PAPER *Special Issue on Communication Theory*

Interlace Coding System Involving Data Compression Code, Data Encryption Code and Error Correcting Code

Takaya YAMAZATO†, Iwao SASASE† *and* Shinsaku MORI†, *Members*

SUMMARY An Interlace Coding System (ICS) involving data compression code, data encryption code and error correcting code is proposed and its error performance on additive white Gaussian noise (AWGN) channel with quadrature phase shift keying (QPSK) is analyzed. The proposed system handles data compression, data encryption and error correcting processes together, i.e. adds error correcting redundancy to the block lists of the dictionary in which compression system constructs to reduce source redundancy. Each block list is encoded by Ziv-Lempel code and Data Encryption Standard (DES). As the catastrophic condition determined by the data compression procedure is not negligible, error correcting redundancy should be added so as to avoid catastrophic condition. We found that the catastrophic condition depends only on the size of the dictionary for our proposed system. Thus, by employing a large dictionary, good error performance can be applied by the proposed system and the catastrophic condition can be avoided.

key words: information theory, coding theory

1. Introduction

As computers and communication networks have been spreading deep into society, the need for secure communication further promoted cryptologic research[1],[2]. Since, this communication system also implies on data compression system which can reduce redundancy of source messages, there has been a strong link between data compression and cryptology throughout development of communication systems [1],[3]. Hellman [4] emphasized a point made by Shannon about the importance of data compression in cryptographic systems and remarked that the best encrypted message can be produced if the plain text is the compressed forms of the source messages. Data compression and encryption systems usually assume the transmission path error free. A more accurate model incorporate a channel that is not error-free. The usual model assumes an additive white Gaussian noise (AWGN) channel which, in turn, is assumed to be modeled accurately with crossover probability *Pec*. Unfortunately, the coded messages produced by data compression and encryption are far more adversely affected by channel errors. It has been pointed out that single channel error propagates through forthcoming data stream[1],[3],[5]. For this reason, some form of redundancy is added, such as error correcting code, by the channel coding process before transmission in a sense of practical use. The degradation due to the error propagation of typical data compression code of Ziv-Lempel code and arithmetic code have been studied by Yeheskel and Parthasarathy and it is shown that even in an event of single error, such error would affect whole decoded sequence be catastrophic[6]. Degradation of the probability of error due to the DES (Data Encryption Standard) has been examined by the several authors and showed that degradation can be eliminated by using the error correcting code[6],[7]. Although the errors in the DES system is not catastrophic, because of its independence of the block, 64 bits, susceptibility to the long error propagation can not be neglected by error correcting code, if the plain text is the compressed messages of the source messages, in order to satisfy the remarks given by Hellman. The susceptibility to error is the main drawback of data compression and data encryption algorithms, therefore, error correcting redundancy should be added so as to avoid error propagation as well as to protect from channel errors. Thus, the methods of limiting the effect of an error, which causes the catastrophe of coded messages on data compression algorithm and data encryption algorithm should be investigated[3].

In this paper, we propose Interlace Coding System (ICS) to avoid error propagation as well as to protect from channel errors. The proposed system handles source coding process (data compression and encryption) and error correcting processes together. That is, by adding the error correcting redundancy to the block lists of the dictionary in which compression system constructs to reduce source redundancy. Each block lists are encoded with data compression code and data encryption code. Although, our scheme has the block list at both coder and decoder, no priori knowledge of dictionary is needed. The Ziv-Lempel code[9] is used as data compression code and DES[2] in a self-synchronous cipher feed back mode is used as encryptor. To prevent error propagation, source coding and decoding are implemented block by block. Initialization is required every block for DES. The basic idea of our system is to prevent error propagation even

Manuscript received December 6, 1991.
Manuscript revised February 10, 1992.

† The authors are with the Faculty of Science and Technology, Keio University, Yokohama-shi, 223 Japan.

if we introduce the method of data compression system. The main objective in employing Interlace Coding System is to reduce the redundancy of source data as well as to ensure secrecies by DES and good recoverity of source data from channel noise. This should be done without much increasing of error correcting redundancy. In order to clarify the benefit of our scheme, we first analyze the catastrophic condition of our proposed system and then derive the expression of probability of error. We examined the two types of the scheme to clarify the effect of channel errors and compared with the conventional system, which error correcting redundancy is added just before the channel, regardless of error propagation. This is the case of post-channel-coding system. For the case of pre-channel-coding system (TYPE1-ICS), error correcting redundancy is added only when the new codeword, which will be contained in the dictionary as the block list, is transmitted. For the case of combined system of pre-channel-coding and post-channel-coding (TYPE2-ICS), one code is used as same as pre-channel-coding system, and a second coding process to deal with channel error.

