**SERBIAN JOURNAL OF ELECTRICAL ENGINEERING**
**Vol. 14, No. 3, October 2017, 313-321**

**UDC: 004.623:347.7** **DOI: https://doi.org/10.2298/SJEE1703313N**

# Steganography Method for the G.711 Channel

**Anton Nikitin[1], Sergey Makov[1], Sergey Klimenko[1]**

**Abstract:** This paper deals with an improved algorithm developed for the transmission of the hidden information in the G.711 channel [1]. The subject of the research is a method of improving characteristics of a steganography system by means of using specially developed codes. Also analysis of transmission characteristics of the hidden information depending on a number of bits of the original data replaced at a given threshold was conducted.

**Keywords:** Steganography, Hidden data transmit, Data rate, G.711.

## 1 Introduction

Information security is an actual problem of telecommunication technologies and it stimulates the search of new methods protecting information. This topic is relevant for the copyright protection to protect broadcast of confidential, production or government information intended for special services, diplomats, brokers,.

Steganography is a way to broadcast hidden data in a digital stream. Methods of steganography allow to covert transmitted data, and also to solve the tasks of noise-resistant authentication, protect information from unauthorized copying, monitor the distribution of information over communication networks, and searching for information in multimedia databases: text, image, audio files, etc. can be used as containers for inserting secret messages?

In the papers of authors: Naofumi Aoki [2], Fatiha Djebbar [3], Wojciech Mazurczyk [4], Fatiha Djebbar [5], describe the methods and applications of steganography.

General model of the stegosystem is shown on the Fig. 1.

There are several methods used in steganography, such as:

### 1.1 LACK (Lost Audio Packages Steganography) method

LACK (Lost Audio Packages Steganography) is a method of hiding messages during conversations using IP telephony. It is based on the use of packages that are delayed or intentionally damaged and ignored by the receiver

[1]Institute in Shakhty of DSTU, Shevchenko str. 147, Shakhty, Rostov region, 346500, Russia;
E-mails: chaosvarp14@rambler.ru; makovs@rambler.ru; klimenko.sg@gmail.com

or hiding information in header fields that are not used. The Method works as follows. The transmitter selects one of the voice stream packages and its payload is replaced by bits of a secret message − a steganogram that is embedded in the package. Then the selected package is intentionally delayed. If the recipient does not know about the procedure of sending a secret message, then the delayed package is discarded. However, if the recipient knows about the hidden connection, then he removes the RTP packages and retrieves the hidden information.

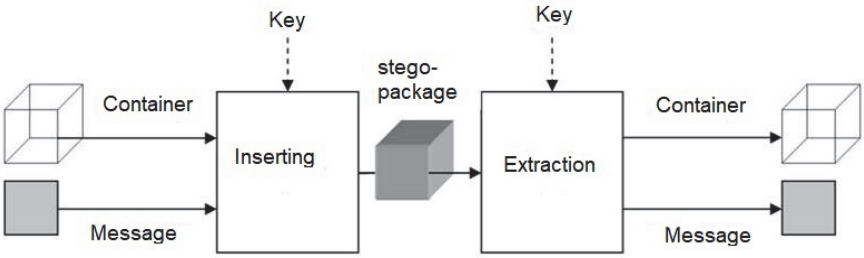


**Fig. 1** – *A General structure of steganography system.*

Advantage:

– transmission of the information without changing it from the sender to the recipient;

– easy to implement;

– has good bandwidth.

Disadvantage:

– deterioration of communication quality.

### 1.2 The LSB method

The least significant bit (LSB is the Least Significant Bit) carries within the least information. A human is usually unable to notice a change in this bit. This part of signal can be used to insert information. The essence of this method is to replace the last bits in the container (images, audio or video) with bits of the hidden message.

The difference between empty and filled containers should not be perceived by human sense organs.

The method is effective when the replacement of the least significant bit does not entail a significant deterioration in quality.

