternative techniques, has drawn more and more attentions both in research and application communities (Tian *et al*., 2008). Steganography, also known as information hiding, is an rapidly developing research area, which including many applications and concepts, such as digital watermarking used for the copyright protection for digital multimedia arts, digital fingerprinting for the authentication and content-based retrieving of digital multimedia and etc (Bassia *et al*., 2001). Unlike the traditional cryptography technique, whose purpose is to hide the content of secret message being transmitted between communicating entities, the main goal of steganography is to hide not only the content but also the very existence of the ongoing communication of secret messages. Thus, through steganography, the adversary even doesn't know that the secret message is being exchanged, not to mention to extract the secret messages or maliciously obstruct the transmission channel. In practical implementation, the cryptography and steganography are often combined together to make the covert communication system more secure. Many audio (or speech) watermarking and steganography algorithms appropriate for the covert communication application have been developed in these years. For the embedding capacity (or payload) and the computation complexity consideration, most of the practical realization of the covert communication system is based on the Least Significant Bit (LSB) modification method (Gopalan, 2003; Xiong and Ming, 2006; Huang *et al*., 2008; Tian *et al*., 2008). A method of embedding a secret audio message in a cover utterance for secure communication is presented by Gopalan (2003). The secret audio message is first compressed and encrypted to improve the security and then one bit in each of the samples of a given cover utterance is modulated by the processed secret message data and a key. The same key is used to retrieve the embedded bits in the receiver part. Different embedding positions and the influence to the quality of the covert utterance signal are evaluated. The spread spectrum technique is also applied to the processed secret data and the effect to the security and integrity is evaluated by experiment. An audio watermarking for covert communication in wavelet transform domain and applying the chaotic technique is proposed by Xiong and Ming (2006). The advantage of this algorithm is that it uses the embedded synchronization data to search the watermark location, so as to be robust to some common attacks such as resampling and cropping. Problems of covert communication via VoIP are studied deeply and two implementations are reported, one is the Session Initiation Protocol (SIP) based User Agent (UA) Huang *et al*., 2008; Tian *et al*., 2008). Which can adaptively embed some secret message into the speech carrier signal with good efficiency, the other is Stega-Talk which is realized based on the covert communication model proposed in (Tian *et al*., 2008). These implementations are designed properly and have solved problems induced by the

practical limitations such as the security of secret messages and real-time performance requirement of the VoIP platform. The robust audio watermarking technique based on spread spectrum technology is studied thoroughly (Tavakoli *et al*., 2006; Kirdvski and Malvar, 2001). The watermark is robust against many telephone channel attacks such as Addition of White Gaussian Noise (AWGN), low pass filtering, A/D and D/A conversion, A-law and ì-law conversion and Time Scale Modification (TSM), etc. But the drawbacks of this Spread Spectrum based covert communication method are its huge computational complexity and the complex and expensive terminal. These drawbacks cause the system is unfeasible and non-prevalent and is not adapt to the realization of a real-time covert communication system.

In this study, a novel realization of cover communication system using VQ-based information hiding algorithm in PSTN is presented. The simple encryption and the structure of to-be-embedded secret messages by Tian *et al*. (2008) are adopted to provide effective short-term protection and low latency for real-time utterance through PSTN service. Furthermore, an effective VQ-based information hiding algorithm is described to achieve the embedding and extraction of the secret data. This method is operated in the speech coding and decoding procedure. It is more secure and can provide higher payload with a low degradation of the speech quality. The ITU-T G.729a speech codec (or vocoder) is adopted in StegoPhone, which is our software platform for study covert communication via PSTN. The characteristic of the information hiding algorithm presented in this paper makes the covert transmission speed to be adjustable. The experimental results demonstrate that our method introduces negligible distortions to the speech utterance signal and well satisfies the real-time and secure requirements of the covert communication system via PSTN.

VECTOR QUANTIZATION AND G.729A SPEECH CODEC

Vector quantization: Vector quantization is an effective lossy compression method with a high compression ratio and a simple table lookup decoder. A k-dimensional vector quantizer Q of size N is a mapping from the k-dimensional Euclidean space R^k into a finite set (or codebook) $C = \{c_0, c_1, ... c_{N-1}\}$ where $c_i \epsilon R_k$ is called a codeword and N is the codebook size. The codebook is often generated offline by the LBG algorithm (Linde *et al*., 1980) from a training set. The signal to be coded are first divided into vectors and then encoded by the trained codebook. For each k-dimensional input vector x, we can find its nearest codeword c_i under a certain distance metric as in the following formula:

$$d(x,c_i) = \min_{0 \le j \le N-1} d(x,c_j) \quad (1)$$

where, $d(x, c_j)$ is the distortion between the input vector x and the codeword c_j and it can be calculated as follows:

$$d(x,c_j) = \sum_{l=0}^{k-1} (x_l - c_{jl})^2 \quad (2)$$

Then, the corresponding index i is transmitted over the channel to the decoder. The decoder holds an exact copy of the same codebook. For each index i, the decoder only performs a simple table lookup operation to obtain I and then uses it to reconstruct the input vector x. So, lossy compression is achieved by substituting a codeword for the input vector and transmitting or storing only the index of the codeword rather than the codeword itself.

G.729a speech codec: The ITU-T G.729a recommendation contains the description of an algorithm for the coding of speech signals at 8 kbps using Conjugate-Structure Algebraic-Code Excited Linear Prediction (CS-ACELP). The CS-ACELP coder is fed with a digital signal resulting from telephone bandwidth filtering (Recommendation G.712) of an analog signal sampled at 8 kHz, followed by conversion to 16-bit linear PCM for input to the encoder. The output of the decoder is converted back into analog signal by similar means. The input signal is high-pass filtered and scaled in the pre-processing block. The pre-processed signal serves as the input signal for all subsequent analysis. LP analysis is done once per 10 msec frame to compute the LP filter coefficients. These coefficients are converted to Line Spectrum Pairs (LSP) and quantized using predictive two-stage vector quantization with 18 bits. The excitation signal is chosen by using an analysis-by-synthesis search procedure in which the error between the original and reconstructed speech is minimized according to a perceptually weighted distortion measure. This is done by filtering the error signal with a perceptual weighting filter, whose coefficients are derived from the un-quantized LP filter. The amount of perceptual weighting is made adaptive to improve the performance for input signals with a flat frequency-response (ITU-T Group, 1996).