2. Interlace Coding System

The channel model of our scheme is shown in Fig. 1 and its interlace process is shown in Fig. 2. To prevent error propagation, source message is separated and contained in block list that is constructed by data itself. Each block list is encoded separately by data compression procedure and data encryption procedure before sending to the channel. The Ziv-Lempel code and DES in a self-synchronous cipher mode are implemented block by block. Initialization is required every block for DES, and no error propagation will occur beyond this block list. Related idea of compression process can be found in locally adaptive data compression algorithm known as BSTW algorithm[10], except that we add error correcting redundancy only when the system transmits new message that the sender and the receiver maintain identically. That is, instead of transmitting same message which is already contained in the block lists of s-1 elements, our scheme transmits a pointer (Reference Pointer: RP) of the block list which the message is present. If the message is not in the list, the sender sends s-th pointer (Insertion Pointer: IP) followed by the encoded codeword of compressed and encrypted message with error correcting code, then both sender and receiver updating the list. Let the input message is shown with upper case letter, compressed and encrypted message is shown with lower case letter, error correcting redundancy is shown as "Δ". An integer denotes the pointer of the block list. If the transmitted messages are;

THE CAR ON THE LEFT HIT THE CAR

I LEFT.

Then the coded messages are;

1theΔ 2carΔ 3onΔ 1 4leftΔ 5hitΔ 1 2 6iΔ 4.

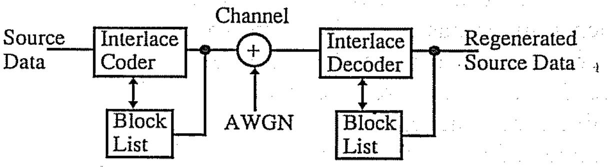


Fig. 1 Channel model of interlace coding system.

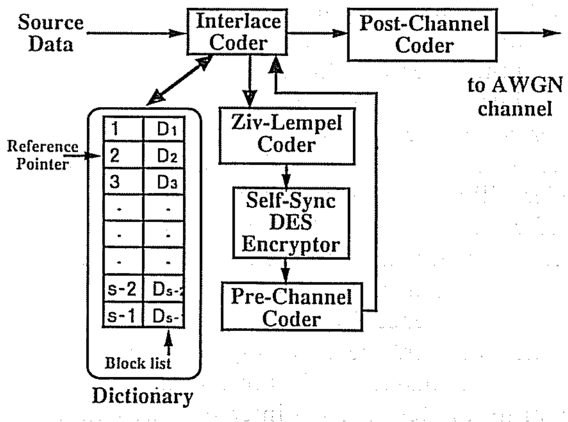


Fig. 2 Interlace process of interlace coding system (coding process).

Table 1 shows the input source length, its code length, average number of appearance of same symbol, Na, and its compression ratio of Interlace Coding System for various source data without error correcting redundancy. Here, the size of block lists are 256[byte]. Although our scheme is designed mainly to combat with the channel noise, or to prevent error propagation, it still compacts source data as conventional data compression system[5]. In this paper, we consider two types of Interlace Coding System and the conventional

Table 1 Source length, code length, Na and compression ratio, over-all compression ratio (OCR) of input strings for the case of TYPE1-ICS, TYPE2-ICS and the conventional system.

	without error correcting code				error correcting power $\alpha=\beta=3$		
File Type	Source Length (byte)	Code Length (byte)	Na	Compression Ratio	OCR of conventional system	OCR of TYPE1-ICS	OCR of TYPE2-ICS
Program Text (C)	8991	4297	2.943	0.477	0.488	0.480	0.491
	11653	4931	3.232	0.423	0.433	0.426	0.436
	7478	3228	3.750	0.431	0.441	0.434	0.444
Text File (TEX)	39845	13904	2.851	0.348	0.356	0.350	0.358
	11189	4563	2.864	0.407	0.417	0.409	0.419
	43475	21471	2.366	0.493	0.505	0.496	0.508
EXE File	28970	22214	3.742	0.766	0.784	0.771	0.789
	25480	15399	7.088	0.604	0.618	0.608	0.622
	26722	20399	3.291	0.763	0.781	0.768	0.786
	97766	53661	4.960	0.548	0.561	0.551	0.564
COM File	2406	2105	5.384	0.874	0.895	0.879	0.900
	16638	13192	2.429	0.792	0.811	0.797	0.816
	23056	12901	4.207	0.559	0.572	0.562	0.576

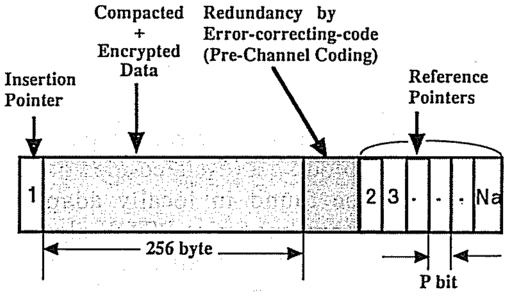


Fig. 3 Block diagram of the codeword of TYPE1-ICS.

system of source coding process and error correcting process are implemented separately, regardless of error propagation determined by source coding process.

TYPE1-ICS (Pre-Channel-Coding System); This system adds the error correcting redundancy only when the coder transmits the new codeword of compressed and encrypted message. The example previously shown is the case of TYPE1-ICS, pre-channel-coding system. Figure 3 shows the block diagram of the arbitrary codeword of TYPE1-ICS in steady state. Here, length of pointer is p[bit] and length of compressed and encrypted codeword is 256[byte], which is the size of the block list. *Na* denotes the average number of occurrence of all same symbols in source messages, therefore, the word list is referred *Na*-1 times by the Reference Pointers and occurrence probability of arbitrary codeword is $1/Na$.

