DOI: https://doi.org/10.36910/6775-2524-0560-2023-53-07
UDC 004.056:654.9:681.5
Dymova Hanna, Candidate of Technical Sciences, Phd., Associate Professor
https://orcid.org/0000-0002-5294-1756
Kherson State Agrarian and Economic University, Kherson, Ukraine

APPLICATION OF FAST FOURIER TRANSFORM TO THE SPEECH SIGNALS SCRAMBLING

Dymova H. Application of Fast Fourier Transform to the Speech Signals Scrambling. The article is devoted to the closure of speech signals by implementing a fast Fourier transform in a bandpass scrambler. The most radical measure to prevent the interception of speech signals is the use of cryptographic security methods. The first technical security systems began to be developed immediately after the invention of the telephone. The main goal when developing speech transmission systems is to preserve those characteristics that are most important for the listener to perceive. Communication security in the transmission of voice messages is based on the use of a large number of different methods of blocking signals that change the characteristics of speech in such a way that it becomes illegible and unrecognizable to attackers who listen to or intercept the closed voice message. The choice of closure methods depends on the specific application and the technical characteristics of the transmission channel. That is, technical channels of information leakage are a source of information for technical intelligence, which extracts information using technical means. Therefore, the problem of protecting information from technical intelligence is of particular relevance. The object of the study is the transmission of voice messages. The subject of the research is real-time speech closing systems. The purpose of the paper is to use fast Fourier transform to close speech signals in a bandpass scrambler. To do this, it is necessary to assess the capabilities of technical intelligence to intercept information of limited distribution; analyze types of speech signal closing systems.

The paper presents a block diagram of a combined scrambler, an algorithm for rearranging input signal values using the fast Fourier transform, and hashing functions that are used to obtain a speech signal from a combined scrambler. It has been determined that "through-window" scramblers are the most reliable, and for greater levels of closure, combination scramblers should be used. The task set for further development of the topic is the development of a software application for the operation of streaming data encryption methods in real time.

Keywords: speech signal, reconnaissance object, hash function, combined scrambling, fast Fourier transform, communication channel.

Димова Г.О. Скремблювання мовних сигналів за допомогою швидкого перетворення Фур'є. Стаття присвячена закриттю мовних сигналів шляхом реалізації в смуговому скремблері швидкого перетворювання Фур'є. Найбільш радикальною мірою запобігання прослуховування мовних сигналів є використання криптографічних методів захисту. Перші технічні системи захисту почали розроблятися відразу після винайдення телефону. Головною метою при розробці систем передачі мови є збереження тих її характеристик, що найбільш важливі для сприйняття слухачем. Безпека зв'язку при передачі мовних повідомлень ґрунтується на використанні великої кількості різних методів закриття сигналів, що змінюють характеристики мови таким чином, що вона стає нерозбірливою і невпізнаною для зловмисників, які прослуховують або перехватили закрите мовне повідомлення. Вибір методів закриття залежить від виду конкретного застосування і технічних характеристик каналу передачі. Тобто технічні канали витоку інформації є джерелом інформації для технічної розвідки, що здійснює добування інформації за допомогою технічних засобів. Тому проблема захисту інформації від технічної розвідки має особливу актуальність. Об'єктом дослідження є передача мовних повідомлень. Предметом дослідження є системи закриття мови в реальному часі. Метою статті є використання швидкого перетворювання Фур'є для закриття мовних сигналів в смуговому скремблері. Для цього необхідно оцінити можливості технічних розвідок з перехоплення інформації обмеженого поширення; проаналізувати види систем закриття мовних сигналів

В роботі приведена структурна схема комбінованого скремблера, алгоритм перестановки значень вхідного сигналу за допомогою швидкого перетворення Фур'є та функції хешування, які використовуються для отримання мовного сигналу з комбінованого скремблера. Визначено, що найбільш надійними є скремблери з "назкрізним вікном", а для більшого рівня закриття слід застосовувати комбіновані скремблери. Поставлена задача для подальшого розкриття теми – розробка програмного додатку роботи потокових методів шифрування даних в реальному часі.