During the decoding process, the parameter's indices are extracted from the received bit-stream. These indices are decoded to obtain the coder parameters corresponding to a 10 msec speech frame. These parameters are the LSP coefficients, the two fractional

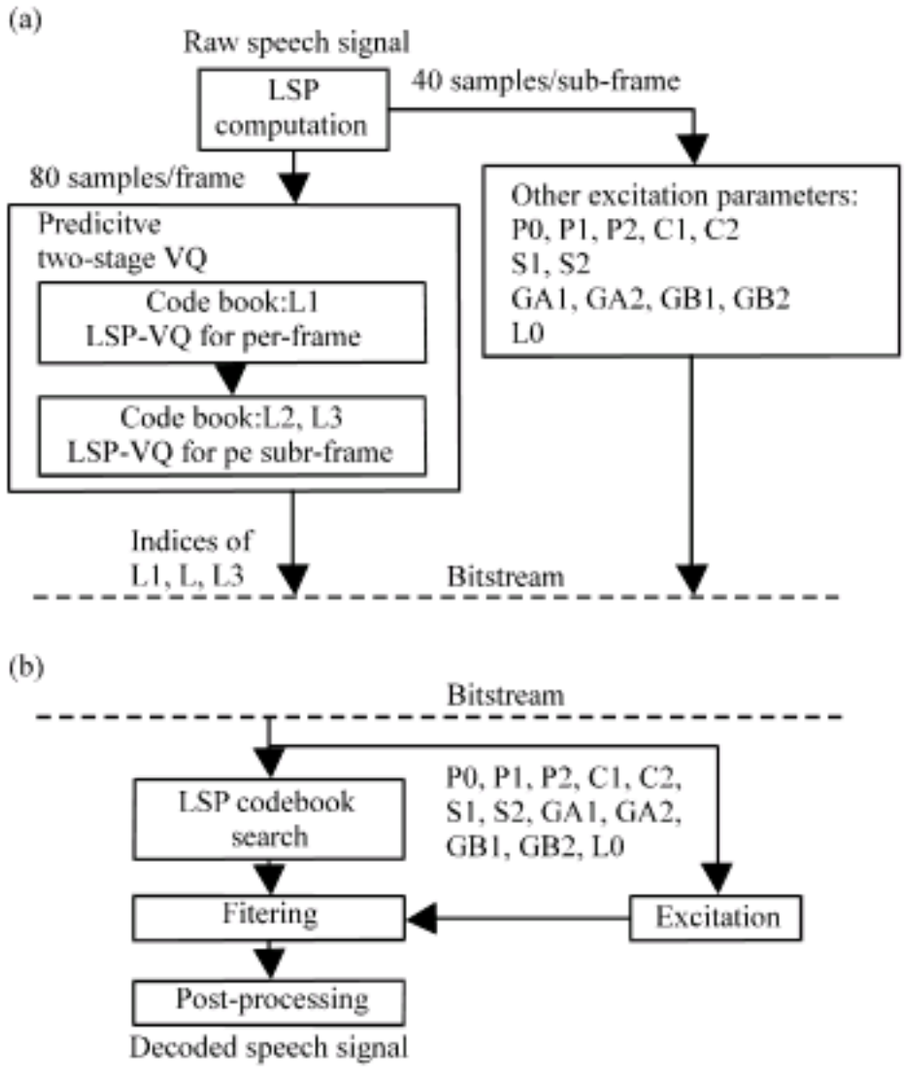

Fig. 1: G.729a vocoder scheme, (a) G. 729a encoder and (b) G. 729a decoder

pitch delays, the two fixed-codebook vectors and the two sets of adaptive and fixed-codebook gains. The LSP coefficients are interpolated and converted to LP filter coefficients for each sub-frame. Then, for each 5 ms sub-frame, the excitation is constructed by adding the adaptive and fixed-codebook vectors scaled by their respective gains and then the speech is reconstructed by filtering the excitation through the LP synthesis filter. At last, the reconstructed speech signal is passed through a post-processing stage, which includes an adaptive post-filter based on the long-term and short-term synthesis filters, followed by a high-pass filter and scaling operation.

The encoding and decoding procedure are shown in Fig. 1 (Sakai and Komatsu, 2004).

THE VQ-BASED INFORMATION HIDING ALGORITHM

To embed the watermark bits into the G.729a compressed speech bits-stream, a kind of index-constrained watermarking method (Lu *et al*., 2003) is used during the predictive two-stage vector quantization procedure of the LSP coefficients. Because it is the two-stage vector quantization and each frame speech signals is first quantization by a 10 dimension codebook, then each sub-frame's LSP residual signal quantized by a 5-dimension codebook. The embedding process for each

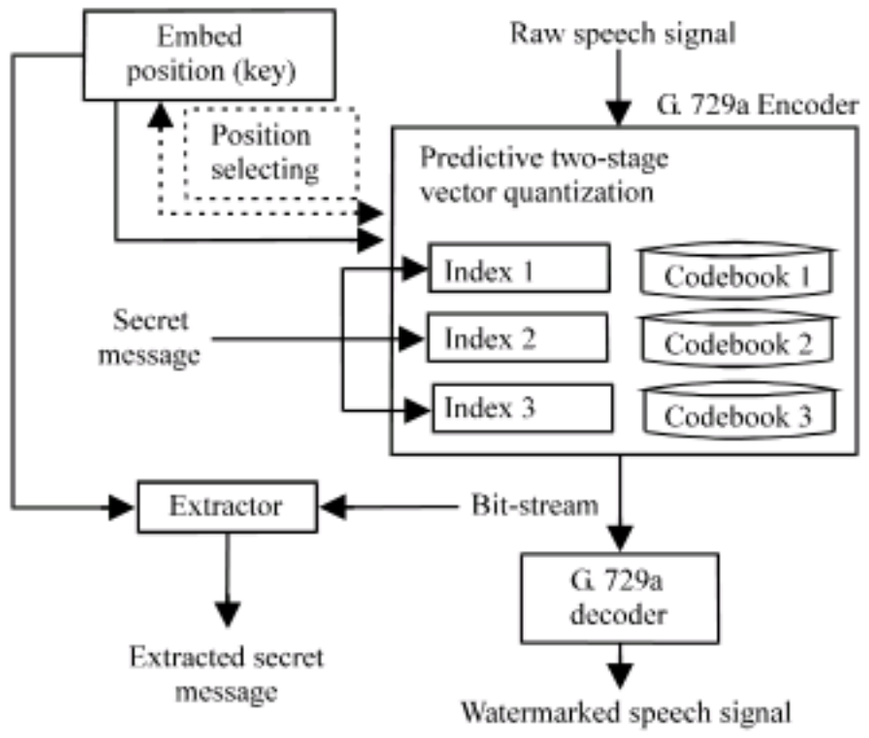

Fig. 2: The index-constrained information hiding in G.729a vocoder

secret message bit can be achieved by searching the best matched codeword for each input LSP and LSP residual vector under the constraints that the randomly selected bits of the indices are consistent with the secret message bits to be embedded. It is obvious that at least 1 bits of secret message can be embedded into each speech frame. For the purpose of embedding more information and keeping the covert speech quality, the embedding position is selected adaptively maintaining the segmental SNR in a predefined range.

