愛知工業大学研究報告
第２９号　　平成６年

Adopting the Isomorphic Emphasis to Speech Security on the Time Domain Scrambling

送受同形エンファシスの時間域スクランブラへの適用

岸　政七†,　　岩田 宏†
Masahichi KISHI, Hiroshi IWATA

ABSTRACT *The isomorphic emphasis has previously reported on spectrum inversion to prevent frequency resources from exhaustion. In this paper, we discuss about that the isomorphic emphasis has also succeeded in preventing speech quality from degradation during time domain scrambling without any expansion of frequency occupancy bandwidth over radio security speech channels. The isomorphic emphasis is again realized with the canonical form, which consists of cascaded a differentiator, a time domain scrambler with arbitrary sequential pattern, and a integrator. As well known, PM transmission systems being featured of f^{-2} fading noise shape, this time domain scrambler degrades consequentially speech quality by changing power ratio of speech signal to fading noise over subjective frequency domain. However, the isomorphic emphasis is shown to prevent time scrambled signal from both expansion and degradation over all of the subjective frequency domain , even if there exists discontinuity among input data according to time scrambling. These facilities of the isomorphic emphasis in the time domain scrambling for speech security are verified from theoretical analysis and computer simulations over poor fading channels.*

1.INTRODUCTION

With advances and diversification in the social activities, the use of vehicular and portable communication systems is spreading at a quickening pace. Whereas these systems allows their users to place and receive calls whenever and wherever they desire, on the other hand, because these calls are carried via radio channels the change of eavesdropping on them exists. In order to guard against infringement of confidentiality in such communication systems, it goes without any discussion that cryptogram is a matter of great importance.

Therefore, the ideal of adding encryption facility to radio communications has been studied from various approaches. Unfortunately, however, the existing methods have defect which the frequency occupancy is enlarged by the increase of effective modulation index, or which complicated circuits is implemented in huge economical cost.

With such a background in mind, this investigation establishes an appropriate circuitry realization method and economical optimum configuration of the isomorphic emphasis for the time domain scrambling. The isomorphic emphasis keeps speech quality without widening the frequency occupancy, and saves the cost which perfectly same signal processing unit were provided on the sending and receiving sites. To realize an equivalent circuit for the isomorphic emphasis, a canonical topology was employed in which a differantiator, a time domain scrambler, and an integrator cascad-

†愛知工業大学　情報通信工学科（豊田市）

ed in topology.

A look has also been taken at fading noise which is the dominant noise in vehicular telephones, to analyze the effect in maintaining speech quality equal to non-encryption PM transmission system.

2.STRUCTURE OF THE ISOMORPHIC EMPHASIS AND ITS CANONICAL TOPOLOGY

Necessary conditions to realized the isomorphic emphasis system is itemized in the following.

1). PM effective modulation index of the isomorphic emphasis is independent both of input signals and the time domain scramblings in order to agree with the effective modulation index in the non-encrypted PM channel.
2). PM channel is free from any distortions.
3). All emphasis functions, at sending and receiving sites must be equal to each other.

The condition 1 is required to be possible to use existing transmission system without any reorganizations so long as the isomorphic emphasis being employed if any encryptions are adopted in it.

The condition 3 gives the economical advantage of repeatability in implementation the isomorphic emphasis functions with the same circuits at both sending and receiving sites. Especially, it becomes very economical to realize the same emphasis with unique circuits

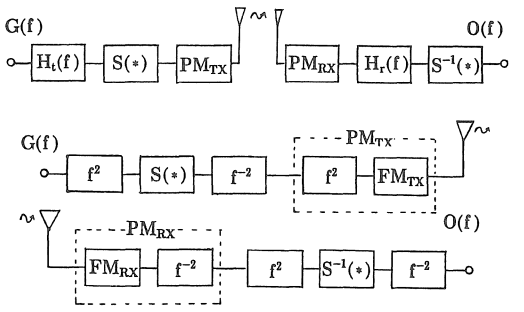

Fig.1 Circuitry topology of the Time Domain Scrambling System with the Isomorphic Emphasis, TDSS-IE

while sending or receiving in the simplex communication system. In mobile and portable phones of the duplex communication system, component space can be reduced and the effect of mass production is raised.

When all three conditions in aboves are satisfied, the isomorphic emphasis is approved.

Figure 1. (a) shows the functional block of objective transmission system, in which the time domain scrambler $S(*)$ is adopted to give speech security with the isomorphic emphasis. Hereafter, this system is called by Time Domain Scrambling System with Isomorphic Emphasis abbreviated to TDSS-IE.

