Into Table 4 we'll place the fixed dots.

Table 4

Type of permutation	Number of current type permutations	Number of fixed dots
$<1,1,1,1,1,1,1,1>$	1	48
$<2,2,2,2>$	9	44
$<3,3,1,1>$	8	44
$<4,4>$	6	42

According to Burnside's lemma we'll obtain:

$$t(G)=\frac{1}{24}(4^8+9\cdot4^4+8\cdot4^4+6\cdot4^2)=2916.$$

Therefore, there are 2916 ways of painting the cube apexes into four colours.

Conclusion

A key step for solving similar tasks is the heuristic search of permutations.

REFERENCES

1. Kaluzhnin, L.A. Transformations and permutations / L.A. Kaluzhnin, V.I. Suschanski. – Moscow: Science, 1979. – 113 p

UDC 534; 53.08:681.3

FAST ALGORITHM FOR ESTIMATING SPEECH LEGIBILITY BY FREQUENCY-TIME PROCESSING OF THE LFM- SIGNAL

KANSTANTSIN RAKHANAU, ULADZIMIR ZHALIAZNYAK
Polotsk State University, Belarus

The authors propose a fast algorithm for time-frequency processing of the LFM-signal for estimating speech intelligibility. The efficiency of the algorithm, which increases because of the decrease in the quantity of strips of splitting, is considered. The paper presents theoretical and practical results of the research into the effectiveness of the algorithm under discussion.

Introduction

To improve the methodological precision of speech intelligibility estimation [1; 2], the method of LFM signal was developed to implement it in hardware and software system. The new hardware and software system must include, along with hardware, a specific software package, the purpose of which is to simulate the functioning of some of the hardware. The functions of the hardware and software system should be: automatic control and generation of stimulatory signal, adaptive digital signal processing, calculation and presentation of the results of the security information leakage channels evaluation. The main requirements for the software complex – adequacy of the operation, performance, minimum amount of memory occupied.

To estimate speech intelligibility the LFM signal method is required to make the maximum number of features into a special software complex. This will simplify the hardware implementation of hardware and software systems and, consequently, reduce its cost. In addition, a special software complex with a maximum number of integrated functions (management, synchronization, signal generation, filtering, performance assessment, etc.) will improve the reliability, scalability, stability and adaptability of the system.

Technique solutions

The application of the time-frequency representation of the signal energy by Wigner function allows to estimate the intensity of the physical fields outside the information object of the above-threshold LFM signal. According to the results of the estimation, based on the correlation theory of speech intelligibility [3], an information criterion of protection, that is, the intelligibility factor, is defined. The calculation of speech intelligibility is offered to be carried out by means of speech intelligibility evaluation algorithm with the help of LFM signal method shown in Figure 1. The combined efficiency of the algorithm consists of the temporal and spatial efficiency. The temporal efficiency is a measure of the algorithm speed. The spatial efficiency indicates how much additional RAM is needed for the algorithm.

Modern requirements for additional RAM, necessary for the work of a program complex, have become not so important, as they used to be. It should be noted that there is a significant difference between the fast main memory, secondary relatively slow memory and cache memory. However, the main focus should be on time performance.

To analyze the time efficiency of the algorithm we can use the time between the presentation of the input data in the program complex and the appearance of the results in the output. The generally accepted unit of assessment is time (seconds, milliseconds, etc.). However, such an approach has obvious disadvantages, since the measurement results will depend on the following extraneous factors:

- specific performance of a computer;
- thoroughness of the algorithm implementation in the form of a program;
- type of the compiler;
- timing accuracy of the real-time execution.