The embedding position as a key is transmitted to the receiver through a security channel. The framework of this information hiding scheme is show in Fig. 2.

During the watermark embedding process, the G.729a encoder searches for the codeword that provides the minimum distortion between the input LSP (also residual) vector and the reconstructed vector within the constraint of the index. The position selecting block in Fig. 2 embraces the G.729a decoder and it can select the embedding position according to predefined quality requirements (the segmental SNR range). Very close reconstruction vector may be obtained under the constraint and the position selecting block may fulfill the expected tradeoff between the quality and the payload.

This scheme is not like the method proposed by Liu *et al*. (2008) which substitute the perceptually unimportant bits in the bitstream. After the substitution, it only has very small probability that the changed codeword (reconstruction vector) best matches the input vector. It can be better understood by Fig. 3. The input vector v1 should be quantized as c1 if no watermark bits embedded, but using the perceptually unimportant bit substitution method, the input vector may be quantized as c3, c4, c5 and so on. The probability of quantized as c2 is

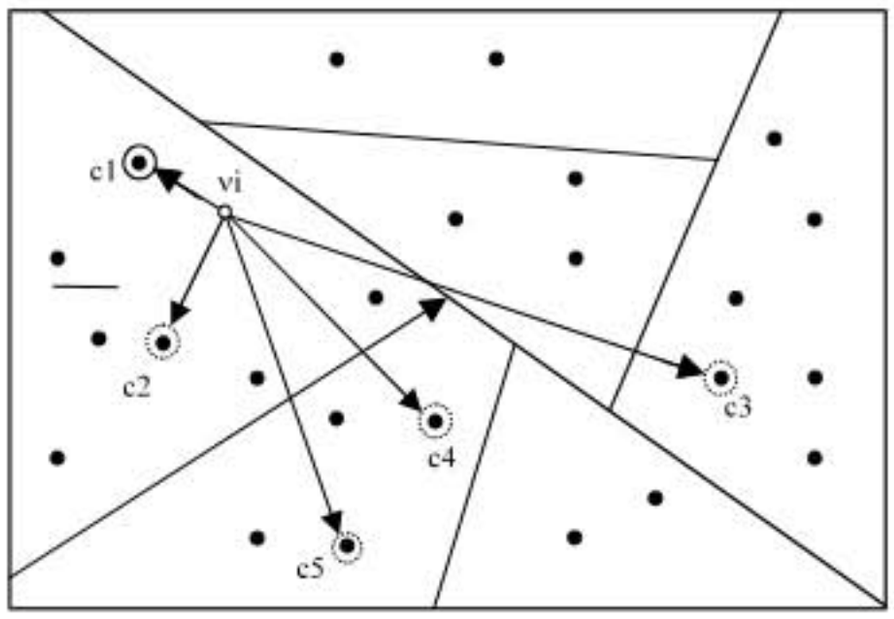

Fig. 3: Comparison of the proposed method and other method

very little. Because of the best match searching process of the vector quantization process, the c2 will be selected by using the method proposed by this study and this may minimum the distortion after secret information embedding.

REALIZATION OF THE STEGOPHONE SYSTEM

Here, the realization of stegophone system, the software platform to study the covert communication via PSTN, is detailedly described. Firstly, the scheme of the whole system is shown in Fig. 4. In this framework, the personal computer is connected to the 56 K modem through the serial port and the 56 K modem is connected to the PSTN network through a phone line. The stegophone software is running on each of the personal computers of the users. The speech signal is coded by using the G.729a vocoder and during this process, the preprocessed secret binary image message is embedded into the bitsream of the speech vocoder using the proposed VQ-based information hiding algorithm. Then, the bitsream is transmitted to the receiver by using the Reliable COM Communication (RCC) protocol, which can achieve reliable data communication through the 56 K modem and the serial port. The receiver extracted the secret binary image message using the received real-time speech bitsream. Through these procedures, the secret binary image messages are securely and snugly transmitted between the system users.

For the preprocessing and the restituting of the secret binary image messages, the method proposed by Tian *et al*. (2008) is applied in our system. It can achieve a good tradeoff between the effective short-term protection for secret message and real-time performance for the calling application via PSTN. Moreover, the structure of the embedded messages designed by

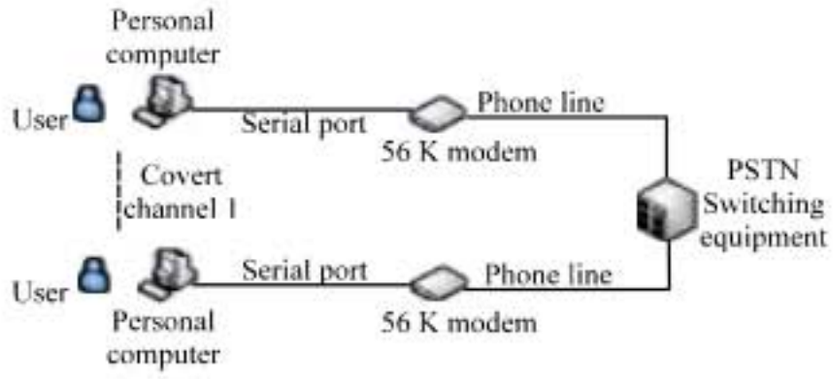

Fig. 4: Scheme of the stegophone system.

Tian *et al*. (2008), which can offer flexible message length and avoidance of both the extraction attack and the deceptive attack, is also adopted in our final realization.

The stegophone software is developed by using the Microsoft Visual C++ 6.0. The speaker identification component is also implemented in this software for the purpose of avoiding its misuse by unauthenticated users. The User Interface (UI) of the speaker identification component is shown in Fig. 5. The user name, password and three pieces of voices of the specified sentence are required to accomplish the feature training and user adding function. Once the user information is added into the user database, he can use the software to achieve covert communication by logon it.

After the hardware of the system is connected correctly, the working procedure of this software is described as follows: Firstly, the users who will accomplish covert communication open the stegophone software and the user logon interface will show up as in Fig. 6. By providing the correct user name and password and pass the speaker identification successfully, the main interface of the stegophone software will show as in Fig. 7. Then, the user should open the parameter setup dialog to specify the embedding key (for the secret binary image message preprocessing), the position key (for the embedding position selection), the speech codec (only G.729a vocoder available) and the quality measures of the speech and secret message (Fig. 8). After doing these, the user can open the secret binary image and preprocess it, then dial the number of the counterpart. The software will turn into covert communication process until one user submits a hang up operation. Then the users can extract the secret binary image message respectively. By these steps, one covert communication procedure is accomplished. And the final interface of the stegophone software is shown in Fig. 9. The working flow of the stegophone system is shown in Fig. 10.