Ключові слова: мовний сигнал, об'єкт розвідки, хеш-функція, комбіноване скремблювання, швидке перетворення Фур'є, канал зв'язку.

Formulation of the problem. Protection of information from leakage through technical channels is a set of organizational, organizational, technical and technical measures that exclude or weaken the uncontrolled release of confidential information outside the controlled area.

Information leakage is based on the uncontrolled transfer of confidential information using acoustic, light, electromagnetic, radiation and other fields and material objects, at the attempt of an intruder [1].

The causes and conditions of information leakage, despite all their differences, have much in common.

The reasons for information leakage are usually associated with imperfect standards for storing information, as well as violation of these standards (including imperfect ones), deviations from the rules

for handling relevant documents, technical means, product samples and other materials containing confidential information.

The conditions include various factors and circumstances that arise in the process of scientific, production, advertising, publishing, reporting, information and other activities of the enterprise and create the preconditions for information leakage. Such factors and circumstances may include, for example:

- insufficient knowledge by enterprise employees of information protection rules and lack of understanding of the need for their careful compliance;
- use of uncertified technical means for processing confidential information;
- weak control over compliance with information protection rules by legal, organizational and engineering measures;
- turnover of personnel, including those with confidential information.

Thus, most of the reasons and conditions that create the preconditions and possibility of information leakage arise due to shortcomings of enterprise managers and their employees.

In addition, information leakage is facilitated by:

- natural disasters (storm, hurricane, tornado, earthquake, flood);
- unfavorable external environment (thunderstorm, rain, snow);
- disasters (fire, explosions);
- malfunctions, failures, accidents of technical means and equipment.

Technical channels of information leakage are a source of information for technical intelligence, which extracts information using technical means [2]. It is believed that technical intelligence accounts for more than 50% of all information obtained. Therefore, the problem of protecting information from technical intelligence is of particular relevance.

Research analysis. Unmasking signs of objects in the speech wavelength range are divided into direct and indirect. Direct demassing signs include acoustic fields and waves created by a speech signal. Indirect demassing features include the spatial coordinates of premises (dedicated or protected), in which speech information that must be protected from technical intelligence means can circulate. In addition, these include the number and composition of professional people located in these premises, the start and end times of negotiations and other characteristics not directly related to the formation of speech signals subject to protection from technical intelligence means [2, 3].

The difference between speech signals and other types of acoustic fields and waves lies in the characteristics and parameters of the emitted speech signals. As a rule, acoustic (linguistic) signals belong to the category of random, therefore they are determined by distributions by level, frequency and time and the corresponding average values by level, dynamic range, spectrum shape, frequency range, distribution of formants by frequency and time correlation of individual sections of speech signals [4, 5]. The main characteristics that make it possible to distinguish a speech signal from other forms of acoustic signals include:

- period (frequency) of the fundamental tone in the time domain;
- spectrum of a speech signal in the frequency domain.

Communication security during the transmission of voice messages is ensured by changes in the characteristics of the language so that it becomes illegible and unrecognizable to attackers who eavesdrop on or intercept a closed voice message. The choice of methods for terminating speech signals depends on the specific use and the characteristics of the transmission channel.

The closure of speech signals is discussed in the works of Doctor of Technical Sciences, Professor G.F. Konakhovich. Speech closure systems differ in quality and degree of secrecy. There are two main methods of closing speech signals, divided by the method of transmission over the communication channel [5]:

- analog scrambling;
- speech sampling followed by encryption.

Presentation of the main material and justification of the obtained results. The combination of time and frequency scrambling can significantly increase the degree of closure of the initial signal. The diagram of the combined scrambler is shown in Fig. 1.

