UDC 621.391

RESEARCH ALGORITHM OF HIDE THE SPEECH MESSAGING BASED ON THE SPREAD SPECTRUM METHOD

P. Likholob, A. Bukhantsov, A. Vodounou, Ya. Baka

Belgorod State National Research University, Belgorod, Russia
Likholob@bsu.edu.ru, Bukhantsov@bsu.edu.ru, Aaron.Vodounou@gmail.com, BakaYana@mail.ru

Reviewer: Alexandr Kuznetsov Dr., Full Professor, V.N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
kuznetsov@karazin.ua

Received on January 2017

***Resume**: In the work the approach, which makes it possible to modify the method of expanding the spectrum for the realization of the reserved coding of voice communication in vocal data, is proposed. The results of investigating the dependence of different estimations on the values of the assigned parameters are represented. The development algorithm can make it possible to increase the effectiveness of the reserved exchange of voice communications, due to the more effective use of reticence and capacity of vocal material. The use of the orthonormalized basis instead of pseudorandom sequence, allows more effectively from the position of the volume of the coded information to use vocal material for the reserved transfer of communication.*

***Key words:** speech signals, steganography, spread spectrum, measures the differences, the correlation coefficient, the mean square error, relative error, the signal-to-noise ratio.*

1 Introduction

For the large commercial and corporate structures, there is a need for accomplishing the protected exchange of the data by those presenting commercial secret. The use of methods steganography of the concealment of the fact of the transmission of information makes it possible to carry out not only protection of business data, but also in particular, it makes it possible to hide the indirect signs of the fact of the realization of negotiations. Most frequently for the transfer of the informational announcements that not containing the numbers is used spoken language. The use of a spoken language as the means of communication is caused, so by simplicity of its perception by man. Further voice communication, the secretly transferred information, registered in the form of the voice signal, and converted into the digital form.

It is worthwhile to note that the often information resources for the reserved transfer of voice communications, by the methods of cryptography are limited. This is caused by the fact that for the concealment of protected voice communication it is necessary to use the data, whose volume several times must exceed the volume of the protected vocal. Therefore, a quantity of methods and algorithms, which it is possible to use for, purposes the reserved transfer of voice communications not great. The development of method and algorithm of those realizing the principles of the reserved transfer of voice communication in vocal data, can make it possible to increase the effectiveness of the reserved exchange of voice communications, due to the more effective use of reticence and capacity of vocal material. By effectiveness in the work is understood, the use of an approach for coding of voice communication with the guarantee of its reticence, which makes it possible to increase the volume of transferred voice communications without the need for an increase in the volume of vocal material. Cryptography of those making it possible to accomplish a reserved transfer of voice communication in vocal data are widely known several methods. To the bases, the method of the least significant bit (LSB) and method of expanding the spectrum (SSp) carry [1,3,6]. Its durability is the main disadvantage in the method of LSB; therefore, wide application obtained the method of expanding spectrum [6]. The essence of method consists in the addition to the section of the initial voice signal of pseudorandom sequence in accordance with the expression [5,7,8]:

$$\vec{y} = \vec{x} + \alpha \cdot e \cdot \vec{u} \; ; \qquad (1)$$

where $\vec{x}$ – the initial section of vocal data; $\vec{u}$ – the section, which corresponds to pseudorandom sequence; α – weight coefficient; e – the code mapping of the binary bit of hidden voice communication, determined from the formula:

$$e = 2\mathrm{e} - 1,\ m = 1,\ldots,M; \tag{2}$$

where e_m – bit of control information in the binary number system $\mathrm{e}_m \in \{0,1\}$; e_m – the code mapping of the binary bit of control information $e_m \in \{-1,1\}$; m – the ordinal number of the bit of control information is m-th. The weight coefficient of αm determines the reticence of system. In the works [9, 10] it's proposed to select equal:

$$\alpha = \langle \vec{x}, \vec{u} \rangle / \|\vec{u}\|^2. \tag{3}$$

The decoding of the bit of control information from the data occurs by determining the sign of the scalar product of the section of the data and of the pseudorandom sequence:

$$\tilde{e} = sign(\langle \vec{y}, \vec{u} \rangle); \tag{4}$$

where $sign(\ )$ – the operation of the isolation of sign.