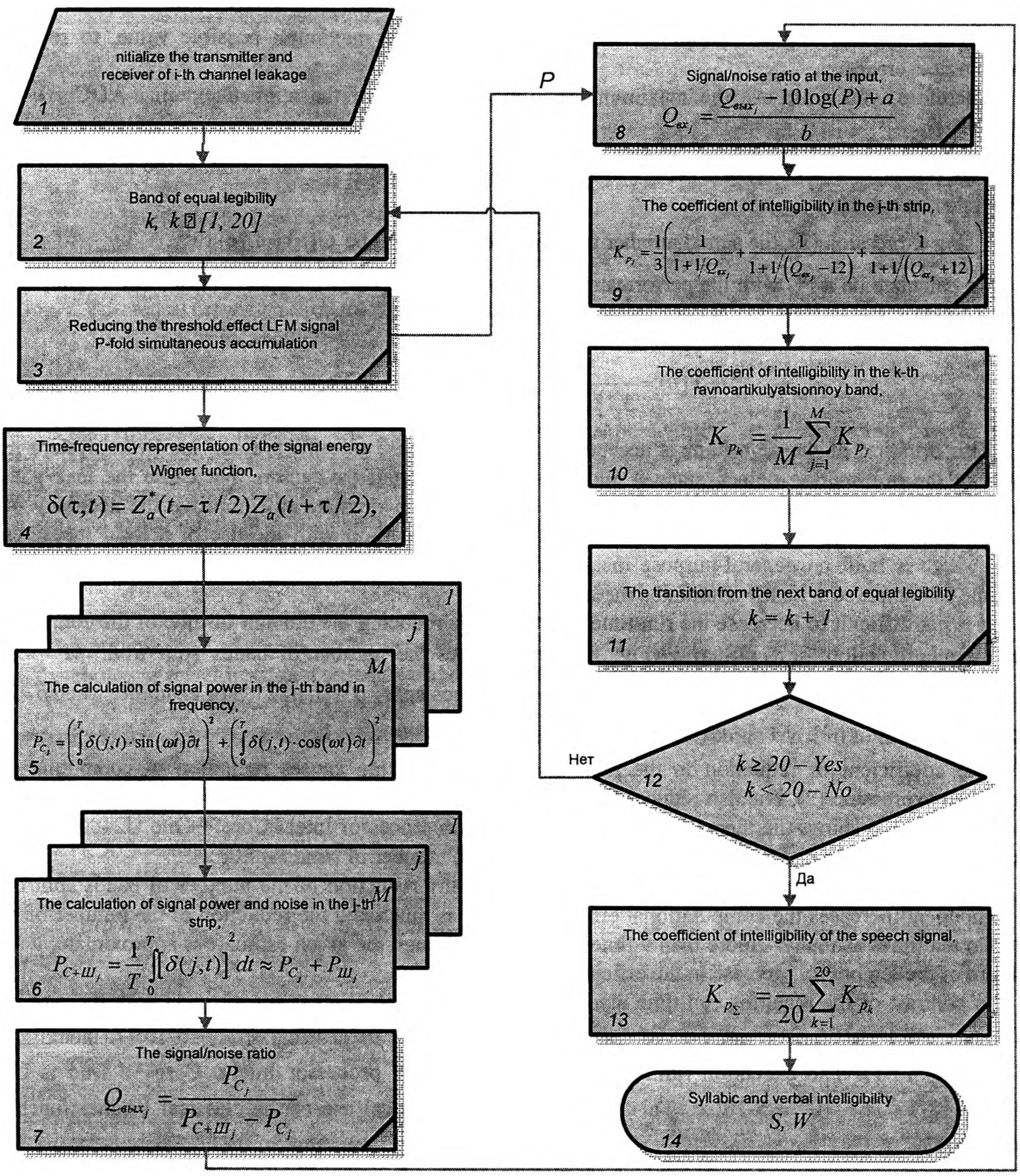

Fig. 1. Algorithm for estimating speech intelligibility by LFM signal method

In this case, the performance analysis should be used counting the number of basic operations, which make the largest contribution to the total execution time of the algorithm. This approach does not depend on extraneous factors. The run-time software implementation of this algorithm $T(n)$ on a particular PC can be seen in the following formula [4]:

$$T(n) \approx c_{op}C(n), \tag{1}$$

where c_{op} – run-time, the basic operation of the algorithm on a specific PC, $C(n)$ – number of basic operations performed depending on the size of the input data n for the algorithm.

