愛知工業大学研究報告
第２９号　　平成６年



# Application of the Isomorphic Emphasis to Spectrum Scrambling Encryption over Analog Speech Channels

# アナログ通話路におけるスペクトラムスクランブル秘話への送受同形エンファシスの適用

岸　政七†,　　服部徳宏†
Masahichi KISHI, Norihiro HATTORI

ABSTRACT *The mobile communication has the danger that the content of communication is intercepted, therefore, the encryption which protects confidentiality has been studied from various approaches. The existing method which was merely adding an encryption function, increases effective modulation index above the level of without encryption, and brings on a spread of radio frequency bandwidth. It is already reported that effective modulation index is maintained, when isomorphic emphasis applies to spectrum inversion encryption. This paper establishes that isomorphic emphasis maintains aforementioned feature, even if it applies to arbitrary spectrum scramble pattern, and it can be realized simple circuit. And this circuitry configuration is the most economical when it introduced into PM transmission.*

## 1. INTRODUCTION

The use of mobile communication has been spreading quickly in recent years, and those who posses this equipment enjoy the advantage of being able to place call whenever and wherever they desire. However, since these calls are carried by radio waves, the content of communication being jeopardized by interception. In order to guard this, adding encryption functions to vehicular communication has been studied from a variety of approaches[1].

Among the existing methods which merely add an encryption function, effective modulation index will increase above the level of without encryption. This increase brings on a spread of radio frequency bandwidth. It is necessary to reduce the input signal level greatly in order to avoid a extent of bandwidth. However, the noise level, which is a major cause of speech quality degradation in transmission systems, is not dependent on input signal level[2]. Therefore, reducing the input signal level is significant degradation of the speech quality. In this background, several methods have been proposed for carrying out emphasis while suppressing increase in effective modulation index[3,4]. One of the authors has shown the existence of a new kind of emphasis, called "Isomorphic Emphasis"[5, 6], and described that isomorphic emphasis maintains effective modulation index, focused on a spectrum inversion function[7].

This paper establishes that isomorphic em-

† 愛知工業大学　情報通信工学科（豊田市）

phasis maintains aforementioned feature, even if it applies to arbitrary spectrum scramble pattern. Then, this emphasis function is realized simple circuitry configuration without relating to the spectrum scramble pattern, when a canonical topology is employed based on isomorphic projection. And this circuitry configuration is the most economical when it applies to the existing analog vehicular communication system.

## 2. OUTLINE OF SPECTRUM SCRAMBLING TRANSMISSION SYSTEM WITH ISOMORPHIC EMPHASIS

The configuration of a spectrum scrambling transmission system employing isomorphic emphasis is shown in fig.1. This system is referred as the IESSE system, which is short for Isomorphic Emphasis Spectrum Scrambling Encryption system. Since this transmission system employs the isomorphic emphasis, it must satisfy the following conditions:

1) Irrespective of the input signal and spectrum scrambler characteristics, effective modulation index must always match the effective PM index of an input signal which has not undergone spectrum scrambling.

2) The transmission system must be distortion-free.

3) The emphasis circuit of the sending PHU and that of the receiving PHU must take the same form.

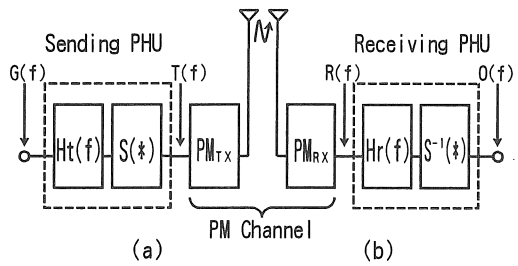


*Fig.1 A configuration of a spectrum scrambling transmission system employing isomorphic emphasis (IESSE), (a) sending system, (b) receiving system.*

## 3. DEFINITION OF IESSE TRANSMISSION SYSTEM

### 3.1 Maintainability of Isomorphic Emphasis Effective Modulation Index

Even if some kind of spectrum scrambling is carried out on the arbitrary input signal, that effective modulation index is always maintained. Then, to the extent that optimum design is employed it is possible for spectrum scrambling transmission system to make optimum use of radio wave resources using the existing equipment. From this viewpoint, isomorphic emphasis $H_t(f)$ which maintains the effective modulation index of transmission system shown in fig.1(a) is found below.

