愛知工業大学研究報告
第２９号　平成６年

Quantitative Estimation of Improving Speech Quality by the Isomorphic Emphasis in Spectrum Scrambling Encryption over Poor Radio Channels

スペクトラムスクランブル秘話のフェーディング伝送路における送受同形エンファシスによる通話品質改善効果の定量評価

岸　政七†，　岩田　宏†，　小崎康成†
Masahichi KISHI, Hiroshi IWATA, Yasunari KOZAKI

ABSTRACT *Phenomena of speech quality being hardly damaged from surrounding noise in comparison with SNR or segmental SNR are many times encountered in running vehiculars or airbornes even if the communication is carried without any encryptions. This difference between these evaluations and speech quality is comes from so called masking effect, which strongly appears when communications being carried through such noise with high frequency component as in running vehiculars or airbornes. Especially, the masking effect strongly appears when encryption is employed to prevent communication security from jeopardy according to genius of human voice. At first, in this paper, a new estimation method of speech quality is proposed with base on the Zwicker's method to evaluate qualitative speech degradation when various encryptions being employed. The isomorphic emphasis previously reported by one of this paper's authors, is secondly discussed to quantitatively evaluate the effect in improving speech quality over poor radio channels when encryption is employed. The amount of improving speech quality by employing isomorphic emphasis over radio channel with spectrum inversion is count up to 12 dB through both theoretical analysis and experimental results.*

1.INTRODUCTION

Accompanying social advances and diversification, it becomes to be eager to take communication on vehiculars, airbornes, and etc.

The user of these vehicular communication systems finds merit in being able to place and receive calls whenever or wherever he wants. However, since these calls is carried by radio waves, it is easy to eavesdrop on them, placing their confidentiality in jeopardy. To overcome this demerit, the idea of adding an encryption function to radio communications has been investigated from various approaches. However, as is common with most radio communication systems to which as encryption function has been added, the spectrum scrambler requires sacrifice in speech quality. The increase of effective modulation deviation produced in the spectrum scrambling process is a major cause of transmission SNR degradation. Therefore, it is necessary to avoid this increase in effective PM index when providing an encryption function to a communication system.

The isomorphic emphasis suppresses increase of the effective modulation on spectrum scrambled channels, to reduce fading noise over poor radio channels, and also to avoid any installation of arbitrary spectrum scramble circuit. Furthermore, it has strongness in this production since both sending and receiving emphasis being equal in implementations.

†愛知工業大学　情報通信工学科（豊田市）

The following sections will evaluate quantitatively noise reduction effect of isomorphic emphasis over encryption channel with spectrum scrambling according to the method proposed in this paper.

2. THE CONCEPT OF QUANTITATIVELY MEASURING SPEECH QUALITY

As well known, there exists two measuring methods in audiometric level for widely spread spectrum of time continuous noise, 1. Stevens' method which introduces loudness index as describing function corresponding to both frequency and sound pressure level, 2. Zwicker's method based on the model of the using stimulus patten on critical band[1].

Now, we propose new measuring method of speech quality based on Zwicker's method in the case both signal and noise being spectrum. Same as to Zwicker's method, let sound pressure level of noise be $SPL(f)$, noise power of critical band i be E_{Gi}, that is, noise level of the same critical band i is defined by $L_{Gi}\,(phon)$, equivalent sound pressure level being L_{EQi} respectively. These are defined as follows.

$$E_{Gi} = \int_{f_{Li}}^{f_{Ui}} SPL(f)df \tag{1}$$

$$L_{Gi} = 10\log_{10} E_{Gi} \tag{2}$$

$$L_{EGi} = L_{Gi} + \delta L_{Gi}. \tag{3}$$

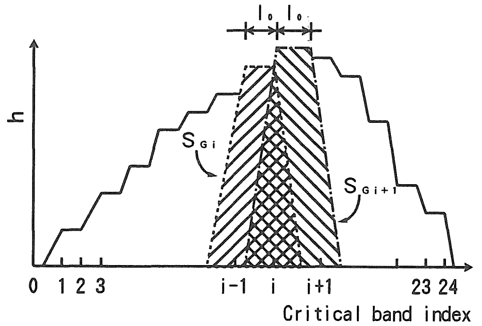

Fig.1 Auditory stimulus pattern model

Here, f_{Li} and f_{Ui} are the infimum and supremum of each critical band i. δL_{Gi} is scaling factor for equivalent sound pressure level at 1 kHz.