The use of a large volume of vocal data for the transfer of short voice communication is a drawback in approach described above. This is caused by the fact that in one section of the data coding the one-bit of protected voice communication is possible. With the frequency of discreteness of 48Gts, it is possible to reach the capacity of vocal data of 92 bytes/s. For increasing the capacitance, it is proposed in one section of vocal data to code 4 bytes of information, i.e. to reach the capacity of 3000 bytes/s.

2 Proposed method

Model of the reserved coding:

$$\vec{y}_i = \vec{x}_i + \lambda \cdot w_i \cdot \vec{u}_i - b \cdot \alpha_i \cdot \vec{u}_i,\ i = 1,..,J; \tag{5}$$

where $\vec{x}_i$ – initial section (vocal material); $\vec{y}_i$ – section containing the coded information by steganography (Filled container); α_i – the constant of proportionality, which determines mutual energy pseudorandom sequence and initial section; λ – coefficient determining reticence and the durability of the coded information by steganography; w_i – the secretly coded byte of voice communication; $\vec{u}_i$ – function from the orthogonal basis of Radamacher, illustrated by Fig. 1; M – it corresponds to a quantity of utilized functions.

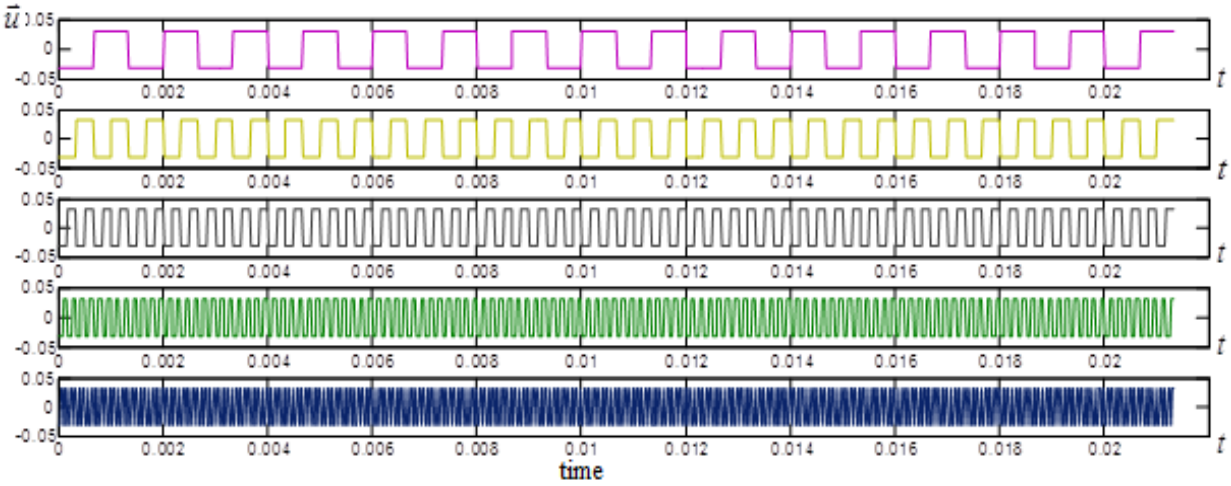

Fig. 1 – Plot of orthogonal basis Rademacher

The decoding of information from filled container occurs, by means of the scalar product of the section of vocal data containing voice communication and corresponding function of the utilized orthogonal basis:

$$\tilde{w}_i = \langle \vec{y}, \vec{u}_i \rangle, \; i = 1,..,J; \tag{6}$$

where $\tilde{w}_i$ – the decoded from the section of voice signal byte of voice communication.

3 Experimental results

For investigating the sensitivity of the measures of the quality of the concealment of information examined, were carried out computational experiments with the use of different sounds of Russian speech. In Fig. 2,3 are represented the sections of the voice signals, which correspond to some sounds of Russian speech, and distribution of their energy on the frequency intervals.

The use of a large volume of vocal data for the transfer of short voice communication is a drawback in approach described above. This is caused by the fact that in one section of the data coding the one-bit of protected voice communication is possible. With the frequency of discreteness of 48Gts, it is possible to reach the capacity of vocal data of 92 bytes/s. For increasing the capacitance, it is proposed in one section of vocal data to code 4 bytes of information, i.e. to reach the capacity of 3000 bytes/s.