Now, by making the instantaneous power $G(f)$ of the arbitrary input signal, instantaneous power $T(f)$ of the input signal to the equivalent PM transmitter of the IESSE system can be expressed

$$T(f) = S[H_t(f)G(f)]. \tag{1}$$

Here, $S[*]$ denotes arbitrary spectrum scrambling, and $H_t(f)$ denotes the square amplitude function of isomorphic emphasis.

Accordingly, the effective modulation index $Div_{IE}$ of the IESSE system is expressed

$$Div_{IE} = \int_{f_1}^{f_2} f^2 T(f)df = \int_{f_1}^{f_2} f^2 S[H_t(f)G(f)]df. \tag{2}$$

Where, $f_1$, $f_2$ stands for the infimum and supermum ends of the subjection frequency band.

It is necessary condition that the effective modulation index given in eq.2 agree with effective PM index $Div_{PM}$ (eq.3) of the PM transmission system.

$$Div_{PM} = \int_{f_1}^{f_2} f^2 G(f)df. \tag{3}$$

Here, the following proposition is consid-

ered: That effective modulation index for arbitrary spectrum scrambling can be maintained.

Effective modulation index $Div'_{PM}$ which is spectrum scrambling of effective PM index $Div_{PM}$ is given

$$Div'_{PM} = \int_{f_1}^{f_2} S[f^2 G(f)]df. \tag{4}$$

Returning back to the integral definition, eq.4 is transformed as follows:

$$\begin{cases} Div'_{PM} = \lim\limits_{\Delta f \to 0} \sum\limits_{i=1}^{N} S[f_i^2 G(f_i)]\Delta f \\ \Delta f = (f_i - f_{i-1}) \\ N = (f_2 - f_1)/\Delta f. \end{cases} \tag{5}$$

However, all of the minute frequency domains $\Delta f$ having equal bandwidths. As shown in eq.5, effective modulation index $Div'_{PM}$ is given as the sum of the products of the minute domains $\Delta f$ and instantaneous power $S[f_i^2 G(f_i)]$, which is the integral value.

On the other hand, as shown in fig.2, no matter how complicated spectrum scrambling and descrambling may be, they can be thought of as arbitrary interchange of one to one between the above minute frequency domain. For example, with spectrum inversion given when the suffixes of the minute domains are in decreasing order, and with band division given when the suffixes of the minute domains are in the same order in prior divided band. Then, inversion within the divided band is equivalent to inverting the order of the minute domain suffixes within the cluster corresponding to that band.

Attention must be paid to carry out summing that there is no redundancy in any of the minute domain suffixes. Therefore, in defining one set of suffixes, eq.5 is rewritten as follows:

$$Div'_{PM} = \lim_{\Delta f \to 0} \sum_{i \in I} S[f_i^2 G(f_i)]\Delta f,$$
$$I = \{i \mid 1 \leq i \leq N\}. \tag{6}$$

In the above equation, the spectrum scrambling $S[*]$ changes only the order of the sum, do not change the value of the summation. Therefore, the next series of transformations becomes possible, and the proposition is proven.

$$\begin{aligned} Div'_{PM} &= \lim_{\Delta f \to 0} \sum_{i \in 1} f_i^2 G(f_i)\Delta f \\ &= \lim_{\Delta f \to 0} \sum_{i=1}^{N} f_i^2 G(f_i)\Delta f \\ &= \int_{f_1}^{f_2} f^2 G(f) df \\ &\equiv Div_{PM} \quad QED. \end{aligned} \tag{7}$$

