Hindawi Publishing Corporation
EURASIP Journal on Information Security
Volume 2007, Article ID 32028, 4 pages
doi:10.1155/2007/32028

Research Article

An Efficient Objective Intelligibility Measure for Frequency Domain Scramblers

A. M. C. R. Borzino,[1] J. A. Apolinário Jr.,[1] and D. G. da Silva[2]

[1] *Department of Electrical Engineering, Military Institute of Engineering (IME), Praça General Tibúrcio 80, 22290-270 Rio de Janeiro, RJ, Brazil*
[2] *Center for Telecommunications Studies (CETUC), Pontifical Catholic University of Rio de Janeiro (PUC-Rio), Rua Marquês de São Vicente 225, 22453-900 Rio de Janeiro, RJ, Brazil*

Correspondence should be addressed to J. A. Apolinário Jr., apolin@ime.eb.br

Received 17 August 2007; Accepted 3 December 2007

Recommended by E. Magli

An objective performance measure is proposed to evaluate the intelligibility of a speech signal having its frequency subbands permuted. The proposed tool can be used to generate efficient keys for frequency domain scramblers as well as to assess the results of cryptanalysis.

1. INTRODUCTION

The main goal of a scrambler is to make a speech signal unintelligible via the permutation of its frequency subbands. In this work, we assume a sampling frequency of 8 kHz and a filter bank with 8 channels, each using a filter with 128 coefficients. With N being the number of (permutable) subbands, there are $N!$ possible permutations. However, not all of them are efficient [1]; this is due to the fact that some of them result in a signal with high residual intelligibility. Objective measures in the technical literature, such as spectral distortion and segmental signal-to-noise ratio [2], are not appropriated for the task of evaluating intelligibility in scrambled speech; this is so because the objective is not the difference in spectra but how intelligible the signal is. In [3], a scheme for obtaining scores was proposed. This scheme (Beker score) took into account subbands shift, number of subbands kept in their original positions, continuity of the subbands, and occurrence (or not) of subband inversion (not taken into consideration here due to the structure of our frequency scrambler). From our experiments, we noted that even with a close to perfect continuity as in permutation $[5\ 6\ 7\ 8\ 1\ 2\ 3\ 4]^T$, the listener could not understand the signal. Therefore, the objective measure proposed herein does not take into account the continuity of subbands; instead, it introduces a subband weighing as each subband has its own degree of importance, mainly determined by the presence of formants [4].

2. POSITION DISTANCE

By means of subjective tests, it was observed (for our 8-subband scrambler) that if all subbands are shifted in two or more positions, the scrambled signal becomes completely unintelligible for a nonexpert listener. Nevertheless, if the shift is of only one position, the signal is partially intelligible. In order to set a weight to the shift of one position, two phrases were scrambled with permutation $[2\ 1\ 4\ 3\ 6\ 5\ 8\ 7]^T$ and 14 (nonexpert) people listened four times each. A training session was carried out before the real one. A score was computed as the rate of the number of words correctly written and as the total number of words in the two phrases (including articles and prepositions). The average score was 35%. The following weights were then adopted: 1 for unshifted subbands, 0.35 for subbands shifted by one position, and 0 for subbands shifted by two or more positions.

3. SUBBAND WEIGHTS

Also employing subjective tests, it seemed that subbands containing the first three formants in their correct positions

guarantee 100% of intelligibility in spite of all other subbands being permuted. This fact suggests that an objective measure could be determined based exclusively on the position of these three subbands containing the first three formants. However, this measure would require formant extraction and therefore the measure would be signal-dependent, which should be avoided. In order to weigh each subband without signal dependence, we have extracted, using linear predictive code (LPC) parameters, the first three formants of a set of 10 phonetically based Portuguese spoken phrases. Each phrase was spoken by 20 different speakers, totalizing 200 phrases. The silence intervals were manually removed. The histograms of the first, the second, and the third formants were computed. It is known [4] that the first formant is the most important one for voiced speech and the third formant is the most important (among the 3 first ones) for unvoiced speech. Conversely, the second formant has approximately the same importance for both voiced and unvoiced speeches. According to our investigation, for short-time frames (around 8 milliseconds) from Portuguese, language spoken in Brazil, approximately 75% of the frames are voiced speech and 25% are unvoiced. Taking this information into account, we propose the following expression to weigh the ith subband:

$$\mathrm{SBW}_i = \frac{(0.75M1_i + \ 0.5M2_i + \ 0.25M3_i)}{1.5}, \quad i = 1, \ldots, N, \tag{1}$$

where $M1_i$, $M2_i$, and $M3_i$ are the percentages of the occurrence of the first, second, and third formants in the ith subband (to be obtained from the histograms).

In (1), the value 0.75 multiplying $M1_i$ is due to the fact that the first formant is the most important one for voiced frames, which represent 75% of all frames. Similarly, the value 0.25 multiplying $M3_i$ is due to the third formant being the most important one for unvoiced frames, which represent 25% of frames. Since the second formant has approximately the same importance for all frames, the constant multiplying $M2_i$ was set to 0.5, the mean of the previous values. The division by the normalization factor 1.5 was carried out in order to have the values of SBW_i between 0 and 1.

Table 1 shows the results of each subband weight computed from (1) with the percentages of occurrence of the first three formants at each subband (obtained from the procedure previously described) for all subbands from 1 to $N = 8$. It can be noted from this table that $\sum_{i=1}^{N} \mathrm{SBW}_i = 1$. The next section proposes the new objective measure of intelligibility that takes into account the subband weight and the position distance.

4. COMPUTING THE OBJECTIVE MEASURE

With the results obtained in the two previous sections, we can formulate an expression for an objective performance measure (OM) based on what follows. (a) The intelligibility is a function of the shifts in the subbands of the three first formants. (b) The weights in Table 1 can be understood as the probability of one of the formants to belong to subband i, that is, the importance (weight) of the subbands. (c) By shifting the "x" positions of one subband and multiplying the subband by the weight assigned to that position distance (1 if $x = 0$, 0.35 if $x = 1$, or 0 if $x > 1$), we are giving the due importance to the shifted subband. In order to better explain this new objective measure, we provide the following example.

Assume that we have permutation POS2 = [1 3 2 5 4 7 6 8]^T instead of the original sequence (clear signal) POS1 = [1 2 3 4 5 6 7 8]^T. The following steps are used to describe how to compute the objective measure (OM) for this permutation.

(1) Determine the position distance (PD) as the difference between POS1 and POS2, in absolute values. In this example, PD = [0 1 1 1 1 1 1 0]^T.
(2) Determine the weight vector associated to this position difference (PDW). In this example, PDW = [1 0.35 0.35 0.35 0.35 0.35 0.35 1]^T.
(3) Form the subband weight (SBW) from Table 1 according to vector POS2, that is, SBW = [33.74 12.50 15.36 9.48 9.40 2.61 12.66 4.25]^T/100.
(4) Compute the OM from (2)