It may be difficult to understand directly from fig.1. (a) that TDSS-IE is matched to the three conditions. Once the canonical form of the isomorphic emphasis is remembered, the modules of cascaded $H_t(f)$ and $S(*)$ or $H_r(f)$ and $S^{-1}(*)$ is easily divided into the same topology cascaded three major components of a differantiator, $S(*)$ or $S^{-1}(*)$, and integrator at both sending and receiving sites. Here, $S^{-1}(*)$ is the appropriated time domain descrambler corresponding to the $S(*)$.

Therefore, fig.1. (b) is easily interpreted as the other scheme of the TDSS-IE deduced from the canonical form of the isomorphic emphasis. The circuitry topology shown in fig. 1.(b) is easily recognized that the TDSS-IE is matched to the three conditions in the aboves.

3.ANALYSIS AND EXPERIMENTAL RESULTS OF THE TIME DOMAIN SCRAMBLER

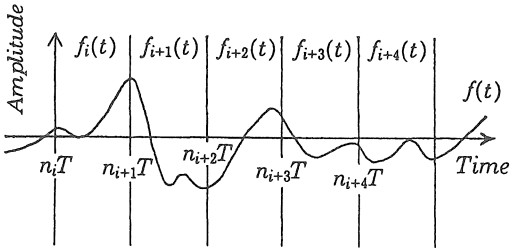

Fig.2 Segmentation employed in the time domain scrambler

The time domain scrambler achieves the encryption function as shown in fig.2 : 1. dividing the speech signal into plural segments, 2. permuting these segments according to encryption rules. That is, continuous signal $f(t)$ is divided into $f_i(t)$ of each segment i as shown in eq.1.

$$f(t) = \sum_i \{ u(t - n_i T) - u(t - n_{i+1} T) \} f_i(t) \quad (1)$$

Here, segment T_i is defined on the duration ($n_i T$, $n_{i+1} T$) , T_i is such time unit as the reciprocal number of the sampling frequency.

The time domain scrambler is considered as permutation between source and the time domain scrambled segments under assumptions that sequential blocks are consists of m number segments in each block, and any blocks for input speech signals are mapped to corresponding blocks for time domain scrambled signals with apriori delay time among these source and corresponding scrambled blocks.

Among these blocks, the permutation is described by time shifting function for each segments. Therefore, segmental signal corresponded to the scrambled signal $\tilde{f}(t)$ is given by eq.2.

$$\widetilde{f_i}(t) = f_i(t - \delta_i) \quad (2)$$

And, scrambled signal $\tilde{f}(t)$ is

$$\tilde{f}(t) = \sum_i \{ u(t - n'_i T) - u(t - n'_{i+1} T) \} \widetilde{f_i}(t) \quad (3)$$

So, the spectrum of $\tilde{f}(t)$ is given by the Fourier transform

$$\widetilde{F}(\omega) = \int_{-\infty}^{\infty} \tilde{f}(t) e^{-j\omega t} dt \quad (4)$$

Owing to linearity of Fourier transform for $\tilde{f}(t)$,
$F(\omega)$ is also defined in piecewise so long as $u(t - \tau_i)$ is defined in piecewise.

$$\widetilde{F}(\omega) = S_i \left\{ \widetilde{G_i}(\omega) \right\} \quad (5)$$

Here,

$$\begin{cases} \widetilde{G_i}(\omega) = \int_{-\infty}^{\infty} f_i(t - \delta_i)\, e^{-j\omega t} d\omega \\ S_i \{ F(\omega) \} = e^{-j\delta_i \omega} F(\omega) \end{cases} \quad (6)$$

It is clearly shown in eq.6 that segmental permutation merely causes linear phase shifting on the power spectrum of the speech signal, because time domain scrambling is mainly executed by truncating the speech signals into plural segments. The power spectrum are preserved while line phase shifting. Any speech signals are described by Fourier series to allow analysis of frequency disturbance through time scrambling based on total signals. Figure 4 shows time scales used in truncating speech signal into segment i , $n_i T$ is start point of truncation and $n_{i+1} T$ means end point of this operation. These time scales are the same to those of eq.1.

Now, consider about frequency disturbance induced from these truncations. Figure 5

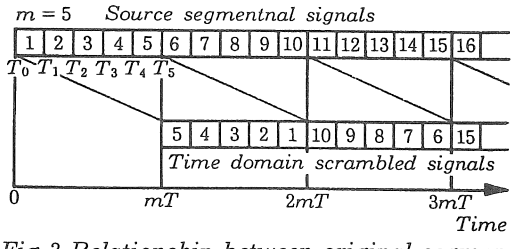

Fig.3 Relationship between original segmental and time domain scrambled signals, m=5