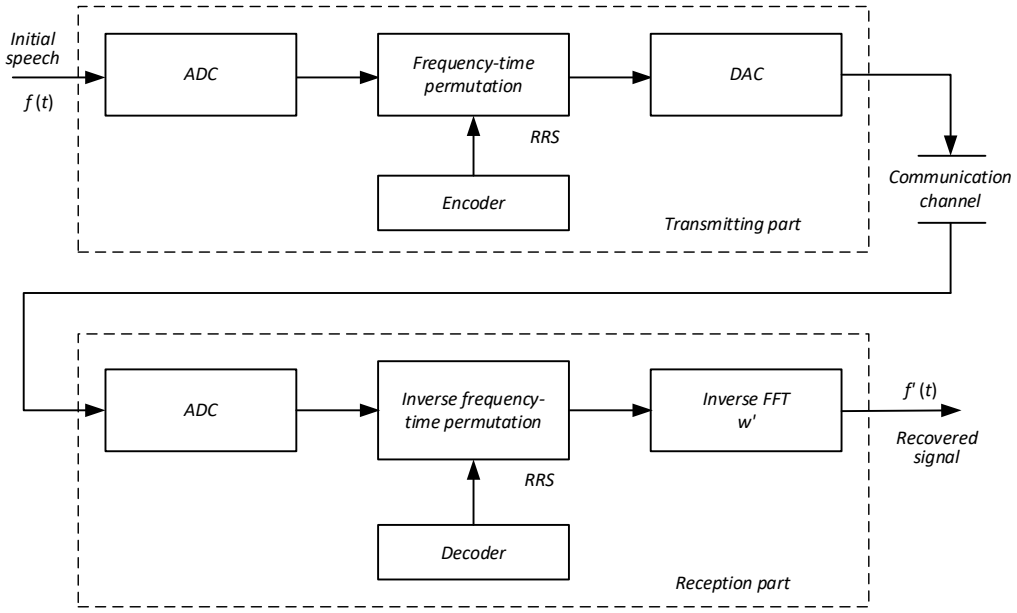

Fig. 1 Block diagram of a combined scrambler

In this scrambler, four digital signal processing processors carry out the operation of time-frequency rearrangements of sampled segments of the output signal. One of the processors implements the function of a random sequence generator (closing system key) [6].

Changing the system key allows you to increase the degree of closure, but requires the introduction of synchronization on the receiving side. Most of the speech signal energy is concentrated in a small region of the low-frequency spectrum (300 to 3500 Hz), so the choice of mixing options is limited.

A significant increase in the degree of tongue closure is achieved by implementing a fast Fourier transform (FFT) in the strip scrambler.

Fast Fourier Transform is an algorithm for quickly calculating the discrete Fourier transform (DFT). Discrete Fourier transform is one of the Fourier transforms widely used in digital signal processing algorithms, as well as in other areas related to the analysis of frequencies in a discrete signal [7].

The expansion of a periodic input signal $f(t)$ with a period of 2π on the main segment $[0, 2\pi]$ into a Fourier series is represented by the relations:

$$f(t) = \sum_{k=-\infty}^{\infty} C_k e^{jkt} \tag{1}$$

$$C_k = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(t) e^{-jkt} dt = \frac{1}{2\pi} \int_{0}^{2\pi} f(t) e^{-jkt} dt. \tag{2}$$

We represent the complex number w as:

$$w = e^{-j(2\pi/N)}, \tag{3}$$

where N – number of data.

In this case, in the DFT, the Fourier coefficients for a number of signal values $\{f_0, f_1, f_2, \dots, f_{N-1}\}$ are expressed by the relation [7]:

$$C_k = \frac{1}{N} \sum_{i=0}^{N-1} w^{ki} f_i. \tag{4}$$

That is, Fourier coefficients are represented as the product of a matrix of complex numbers on a vector of a series of signal values. Calculating these coefficients is a very complex process, so the use of a fast Fourier transform has been proposed.

FFT is an efficient calculation algorithm using patterns hidden inside the matrix expressing the DFT, that is, if the elements of the matrix are rearranged correctly, the number of multiplication operations will decrease.