The most interesting from the standpoint of optimization over time, are steps 4 – 8 (Fig. 1). For their execution considerable computing resources are spent. The total number of basic operations $C(n)$ is described by the expression:

$$C(n) = 14{,}5nM + 2n\log(n) + 3n + 10M\ . \tag{2}$$

According to [1; 2], the sampling frequency should be the maximum possible value, to reduce the methodological error.

Therefore, you must use the maximum sampling frequency of the applied external ADC E14-440D $f_d = 2\cdot10^5$ Hz.

Just considering the duration of LFM signal, which is 2 seconds, we can estimate the maximum size of the input data $n \approx 4\cdot10^5$.

Using expression (2), the actual number of basic operations will be $C(n) = 1{,}16\cdot10^{12}$.

To calculate on a PC with the performance, for example, of $3{,}18\cdot10^9$ flop/s (Intel® Core™ Duo U2400) [5], on the basis of expression (1) the algorithm execution time will be $T(n)$:

$$T(n) = \frac{3}{3{,}18\cdot10^9}\cdot1{,}16\cdot10^{12} = 364{,}782 \text{ c.}$$

This duration of the algorithm is acceptable for practical use of software and hardware system in the analysis of the information object, since it allows to define in detail the factors that cause the leak paths of speech information. The use of only the LFM signal method can dramatically improve the accuracy of the estimates. Such assessment, made by means of non-automated method with the use of a local measurement system, which is built on general-purpose measurement tools, is time consuming and requires three times as much time as compared with the automated method.

It is not difficult to decrease the run-time processing by reducing the amount of time of the components j of the Wigner function $\delta(j,t)$ Step 5 (Fig. 1). This reduces the number of bands split from $M = n/2$ to $M = n/2\rho$, where ρ is the factor reducing the number of bands split, $\rho \in [1; n/2]$. For example, when $\rho = 1$ the number of bands split of LFM signal is $M = n/2$, and for $\rho = n/2$ – $M = 1$.

The coefficient of reduction in the number of bands splitting causes reduction of computing costs, according to expression (2), but also reduces the information content of the thin structure of the LFM signal. For example Figure 2, *a* shows the theoretical time of the algorithm processor Intel®Core™ Duo U2400, depending on the size of the input n and the coefficient of reduction in the number of bands split ρ.

According to the graph it follows that the twice as many reduction of the number of bands split by the time component increases the computational efficiency twice as much and the reduction of the number of bands split up to ten times as many – more than 9 times as much. Although the given estimate is approximate, it shows the nature of the temporary increase in the efficiency of the algorithm.

In contrast of the resulting run-time algorithm to the classical, Wigner function [1] with the size of the input data $n \approx 4\cdot10^5$ has a number of basic operations $C(n) = 2n^3(7 + \log(n)) = 1{,}16\cdot10^{18}$ (including the application of FFT). The execution time of the algorithm for the processor Intel® Core ™ Duo is U2400 $T(n) = 1/3{,}18\cdot10^9\cdot1{,}6\cdot10^{18} = 5\cdot10^8$ c. This suggests that the practical use of the classical Wigner function is hardly possible.

The further implementation of the algorithm in the Microsoft Visual Studio 2008, using C # allows more accurate assessment of the run-time processing software system in practice. Figure 2, *b* is represents the run-time processing CPU AMDSempron ™ 2800 +.

The presented run-time processing allows us to assert that the algorithm is suitable for use in software and hardware system with a coefficient of reduction in the number of bands split $\rho > 10$, which may vary depending on the speed of the processor. So at a sampling rate $f_d = 2 \cdot 10^5$ the coefficient reducing the number of bands split $\rho = 10$ educes the information content of the fine structure of LFM signal from $M = 10^5$ to $M = 10^4$, which insignificantly affects the methodical error.