TYPE2-ICS (Combined System of Pre-Channel-Coding and Post-Channel-Coding) ; This system adds another error correcting redundancy to the codeword produced by TYPE1-ICS. If the input messages are the same as shown in above example (TYPE1-ICS), then the coded messages are;

1theΔ◆ 2carΔ◆ 3onΔ◆ 1◆ 4leftΔ◆ 5hitΔ◆
1◆ 2◆ 6iΔ◆ 4◆.

"◆" indicate the error correcting redundancy of post-channel-coding.

Conventional system (Post-Channel Coding Only) ; Conventional data compression and encryption system with error correcting code. The coded messages are ;

the ◆ car ◆ on ◆ the ◆ left ◆ hit ◆ the ◆
car ◆ i ◆ left ◆.

2. 1 Catastrophic Condition and Error Span

We first consider how the error would affect to Interlace Coding System. If the pointer is corrupted by errors, our scheme may become catastrophic. There are four kinds of errors and two of pointer-errors may become catastrophic. Those catastrophic errors are caused by (a) if the Insertion Pointer is mis-decoded as the Reference Pointer, or (b) if the Reference Pointer is mis-decoded as the Insertion Pointer. These errors result loss of synchronization between the coder and the decoder, and since the state of the coder and the decoder are different, the errors would propagate throughout forthcoming data streams. Although the other errors do not have effect on synchronization between the coder and the decoder, those errors still give some amount of error propagation. Those errors are; (c) the Reference Pointer is mis-decoded as the other Reference Pointer, and (d) the new codeword, which is going to register in the block lists, is corrupted by errors.

(a) If Insertion Pointer is mis-decoded as Reference Pointer, then the decoder will not resister the next codeword as new codeword. Therefore, the decoded message would be catastrophic as this results in the loss of synchronization between the coder and the decoder. For example, let the size of the dictionary be 4 and pointers of each block lists are represented in binary as {00, 01, 10, 11}, respectively. The pointers, {00, 01, 10}, indicate Reference Pointers and {11} indicates Insertion Pointer. If the Insertion Pointer {11} is captured by errors, the possible error-pointers are {00, 01, 10}, which are the other than the Insertion Pointer and those are the Reference Pointers. Therefore, the decoder will output its contained word list. However, the coder was updating after it sent Insertion Pointer and new codeword, the contents of word lists and their respective pointers are different between the coder and the decoder. This loss of synchronization of the coder and decoder will never be recovered, thus errors in Insertion Pointer provoke catastrophic errors. Since each pointer has 3 possible error-pointers, when it is corrupted by errors, the total number of error-pointers are 3×4. Therefore, the probability that Insertion Pointer become catastrophic is defined by the total number of insertion-error-pointer divided by all possible error-pointers, which is $3/(4\times3)=1/4$. In general, there are 2^p-1 insertion-error-pointers among $2^p(2^p-1)$ error-pointers, where p denotes the length of pointer in binary representation. Thus, the probability of Insertion Pointer become catastrophic is 2^{-p}.

(b) If the Reference Pointer is mis-decoded as Insertion Pointer, then the decoder will resister the next pointer as new codeword. For example, if {01} is mis-decoded as {11}, which is Insertion Pointer, the decoder will register the next pointer as new codeword. Therefore, the decoder will be catastrophic because the contents of block lists and their respective pointers are different between the coder and decoder. As the number of Reference Pointer is 2^p-1, and among each Reference Pointer, there is only one reference-error-pointer which mis-decoded as Insertion Pointer. Thus, probability of Reference Pointer become catastrophic is 2^{-p}.

An catastrophic condition is defined by above two condition.

Figure 3 shows the block diagram of the arbitrary codeword of Interlace Coding System for a steady state. With consideration of occurrence probability of new codeword, $1/Na$, which is also the probability of Insertion Pointer, probability of Interlace Coding System being catastrophic is

$$Pe(\text{catastrophic}) = 2^{-p}Na^{-1} + 2^{-p}(1 - Na^{-1}) = 2^{-p}. \quad (1)$$

(c) If the Reference Pointer is mis-decoded as other Reference Pointer, then the decoder will output wrong strings of 256[byte], or 2048[bit]. Since the dictionary is not updating on both the coder and the decoder, they remain synchronized. Thus, expected error span is 2048 bit.

$$Es(\text{pointer}) = 2048 \quad (RP_i \neq RP_j) \qquad (2)$$

Here, $ES(x)$ denotes expected error span of x.