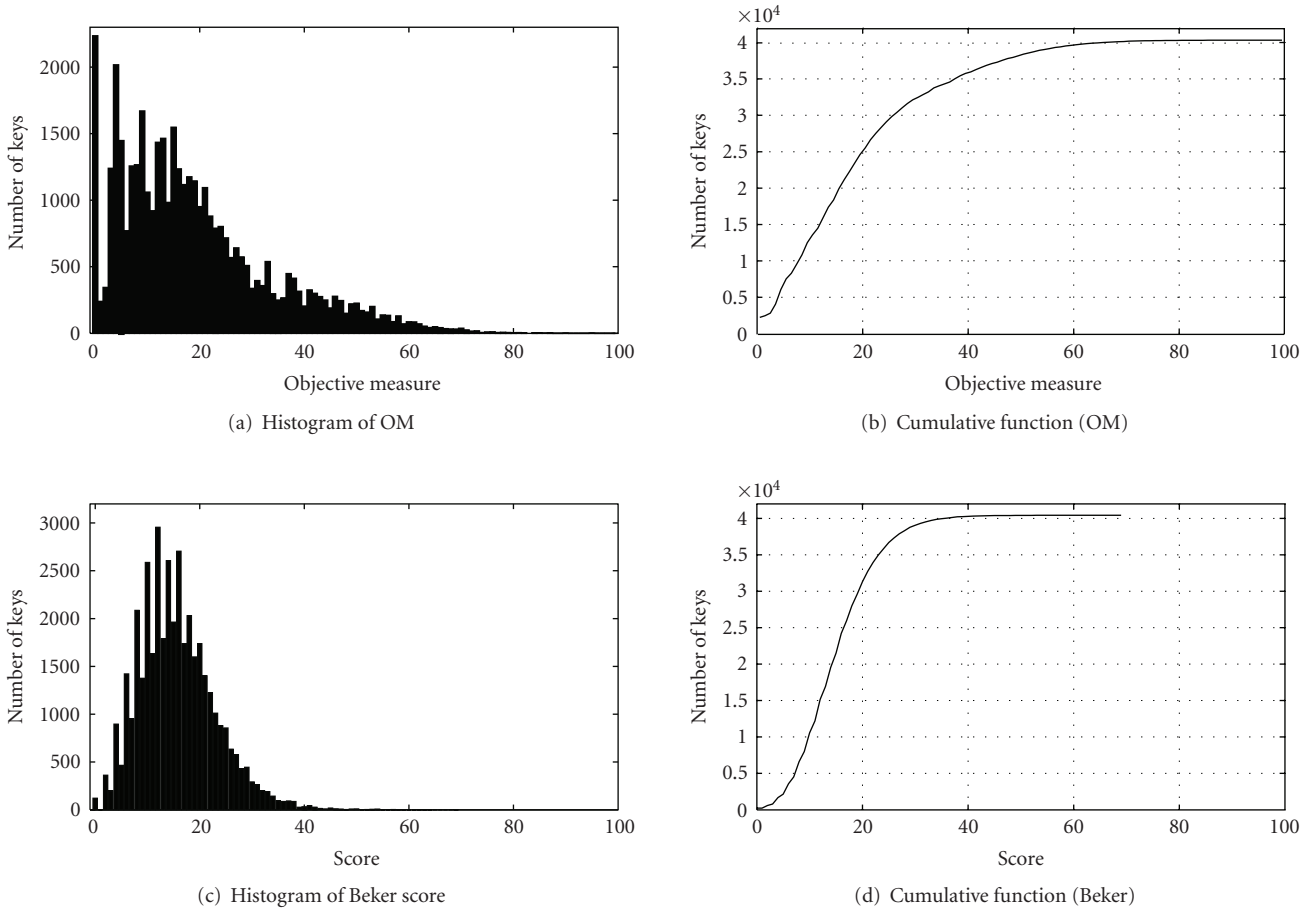
$$\mathrm{OM} = \frac{(\mathrm{PDW}^T \mathrm{SBW})}{\mathrm{MV}}, \tag{2}$$

where the denominator is the maximum possible value for the numerator and is given by MV = [1 1 1 1 1 1 1 1] SBW. For this example, we have MV = 1 and OM = 59.7%.