Advantages:

– simple and relatively large amount of inserted data;

– a size of the container file remains unchanged;

– the ability to change the ability to alter the throughput by changing the number of bits to be replaced.

Disadvantage:

– the average level of security.

### 1.3 Converting spectral characteristics of an audio signal (echo method, phase method)

Echo techniques are used in a digital audio system as they use non-uniform intervals between signal and its echo (time-delayed copies of the signal) for coding levels. This method allowing to insert data into a signal. When imposing a number of restrictions, the condition of information imperceptibility for human's senses is observed. The echo is characterized by the parameters: the initial amplitude, the degree of attenuation, the delay between the original signal and the echo. When a certain threshold is reached between the signal and the echo in a certain human ear, it ceases to distinguish between two signals and the echo is perceived as an additional resonance.

Advantages:

– high stealth message;

– stability of amplitude and frequency attacks;

– high speed of data broadcast.

Disadvantage:

– significant computing costs.

After the analysis the LSB method was chosen for the subsequent improvement of the hidden data transmission algorithm as the simplest method of modification.

## 2 Proposed Method

The LSB method replaces the least significant bits in the original signal to the bits of the hidden message. The more bits of the original signal are replaced, the greater risk of finding a hidden message. Therefore, it is necessary to take in to account the requirements of audio quality. If too many bits are replaced, the distortion will be noticeable. The detection of such hidden message is carried out according to the characteristics of frequency distribution for the lower bits of the digital signal samples. The purpose of the paper is to modify the method of transmitting hidden information for the G.711 channel, with the greatest amount of embedded secret information without the risk of detection information by a human ear.

Fig. 2 contains a block diagram.

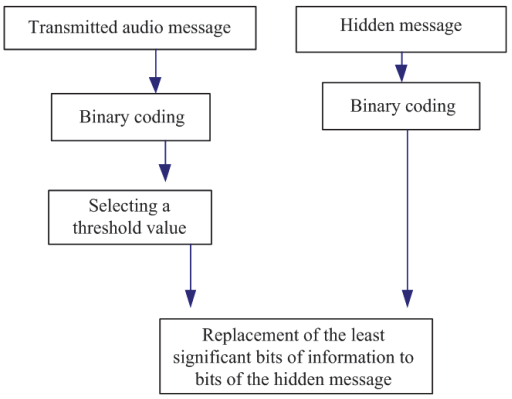


**Fig. 2** – *The Structure of LSB method.*

The transmitted audio message and the hidden message are binary encoded, determined by the number of bits of hidden information. It selects the number of the least significant bits in the digital package to replace them with the bits of the hidden message. The threshold value is selected. The original bits are replaced by the bits of hidden information. The block diagram is shown on the Fig. 2.

## 3 Proposed Method

### 3.1 Evaluation criteria

Methods for assessing the quality of the audio transmission system are mainly determined by the purpose of this system (speech, music, etc.). When transmitted through communication channels, speech is considered to be a random process, with characteristics to determine the parameters of the transmitted signal (dynamic range, spectral width, signal-to-noise ratio). All these parameters are measurable and can be accurately determined. However an audio signal is perceived by the human ear in accordance to psychophysical parameters of a human nature. To obtain a subjective evaluation of signal distortions, subjective statistical tests are carried out with the help of a group of experts [6].

Subjective quality assessments are based on the statistical processing of subjective quality assessments of a sufficiently large number of expert listeners.

There are also criteria for an objective evaluation of the sound signal.

When transmitting digital data over a channel with hidden information, there is always a possibility that the received data will differ from the original data, as it may contain errors. The error frequency occurrence when the received data can`t be used, is determined by the properties of the person's auditory

perception. Namely, the permissible probability of Pm errors should be set, which does not lead to noticeable distortions at the analog output.

There are also criteria for an objective evaluation of the sound signal.