(d) If the new codeword is corrupted by error, then the new codeword will register wrongly. Since the coder encodes new codeword with Ziv-Lempel code and DES, the new codeword will never be recovered unless error correcting decoder precisely correct all errors. Figure 4 shows the DES cryptor and decrypter in a self-synchronous cipher mode. The P_n denotes the n-th character, which consists of m-bits from coded message of Ziv-Lempel code. The K_n denotes the n-th keystream character, which consists of m-bits from DES, and C_n denotes the cipher text character obtained by the binary modulo addition of K_n and P_n. In a self-synchronous stream cipher, each key character, K_n, is derived from a fixed number, M, of the preceding cipher text characters, $C_{n-1}, C_{n-2}, \cdots, C_{n-M}$, by feeding back to the input of the shift register. Initialization is provided by a known input, I_0. Although errors in coded message is catastrophic, the maximum error span is limited by the size of block list, 2048 bits. Thus the expected error span of word list can be written as follow;

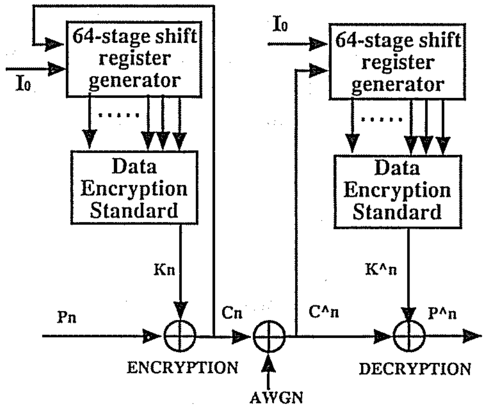


Fig. 4 Data Encryption Standard (DES) in a self-synchronous cipher mode.

$$ES(\text{code word}) = 2048 \qquad (3)$$

Although the proposed system employs DES in a self-synchronous cipher mode, the maximum length of the data going through feedback loop (data being dependent) is limited by the length of the block list (256 byte or 2048 bits), thus only 32 blocks (each block consists 8 byte or 64 bits) are going through feedback loop in order to avoid error propagation. Therefore, the secrecy given by ICS is weaker than the secrecy given by the conventional DES in a self-synchronous cipher mode, which the data is dependant of other data, but the proposed system still holds an advantage over the DES in block cipher mode, which the data (64 bits) is independent of the other data. Moreover, the input message of DES procedure of our proposed system is the coded forms of data compression code (Ziv-Lemple code), as shown in Fig. 4. Therefore, the coded messages of the proposed system consists of the compressed and encrypted forms of the message, which is the best cipher forms according to the Hellman[4]. Although, our scheme is designed mainly to combat with the error propagation due to the source coding procedure, the secrecy given by our scheme still has an advantages over the DES in block cipher mode.

3. Error Performance

An expression of probability of error can be derived from the probability of the decoder being catastrophic and the expected error spans. The probability of error of Interlace Coding System is given as follow.

$$\begin{aligned} Pe = {} & Pr(RP|IP) + Pr(IP|RP) \\ & + ES(\text{pointer})\,Pr(RP_i|RP_j) \\ & + ES(\text{word list})\,Pr(\text{code word}) \end{aligned}$$

where

$$\begin{aligned} Pr(RP|IP) &= \{1 - (1 - P_{RP})^{l(p)}\}2^{-p}Na^{-1} \\ Pr(IP|RP) &= \{1 - (1 - P_{IP})^{l(p)}\}2^{-p}(1 - Na^{-1}) \\ Pr(RP_i|RP_j) &= \{1 - (1 - P_{RP})^{p}\}(1 - 2^{-p}(1 \\ & \qquad - Na^{-1})) \\ Pr(\text{code word}) &= 1 - (1 - P_{dic})^{2048} \end{aligned} \qquad (4)$$

where $Pr(x|y)$ denotes the probability that y was encoded and decoder decodes it as x. P_{IP}, P_{RP}, P_{dic} denote the bit error probability of Insertion Pointer, Reference Pointer and the block list, respectively. $l(p)$ denotes the efficient code length of pointers, given as follow;

$$l(p) = \frac{8pNa}{8pNa + 256}TL \qquad (5)$$

where *TL* is the total length of coded message of source coding process.

3. 1 TYPE1-ICS (Pre-Channel-Coding System)

The error correcting redundancy is added only when the new codeword is transmitted through the channel. Therefore, the error correcting code can correct errors on Insertion Pointer and the new codeword which will be contained in the dictionary. Reference Pointer is transmitted without error correcting code (See Figs. 2 and 3). Probability of error of TYPE1-ICS using α-error-coding (n_α, k_α) code can be derived from Eq. (4), where P_{IP}, P_{RP}, P_{dic} is given as follows:

$$P_{IP}=P_{dic}=\sum_{j=\alpha+1}^{n_\alpha}\frac{1}{n_\alpha}\binom{n_\alpha}{j}Pec^{j}(1-Pec)^{n_\alpha-j}$$
$$P_{RP}=Pec \tag{6}$$

where *Pec* is the probability of channel error[11].