In our case, the signal is represented by a series of 4 frequency bands, denoted $\{f_0, f_1, f_2, f_3\}$, then the DFT of this signal can be expressed as the product of a matrix and a signal vector:

$$\begin{bmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} w^0 & w^0 & w^0 & w^0 \\ w^0 & w^1 & w^2 & w^3 \\ w^0 & w^2 & w^4 & w^6 \\ w^0 & w^3 & w^6 & w^9 \end{bmatrix} \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \end{bmatrix} \tag{5}$$

If in accordance with Fig. 2, substitute the numerical values of the step series w into the matrix, then the result will be

$$\begin{bmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -j & -1 & j \\ 1 & -1 & 1 & -1 \\ 1 & j & -1 & -j \end{bmatrix} \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \end{bmatrix} \tag{6}$$

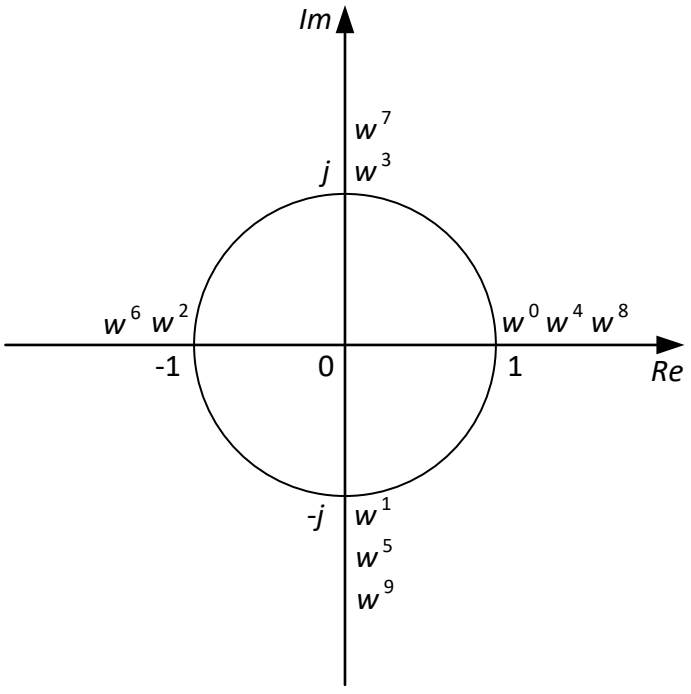

Fig. 2 Step row w for $N = 4$

After this, the matrix elements are replaced. Let us define a special way of representing the product of a matrix and a vector, which is given in the work [7]:

$$\begin{bmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{matrix} [f_0 & f_1 & f_2 & f_3] \\ \begin{bmatrix} w^0 & w^0 & w^0 & w^0 \\ w^0 & w^1 & w^2 & w^3 \\ w^0 & w^2 & w^4 & w^6 \\ w^0 & w^3 & w^6 & w^9 \end{bmatrix} \end{matrix} \tag{7}$$

Let's change the matrix in the expression (7). Having swapped the columns of the matrix, we divide it into two groups: the group f_0, f_2, with even data indices, and the group f_1, f_3 with odd data indices. Therefore, we get

$$\begin{matrix}[f_0 & f_2] & [f_1 & f_3]\end{matrix}$$
$$\begin{bmatrix}C_0\\C_1\\C_2\\C_3\end{bmatrix} = \begin{bmatrix}w^0 & w^0\\w^0 & w^2\\w^0 & w^4\\w^0 & w^6\end{bmatrix} + \begin{bmatrix}w^0 & w^0\\w^1 & w^3\\w^2 & w^6\\w^3 & w^9\end{bmatrix} \quad (8)$$