Using the results of this proposition, emphasis $H_t(f)$ is found from the condition that effective modulation index $Div_{IE}$ of the IESSE system matches $Div_{PM}$. That is, if the integral value of eqs.2 and 3 are equal, the two modulation will be the same. Namely,

$$f^2 S[H_t(f)G(f)] \equiv S[f^2 G(f)]. \tag{8}$$

Because spectrum scrambling is the frequency transformation of the amplitude characteristic of the input signal, eq.8 can be fur-

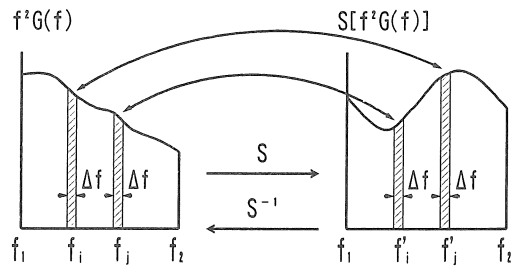


*Fig.2 An illustrative scheme of interchanges between minute frequency domain via spectrum scrambling/descrambling.*

ther transformed as follows:

$$f^2S[H_t(f)]S[G(f)] = S[f^2]S[G(f)]. \quad (9)$$

From this equation, an isomorphic emphasis can be given directly as follows:

$$S[H_t(f)] = f^{-2}S[f^2]. \quad (10)$$

In this equation, isomorphic emphasis $H_t(f)$ can not be expressed explicitly. In the next section, the accurate characteristic of emphasis $H_t(f)$ is cleared.

### 3.2 Circuitry Realization of IESSE transmission System

This section will take for the canonical topology shown in fig.3 and find a unique circuitry configuration in which spectrum scrambling is not affected, under the condition that isomorphic emphasis $H_t(f)$ and canonical topology are equal.

The canonical topology shown in fig.3 contains a skeleton structure wherein spectrum scrambling is sandwiched between the two circuit $H_a(f)$ and $H_b(f)$. Characteristic $H_a(f)$ and $H_b(f)$ of each circuit will be determined. When being made the same input signal that sending PHU to canonical topology to be $G(f)$, the output signal $T'(f)$ is given

$$T'(f) = H_b(f)S[H_a(f)G(f)]$$
$$= H_b(f)S[H_a(f)]S[G(f)]. \quad (11)$$

Substituting isomorphic emphasis eq.10 into eq.1, the characteristic function $H_a(f)$ and $H_b(f)$ are given below from the condition that eqs.1 and 11 are equal.

$$H_b(f)S[H_a(f)] = S[H_t(f)] = f^{-2}S[f^2]. \quad (12)$$

Consequently, if $H_a(f)$ and $H_b(f)$ are defined as

$$\begin{cases} H_a(f) = f^2 \\ H_b(f) = f^{-2} \end{cases} \quad (13)$$

then the condition equation $Div_{IE} = Div_{PM}$ is established irregardless of the spectrum scrambling characteristic. In fact, the effective modulation index of a transmission system which incorporates emphasis circuitry having the topology shown in fig.3, which has the characteristic functions given in eq.13, is expressed

$$\int_{f_1}^{f_2} f^2\{f^{-2}S[f^2G(f)]\}df = \int_{f_1}^{f_2} S[f^2G(f)]df$$
$$= \int_{f_1}^{f_2} f^2G(f)df.$$

This effective modulation index agree with effective PM index $Div_{PM}$. Therefore, with the circuitry topology shown in fig.3 as the precondition, it is proven thateq.13 is the necessary sufficient condition for maintaining effective modulation on the sending side.

The characteristics of the two isomorphic emphasis circuits defined in eq.13 are respectively the differential and integral characteristic. Since these characteristics can be realized by simple circuit, this circuitry configuration warrants excellent cost benefits.