The coding rate (*CR*) and the over-all compaction ratio (*OCR*) of the TYPE1-ICS can be derived from the coding rate of the error correcting code (k_α/n_α), the length of the source messages, *M*, and the total length of coded message of source coding process, *TL*.

$$CR_{\text{TYPE1-ICS}}=\frac{8pNa+256}{8pNa+256(n_\alpha/k_\alpha)} \tag{7}$$

$$OCR_{\text{TYPE1-ICS}}=\frac{M}{TL}\frac{1}{CR_{\text{TYPE1-ICS}}} \tag{8}$$

3. 2 TYPE2-ICS (Combined System of Pre-Channel-Coding and Post-Channel-Coding)

The error correcting redundancy is added as same as TYPE1-ICS, except, TYPE2-ICS adds another error correcting redundancy just before the coder transmits the codeword (see Fig. 2). The first error correcting process is called pre-channel-coding and second error correcting process is called post-channel-coding. α-error-correcting (n_α, k_α) code is used as primary error correcting process (pre-channel-coding) and β-error-correcting (n_β, k_β) code is used as secondary error correcting process (post-channel-coding). The probability of error of TYPE2-ICS can be derived from Eq. (4), where P_{IP}, P_{RP}, P_{dic} is given as follows;

$$P_{IP}=P_{dic}=\sum_{j=\alpha+1}^{n_\alpha}\frac{1}{n_\alpha}\binom{n_\alpha}{j}P_{RP}{}^{j}(1-P_{RP})^{n_\alpha-j}$$
$$P_{RP}=\sum_{j=\beta+1}^{n_\beta}\frac{1}{n_\beta}\binom{n_\beta}{j}Pec^{j}(1-Pec)^{n_\beta-j} \tag{9}$$

The coding rate (*CR*) and the over-all compaction ratio (*OCR*) of the TYPE1-ICS can be written as follows;

$$CR_{\text{TYPE2-ICS}}=\frac{8pNa+256}{8pNa+256(n_\alpha/k_\alpha)}\frac{k_\beta}{n_\beta} \tag{10}$$

$$OCR_{\text{TYPE2-ICS}}=\frac{M}{TL}\frac{1}{CR_{\text{TYPE2-ICS}}} \tag{11}$$

3. 3 Conventional System (Post-Channel-Coding Only)

The data compression, encryption and error correcting process are independently implemented in post-channel-coding system. This is the case of post-channel-coding system, that the catastrophic condition of data compressed messages is no longer negligible. In other words, it is possible for a single error to propagate without any limit. Therefore, maximum expected error span is the total length of the received codeword, *TL*, and the received codewords will be recovered only if all errors in the received codewords are corrected by the error correcting procedure. The probability of error of the conventional system is given as follows:

$$Pe(\text{conventional})=1-(1-Pr_{\text{post}})^{TL}$$
$$Pr_{\text{post}}=\sum_{j=\beta+1}^{n_\beta}\frac{1}{n\beta}\binom{n_\beta}{j}Pec^{j}(1-Pec)^{n_\beta-j} \tag{12}$$

where Pr_{post} denote the bit error probability of post-channel-coding.

The coding rate (*CR*) and the over-all compaction ratio (*OCR*) of the conventional system can be written as follows;

$$CR_{\text{conventional}}=\frac{k_\beta}{n_\beta} \tag{13}$$

$$OCR_{\text{conventional}}=\frac{M}{TL}\frac{1}{CR_{\text{conventional}}} \tag{14}$$

3. 4 Numerical Results

For performance analysis, the white Gaussian noise is added to the transmitted signal. The quadrature phase shift keying (QPSK) is used as the modulator and demodulator. The bit error probability of QPSK is

$$Pe(\text{QPSK})=Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \tag{15}$$

where E_b is the bit energy, N_0 is the one-sided additive white Gaussian noise power spectral density, and $Q(x)$ is

$$Q(x)=\int_x^0\frac{1}{\sqrt{2}}\exp\left\{-\frac{t^2}{2}\right\}dt. \tag{16}$$

Figure 5 shows the effect of error propagation of the

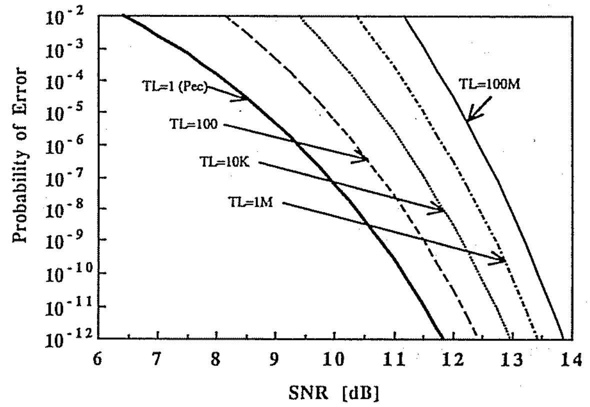
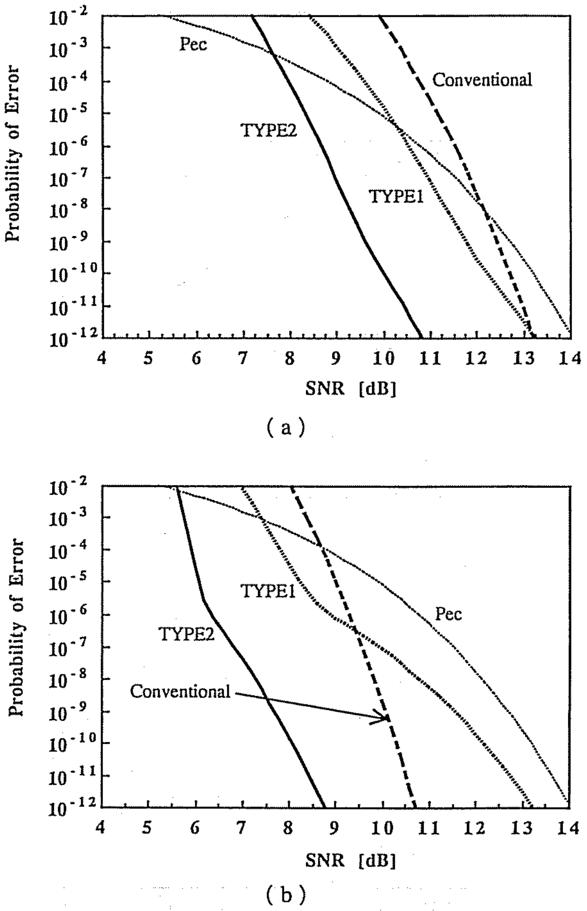