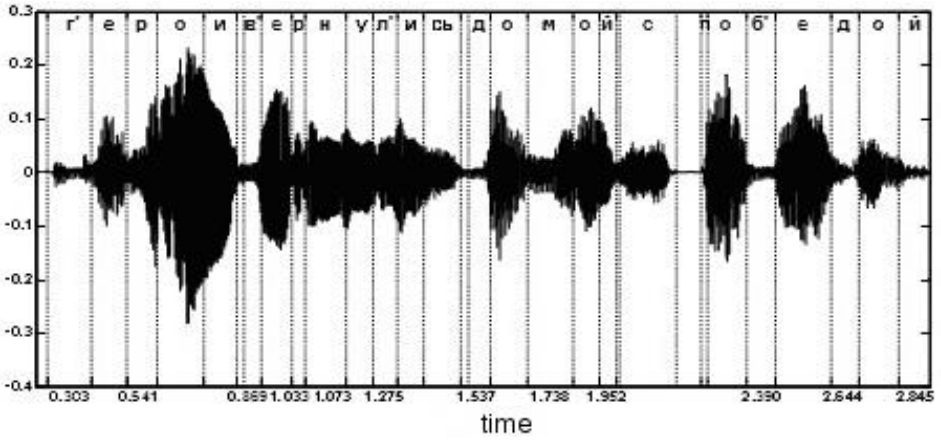

Fig. 2 – An example of digital the original content

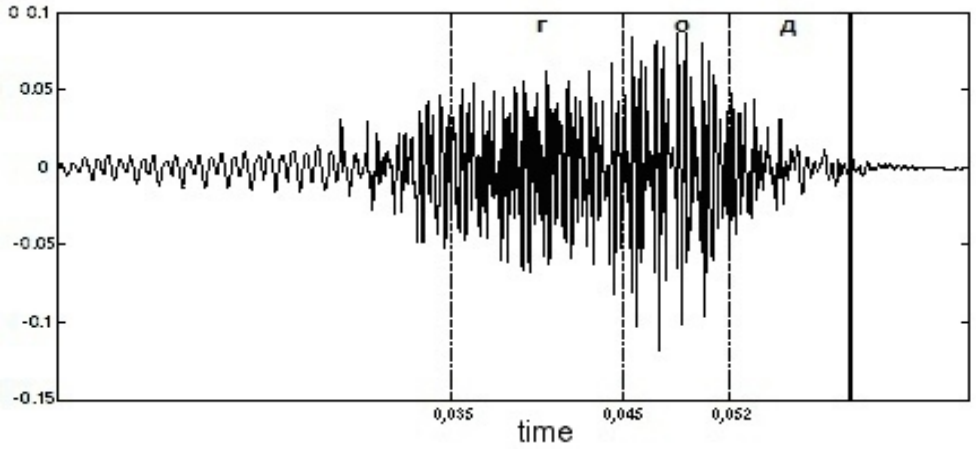

Fig. 3 – An example of hide digital speech audio

In the work are used such estimations of difference as relative error (NSKO), signal to noise ratio (SNR), correlation coefficient (R). Each of these estimations makes it possible to reveal differences in the compared signals [6,7]. In particular, relative error (NSKO) reflects a difference in energy of the sections of signals in the time domain referred to the standard of the initial signal:

$$NSKO = \sum_{n=1}^{N} (x_n - \tilde{x}_n)^2 \Big/ \sum_{n=1}^{N} x_n^{\,2}; \quad (7)$$

where x_n – the value of the amplitude of the initial section of the data; $\tilde{x}_n$ – the value of the amplitude of the section of the data containing additional information, N – quantity of counting of the compared sections of signals.

This measure makes it possible to reveal differences in the envelopes of the amplitudes of the sections of voice signals. The less the changes introduced with the introduction of additional information, the nearer the value of this estimation to zero [1,8,10].

Also to account for the degree of a difference in the initial signal and result of introducing the additional information is used the estimation, sensitive to the time of the recovery of the compared sections of the signals:

$$SNR = 10 \cdot \lg \frac{\sum_{n=1}^{N} x_n^{\,2}}{\sum_{n=1}^{N} (x_n - \tilde{x}_n)^2}; \quad (8)$$

The higher the estimation SNR, the less the changes was introduced. In the case of the equality of two sections (initial and subjected to changes during the coding); the estimation will be equal to infinity (∞). For the evaluation of the degree of the similarity of two sections of the data, frequently is used the evaluation of mutual energy of these signals, determined by correlation coefficient:

$$R = \frac{\sum_{n=1}^{N} \left(x_n - \frac{1}{N} \sum_{n=1}^{N} x_n \right) \cdot \left(\tilde{x}_n - \frac{1}{N} \sum_{n=1}^{N} \tilde{x}_n \right)}{\sqrt{\sum_{n=1}^{N} \left(x_n - \frac{1}{N} \sum_{n=1}^{N} x_n \right)^2 \cdot \left(\tilde{x}_n - \frac{1}{N} \sum_{n=1}^{N} \tilde{x}_n \right)^2}}; \quad (9)$$

The nearer correlation value to one, the higher the similarity of the section of the data containing control information and initial.