The elements of the matrix, which are the second term of expression (8), are represented as $w^{k+1} = w^k w^1$, that is

$$\begin{matrix}[f_0 & f_2] & [\ f_1 & f_3\ ] & [\ f_0 & f_2\ ] & [\ f_1 & f_3\ ]\end{matrix}$$
$$\begin{bmatrix}C_0\\C_1\\C_2\\C_3\end{bmatrix} = \begin{bmatrix}w^0 & w^0\\w^0 & w^2\\w^0 & w^4\\w^0 & w^6\end{bmatrix} + \begin{bmatrix}w^0w^0 & w^0w^0\\w^1w^0 & w^1w^2\\w^2w^0 & w^2w^4\\w^3w^0 & w^3w^6\end{bmatrix} = \begin{bmatrix}w^0 & w^0\\w^0 & w^2\\w^0 & w^4\\w^0 & w^6\end{bmatrix} + \begin{bmatrix}w^0\\w^1\\w^2\\w^3\end{bmatrix}\begin{bmatrix}w^0 & w^0\\w^0 & w^2\\w^0 & w^4\\w^0 & w^6\end{bmatrix} \quad (9)$$

From Fig. 2 shows that $w^4 = w^0 = 1$, $w^6 = w^2 = -1$, and also $w^2 = -w^0$, $w^3 = -w^1$. Let's substitute these values into (9) and get

$$\begin{matrix}[f_0 & f_2] & [f_1 & f_3]\end{matrix}$$
$$\begin{bmatrix}C_0\\C_1\\C_2\\C_3\end{bmatrix} = \begin{bmatrix}1 & 1\\1 & -1\\1 & 1\\1 & -1\end{bmatrix} + \begin{bmatrix}w^0\\w^1\\-w^0\\-w^1\end{bmatrix}\begin{bmatrix}1 & 1\\1 & -1\\1 & 1\\1 & -1\end{bmatrix} \quad (10)$$

Then the Fourier coefficients have the form:

$$\begin{aligned}C_0 &= f_0 + w^0 f_2\\C_1 &= f_0 - w^0 f_2\\C_2 &= f_1 + w^0 f_3\\C_3 &= f_1 - w^0 f_3\end{aligned} \quad (11)$$

The described FFT algorithm for permuting signal values is called the sorting technique based on permutation of digits.

After using the FFT algorithm, a hashing algorithm is used for the combined scrambling.

A hashing function (hash function or shortening function) is a data transformation that transforms a bit string M of arbitrary length into a bit string $h(M)$ of some fixed length (several tens or hundreds of bits) [8].

The hash function $h(C)$ must satisfy the following conditions:

1) the hash function $h(C)$ must be sensitive to any changes in the input sequence C;
2) for a given value of $h(C)$ it should be impossible to find the value of C;
3) for a given value of $h(C)$ it should be impossible to find a value $C' \neq C$ such that $h(C') = h(C)$.

The situation in which for different input sequences C, C' the values of their hash images coincide: $h(C) = h(C')$ is called a collision [8, 9].

When constructing a hash image, the input sequence C is divided into blocks C_i of fixed length and processed block by block according to the formula

$$Hi = f(H_{i-1}, C_i). \quad (12)$$

The hash value calculated when the last block of the message is entered becomes the hash value of the entire message.

We use a simplified version of the hash:

$$H_i = (H_{i-1} + C_i)^2 \ mod \ n, \tag{13}$$

where $n = pq$, p and q – large prime numbers;
H_0 – arbitrary initial content;
C_i – i- th message block $C = C_1 C_2 \dots C_k$.

Conclusions and prospects for further research. The article presents a circuit of a combined scrambler, an algorithm for permuting the values of the input signal using the fast Fourier transform and a hashing function used to obtain the speech signal of the combined scrambler.

Scramblers of all types, with the exception of the simplest one (with frequency inversion), introduce distortion into the reconstructed speech signal. Time segment limits compromise signal integrity, which inevitably leads to out-of-band components. Group delays of the out-of-band speech signal in the communication channel also have an undesirable effect. The result of the twisting is an increase in the minimum acceptable signal-to-noise ratio at which reliable communication can occur. But, despite this, the most reliable, in terms of the degree of tongue closure, are scramblers with a "through window", and for a higher level of closure, combined scramblers should be used. Next, it is planned to develop a software application to study and understand the operation of stream data encryption methods in real time.