Where the stimulus is given by $N_{Gi}\,(sone)$ of noise L_{Gi}, trapezoid area S_{Gi} shown in fig.1, audiometric excitation owing to N_{Gi} is given as follows.

$$S_{Gi} = 2N_{Gi}l_0^2 \quad and \quad S_{Gi} = \frac{1}{2}(n_i+1)h_i l_0^2. \tag{4}$$

Here, h_i and n_i means height and base length of thetrapezoid i.
In eq.4, h_i and n_i are given by

$$h_i = \frac{4N_{Gi}}{(n_i+1)} l_0 \tag{5}$$

$$n_i = 10^{0.0108(L_{Gi}-20)}. \tag{6}$$

The stimulus N_{Gi} is defined by L_{Gi} as follows.

$$\begin{aligned} &\log_2(N_{Gi}) = 0.03(L_{Gi}-40), && if\ L_{Gi} \geqq 20 \\ &N_{Gi} = 0, && else. \end{aligned} \tag{7}$$

S_G also expresses total square measure, S_G whose amount is given by summing up on 24th trapezoid areas $S_{G0} \sim S_{G23}$ as shown in fig.1. Therefore, the S_G corresponding to total stimulus N_G is given by

$$N_G = \frac{S_G}{2l_0^2}. \tag{8}$$

The equivalent sound pressure level L_{EQ} of

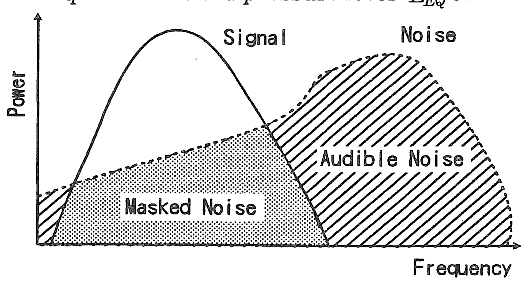

Fig.2 Characteristics both of signal and noise for transmission signals

stimulus N_G is finally given as,

$$L_{EQ} = \frac{\log_{10} N_G}{0.03} + 40. \quad (9)$$

When communication is carried over vehicular telephone systems, speech is always suffered from fading noise. Both signal and fading noise of transmission signals are featured as shown in fig.2 from the spectrum patten on the base band at the receiving site. The noise is audible on the frequency if noise power exceeds more than that of signal. In other wards, noise is masked by signal at where noise power is less than signal power on the same frequency domain. Therefore, we can reach to new solution in getting quantitative measuring method through analyzing L_{EQ} as shown in fig.2 following to Zwicker's method. Zwicker's method is required to stand on time continuous signals, while the dominate component of noise is fading in vehicular communications. In the case when vehicular runs at 40 km/s speed, the fading pitch comes up to 40 Hz at 800 MHz of current systems. Therefore, it becomes reasonable to analyze such discrete fading noise as continuous noise.

3. COMPARISON OF THE EXISTING ENCRYPTION SYSTEM AND THE ISOMORPHIC EMPHASIS ENCRYPTION SYSTEM

3.1 Transmission Circuit

The block diagram with the Isomorphic Emphasis Spectrum Scrambling Encryption system (ab. in IESSE system) is shown in fig.3. As shown in fig.3, the IESSE system is featured of installing order in signal-Processing Half Unit (ab. in PHU) at both sending and receiving sites. That is, pre-emphasis at sending site is prefixed to the scrambler $S[*]$ in similar to ordinally sequence. De-emphasis at receiving site is also prefixed to the de