Table 1 presents the results of evaluating the measures of difference for all sounds of Russian speech examined. In this case for the analysis the sections of the voice signals, recorded with the frequency of discreteness 8 kHz and code length of 16 bits, were used. For the application of the method of expanding the spectrum voice signals were divided in the sections of identical duration on T=32ms. It is important also to note that the study of the measures in question was accomplished in the implementation of the imposition of noise on the signal in the absence of cross-correlation and use of a weight coefficient of the form:

Table 1 – Evaluation of the differences of the original signal and implementation results using steganographic technique spreading

№		Estimation of reticence PC			Estimation extracted PC		
	b	NSKO	SNR	R	NSKO	SNR	R
1	0	0.1×10^{-6}	69.52	0.9989	171.4	-44.66	0.0107
2	0.5	0.1014	24.19	0.9332	42.76	-32.62	0.0431
3	0.98	0,3825	12,82	0,7158	0.0684	23.29	0.9669
4	0.99	0.3903	12.65	0.7100	0.0171	35.33	0.9915
5	1	0.3981	12.48	0.7043	≈ 0	∞	1

4 Conclusions

The use of the orthonormalized basis instead of pseudorandom sequence, allows more effectively from the position of the volume of the coded information to use vocal material for the reserved transfer of communication. Steganographic coding has a number of stages. The first includes coding

in the orthonormal basis. The second accomplishes adaptive filtration, so that the decoding of communication would possess higher authenticity and it was not subjected to distortions. The third stage is direct coding with the adaptive coefficient. As showed experiments, reticence can be ensured due to the use as the coefficients of those reflecting the value of energy of initial section.

References

[1] Gribunin V.G. Digital steganography. Protection Aspects / V.G. Gribunin, I.N. Wintergrasp, I.V. Turintsev. – Moscow: Solon-Press, 2002. – 261 p.
[2] Zharkikh A.A. The method of steganography based on the direct spread spectrum signal / A.A. Hot, A.V. Gurin, V.Y. Plast // Proceedings of the VII International Scientific and Technical Conference INTERMATIC, 7 – 11 December 2009. Part 4. – Moscow: MIREA, 2009. – P. 78 – 83.
[3] Zhilyakov E.G. On the Steganography in Voice Data / E.G. Zhilyakov et al. // Asian J. Inf. Technol. – 2016. – Vol. 15. – № 12. – P. 1949–1952.
[4] Konahovich G.F. Computer steganography. Theory and practice / G.F. Konahovich, A.Y. Puzyrenko. – Kiev: MK – Press, 2006. –288 p.
[5] Fridrich J. Steganography in digital media: Principles, algorithms, and applications / Jessica Fridrich. – Cambridge University Press, 2012. – 441 p.
[6] Furui S. Digital Speech Processing, Synthesis, and Recognition / Sadaoki Furui. – Marcel Dekker, 2001. – 477 p.
[7] Cvejic N. Spread spectrum audio watermarking using frequency hopping and attack characterization / Nedeljko Cvejic, Tapio Seppanen// Signal Processing. – 2004. – Vol. 84. – №11. – P. 207 – 213.
[8] Stanković S. Multimedia signals and systems / S. Stanković, I. Orović, E. Sejdić. – Springer, 2012. – 373 p.
[9] Thierry Dutoit, Ferran Marques. Applied Signal Processing A MATLAB ™- Based Proof of Concept. – Springer, 2009. – 456 p.
[10] Vercoe B.L. Csound: A Manual for the Audio-Processing System / Barry L. Vercoe. – Cambridge: MIT Media Lab, 1995.

Рецензент: Олександр Кузнецов, д.т.н., проф., Харківський національний університет імені В. Н. Каразіна, Харків, Україна. E-mail: kuznetsov@karazin.ua

Надійшло: Січень 2017.