Usually, the quality of the communication system is characterized by the ratio of the energy per information symbol to the one-way noise spectral power, i.e. signal to noise ratio (SNR):

$$h_m = \frac{E_b}{N_m}, \tag{1}$$

which is required to achieve a given error probability Pm. The decrease in SNR (at a given level Pm), is achieved due to channel coding, characterizes the energy gain of encoding.

The signal-to-noise ratio (SNR), which is one of the most common objective measures for estimating the noisiness of a speech signal, is given:

$$SNR = 10\log_{10}\left\{\frac{\sum_{n=0}^{M-1} s^2(n)}{\left(\sum_{n=0}^{M-1}\left(s(n)-\hat{s}(n)\right)^2\right)}\right\}, \tag{2}$$

where $s(n)$ and $\hat{s}(n)$ are selective values of the original and reconstructed speech signal, respectively. $M$ is the total number of samples within the speech signal.

This SNR is an integral measure of the speech restoration quality.

The peak signal-to-noise ratio is denoted by the abbreviation PSNR and it is an engineering term for the relationship between the maximum of the possible signal value and the noise power distorting the signal values. Since many signals have a wide dynamic range, the PSNR is usually measured in a logarithmic scale in decibels.

The easiest way to determine it is through the mean-square error or MSE.

It is calculated by the formula:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left|I(i,j)-K(i,j)\right|^2. \tag{3}$$

In this paper, this approach is chosen as one of the criteria for assessing the quality of the sound signal.

### 3.2 Experimental data

There were 4 samples of the sound signal (male voice (№1), female voice (№2), instrument record (№3), musical record (№4)) and corresponding sound signals, with recorded secret information embedded in one, two or three last bits of the audio signal with different threshold values.

Experts, in number of 5 people, in headphones, assessed the level of distortions audibility, depending on the number of replaced bits and the threshold value, on a five-point scale from 1 to 5, where 1 is “very bad” (high noisiness of the signal), and 5 is “excellent” (the sound signal with the hidden information does not differ from the original one).

According to the results of the survey, it was revealed that when comparing the original sample and the audio signal with the replacement of 1, 2, 3 last bits of information with 7, 3 threshold values, noisy signal is not noticeable for a human ear. When replacing one last bit of information at any threshold value, noisy signal is not noticeable either. At a threshold value of 0, the replacement of two or three last bits of information is characterized by poor noticeable noises.

**Table 1**

*The final average quality estimation of audio files changing.*

| Number of replaced bits at the threshold value | Number of audio file | | | |
|---|---|---|---|---|
| | №1 | №2 | №3 | №4 |
| One last bit, with a threshold value 0 | 5 | 5 | 5 | 5 |
| One last bit, with a threshold value 3 | 5 | 5 | 5 | 5 |
| One last bit, with a threshold value 7 | 5 | 5 | 5 | 5 |
| Two last bits, with a threshold value 0 | 4,6 | 4.6 | 4,2 | 4,6 |
| Two last bits, with a threshold value 3 | 5 | 5 | 4,8 | 4,8 |
| Two last bits, with a threshold value 7 | 5 | 5 | 5 | 5 |
| Three last bits, with a threshold value 0 | 4,2 | 4,4 | 4,2 | 4,4 |
| Three last bits, with a threshold value 3 | 4,6 | 4,6 | 4,6 | 4,6 |
| Three last bits, with a threshold value 7 | 4,8 | 4,8 | 4,8 | 4,8 |

To determine the possibility of detecting secret data, the original sound signals and signals changed by steganography, was studied

As a result of the analysis that was conducted in the Matlab environment, it was established that with the increase in the threshold value, the data transfer rate decreases. As the number of replaced bits increases, the data rate increases too. It is shown on the Figs. 3 and 4.

Partial loss of information is possible due to the development of the LSB digital steganography method. The more noisiness is the audio signal with hidden information, in contrast to the original ones, the greater is the mean squared error (MSE). This metric is dimensionless and insensitive to small changes in audio signals with hidden information. [7].