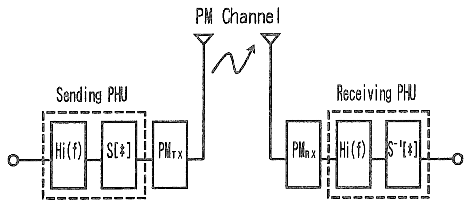

Fig.3 Consideration of Isomorphic Emphasis Spectrum Scrambling System

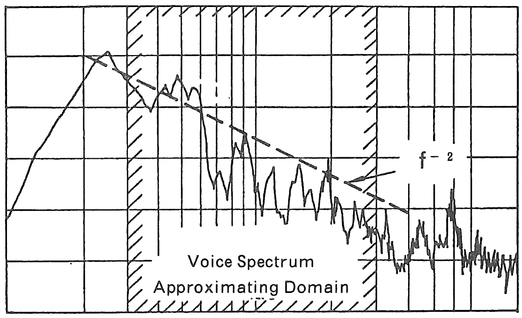

Fig.4 Typical long-time average of human voice

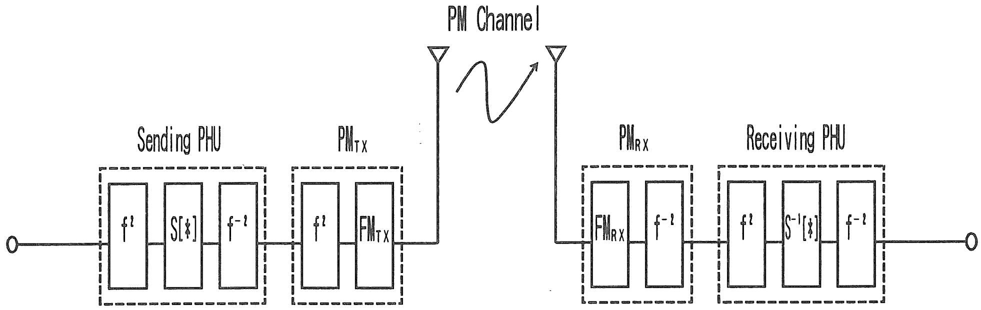

Fig.5 System Configuration of Spectrum Scrambling Transmission

scramble $S^{-1}[*]$ in the receiving PHU. Both pre-emphasis and de-emphasis are uniquely given by the unique isomorphic emphasis $H_i(f)$.

Now, consider circuit configuration of the IESSE system briefly. Where input signal is $G(f)$, the square amplitude function $H_i(f)$ of isomorphic emphasis is given

$$H_i(f) = S[G(f)]/G(f) \tag{10}$$

here, $S[G(f)]$ *is scrambled signal of* $G(f)$.

Let assume the spectrum scramble being spectrum inversion, $S[G(f)]$ is given as,

$$S[G(f)] = G(f_0 - f) \tag{11}$$

where f_0 *is pivotal frequency of spectrum inversion,* $f_0 = f_L + f_U, f_U$, f_L *is the infimum or supremum ends of the frequency band, respectively.*

Typical long-term average of human voice exhibits predominantly f^{-2} characteristic as shown in fig.4. Therefore, the square amplitude function $H_i(f)$ of isomorphic emphasis is consequently given by

$$H_i(f) = f^2(f_0 - f)^{-2}. \tag{12}$$

The output signal $S[H_i(f)G(f)]$ of the PHU is modified as follows,

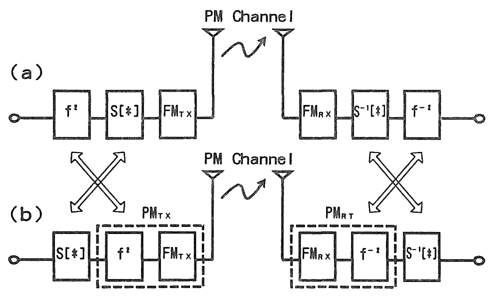

Fig.6 Comparison of transmission system for speech encryption. (a)IESSE System (b)ESSE System

Table.1 An analysis result for auditory stimulus of inverse triangle noise power.

critical band					
No.	band	bandwidth	L_{Gi} (dB)	L_{EGi} (phon)	N_{Gi} (sone)
4	295- 395	100(95)	69.0	65.0	5.62
5	395- 503	108	67.3	64.3	5.36
6	503- 625	120	65.8	63.8	5.18
7	625- 755	130	64.4	63.4	5.04
8	755- 900	145	63.2	62.2	4.63
9	900-1060	160	62.2	62.2	4.63
10	1060-1250	190	61.5	61.5	4.42
11	1250-1460	210	60.5	60.5	4.12
12	1460-1700	240	59.8	59.8	3.93
13	1700-1990	270	59.0	59.0	3.72
14	1970-2290	320	58.5	58.5	3.59
15	2290-2670	380	57.9	57.9	3.44
16	2670-3120	450(330)	56.0	56.0	3.02
				N_G	30.6 (sone)

$$S[H_i(f)G(f)] = S\left[f^2(f_0 - x)^{-2}G(f)\right]. \tag{13}$$

Substituting variable x into $f_0 - f$, it gives,

$$\begin{aligned} S[H_i(f)G(f)] &= x^{-2}(f_0 - x)^2 G(f_0 - x) \\ &= f^{-2}S[f^2G(f)] \end{aligned} \tag{14}$$

Equation 14 suggest that the PHU is realized with canonical form of cascading a differentiator, an arbitrary spectrum scramble, and an integrator as show in fig.5.