The effectiveness of the stegophone covert communication system is evaluated by two aspects: the transmitting data rate of the covert message signal and the quality degradation of the speech signal. Both the AN4 database (CMU Robust Speech Recognition Group,

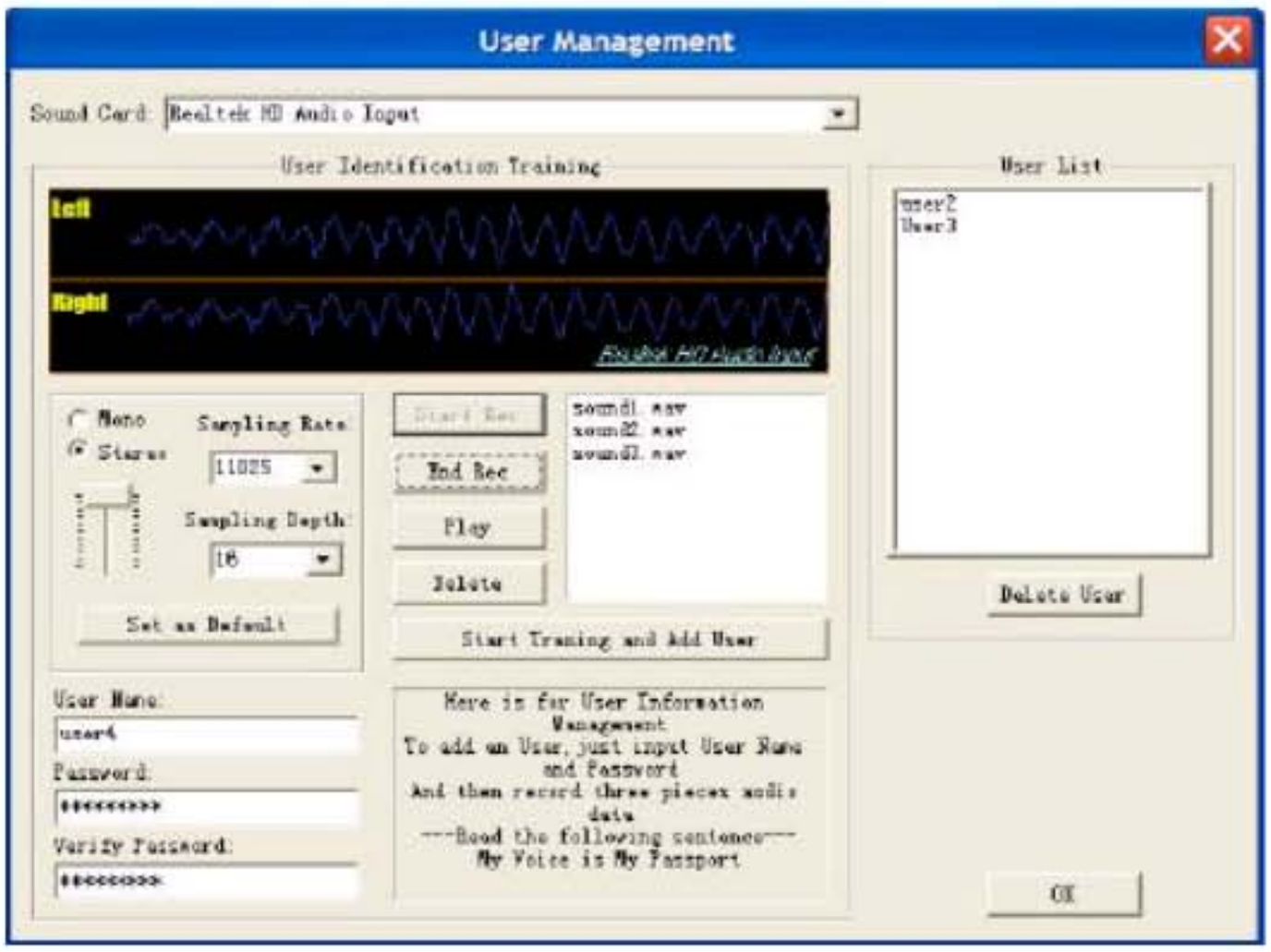

Fig. 5: The user management component

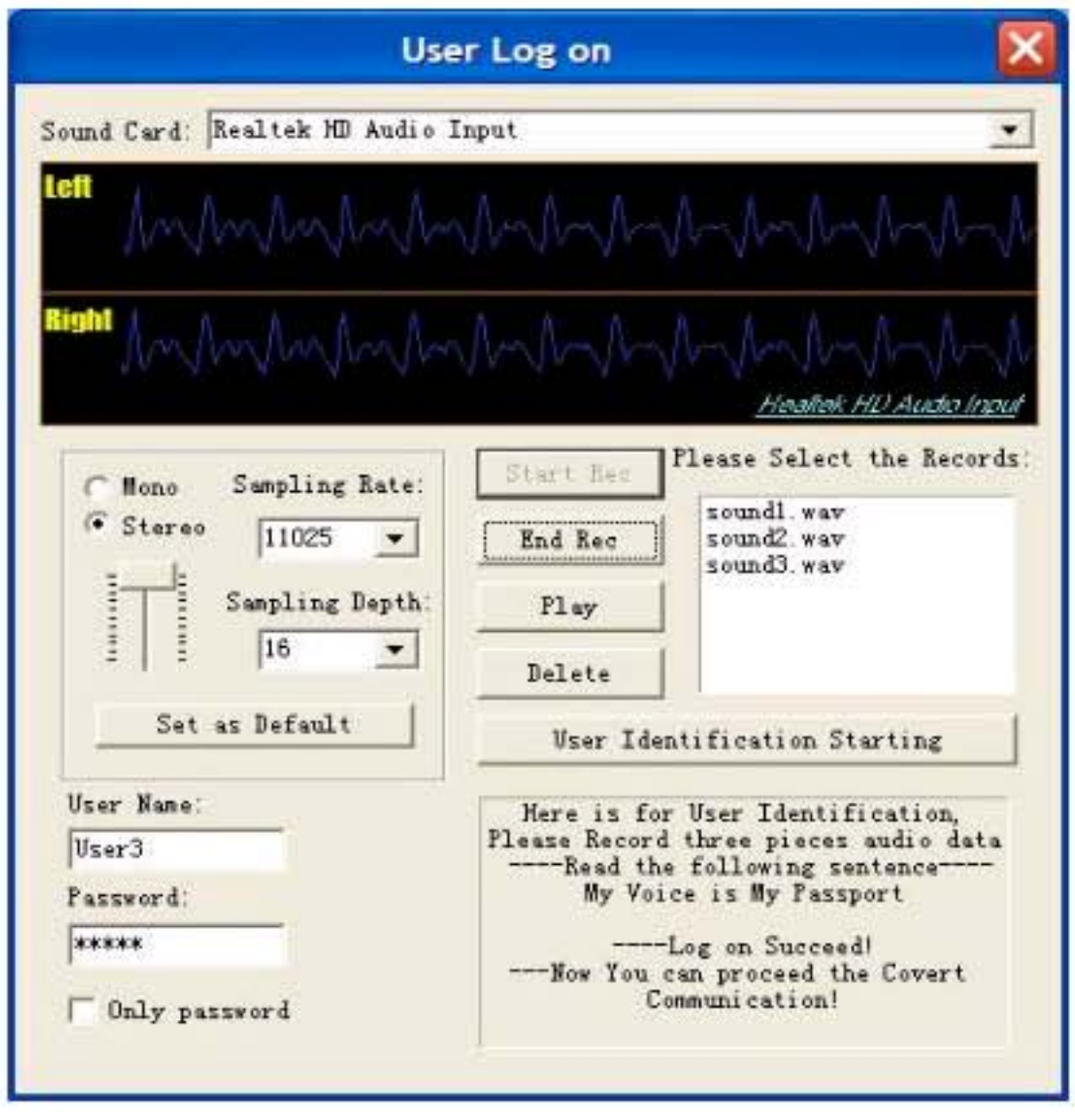

Fig. 6: The user logon component

1991) (which consists of 1078 sentences spoken by male and female persons) and the real-time calling utterance recordings are applied to this evaluation. And the results of the experiment are as follows.

Transmitting data rate: In our experiments for the transmitting data rate, at least 3 bits are embedded in each speech frame during the predictive two-stage vector quantization procedure. All the segSNRs are higher than