In the case of 8 permutable subbands, we have 8! = 40320 different keys. For all possible keys, Figures 1(a) and 1(c) depict the histograms (number of outcomes per range of OM values) of the proposed objective measure and the Beker score [3]. (The Beker score, as implemented in [3], comprises a distance measure instead of an intelligibility measure; we have then mapped the score results such that mapped score = 32-score.) Meanwhile, Figures 1(b) and 1(d), having cumulative functions (similar to estimates of the cumulative probability distribution functions if divided by 8!), show the number of keys for which the objective measure and the Beker score, respectively, are lower than a prescribed value. Note that the histograms from Figures 1(a) and 1(c) suggest that the probability density function of the OM is a superposition of its two effects: one due to the position distance (as in the pdf of the Beker score) and one due to the subband weight (only present in the OM). Based on Figure 1(b), if we assume, for instance, that 10 is the maximum value of the objective measure such that the signal is considered to be unintelligible (i.e., the corresponding key is efficient), then only approximately 13 000 out of the 8! can be used. This result reinforces the information in [1] which states that from the whole set of possible permutations, only a small set of keys can be considered efficient. If the same procedure is carried out employing the Beker score, the result would be around 10 000. We claim from this result that a slightly larger number of keys can be chosen when compared to the number obtained from the technique in [3]. The grounds for this claim come from the next section where we address the correlation of both objective measures with subjective tests.

Table 1: Subband weights.

Subband i	1	2	3	4	5	6	7	8
SBW$_i$	0.3374	0.1536	0.1250	0.0940	0.0948	0.1266	0.0261	0.0425



(a) Histogram of OM

(b) Cumulative function (OM)

(c) Histogram of Beker score

(d) Cumulative function (Beker)

Figure 1: Histograms and cumulative functions of the OM and the Beker score.

5. EVALUATING THE CORRELATION WITH SUBJECTIVE TEST

In order to evaluate the correlation between the proposed objective measure and a subjective measure, an experiment was carried out as follows. Eight phrases from a set of phonetically balanced Brazilian- Portuguese phrases were selected. From subbands 1 to 8, the initial (clear speech) vector is given by POS1 = $[1\ 2\ 3\ 4\ 5\ 6\ 7\ 8]^T$. For this experiment, 8 permutations were chosen (each corresponding to a vector POS2 as in the previous section): P1 = $[8\ 7\ 3\ 4\ 5\ 6\ 1\ 2]^T$, P2 = $[2\ 1\ 4\ 3\ 6\ 5\ 8\ 7]^T$, P3 = $[1\ 3\ 2\ 5\ 4\ 7\ 6\ 8]^T$, P4 = $[3\ 2\ 1\ 4\ 7\ 6\ 5\ 8]^T$, P5 = $[1\ 2\ 8\ 7\ 6\ 5\ 4\ 3]^T$, P6 = $[3\ 4\ 1\ 2\ 5\ 6\ 7\ 8]^T$, P7 = $[2\ 1\ 3\ 4\ 5\ 6\ 7\ 8]^T$, and P8 = $[1\ 4\ 3\ 2\ 5\ 8\ 7\ 6]^T$. Using the same procedure previously described, the OM is computed for each of the 8 permutations. Each phrase was ciphered with a fixed key corresponding to the 8 permutations from P1 to P8, and 14 nonexperts listened 4 times to each phrase. For each of the 8 permutations, a subjective score was computed (SM from subjective measure) as the rate between the number of correct words and the total number of words. Table 2 shows both measures (OM and SM) and the absolute error (|OM-SM|) for the 8 permutations. From Table 2, the mean absolute error is computed and the result is 8.61%; this shows a good correlation between OM and SM. Another form of assessing the correlation is given by the so-called Spearman coefficient [3] which is widely used in nonparametric (ranking) correlation and is considered insensible to outliers. In obtaining the Spearman coefficient, the permutations used in the experiment were ranked (from the largest to the smallest value of the OM, the SM, and the Beker score).

Table 3 presents the resulting rankings (the subjective measure rankings were ordered in the first row and the corresponding permutations were indicated in the last row).

The Spearman coefficient (r) is computed by the following expression:

$$r = 1 - \frac{6 \sum_{i=1}^{N} D_i^2}{N(N^2 - 1)}, \tag{3}$$

Table 2: OM, SM, and the absolute error (|OM-SM|) in % for the 8 permutations.

Permutation	P1	P2	P3	P4	P5	P6	P7	P8
OM	44	35	59.7	41.7	56.9	29	68.1	58.3
SM	39.5	27.5	54.6	31.3	38.9	23.9	57.5	66
|OM-SM|	4.5	7.5	5.1	10.4	18	5.1	10.6	7.7

Table 3: Rankings for SM, OM, and Beker score.