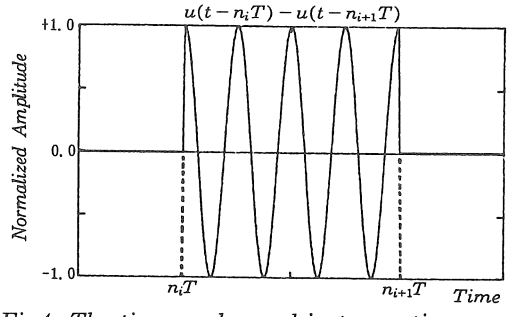

Fig4. The time scale used in truncating continuous signal f(t) into segmental signal $f_i(t)$

shows the instantaneous power spectrum analyzed by ST DFT at time of turn-on point if input signal is 1kHz total. This spectrum featured of hyperbolically distributed distortion in the neighboring around the input signal frequency is observed at below -40dB even if the signal such catastrophically changes as truncations. Figure 6 shows transient response of harmonic distortion observed at time $n_iT \leqq t < n_{i+1}T$.

Here, the horizontal axis is time plotted in logarithm and counted from catastrophical changes at n_iT, vertical one means harmonic distortion induced from the truncation at the time n_iT. The distortion is shown to be low below than -23dB and also to converse rapidly into null after catastrophic changes at time n_iT.

Transient response of the harmonic distortion around the tail-end of segment i is illustrated in fig.7 to show the disturbance caused by truncation being reasonably small. In fig. 7, horizontal is time scaled in linear and vertical means harmonic distortion in dB. Even the maximum value which appears at $t=0$ of the tail-end is less than -23dB to be enough small to sweep away the ordinable influence. It simultaneously shows the rapid convergence around the catastrophic changes. It seems to be analysis error owing to window function in the ST DFT that harmonic distortion is observed before the catastrophic change occasion.

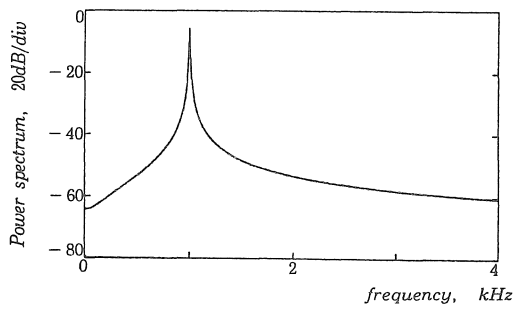

Fig.5 Instantaneous spectrum analyzed by the short time DFT at turn-on time, n_iT for segment i

Consequently, it gives a conclusion in analyzing the frequency disturbance by segmentations that high speech quality is maintained with suppression the frequency divergence only at front-end of each segment as shown in eq.1. Because the tail-end is easily deduced from superposing $u(t-\tau_i)$ and unity. That is, if the catastrophic change at the front-end of each segment is analyzed in details for apriori tonal signals, it is sufficient to know what disturbance will be introduced into spectral signals through truncating or concatenating segments.

Figure 8 shows detailed results examined under following assumptions; the disturbance is measured by harmonic distortions within subjective domain (0.3, 3.0) kHz, the tonal signal is set to be from 0.3 till 3.0 kHz by every 0.3 kHz, the front-end is moved from 0 till 2π radian within one cycles of the signals, and sampling frequency is 8 kHz.

The harmonic distortions are featured of flat-top over all phase of the front-end position within the tonal signals and of swingings within ± 5 dB at the level below -30 dB for all frequencies.

The flatness of the frequency disturbance induced from segmentation suggests to be equal in power spectrum to the dominant fading noise over poor radio channels. If the power spectrum is modified as flat before the time domain scrambling encryption, the speech quality will be optimized in maintaining the

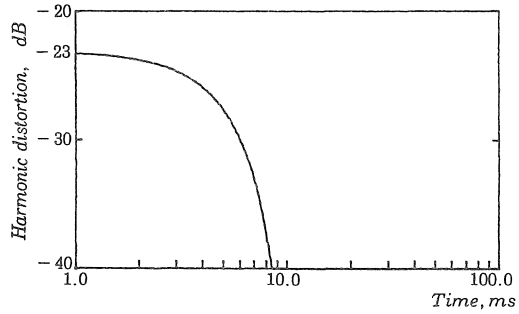

Fig.6 The transient response of the harmonic distortion caused by truncation at turn-on point, f_s=8kHz

ratio between signals and frequency disturbance induced from segmentation over all subjective frequency domain in similar to PM transmission systems.

4. NOISE REDUCTION EFFECT

The dominant noise is fading as clicking audible to produce integral power distribution through PM detecting. It is therefore easy to understand that PM transmission system is ideal to keep the ratio of speech to noise be nearly uniform over all frequency.