## 4. DETERMINATION OF IESSE RECEIVING SYSTEM

### 4.1 Distortion-free Transmission Characteristic of Receiving Emphasis

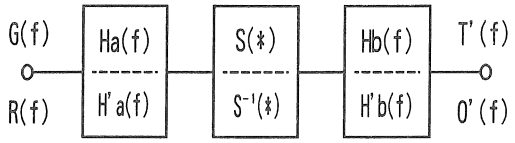


*Fig.3 Canonical topology of sending PHU and of receiving PHU.*

This section will through a transmission system applying sending emphasis $H_t(f)$, determine the receiving emphasis $H_r(f)$. Then, the circuit configuration of sending PHU, which is applied the characteristic function given in eq.13 and the canonical topology shown in fig.3, holds as a precondition. Also, in order not to lose generality in analysis, it supposes that the PM transmission channel is distortion-free.

In adopting the above topology, the input signal to be $T(f)$ of the PM modulator shown in fig.1(a) is given

$$T(f) = f^{-2}S[f^2G(f)] = f^{-2}S[f^2]S[G(f)]. \quad (14)$$

In fig.1(b), if the output signal of the PM demodulator is made to be $R(f)$, the output signal of the transmission system to be $O(f)$ is given

$$O(f) = S^{-1}[H_r(f)R(f)] = S^{-1}[H_r(f)]S^{-1}[R(f)]. \quad (15)$$

Here, if the condition that the PM transmission channel be distortion-free; that is, the input signal of the PM modulator be equal to the output signal of the PM demodulator, is applied, eq.15 will transform as follows:

$$O(f) = S^{-1}[H_r(f)]S^{-1}[R(f)] = S^{-1}[H_r(f)]S^{-1}[f^{-2}]f^2G(f). \quad (16)$$

Then by substituting the condition that the IESSE system be distortion-free; that is, output signal of the IESSE system be equal to its input signal, receiving emphasis $H_r(f)$ is given

$$S^{-1}[H_r(f)]S^{-1}[f^{-2}]f^2 = 1. \quad (17)$$

In the above equation, since receiving emphasis $H_r(f)$ is given by inverse mapping $S^{-1}[H_r(f)]$ spectrum scrambling, it cannot be realized explicitly. However, in fact, in the same way as sending emphasis, it can be realized by a simple circuit which incorporates isomorphic form.

### 4.2 Circuitry Realization of IESSE Receiving system

In meeting the condition that receiving emphasis $H_r(f)$ and a canonical topology shown in fig.3 taking on isomorphic form; this is, the same input signal that receiving PHU applied to the canonical topology, and the its output signal is corresponding to eq.15, characteristic function $H'_a(f)$ and $H'_b(f)$ are determined.

Being made the input signal to canonical topology to be $R(f)$, and the output to be $O'(f)$ is expressed as follows:

$$O'(f) = H'_b(f)S^{-1}[H'_a(f)R(f)] = H'_b(f)S^{-1}[H'_a(f)]S^{-1}[R(f)]. \quad (18)$$

From the condition that eqs.16 and 18 are equal, the isomorphic condition of receiving emphasis is given

$$S^{-1}[H_r(f)] = H'_b(f)S^{-1}[H'_a(f)]. \quad (19)$$

Being multiplied the value $S^{-1}[f^{-2}]f^2$ on the both sides, eq.19 is modified as

$$\begin{cases} Left\ \ side\ \ of\ \ eq.19 \\ \quad = S^{-1}[H_r(f)]S^{-1}[f^{-2}]f^2 \\ \quad = S^{-1}[H_r(f)f^{-2}]f^2 \\ Right\ \ side\ \ of\ \ eq.19 \\ \quad = H'_b(f)S^{-1}[H'_a(f)]S^{-1}[f^{-2}]f^2 \\ \quad = \{H'_b(f)f^2\}\{S^{-1}[H'_a(f)f^{-2}]\}. \end{cases} \quad (20)$$

The first equation of eq.20 matches with the left side of eq.17. Therefore, the condition for setting the last equation of eq.20 to be unity is a necessary sufficient condition for achieving isomorphic form. Namely,

$$\begin{cases} H'_a(f)f^{-2}=1 \Rightarrow H'_a(f)=f^2 : \\ \qquad\qquad differential\ function \\ H'_b(f)f^2=1 \Rightarrow H'_b(f)=f^{-2} : \\ \qquad\qquad integral\ function. \end{cases} \tag{21}$$

It is made clear that the characteristic function of each receiving emphasis circuit is independent of the spectrum descrambling characteristic.