SM ranking	1	2	3	4	5	6	7	8
OM ranking	3	1	2	5	4	6	7	8
Beker ranking	3	1	5	6	8	3	7	2
Permutation	P8	P7	P3	P1	P5	P4	P2	P6

where D_i is the difference between the positions of the ith ranking and N is the size of the ranking (8 in the present case).

The values of r for both cases, between the OM and the SM and between Beker score and the SM, were computed (with D_i from Table 3) and the results were 0.9048 and 0.2024, respectively. These results show a strong correlation between the OM and the SM. In another experiment carried out by the authors with 23 permutable subbands, the Spearman coefficient obtained for the proposed measure, with respect to the subjective measure, was 0.9636, suggesting a higher correlation as the number of subbands increases. The Spearman coefficient of the Beker score was particularly low in this case; this results from the fact that the permutations used aimed to highlight the importance of each subband. It is worth mentioning that the score does not take into account which subbands are kept in their original positions; permutations $[1\ 2\ 3\ 4\ 8\ 7\ 6\ 5]^T$ and $[4\ 3\ 2\ 1\ 5\ 6\ 7\ 8]^T$, for example, have the same Beker score, but if we listen to a signal ciphered by them, the resulting intelligibilities are quite different (note that the first subband, due to the high probability of having the first formant, has a higher weight and is more intelligible if kept unaltered).

6. CONCLUSION

A new objective measure is proposed to evaluate the degree of intelligibility of a signal having its subbands permuted by a frequency domain scrambler. The measure can be used to generate efficient keys for frequency scramblers as well as to assess the performance of cryptanalysis schemes. All values presented in our simulations were specially tailored for this particular experiment: 8 subbands and Portuguese language.

REFERENCES

[1] N. S. Jayant, "On the effective number of keys in a voice, privacy system based on permutation scrambling," *AT&T Technical Journal*, vol. 66, no. 1, pp. 192–196, 1987.

[2] S. Sridharan, E. Dawson, and B. Goldburg, "Fast Fourier transform based speech encryption system," *IEE Proceedings I*, vol. 138, no. 3, pp. 215–223, 1991.

[3] H. J. Beker and F. C. Piper, *Secure Speech Communications*, Academic Press, Boston, Mass, USA, 1985.

[4] D. Klatt, "Prediction of perceived phonetic distance from critical-band spectra: a first step," in *Proceedings of the IEEE International Conference on Acoustics, Speech ,and Signal Processing (ICASSP '82)*, vol. 7, pp. 1278–1281, Paris, France, May 1982.

:: Open Access ::

EURASIP Journal on

Bioinformatics and Systems Biology

http://www.hindawi.com/journals/bsb/

Special Issue on

Network Structure and Biological Function: Reconstruction, Modelling, and Statistical Approaches

Call for Papers

We are particularly interested in contributions, which elucidate the relationship between structure or dynamics of biological networks and biological function. This relationship may be observed on different scales, for example, on a global scale, or on the level of subnetworks or motifs.

Several levels exist on which to relate biological function to network structure. Given molecular biological interactions, networks may be analysed with respect to their structural and dynamical patterns, which are associated with phenotypes of interest. On the other hand, experimental profiles (e.g., time series, disturbations) can be used to reverse engineer network structures based on a model of the underlying functional network.

Is it possible to detect the interesting features with the current methods? And how is our picture of the relationsship between network structure and biological function affected by the choice of methods?

Perspectives both from simulation approaches as well as the evaluation of experimental data and combinations thereof are welcome and will be integrated within this special issue.

