Truthfulness of estimation of voice information protection from leakage through technical canals

I L Reva, V A Trushin, A A Ivanov, T V Borbotko

1 Novosibirsk State Technical University, 20, Karla Marksa Ave., Novosibirsk, 630073, Russia
2 Belarusian State University of Informatics and Radioelectronics, 6 P. Brovki Str., Minsk 220013, Belarus

E-mail: reva@corp.nstu.ru

Abstract. The purpose of this study is to survey an improvement of the voice information security estimating method on the basis of immediate appreciation tests with connected texts results. Estimation of voice information protection from leakage through information leakage canals is necessary for certification of informatization objects, and for efficiency control of protection means and systems. A word legibility coefficient (W) is the main quantitative criterion of voice information security. Its instrument estimation is based on the Pokrovskiy’s experimental tests results. As we think, the main flaw of the speech intelligibility instrumental estimation method is the absence of testing with connected texts. This should lead to an increase of real speech intelligibility relatively the method estimation. The paper shows the imperfection of the method of Pokrovskiy’s for connected texts.

1. Introduction

Estimation of voice information protection from leakage through information leakage canals is necessary for certification of informatization objects, and for efficiency control of protection means and systems. The word legibility coefficient (W) is the main quantitative criterion of voice information security. Its instrument estimation is based on the Pokrovskiy’s experimental tests results [1].

The essence of the method [2] is the following:

1. The entire frequency range of the speech signal is partitioned into five octave bands with center frequencies of 250, 500, 1000, 2000, 4000 Hz, respectively.
2. In each octave band, the noise is measured in $L_{ni}$ sound pressure levels of a mixture of signal + noise $L_{s+n}$ (in dB relative to the threshold of hearing $= 2 \cdot 10^{-5} \text{Pa}$). The measuring equipment is used in the procedure of the noise and vibration meters.
3. Let us calculate the signal level for each octave band:

$$L_{Si} = 10 \cdot \log (10^{0.1 \cdot L_{s+n}_{i}}) = 10^{0.1 \cdot L_{ni}}$$

4. Let us calculate the level of feelings for each octave band:

$$Q_{i} = L_{Si} - L_{ni} - \Delta A_{i}$$

where $\Delta A_{i}$ - formant excess (known value)
5. The formant perception factor is defined for each octave band at the center frequencies.
6. Let us calculate the formant intelligibility in the following formulas:

\[
R_i = p_i \cdot k_i \\
R = \sum_{i=1}^{N} R_i,
\]

(4) (5)

where \( k_i \) - contribution to the \( i \)-th octave band in total clarity that characterizes the probability of speech formants in the band.

7. There is a conversion from values of formant intelligibility \( R \) to verbal intelligibility \( W \):

\[
W = \begin{cases} 
1.54 \cdot R^{0.25} & \text{if } 0 < R < 0.15 \\
1 - \exp\left(-\frac{11}{1 + 0.7R}\right) & \text{if } R \geq 0.15 
\end{cases}
\]

(6)

2. The main flaws of this method

Different authors [3÷6] suppose that the main flaws of this method are the following:

- Theoretical difficulty;
- Use of only 5 octave bands theoretically leads to 9% «loss» of formant intelligibility;
- The coefficient of perception’s dependence on frequency is not taken into account;
- The character of \( p_i \) curve’s dependence on the noise level is not taken into account (basic dependencies of Pokrovskiy used in [2], hold for the noise not exceeding 40 dB [1, chapter 9]).

However, these flaws are not critical and could be simply removed by contemporary hardware-software technologies.

As we think, the main flaw of the speech intelligibility instrumental estimation method based on Pokrovskiy’s tests is methodical (Bykov Y.S. [7] and Sapozhkov M.A. [8] similarly to the method of Pokrovskiy’s) and it consists in the following:

Speech intelligibility research started in the middle of the past century due to necessity of communication tools quality estimation. Immediate appreciation tests with the use of custom tables were the basis of such research. As the result, particularly, basic dependencies between different types of intelligibilities - syllabic, wordy, phrasal - were derived. The tables were made maximally non correlative, which is important for exception of the «human factor», i.e. achievement of maximal objectivity. Tests with connected texts were carried out only for derivation of dependence between different types of intelligibilities [1, chapter 3].