Автори:
Петро Ліхолоб, ст. викладач, кафедра інформаційно-телекомунікаційних систем і технологій, федеральна державна автономна освітня установа вищої освіти «Білгородський державний національний дослідницький університет» (НДУ «БелГУ»), Білгород, Росія.
E-mail: Likholob@bsu.edu.ru

Андрій Буханцов, к.т.н., доцент, кафедра інформаційно-телекомунікаційних систем і технологій, федеральна державна автономна освітня установа вищої освіти «Білгородський державний національний дослідницький університет» (НДУ «БелГУ»), Білгород, Росія.
E-mail: Bukhantsov@bsu.edu.ru

Аарон Водуну, студент, каф. інформаційно-телекомунікаційних систем і технологій, федеральна державна автономна освітня установа вищої освіти «Білгородський державний національний дослідницький університет» (НДУ «БелГУ»), Білгород, Росія.
E-mail: Aaron.Vodounou@gmail.com

Яна Бака, студент, каф. інформаційно-телекомунікаційних систем і технологій, федеральна державна автономна освітня установа вищої освіти «Білгородський державний національний дослідницький університет» (НДУ «БелГУ»), Білгород, Росія.
E-mail: BakaYana@mail.ru

Дослідження алгоритму прихованої передачі мовного повідомлення заснованого на методі розширення спектра.

Анотація. В роботі запропонований підхід, що дозволяє модифікувати метод розширення спектра для здійснення таємного кодування мовного повідомлення в речових даних. Представлені результати дослідження залежності різних оцінок від значень параметрів, що задаються. Розроблений алгоритм дозволяє підвищити оперативність таємного обміну мовними повідомленнями за рахунок більш ефективного використання скритності і таємності мовного матеріалу. Використання ортонормованого базису замість ПСП дозволяє більш ефективно, з позиції обсягу кодованої інформації, використовувати мовний матеріал для прихованої передачі повідомлення.

Ключові слова: мовні сигнали, стеганографія, метод розширення спектра, заходи відмінності, коефіцієнт кореляції, середньоквадратична помилка, відношення сигнал-шум.

Рецензент: Александр Кузнецов, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: kuznetsov@karazin.ua

Поступила: Январь 2017.

Авторы:

Петр Лихолоб, ст. преподаватель, каф. информационно-телекоммуникационных систем и технологий, федеральное государственное автономное образовательное учреждение высшего образования «Белгородский государственный национальный исследовательский университет» (НИУ «БелГУ»), Белгород, Россия.
E-mail: Likholob@bsu.edu.ru

Андрей Буханцов, к.т.н., доцент, каф. информационно-телекоммуникационных систем и технологий, федеральное государственное автономное образовательное учреждение высшего образования «Белгородский государственный национальный исследовательский университет» (НИУ «БелГУ»), Белгород, Россия.
E-mail: Bukhantsov@bsu.edu.ru

Аарон Водуну, студент, каф. информационно-телекоммуникационных систем и технологий, федеральное государственное автономное образовательное учреждение высшего образования «Белгородский государственный национальный исследовательский университет» (НИУ «БелГУ»), Белгород, Россия.
E-mail: Aaron.Vodounou@gmail.com

Яна Бака, студент, каф. информационно-телекоммуникационных систем и технологий, федеральное государственное автономное образовательное учреждение высшего образования «Белгородский государственный национальный исследовательский университет» (НИУ «БелГУ»), Белгород, Россия.
E-mail: BakaYana@mail.ru

Исследование алгоритма скрытной передачи речевого сообщения, основанного на методе расширения спектра.

Аннотация. В работе предложен подход, позволяющий модифицировать метод расширения спектра для осуществления скрытного кодирования речевого сообщения в речевых данных. Представлены результаты исследования зависимости различных оценок от значений задаваемых параметров. Разработанный алгоритм позволяет повысить оперативность скрытного обмена речевыми сообщениями за счет более эффективного использования скрытности и емкости речевого материала. Использование ортонормированного базиса вместо ПСП позволяет более эффективно, с позиции объема кодируемой информации, использовать речевой материал для скрытной передачи сообщения.

Ключевые слова: речевые сигналы, стеганография, метод расширения спектра, меры различия, коэффициент корреляции, среднеквадратическая ошибка, относительная погрешность, отношение сигнал-шум.