Список бібліографічного опису

1. Юдін О.К., Богуш В.М. (2005) Інформаційна безпека держави. Харків: Консул.
2. Антонов В.М., Пермяков О.Ю. (2005) Комп'ютерні мережі військового призначення. Київ: МК-Прес.
3. Антонов В.М. (2005) Сучасні комп'ютерні мережі. Київ: МК-Прес.
4. Конахович Г.Ф. (2004) Системи радіозв'язку. Київ: НАУ.
5. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г., Чуприн В.М., Горбунов О.О. (2009) Захист інформації в телекомунікаційних системах: Навчальний посібник. Київ: НАУ.
6. Димова Г.О., Димов В.С. (2018) Генерування випадкових процесів динамічними системами. Прикладні питання математичного моделювання. Том 1 № 2. Херсон,. DOI: 10.32782/2618-0340-2018-2-55-64.
7. Сато Ю. (2009) Обробка сигналів. Перше знайомство. URL: https://balka-book.com/obrobka_signaliv-318/obrobka_signaliv_pershe_znayomstvo-1542
8. Димова Г.О. (2021) Аналіз методів оцінки ефективності систем фізичного захисту. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. Луцьк. № 45. DOI: https://doi.org/10.36910/6775-2524-0560-2021-45-02
9. Димова, Г. О. (2021). Інформаційний простір об'єкту в системах ідентифікації. Вісник Херсонського національного технічного університету, (4 (79)).

References

1. Yudin O.K., Bohush V.M. (2005) Informatsiyna bezpeka derzhavy [Information security of the state]. Kharkiv: Consul. [in Ukrainian].
2. Antonov V.M., Permyakov O.YU. (2005) Komp″yuterni merezhi viys′kovoho pryznachennya [Military Computer Networks]. Kyiv: MK-Press. [in Ukrainian].
3. Antonov V.M. (2005) Suchasni komp″yuterni merezhi [Modern Computer Networks]. Kyiv: MK-Press. [in Ukrainian].
4. Konakhovych H.F. (2004) Systemy radiozv″yazku [Radio communication systems]. Kyiv: NAU. [in Ukrainian].
5. Konakhovych H.F., Klymchuk V.P., Pauk S.M., Potapov V.H., Chupryn V.M. & Horbunov O.O. (2009) Zakhyst informatsiyi v telekomunikatsiynykh systemakh: Navchal′nyy posibnyk [Information Security in Telecommunication Systems: Tutorial]. Kyiv: NAU. [in Ukrainian].
6. Dymova H.O., Dymov V.S. (2018) Heneruvannya vypadkovykh protsesiv dynamichnymy systemamy [Generation of random processes by dynamic systems]. Applied problems of mathematical modeling. Volume 1 No. 2. Kherson. DOI: 10.32782/2618-0340-2018-2-55-64.
7. Sato YU. (2009) Obrobka syhnaliv. Pershe znayomstvo [Signal Processing. First acquaintance]. URL: https://balka-book.com/obrobka_signaliv-318/obrobka_signaliv_pershe_znayomstvo-1542. [in Ukrainian].
8. Dymova H.O. (2021) Analiz metodiv otsinky efektyvnosti system fizychnoho zakhystu [Analysis of methods for assessing the effectiveness of physical protection systems]. Computer-integrated technologies: education, science, production. Lutsk. No. 45. DOI: https://doi.org/10.36910/6775-2524-0560-2021-45-02. [in Ukrainian].
9. Dymova H. O. (2021). Informatsiynyy prostir ob″yektu v systemakh identyfikatsiyi [Information space of the object in identification systems]. Bulletin of the Kherson National Technical University, (4 (79)). [in Ukrainian].