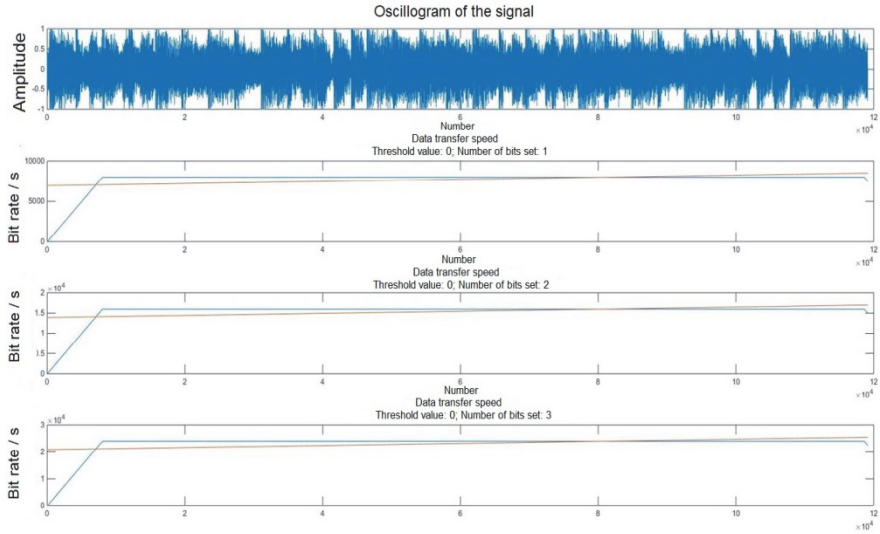


**Fig. 3** – *Changes in the data broadcast rate when one, two, three bits of information are replaced at a given threshold 0.*

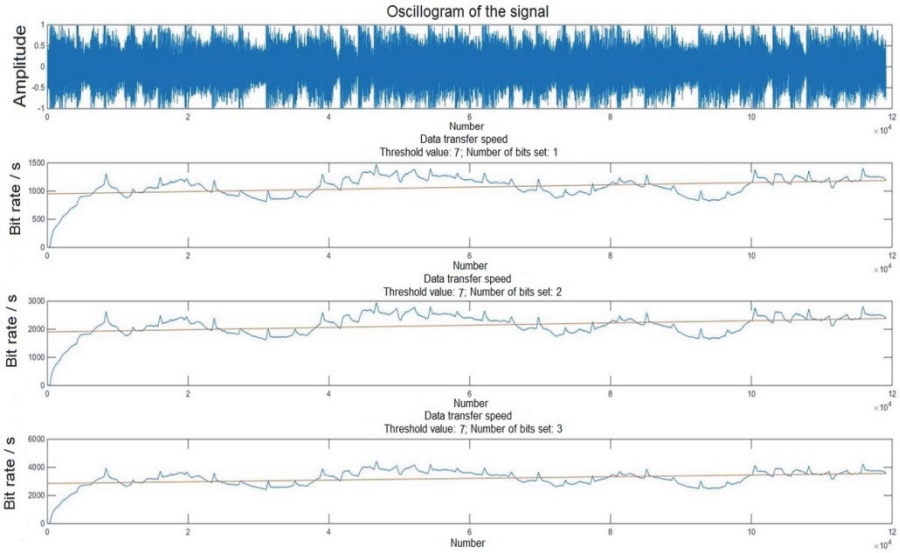


**Fig. 4** – *Changes in the data broadcast rate when one, two, three bits of information are replaced at a given threshold 7.*

For the study the criterion of the standard deviation, 4 audio files with different amount of built-in information and a different threshold value were selected.