For ease of realizing PM modulator, it is equivalently realized with prepositioning a differentiator to FM modulator, and the PM demodulator being also realized with postpositioning an integrator to FM demodulator as

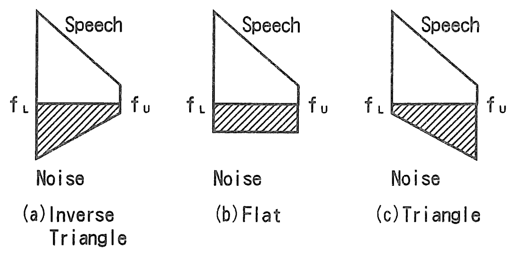

Fig.7 Typical power spectrum of the fading-noise

shown in fig.5. So long as these equivalent circuits being adopted to IESSE systems, both the integrator and differentiator are canceled out among equivalent circuit and PHU at each site, if only if both are ideal on the subjective frequency domain.

Finally, we get simple configuration for IESSE system as shown in fig.6(a), where all of expressive circuits are excluded from realization.

As just mentioned aboves, the isomorphic emphasis is facilitated in factor without installing any additional circuits, which makes the cost benefit maximum in applying it to spectrum scrambling system. As shown clearly in fig.6, only installing order of IESSE shown in fig.6(a) is different from that of without emphasis **E**xisting **S**pectrum **S**crambling **E**ncryption system (ab. in ESSE system) shown in fig.6(b), even if there exists such the same elements as differentiator, scrambler, and FM_{TX} at sending site, or as FM_{RX}, descrambler, and an integrator at receiving site [2,3].

3.2 Effective Modulation

Now, we consider the effective modulation to know how being suppressed occupied frequency bandwidth. Set Div_{PM} to be effective modulation index of PM transmission without encryption, Div_{ES} to be that of ESSE, and Div_{IE}

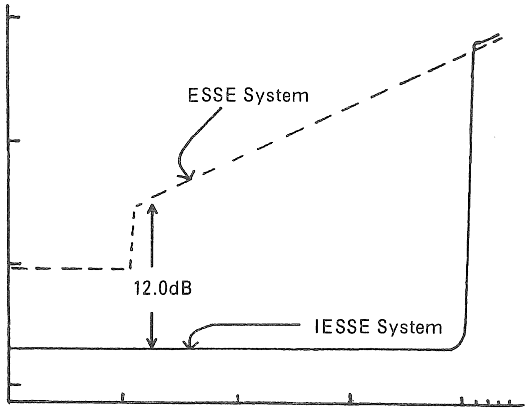

Fig.8 Characteristic of equivalent sound pressure level vs signal-to-noise ratio

Table.2 Audiometric levels for three typical spectrum paterns of the fading noise.

	Pattern of noise spectrum	Inverse Triangle	Flat	Triangle
Analyzed value	Zwicker's metod (sone)	30.6	33.9	40.6
	Relative Indication (dB)	0	3.3	10.5
Measurement value	JIS-A(IEC-A) (dB)	-45	-43.5	-41
	CCIR (dB)	-29	-26	-21
	DIN (Noise) (dB)	-30	-27	-23

* bandwidth from 0.3 to 3.0 kHz

to be that of IESSE. These indexes are given as follows.

$$Div_{PM} = \int_{f_L}^{f_U} f^2 G(f) df \tag{15}$$

$$Div_{ES} = \int_{f_L}^{f_U} f^2 S[G(f)] df \tag{16}$$

$$Div_{IE} = \int_{f_L}^{f_U} S[f^2 G(f)] df. \tag{17}$$

For clarity of discussing in modulation increase, the scrambling is assumed without any loss of generality to be spectrum inversion which gives the maximum increasing effective modulation.

$$\begin{aligned} Div_{ES} &= \int_{f_L}^{f_U} f^2 S[G(f)] df \\ &= \int_{f_L}^{f_U} f^2 G(f_0 - f) df \end{aligned} \tag{18}$$

$$\begin{aligned} Div_{IE} &= \int_{f_L}^{f_U} S[f^2 G(f)] df \\ &= \int_{f_L}^{f_U} (f_0 - f)^2 G(f_0 - f) df, \\ &\quad substitute x = f_0 - f,\ dx = -df \\ &= \int_{f_L}^{f_U} x^2 G(x)(-dx) \\ &= \int_{f_L}^{f_U} f^2 G(f) df \\ &= Div_{PM} \end{aligned} \tag{19}$$

Eq.19 guarantees the isomorphic emphasis being maintable in effective modulation index wherever any scramble are adopted into its transmission systems.