When applying receiving emphasis shown in eq.21, the transmission system takes on the configuration shown in fig.4. Then a circuit structure with equal sending and receiving emphasis is adopted and condition 3 of the isomorphic emphasis is satisfied. Such a transmission system can be proven as follows to meet the necessary sufficient condition of distortion-freeness.

If the input signal to the transmission system is made to be $G(f)$ and the input signal to the PM modulator is to be $T(f)$, then

$$T(f)=f^{-2}S[f^2G(f)].$$

Also, assuming the PM transmission channel to be distortion-free, and making the output signal of the PM demodulator to be $R(f)$ and the output signal of the transmission system to be $O(f)$, then

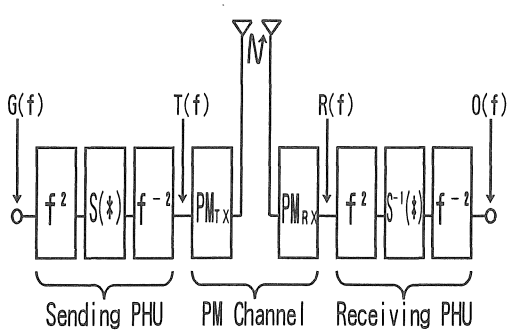


*Fig.4 Structural characteristics of IESSE system with PM modulator and PM demodulator.*

$$\begin{aligned} O(f) &= f^{-2}S^{-1}[f^2R(f)] \\ &= f^{-2}S^{-1}\{f^2f^{-2}S[f^2G(f)]\} \\ &= G(f) \quad QED. \end{aligned}$$

## 5.CONCLUSION

This paper first addressed a realization method for isomorphic emphasis, placing emphasis on the accuracy. An ideal circuitry realization method was elucidated in which attention was paid that a canonical topology consisting of two partial circuits for isomorphic emphasis manifest in a differential circuit – spectrum scrambling circuit – integral circuit series was introduced. Moreover, when an equivalent PM modulator/demodulator is using for PM transmission, if the integral circuit of the sending PHU and the differential circuit of the equivalent PM modulator each have primitive characteristic, they will cancel each other out. Likewise, if the integral circuit of the equivalent PM demodulator and the differential circuit of the receiving PHU have primitive characteristic, they will also cancel each other out. As a result, isomorphic emphasis can be realized by only changing place that the spectrum scrambling circuit is installed, and no added circuits at all are required.

## REFERENCES

(1) N.S. Jayant, B.S. McDermott, S.W. Mchistensen and A.M. Qinn, "A Comparison of four Method for Analog Speech Privacy", IEEE Transaction on Communications, Vol.COM-29, No.1, pp.23-29, Jan. 1981

(2) Masahichi Kishi, "A Proposal of Isomorphic Emphasis Spectrum Inversion for Encryption Transmission System", Transactions of the IECE Japan, Vol.J67-B, No.2, pp.228-229, Feb. 1984

(3) Kenji Imamura, Takeshi Hattori and Shigeru Kosono, "Voice Quality Improvement Using Com-

pander and/or Emphasis on Frequency Spectrum Inverted Security System", Transactions of the IECE Japan, Vol.J64-B, No.5, pp.425-432, May 1981

(4) Michael Faulkner and Giovanni A. Villain, "Noise Reduction in Signal Channel Radio Bearers Employing Privacy", IEEE Trans. on Veh. Tech., Vol.VT-34, No.3, pp.141-145, Aug. 1985

(5) Masahichi Kishi, Seizo Seki and Noboru Kanmuri, "A Radio Transmission System for a Phase Modulation Signal", Applicant No.84306657.2, Sep. 28, 1984

(6) Masahichi Kishi, Seizo Seki and Noboru Kanmuri, "A Radio Transmission System for a Phase Modulation Signal", Applicant No.84306658.0, Sep. 28, 1984

(7) 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

（受理　平成6年3月20日）