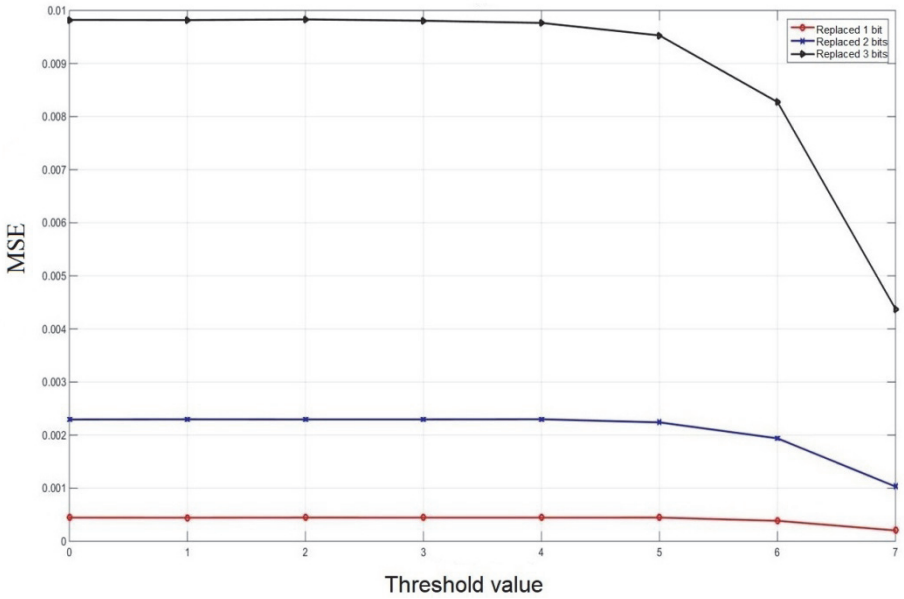


**Fig. 5** – The *MSE of the replacement of one, two, three bits.*

As a result of the analysis of the obtained data, one can conclude: with the increase in the threshold value, the data transfer rate decreases. As the number of replaced bits increases, the data rate increases

## 4 Conclusion

A program code was developed for the transmission of the hidden information in the G.711 channel, based on the LSB method. The proposed method was researched with a various threshold value and a different number of replaced least bits of information. In the research we have obtained objective and subjective qualitative assessments. The proposed method of replacing the original information with a hidden message allows to organize a reliable hidden information transmission channel, with the introduction of a large amount of hidden information, without the risk of detection.

## 5 Acknowledgement

This work was supported by Russian Ministry of Education and Science in frame of the Federal Program "Research and development on priority directions of scientific-technological complex of Russia Federation in 2014-2020" (contract № 14.577.21.0212 (RFMEFI57716X0212)).

# 6 References

[1] Pulse Code Modulation (PCM) of Voice Frequencies, ITU Recommendation G.711, 1988. Available at: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=911.

[2] N. Aoki: A Technique of Lossless Steganography for G. 711 Telephony Speech, International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin, China, 15-17 Aug. 2008, pp. 608 − 611.

[3] F. Djebbar, B. Ayad, H. Hamam, K.A. Meraim: A View on Latest Audio Steganography Techniques, International Conference on Innovations in Information Technology, Abu Dhabi, United Arab Emirates, 25-27 April 2011, pp. 409 − 414.

[4] W. Mazurczyk, P. Szaga, K. Szczypiorski: Using Transcoding for Hidden Communication in IP Telephony, Multimedia Tools and Applications, Vol. 70, No. 3, June 2014, pp. 2139 − 2165.

[5] F. Djebbar, B. Ayad, K.A. Meraim, H. Hamam: Comparative Study of Digital Audio Steganography Techniques, EURASIP Journal on Audio, Speech and Music Processing, Dec. 2012, p. 25.

[6] B. Kostek: Perception-based Data Processing in Acoustics - Application to Music Information Retriaval and Psychophysiology of Hearing, Springer-Verlag, Berlin, Germany, 2005.

[7] C. Cachin: Encyclopedia of Cryptography and Security - Digital Steganography, pp. 348 – 352, Springer, NY, USA, 2011.