Fig. 5 Effect of the code length of the conventional system (Effect of error propagation).
Error correcting power is 1 ($\beta=1$), $TL=1$, 100, 10 K, 1 M, 100 M[byte].

conventional system (post-channel-coding system), where the error correcting power is 1. Since the error span is given by the total length of the coded message, TL, the error performance degradation due to the effect of error propagation is function of TL. As TL becomes longer, the error performance becomes worse. Figure 6 shows the error performance of Interlace Coding System along with uncoded QPSK, which we assume as the channel error probability, *Pec*. Figure 6 (a) is for the case of using same error correcting power, α and β equal to 1, the total code length, TL, is 100 kbyte, $Na=3.0$ and the size of pointer is 32 bit. Rate 0.992 (255, 253) Reed-Solomon (RS) code is used as error correcting code, thus, the coding rate of the conventional system is 0.992. The coding rate of TYPE1-ICS and TYPE2-ICS are 0.998 and 0.990, respectively. The error performance of TYPE2-ICS shows the best among three systems, however the coding rate is the worst. TYPE2-ICS system shows the about 2.5 dB better error performance than both TYPE1-ICS and the conventional system at the error probability of 10^{-12}. Although the error performance of TYPE1-ICS is approaching to that of the conventional system when SNR gets higher, TYPE1-ICS shows the better error performance than that of the conventional system and it also shows the best coding rate. Figure 6(b) shows the error probabilities of ICS for the case of using the same error corecting power, α and β equal to 3. The other conditions are as same as Fig. 6(a). Rate 0.976 (255, 249) Reed-Solomon (RS) code is used as error correcting code. The coding rate of TYPE1-ICS, TYPE2-ICS and the conventional system are 0.994, 0.971 and 0.976, respectively. The over-all compression ratio (OCR) of input strings for the case of TYPE1-ICS, TYPE2-ICS and the conventional system are summarized in Table 1, for various source data. The error performance of TYPE1-ICS is better than that of the conventional system at low SNR, however, it becomes worse as SNR increases. This is because that in ICS (both TYPE1 and TYPE2), there are two predominant factors which affect to the error performance. At low SNR, the error probability of block lists dominate the error performance of the system and the effect of pointers being catastrophic is neglected by the size of the pointer and the error correcting procedure. However, at high SNR, uncoded or weak-error-correcting-coded Reference Pointer dominate the error performance of the system. Therefore, the error performance of TYPE1-ICS is worse than that of the conventional system at high SNR for a fact of uncoded Reference Pointer. And since the error correcting capability of Reference Pointer of TYPE2-ICS is as same as that of the conventional system, because post-channel-coding procedure is the only influential factor of Reference Pointer, the error performance of TYPE2-ICS is always better



(a)

(b)

Fig. 6(a) Probability of error of ICS (TYPE1 and TYPE2) and the conventional system along with uncoded QPSK (*Pec*). $\alpha=\beta=1$, $Na=3.0$, $p=32$[bit], $TL=$ 100 k[byte].
(b) Probaility of error of ICS (TYPE1 and TYPE2) and the conventional system along with uncoded QPSK (*Pec*). $\alpha=\beta=3$, $Na=3.0$, $p=32$[bit], $TL=$ 100 k[byte].