But the voice information security situation is quite opposite. There are only connected texts and, moreover, an «intruder» has a possibility to record a text (a conversation, a talk etc.) on a voice recorder and to listen to it repeatedly.

The above-mentioned information should lead to an increase of real speech intelligibility relatively the method estimation. An experiment was carried out to justify the fact and to estimate quantitatively the fact of the possible speech intelligibility increase.

3. Experiment

Roughly, its essence consists in the following.

1. A set of 10 connected texts (discussions, conversations) was formed. Each recording lasts 3 minutes.
2. An auditors team was created (4 men and 4 women from 20 to 30 years old).
3. The integrated speech level was 70 dB (a speech with the medium volume).
4. The following types of noise were generated: white noise, pink noise, speech-like noise (from white noise), speech noise (cuts of connected texts speech chorus), formant-like noise (speech chorus with envelope corresponding formant spectra). An envelope shape was set in 7 octave bands with central frequencies 125, 250, 500, 1000, 2000, 4000, 8000 correspondingly.

5. For each noise type, integrated levels 70 dB (+5,+10,+15) dB, (-5,-10) dB were set, i.e. to make integrated signal/noise ratios -15, -10, -5, 0, +5, 10 dB.

6. Thus, every auditor was offered a set of 25 recordings to listen. After listening to the recordings, the word legibility coefficient was estimated. Average (by 8 auditors) word illegibility dependencies on the integrated signal/noise ratio for different noise types are shown in Figure.1

\[ W_n,\% \]

\[ q, \text{dB} \]

**Figure 1.** Dependence of word illegibility \( W \) on integrated signal/noise ratio \( q \) in frequency range 90÷11200 Hz for different noise types.

Similar dependencies, derived with the traditional method [2], are shown in Figure.2 for comparison.

\[ W \]

\[ q, \text{dB} \]

**Figure 2.** Dependence of word illegibility \( W \) on integrated ratio signal/noise \( q \) in frequency range 180÷5600 Hz. 1 – white noise, 2 - pink noise, 3 – noise with
4. Conclusion
This experiment is considered as a real example, pointing to the attainability of a significant increase in speech intelligibility with connected texts, and hence reduction of the level of security.

Comparative analysis of the diagrams allowed us to make an implication about an increase of word intelligibility of connected texts for the same types of noises and a similar signal/noise ratio.

Of course, presented results are tentative and there should be additional research with more auditors.

Undoubtedly, presented results can be improved with participation of more auditors.

References
[1] Pokrovskiy N B. 1962 Calculation and measurement of speech intelligibility. (Moscow, Svyaz'izdat Publ.) p 390
[2] Zhelezniak V K., Makarov J K and Horev A A. 2000 Some methodological approaches to evaluating the effectiveness of protection of speech information. Special Appliances. 4 39-45
[3] Kargashin V L. 2001 Improvement of methodic principles of room protection from voice information leakage estimation. (Moscow, Special technics) 6
[4] Grigoriev S V. 2003 Spectre-optimized noise. Saint-Petersburg, Information security Confident. 4
[5] Trushin V A. 2007 About speech intelligibility. 9-th Russian practical science conference on Information security of country, society and personality problems. (Tomsk) pp 115-119.
[6] Didkovskiy V S, Didkovskiy M L and Prodeus A N. 2008 Acoustic expertise of speech information channel. (Kiev) p 418
[7] Bykov Y S. 1959 Theory of intelligibility and efficiency increase of radio telephony. (Moscow, Government energetic publishing house) p 351
[8] Sapozhkov M A. 1963 Speech signal in cybernetics and connection. (Moscow, Svyaz'izdat) p 452