Authors should follow the EURASIP Journal on Bioinformatics and Systems Biology manuscript format described at the journal site http://www.hindawi.com/journals/bsb/. Prospective authors should submit an electronic copy of their complete manuscript through the journal Manuscript Tracking System at http://mts.hindawi.com/, according to the following timetable:

Manuscript Due	June 1, 2008
First Round of Reviews	September 1, 2008
Publication Date	December 1, 2008

Guest Editors

J. Selbig, Bioinformatics Chair, Institute for Biochemistry and Biology, University of Potsdam, Germany; selbig@mpimp-golm.mpg.de

M. Steinfath, Institute for Biochemistry and Biology, University of Potsdam, Germany; steinfath@mpimp-golm.mpg.de

D. Repsilber, AG Biomathematics & Bioinformatics, Genetics and Biometry and Genetics Section, Research Institute for the Biology of Farm Animals, Dummerstorf, Germany; repsilber@fbn-dummerstorf.de

Hindawi Publishing Corporation
410 Park Avenue, 15th Floor, #287 pmb, New York, NY 10022, USA

HINDAWI

:: Open Access ::

EURASIP Journal on Embedded Systems

http://www.hindawi.com/journals/es/

Selected Papers from SLA++P 2007 Model-Driven High-Level Programming of Embedded Systems

Call for Papers

Model-based high-level programming of embedded systems has become a reality in the automotive and avionics industries. These industries place high demands on the efficiency and maintainabiliy of the design process as well as on the performance and functional correctness of embedded components. These goals are hard to reconcile in the face of the increasing complexity of embedded applications and target architecures that we see today. Research efforts towards meeting these goals have brought about a variety of high-level engineering design languages, tools, and methodologies. Their strength resides in clean behavioral models with strong semantical foundations providing a rigorous way to go from a high-level description to provable, that is, mathematically certifiable, executable code.

Undebatably, the most successful representatives of this trend of putting logic and mathematics behind design automation in embedded systems (known as Mike Fourman's "Lambda" programme) are synchronous languages. Firmly grounded in clean mathematical semantics, they have been receiving increasing attention in industry ever since they emerged in the 1980s. Lustre, Esterel, Signal are now widely and successfully used to program real-time and safety critical applications, from nuclear power plant management layer to Airbus air flight control systems. Their recent successes in the automatic control industry highlight the benefits of formal verification and automatic code generation from high-level models.

Model-based programming is making its way in other fields of software engineering, too, often involving cyclic synchronous paradigms. Strong interest is emerging in component programming for large-scale embedded systems, in the link between simulation tools and compiler tools, in languages for describing the system and its environment, integrated tools for both compilation and simulation of more general models of communication and coordination, and so on. The impact of such unifying methodologies will depend, among other things, on the extent to which it will be possible to maintain the high degree of predictability and verifiability of system behavior that is the strength of the classic synchronous world.

Topics of interest for this special issue cover, among others, the following:

- Synchronous programming formalisms
- Novel language paradigms blending synchrony with asynchrony and nondeterminism, discrete with continuous control
- Techniques for component abstraction and refinement
- New models of communication and coordination for embedded systems
- Model-based compilation and simulation techniques
- Specification, verification, and model-based testing
- Case-studies, industrial and teaching experiences

Submission to this special issue limited to the participants of the SLA++P conference who have been invited to submit to this issue.

Authors should follow the EURASIP Journal on Embedded Systems manuscript format described at the journal site http://www.hindawi.com/journals/es/. Prospective authors should submit an electronic copy of their complete manuscript through the journal Manuscript Tracking System at http://mts.hindawi.com/, according to the following timetable:

Manuscript Due	March 1, 2008
First Round of Reviews	June 1, 2008
Publication Date	September 1, 2008

Guest Editors

Florence Maraninchi, VERIMAG Laboratory, 38610 Gieres, France; florence.maraninchi@imag.fr

Michael Mendler, University of Bamberg, 96045 Bamberg, Germany; michael.mendler@wiai.uni-bamberg.de

Marc Pouzet, Laboratoire de Recherche en Informatique (LRI), Université Paris-Sud 11, 91405 Orsay Cedex, France; marc.pouzet@lri.fr

Hindawi Publishing Corporation
410 Park Avenue, 15th Floor, #287 pmb, New York, NY 10022, USA

HINDAWI