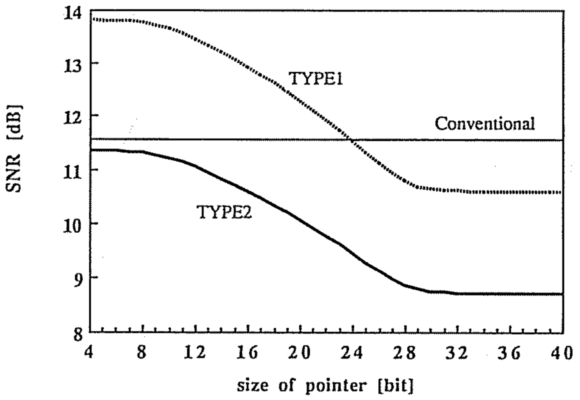
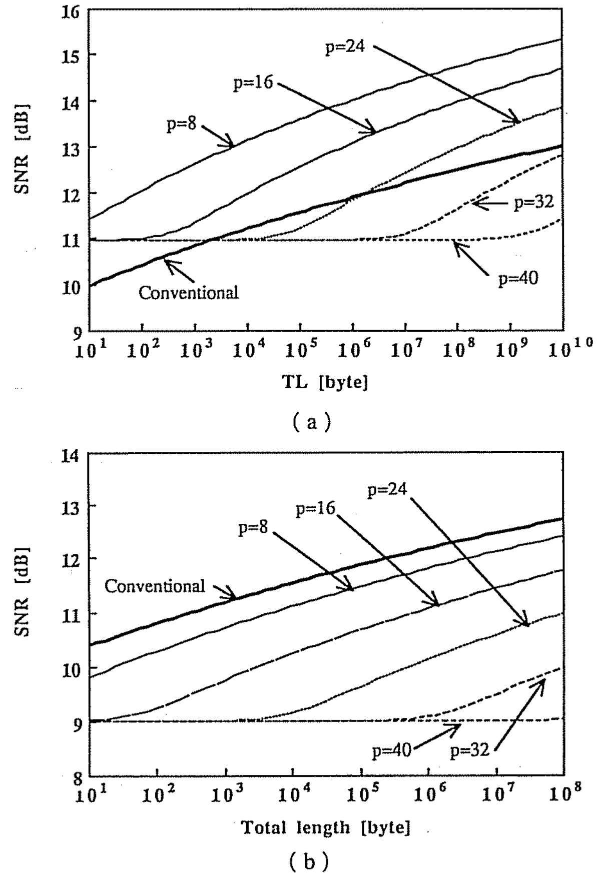


Fig. 7 Effect of the pointer size of ICS (TYPE1 and TYPE2) along with the conventional system to achieve $Pe=10^{-7}$. $\alpha=\beta=1$, $Na=3.0$, $TL=100$ k[byte].



(a)

(b)

Fig. 8 (a) Effect of the code length of TYPE1-ICS along with the conventional system to achieve $Pe=10^{-7}$, $\alpha=\beta=1$, $Na=3.0$, $p=8, 16, 24, 32, 40$ [bit].

(b) Effect of the code length of TYPE2-ICS along with the conventional system to achieve $Pe=10^{-7}$, $\alpha=\beta=1$, $Na=3.0$, $p=8, 16, 24, 32, 40$ [bit].

than both TYPE1-ICS and the conventional system. As we mentioned in Sect. 2, the catastrophic condition depends only on the error probability of the pointers, and pre-channel-coding process has effect only on Insertion Pointer. If the reliability of channel is good or strong error correcting code is applyed at post-channel-coding procedure, the influence given by the pre-channel-coding process to the Insertion Pointer is covered by post-channel-coding process, which has the influence on both Insertion and Reference Pointers. Therefore, the effect of pre-channel-coding become so little that post-channel-coding dominate the error performance of the system. Thus, the error performance of the conventional system using the strong error correcting code (see Fig. 6(b)) is better than that of TYPE1-ICS when the size of the pointer is same. However, the error probability (catastrophe) of the pointers depends not only the error correcting process, but it heavily depends on the size of pointer. In Figs. 7 and 8, we compare the systems by holding the error probability, Pe, equals to 10^{-7} and varying the size of the pointer for $Na=3.0$, error correcting power $\alpha=\beta=1$. The effect of pointer size is shown in Fig. 7, where the code length, TL, is fixed to 100 kbyte. As the size of pointer increase, the SNR to achieve the error probability of 10^{-7} becomes lower. However, the size of the pointer is not only the predominant factor, but also the size of the code length to achieve better error performance than the conventional system for the case of TYPE1-ICS. The effect of pointer size and the code length for the case of TYPE1-ICS and TYPE2-ICS are shown in Figs. 8(a) and 8(b), respectively. For long code length, the size of pointer must be chosen larger. For example, at the code length of 100 kbyte (see Fig. 7), if the size of the pointer of TYPE1-ICS is larger than 24 bit, the error performance of TYPE1-ICS will be better than that of the conventional system. Since the size of the pointer and the code length are predominant factors, the size of the pointer should be chosen large enough to cover the effect of the error propagation to achieve better error performance of Interlace Coding System.

4. Conclusions

Interlace Coding System involving data compression, encryption and error correcting code has been proposed and the error performance on additive white Gaussian noise channel with QPSK has been analyzed. We found that the catastrophic condition depends only on the size of dictionary. If we choose efficiently large dictionary, the catastrophic condition is negligible. The error performance of TYPE1-ICS system, pre-channel-coding only, is better than that of the conventional system on the condition of size of the pointer is large enough to cover the catastrophic condition given by the uncoded factor of Reference Pointer and TYPE1-ICS also improves the coding rate. However, the size of the pointer exceeding 24 bits is too large from the practical points of view. The minimum memory size, i.e., the total size of the dictionary, for the case of the pointer being 24 bits is $2^{24} \times 256 = 4294$ Mbyte, which may be impossible value. This is the main draw back of the proposed system, and the method of reducing the size of the pointer (i.e., reducing the memory size) should be investigated in order to put ICS to practical use. For the case of TYPE2-ICS, because the Reference Pointer is coded for this system, the best error performance has been achieved with a little decrement of the coding rate comparing to the conventional system. Thus, TYPE2-ICS is more practical coding system which can reduce the error propagation due to the source coding system of data compression and data encryption procedure.