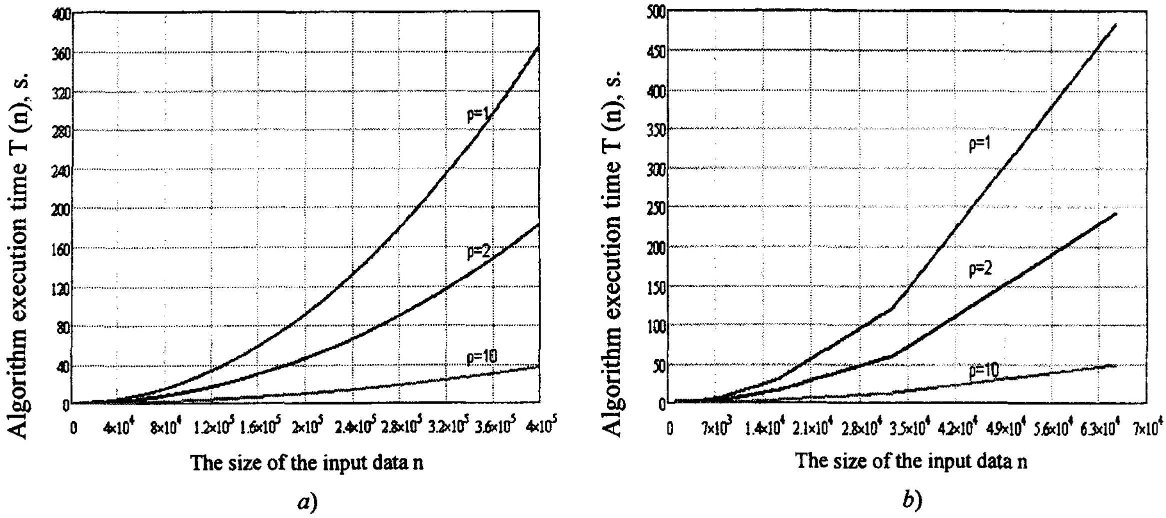

Fig. 2. Theoretical (*a*) and practical (*b*) algorithm execution time by Processor Intel ® Core ™ Duo U2400 with a coefficient of reducing the number of bands split $\rho = 1; 2; 10$

The processing capacity can be also increased by [6]:

- vector processor modules, in which data sets are treated almost in parallel, making them several times faster than when running in scalar mode (SIMD-machines). The examples of vector processors are Intel-compatible processors that support the instruction sets MMX, SSE;
- parallel execution of multiple independent components of the time slices using MIMD-machines.

Conclusion

1. The algorithm for speech intelligibility evaluation by the LFM signal, including the addition to the correlation theory of speech intelligibility has been worked out.
2. The optimization of the algorithm execution time of speech intelligibility evaluation by LFM signal based on the choice of the chirp signal resolution has been carried out.
3. The determined time of the algorithm allows the receiver chirp signal to assess speech understanding in the form of a software component for its further use in hardware-software system.

REFERENCES

1. Раханов, К.Я. Методы оценки защищенности речевой информации / К.Я. Раханов, В.К. Железняк // Вестн. Полоц. гос. ун-та. Серия С. Фундаментальные науки. – 2011. – № 12. – С. 2 – 8.
2. Раханов, К.Я. Имитационная модель автоматизированной помехоустойчивой оценки разборчивости речи методом ЛЧМ-сигнала / К.Я. Раханов, В.К. Железняк // Вестн. Полоц. гос. ун-та. Серия С. Фундаментальные науки. – 2011. – № 12. – С. 35 – 41.
3. Железняк, В.К. Корреляционная теория разборчивости речи / В.К. Железняк, А.А. Колесников, В.Ф. Комарович // Вопросы радиоэлектроники. – 1995. – № 2. – С. 3 – 7.
4. Левитин, А. Алгоритмы: введение в разработку и анализ / А. Левитин; пер. с англ. – М.: Издат. Дом "Вильямс", 2006. – 576 с.
5. Features of the Intel ® in accordance with the requirements of export (date of last revision: February 9, 2011) [Electronic resource] // Intel Corporation, 2011. – Mode of access: http://www.intel.com/support/ru/processors/sb/CS-023143.htm#8. – Date of access: 06.10.2011.
6. Долматов, А.В. Основы развивающего образования: теория, методы, технологии креативной педагогики / А.В. Долматов. – СПб.: ВУС, 1998. – 196 с.