TDSS-IE adopts the equivalent PM system. The differantiator of the equivalent PM transmitter and the integrator of the emphasis are counterbalanced with each other at the sending site, and the integrator of the equivalent PM receiver and differantiator of the emphasis are canceled out at receiving site as shown in fig.1.(b).

Therefore, TDSS-IE is implemented at send site only with fundamental facilities of a differentiator, a scrambler, and an FM transmitter without any additional circuits in the order of installation the scrambler among equivalent PM transmitter to execute isomorphic emphasis in function.

At receiving site, TDSS-IE is also implemented with only enevitable circuits of an FM receiver, a descrambler, and an integrator to form equivalent PM receiver with encryption facility.

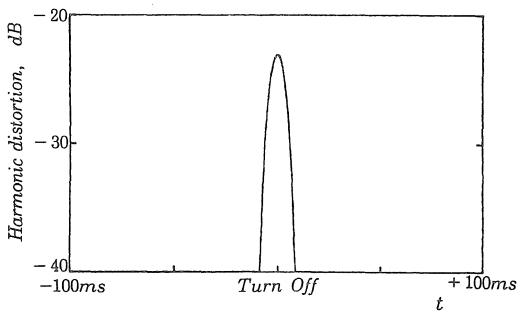

Fig.7The transient response of the harmonic distortion induced from the truncation at turn-off point, $n_{i+1}T$, f_s=8kHz

The input speech signals, which are featured of integral shape in power spectrum, are modified into flat shape in power spectrum by the differantiator at the front-end of the TDSS-IE system. Then, flat-shaped speech signals are scrambled on the time domain to produce excessive scrambling noise at truncation points. Attentions must be played on these truncation noise being also flat as discussed in the previous session.

The FM detector reproduces both the flat-shaped speech and white fading noise to let into the apriori descrambler to descriptive speech signals. The excessive and white noise is again added into speech signal through descrambling on the time domain. The excessive noise induced both in scrambler and descrambler are nearly flat within subjective domain from 0 to f_s, and rapidly convergences to zero around all the catastrophic changes. All such noise as fading and truncating and concatinating speech are fortunately white in power spectrum to maintain spectrum distribution through these encrptiogram processings. The integrator at the tail-end of TDSS-IE system weights descrambled signals to reproduce integral distribution in the power spectrum of speech signals. The optimized SNR is given by integral distribution both to speech and noise

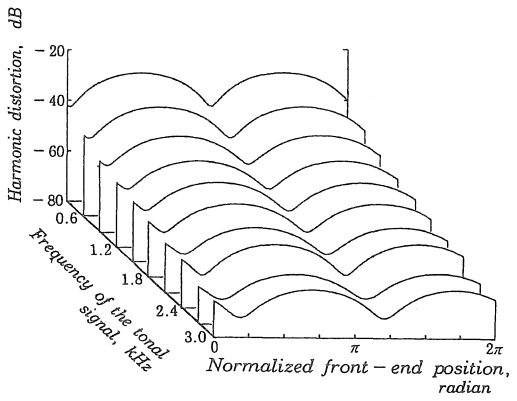

Fig.8 The harmonic distortions observed at the front-end of each segment as input tonal signals being taken as 0.3 to 3.0kHz and as the front-end positionings from 0 to 2π of the tonal signal, f_s=8kHz

induced in transmission in similar to the existing PM transmission system.

5. CONCLUSION

The isomorphic emphasis was discussed on the noise reduction effect with emphasis on application to time domain scrambler. The noise induced from time domain scrambling is analyzed in details to be almost white over subjective frequency domain.

It is successfully discussed to be most economical in implementation of encryption system because of requiring no additional circuits that the isomorphic emphasis garntees the apriori speech quality in SNR meanings.

The authors would express their acknowledgement to Director Toshihiko KOTOH, Fujitsu Ltd and his colleagues for their assistance in printing and Mr. Hirotaka HASEGAWA for his cooperation in computer simulations.

REFERENCE

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

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

(3) Kenji Inamura, Takeshi Hattori and Shigeru Kosono, "Voice Quality Improvement Using Compander and/or Emphasis on Frequency Spectrum Inverted Security System", Transactions of the IEICE Japan, Vol.J64-B, No.5, pp.425-432, May 1981

(4) Michael Faulkner and Giovanni A. Villani, "Noise Reduction in Single Channel Radio Bearers Employing Privacy", IEEE Transaction On Veh. Tech., Vol.VT-34, No3, 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

(6) 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

(7) A. Bateman, J. D. Marvill & J. P. McGeehan, "VOICE SCRAMBLING FOR RADIO, CELLULAR & TELEPHONE SYSTEMS", IEEE VTC'92, Denver, Colorado, pp.968-972, May 1992

(受理 平成6年3月20日)