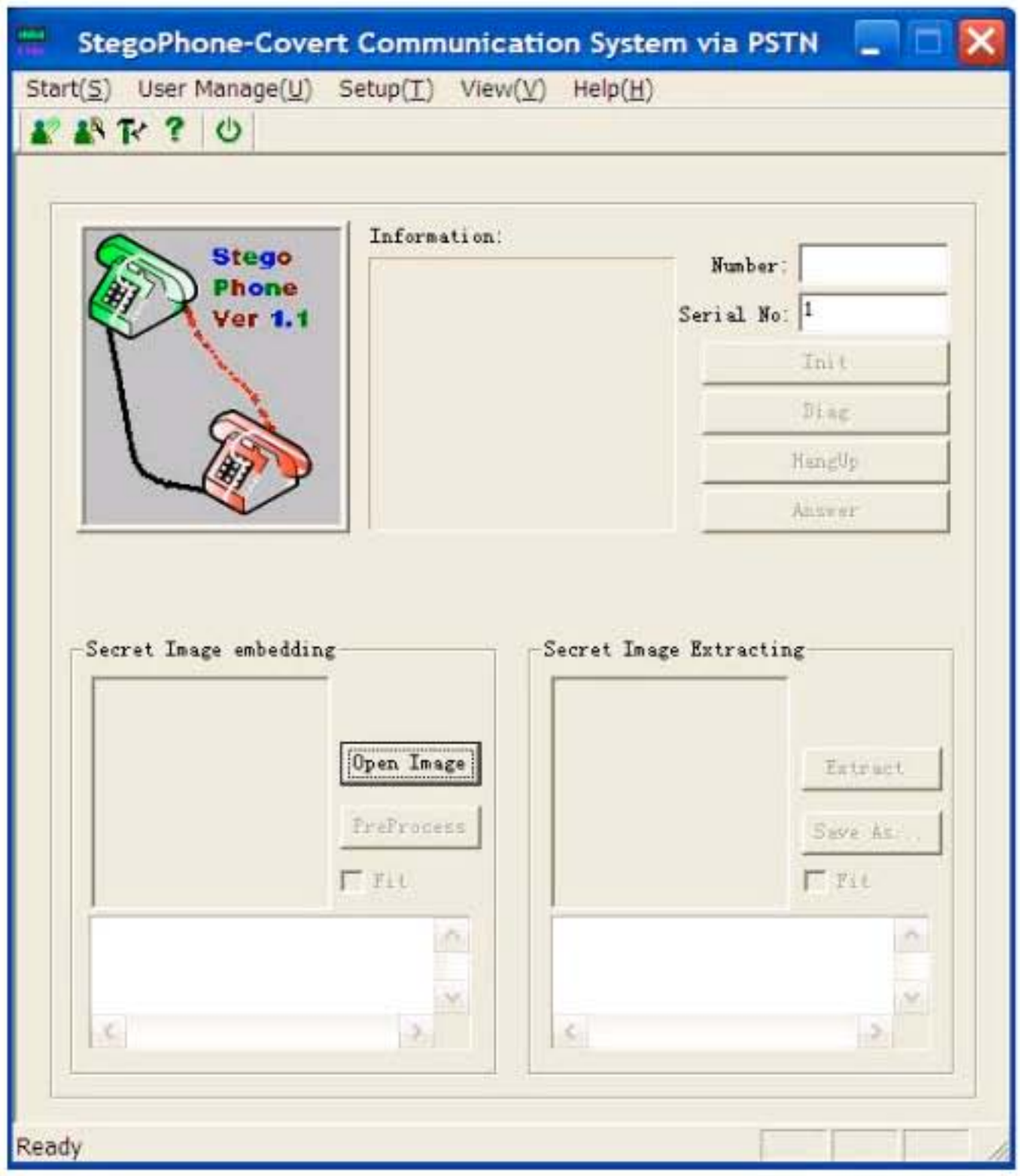

Fig. 7: The main interface of the stegophone software

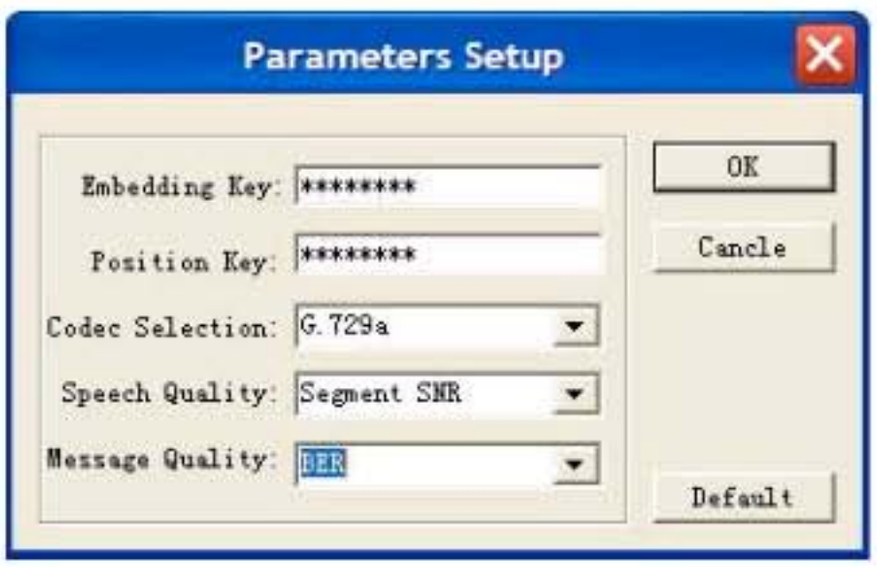

Fig. 8: The parameter setup component

19.30. Thus the Embedding Rate (ER), which is the ratio of the number of the embedded data bits and te bitstream size of one speech frame, could be given as:

$$RE = 3/80 = 3.75\%$$

Because of the additional information introduced during the preprocessing procedure for each covert communication process, the transmitting data rate (TR) will be a little lower than the ER, but still higher than 3.00%. Note that this is the smallest transmitting data rate with only 3 bits embedded in one frame and the TR will be higher if embed more bits in one frame. Even so, the transmitting data rate is higher than the perceptually unimportant bits substitution method (Liu *et al*., 2008) and some existing information hiding approaches referring to the speech coding stage.

Speech quality evaluation: Like the assessment method by Liu *et al.* (2008), the speech quality degradation after information hiding is evaluated by:

- Waveform compare
- Objective distortion measure
- Subjective listening test

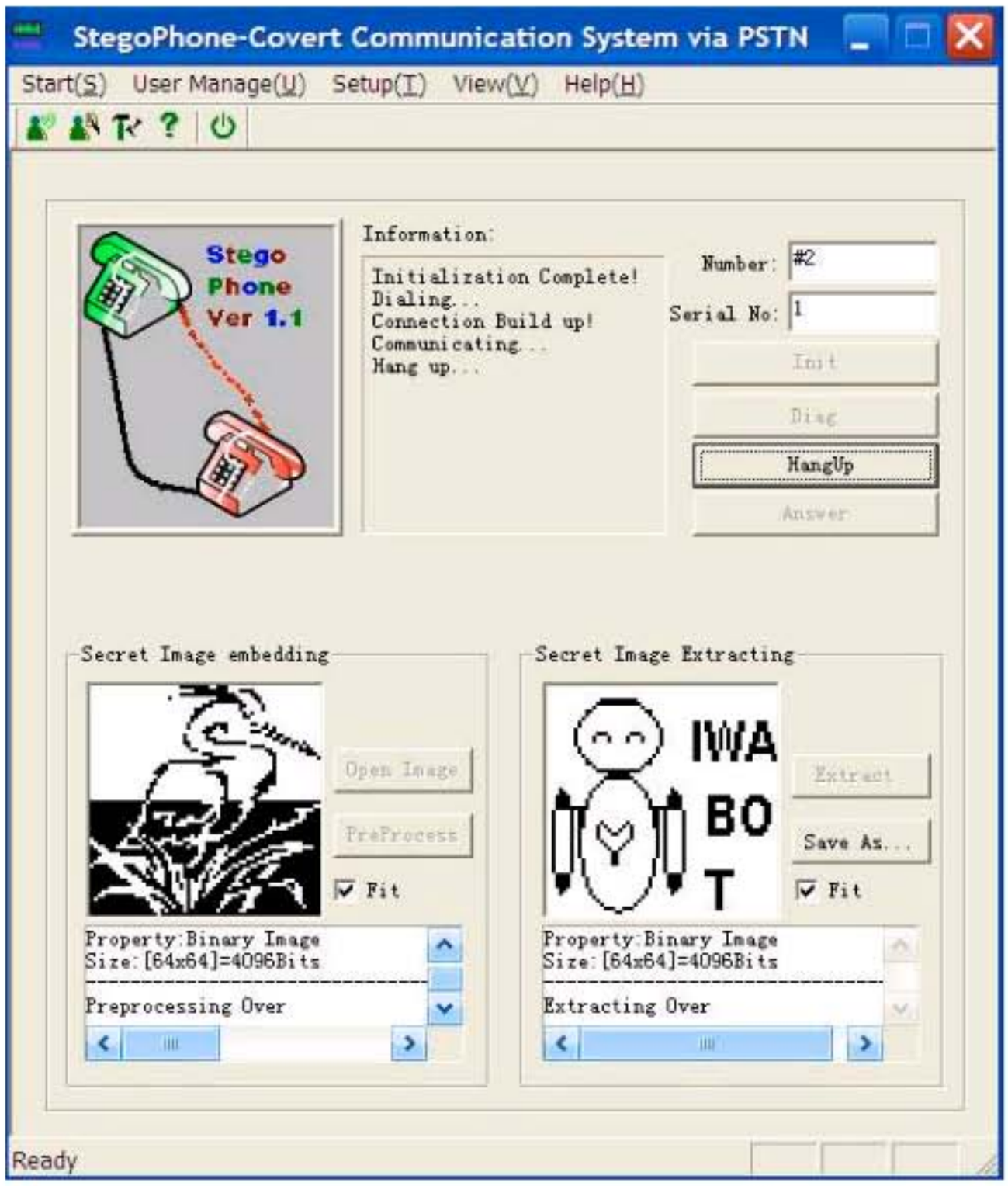

Fig. 9: The interface of the Stegophone after one covert communication procedure

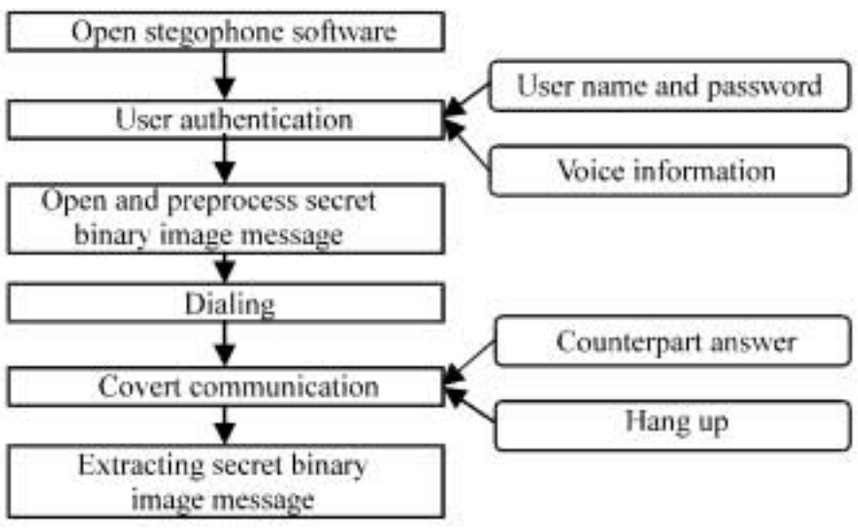

Fig. 10: The working flow of the stegophone system

The waveform of an example speech piece is shown in Fig. 11. The spectrogram of these speech segments are shown in Fig. 12. Comparing these figures, we can find that the signal of the covert speech and the speech signal decoded from the clear bitstream are nearly the same.

Table 1: SegSNRs of different embedding bits

	Average segSNR(dB)	
Payload (bits/frame)	Female speech signals	Male speech signals
3 bits	19.63	19.45
4 bits	19.10	19.03
5 bits	18.20	18.34
6 bits	14.02	14.17