4. NOISE REDUCTION EFFECT

Typical power spectrum of fading noise generated through various transmission system are categorized in fig.7. Upper side of each figure means speech component and lower means noise. Fig.7(a) shows the typical pattern for PM receiving signals which features two inverse triangles along to frequency axis, fig.7 (b) shows FM signals which features flat spectrum of fading noise, and fig.7(c) shows PM signals which is featured of inverse triangle of speech and of normal triangle of noise when spectrum inversion being employed in such ESSE systems. Now, we quantitatively compare audiometric levels of these typical power spectrums shown in fig.7(a),(b),(c), under following assumption that these patterns being compensated to be equal in sound pressure level *SPL* , inverse triangle of fig.7(a) being described with f^{-2}, flat of fig.7(b) being unity, normal triangle of fig.7(c) being defined by $(f_0-f)^{-2}$. An analysis result for audiometric stimulus of inverse triangle noise power is shown in table.1. Audiometric levels for three typical spectrum patterns of the fading noise are analyzed as shown in table.2. The audiometric stimulus of inverse triangle is given as 30.6 sone, that of flat is 33.9 sone, and that of triangle is 40.6 sone.

The most superior speech quality is given when noise shape is inverse triangle pattern, and the most inferior speech quality is given when noise is normal triangle pattern. The difference in speech quality is given by more than 10 dB. These terms are also examined to be similar to MOS value and also ensured by another measuring criteria givenly ref.4,5.

The speech quality is shown to be most hardly damaged from spectrum inversion in comparison with three typical noise pattern even if with common speech spectrum. Therefore, noise suppression effect is hereafter quantitatively analyzed under assumption with employing isomorphic emphasis, i.e., being concerned with IESSE systems. The long-term average of fading noise is white before scrambling. This frequency characteristics of the white is still remained in any spectrum scrambling processing. Therefore, it is easy to conjecture that the spectrum of being white contained in the output of the scrambler which is able to integrate output signal would have an f^{-2} characteristic of inverse triangle as shown in fig.7(a). Therefore, IESSE system guarantees that the frequency characteristic of noise power is maintained during any kind of spectrum scrambling to give no excessive audiometric stimulus as shown in table.2.

The quantitative amount of improving speech quality by employing isomorphic emphasis in the spectrum inversion encryption is shown in fig.8 as the characteristic of equivalent sound pressure level vs. signal-to-noise rate. Here, human voice speech is assumed to be given by f^{-2}, noise of IESSE system is assumed to be proportional to f^{-2}, and noise of ESSE system is given by inverted form of $(f_0-f)^{-2}$. The equivalent sound pressure level of the IESSE system is less than that of the ESSE system over all range of SNR. The IESSE system is recognized to improve audiometric level of speech quality by more than 12 dB at the range of SNR being from 30 to 0 dB, and by more than 6 dB from 40 to 30 dB.

5. CONCLUSION

In this paper, isomorphic emphasis is quantitatively analyzed its effect of suppressing noise to prevent speech quality from degradations.

Modifying Zwicker's method, audiometric stimulus is calculated for typical three noise spectrum patterns generated through PM transmission system, FM one, and with spectrum inversion as the most hardly damaged among various spectrum scrambling.

Whatever scrambler being employed into transmission for implementation of speech security, isomorphic emphasis guarantees the speech quality by up to 12dB in comparison with without isomorphic emphasis function.

REFERENCES

[1]E.Zwicker and R.Feldikller, "Über die Lautstärke von gletchformigen Gerauschen", Acustica, 5, 303, 1955.

[2]Masahichi Kishi and Toshiyuki Maeshima, "Proposal of Isomorphic Emphasis in Spectrum Inversion of Analog PM Channels and Its Noise Reduction Effect", IEEE VTC'92, Denver, Colorado, pp.973 - 976, May 1992.

[3]Masahichi Kishi, "Illustrative Scheme of the Isormorphic Emphasis Spectrum Scramble Encryption", Transactions of the IECE Japan, Vol.J67 - B, No.4, pp.455 - 456, Apl. 1984.

[4]Masahichi Kishi, "Application of the Isomorphic Emphasis to Spectrum Scramble System and Its Noise Reduction", Transaction of the IECE Japan, Vol.J67 - B, No.7, pp.830 - 831, Jul.1984.

[5]Hugh Ford, "Noise Measurement", Studio Sound, pp.48 - 51, Nov.1980.

（受理　平成 6 年 3 月20日）