References

(1) van Tilborg H. C. A.: "An Introduction to Cryptology", Kluwer Academic Publishers (1991).

(2) Orceyre M. J. and Heller R. M.: "An Approach to Secure Voice Communication Based on the Data Encryption Standard", IEEE Communications Society Magazine, **16**, 6, pp. 41-55 (Nov. 1978).

(3) Williams R. N.: "Adaptive Data Compression", Kluwer Academic Publishers (1991).

(4) Hellman M. E.: "An Extension of the Shannon Theory Approach to Cryptography", IEEE Trans. Inf. Theory, **23**, 3, pp. 289-294 (1977).

(5) Lelewer D. A. and Hirshberg D. S.: "Data Compaction", ACM Computing Surveys, **19**, 3, pp. 261-294 (Sept. 1987).

(6) Bar-Ness Y. and Narasimhan P.: "Error Propagation and Error Correction in Universal Coding Systems", Proc. of ISITA '90, 27-3, pp. 419-422 (Nov. 1990).

(7) Agnew G. B.: "Cryptographic Systems Using Redundancy", IEEE Trans. Inf. Theory, **36**, 1, pp. 31-39 (Jan. 1990).

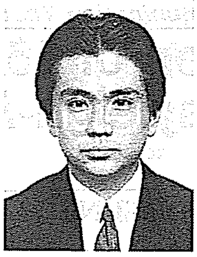
(8) Kwon H. M. and Tu K.: "Degradation of the Space Station Freedom Ku-Band Return Link Due to Encryption", Proc. of ICC '91, pp. 1123-1137 (June 1991).

(9) Ziv J. and Lempel A.: "A universal algorithm for sequential data compression", IEEE Trans. Inf. Theory, **IT-23**, 3, pp. 337-334 (May 1977).

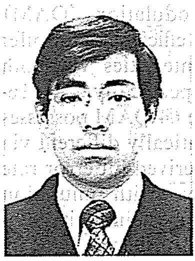
(10) Bentley J. L., Sleatorm D. D., Tarjan R. E. and Wei V. K.: "A Locally Adaptive Data Compression Scheme", Commun. ACM, **29**, 4, pp. 320-330 (April 1986).

(11) Lathi B. P.: "Modern Digital and Analog Communication Systems", Holt-Saunders International Editions (1987).

(12) Yamazato T., Sasase I. and Mori S.: "Interlace Coding System Involving Error Correcting Code and Data Compaction Code", Proc. of 1991 IEEE Pacific Rim Conference, No. 196, pp. 196-199 (May 1991).



Takaya Yamazato was born in Okinawa, Japan in 1964. He received the B.E. and M.E. degrees in Electrical Engineering from Shinshu University, Nagano, Japan in 1988 and 1990, respectively. He is currently a doctoral candidate in Keio University, Japan. He is engaged in research on information theory and communication theory.



Iwao Sasase was born in Osaka, Japan on November 17, 1956. He received the B.E., M.E., and Ph.D. degrees in Electrical Engineering from Keio University, Yokohama, Japan in 1979, 1981, and 1984, respectively. From 1984 to 1986 he was a Post Doctoral Fellow and a Lecturer of Electrical Engineering at University of Ottawa, Canada. He is now an Assistant Professor of Electrical Engineering at Keio University, Japan. His research interests include modulation and coding, satellite and microwave communications, optical communications, communication networks, and information theory. He received 1984 IEEE Communication Society Student Paper Award (Region 10), 1988 Hiroshi Ando Memorial Young Engineering Award, and 1988 Shinohara Memorial Young Engineering Award. Dr. Sasase is a member of the Institute of Electrical and Electronics Engineers (IEEE), and the Society of Information Theory and Its Applications.

Shinsaku Mori was born in Kagoshima, Japan on August 19, 1932. He received the B.E., M.E., and Ph.D. degrees in Electrical Engineering from Keio University, Yokohama, Japan in 1957, 1959, and 1965, respectively. Since 1957, he has been with the Department of Electrical Engineering, Keio University, Japan, where he is a Professor. During the academic year 1978-1979 he was on leave from Keio University as a Visiting Professor of Electrical Engineering at University of Wisconsin, U. S. A.. His research interests include circuit theory, communication engineering, synchronization, information theory, and medical engineering, especially on nonlinear circuits, chaos, digital phase-locked loops, modulation and coding, and hyperthermia. Dr. Mori is a member of the Institute of Electrical Engineers of Japan, the Japan Society for Simulation Technology, the Society of Instrument and Control Engineers, the Society of Information Theory and Its Applications, the Japanese Society of Hyperthermic Oncology, and the Institute of Electrical and Electronics Engineers (IEEE).