The objective test method used in this study is the segmental SNR (segSNR) which is a better measure than the SNR. The segSNR is calculated for every 10 msec, non-overlapping speech segment. The average segSNRs of all the speech signals in AN4 database under different embedding rate is shown in Table 1. It can be seen from the table that even 6 bits are embedded for each speech frames, the average segSNR is still more than 14.00 dB.

Though, segSNR is a good objective quality evaluation measure, the subjective listening test also should be done to assess the quality of speech signals. The test aggregate consists of 50 speech clips randomly

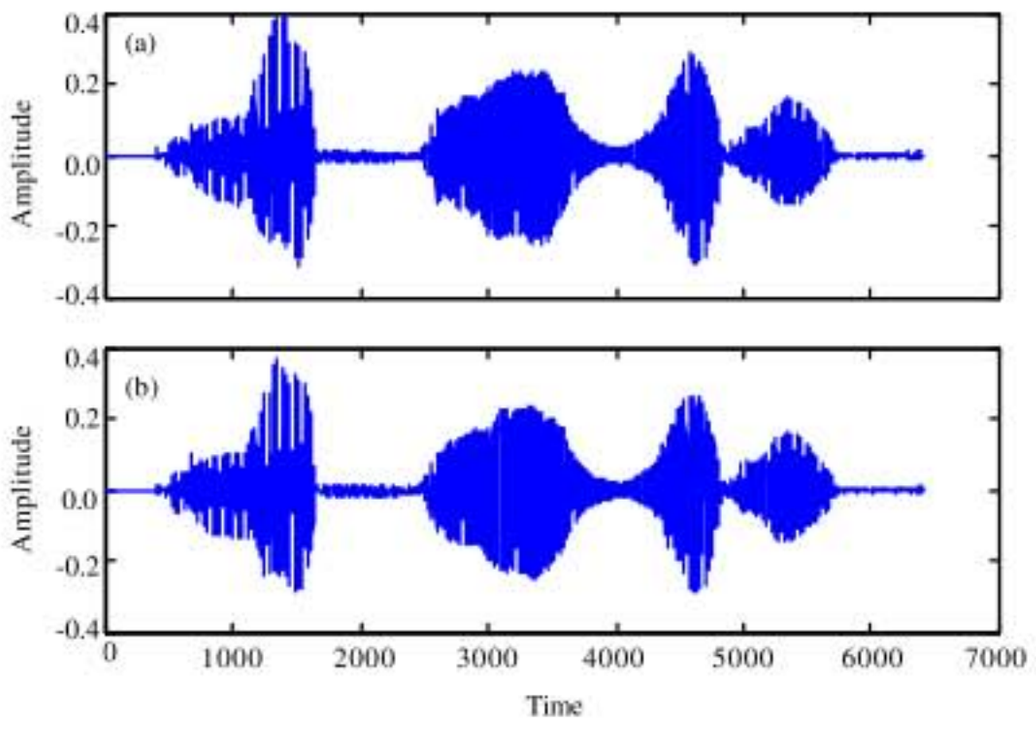

Fig. 11: Wave forms of the clear and covert speech signals, (a) speech signal after G. 729a vocoder and (b) speech signal after watermarking

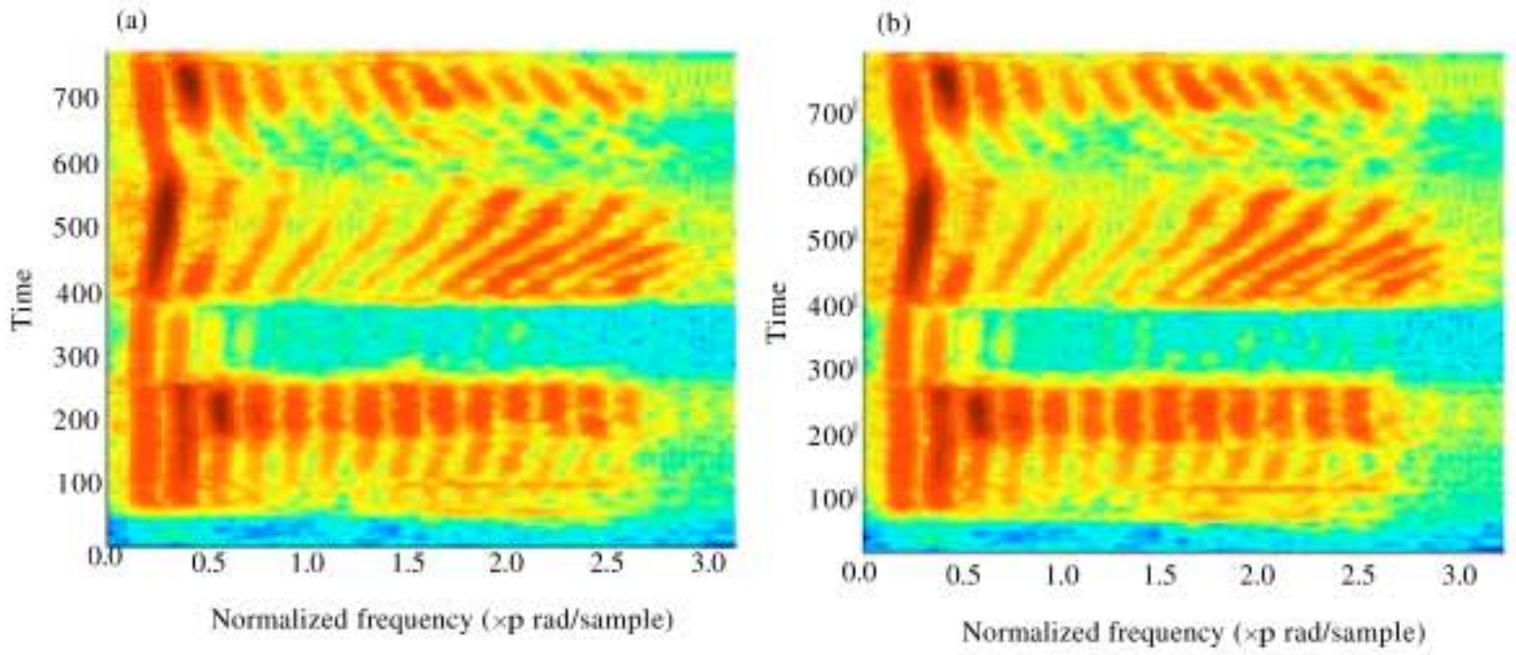

Fig. 12: Spectrogram of the speech signal after G.729a codec and the covert speech signal, (a) spectrogram of speech signal after G. 729a vocoder and (b) spectorgram of the covert speech signal

selected from the database and for all these speech clips, the covert speech signals are generated by using the proposed information hiding method. These testing materials are presented to 3 different listeners, all using the same headphones and being in the same controlled environment. There will be 300 different answers for the listening test. Then randomly select other 50 speech clips for the test and these steps are repeated about 3 times. The result is that about 50% (453 out of 900) of the answers are wrong, which means that the listeners cannot distinguish whether the speech signals are embedded with secret information or not.

CONCLUSION

An Implementation of a covert communication system based on information hiding and the PSTN is demonstrated in this study. The system can offer good security of the secret binary image message and the real-time performance that is very important for the telephone calling service. A simple and effective encryption method for the secret message is adopted prior to the embedding process to fulfill the requirements. Furthermore, an information hiding algorithm based on vector quantization is proposed for the secret message embedding and extracting and the advantage of this algorithm is that it can provide higher transmitting data rate with a lower degradation of the covert speech quality. The effectiveness of this algorithm is further justified by using some experimental results. At last, the detailed implementation of the stegophone system and its working principle are discussed.

REFERENCES

Bassia, P., I. Pitas and N. Nikolaidis, 2001. Robust audio watermarking in time domain. IEEE Trans. Multimedia, 3: 232-241.

CMU Robust Speech Recognition Group, 1991. AN4 database. http://www.speech.cs.cmu.edu/databases/an4/.

Danezis, G., 2005. Covert communications despite traffic data retention. Technical Report, ESAT, University of Leuven, January 2005.

Diez-Del-Rio, L., S. Moreno-Perez, R. Sarmiento, J. Parera, M. Veiga-Perez and R. Garcia-Gomez, 1994. Secure speech and data communication over the public switching telephone network. Proc. Int. Con. Acoustics Speech Signal Process. IEEE, 2: 425-428.

Gopalan, K., 2003. Audio steganography using bit modification. Proceedings of the International Conference on Acoustics, Speech and Signal Processing, Apr. 6-10, IEEE Computer Society, Washington, DC. USA., pp: 412-424.

Huang, Y., B. Xiao and H. Xiao, 2008. Implementation of covert communication based on steganography. Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Aug. 15-17, IEEE Computer Society, China, pp: 1512-1515.

ITU-T Group, 1996. Coding of speech at 8kbit/s using conjugate-structure algrebric-code-excited linear-prediction (CS-ACELP). Recommendation G.729.

Kirovski, D. and H. Malvar, 2001. Robust Covert Communication Over a Public Audio Channel Using Spread Spectrum. In: Lecture Notes in Computer Science: Information Hiding, Moskowitz, I.S. (Ed.). Springer, Berlin/Heidelberg, pp: 354-368.

Linde, Y., A. Buzo and R.M. Gray, 1980. An algorithm for vector quantizer design. IEEE Trans. Commu., 28: 84-95.

Liu, L., M. Li, Q. Li and Y. Liang, 2008. Perceptually transparent information hiding in G.729 bitstream. Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Aug. 15-17, IEEE Computer Society, Washington, DC. USA., pp: 406-409.

Lu Z.M., C.H. Liu and D.G. Xu, 2003. Semi-fragile image watermarking method based on index constrained vector quantization. Electronics Lett., 39: 35-36.

Narayanan, R.M. and J. Chuang, 2007. Covert communications using heterodyne correlation random noise signals. Electronics Lett., 43: 1211-1211.

Orr, R., C. Pike, M. Bates, M. Tzannes and S. Sandberg, 1993. Covert communications employing wavelet technology. 27th Asilomar Conf. Signals Syst. Comput., 1: 523-527.

Radhakrishnan, R., K. Shanmugasundaram and N. Memon, 2002. Data masking: A secure-covert channel paradigm. Proceedings of the IEEE Workshop on Multimedia Signal Processing, Dec. 9-11, IEEE Computer Society, Washington, DC. USA., pp: 339-342.

Roy, A. and J.F. Doherty, 2009. Covert communications using empirical mode decomposition. Proceedings of the Sarnoff Symposium, Princeton, New Jersey, Mar. 30-Apr. 1, IEEE Computer Society, Washington, DC. USA., pp: 1-5.

Sakai, T. and N. Komatsu, 2004. Digital watermarking based on process of speech production. Proc. Security Steganogr. Watermark. Multimed. Contents VI, 5306: 127-138.

Tao, Y. and L.O. Chua, 1996. Secure communication via chaotic parameter modulation. IEEE Trans. Circ. Syst. I: Fundam. Theor. Appli., 43: 817-819.

Tavakoli, E., B.V. Vahdat, M.B. Shamsollahi and R. Sameni, 2006. Audio watermarking for covert communication through telephone system. Proceedings of the IEEE International Symposium on Signal Processing and Information Technology, Aug. 27-30, Vancouver, BC, Canada, pp: 955-959.

Tian, H., K. Zhou, Y. Huang, D. Feng and J. Liu, 2008. A covert communication model based on least significant bits steganography in voice over IP. Proceedings of the International Conference for Young Computer Scientists, China, Nov. 18-21, IEEE Computer Society, Washington, DC. USA., pp: 647-652.

Xiong, Y. and Z.X. Ming, 2006. Covert communication audio watermarking algorithm based on LSB. Proceedings of the International Conference on Communication Technology, China, Nov. 27-30, IEEE Computer Society, Washington, DC. USA., pp: 1-4.