A Chaos-based Unequal Encryption Mechanism in Wireless Telemedicine with Error Decryption

Chin-Feng Lin, Cheng-Hsing Chung, Zhi-Lu Chen , Chang-Jin Song , and Zhi-Xiang Wang

Department of Electrical Engineering
National Taiwan-Ocean University

Pei-Ning Road, Keelung, Taiwan ROC

Abstract:- In this paper, we have developed a chaos-based unequal encryption mechanism which can be applied in the wireless telemedicine with error decryption. The main idea for using chaos sequence is to increase the unpredictability compared with other kinds of random sequences. An essential feature of this unequal encryption scheme is that a bit stream mapping of 1D chaotic scrambler and a permutation scheme are allocated to the medical information that requires higher level encryption. In addition, a bit stream mapping of 1D chaotic scrambler is provided to messages that can meet high speed encryption. Simulation results show when a correct deciphering parameter is put in, these signals will be completely recovered. As long as there is an input parameter error, for example, with 0.00000001% initial point error, these signals will not be recovered.

Key-Words: - chaos, unequal encryption mechanism, wireless telemedicine.

1 Introduction

We adopt high speed and robust advanced wireless communication system to achieve ubiquitous emergent or health-monitoring medical services [1-2]. Transmission information is confidential information for patients. Encryption is an essential mechanism to keep confidential. The current method to do this is to encrypt the names of patients, instead of encrypt transmission medical signal. This method of encryption has the advantage of a fast encryption speed and low complication. However, its robustness is not strong enough. In order to increase robustness for encryption, we apply a chaos-based unequal encryption mechanism to wireless telemedicine. Chaos theory with excellent unpredictability is suitably used in encryption system [3-4]. It is a new and interesting research topics for real time encryption, such as audio and video signal [5-9]. The performance of chaos based visual encryption mechanism that applies in JPEG2000 X-ray and electrocardiogram (ECG) medical signals, has been scrupulously studied in our earlier work [10-13]. Adding security to quality of service (QoS) architectures are discussed in [14]. We adopt an unequal level encryption mechanism in various signals without transmission error [15]. In this paper, we propose a chaos-based unequal encryption mechanism in wireless telemedicine system with transmission error. We based on a bit streams mapping of 1D chaotic scrambler and a permutation scheme to achieve EEG medical signal encryption. A way to realize the encryption mechanism is to scramble the bit streams of the input EEG signal by scrambling 1D chaotic sequence to randomize EEG signal bit streams, and then a chaotic address scanning order encryption is applied to the randomized reference bit streams. In addition, a bit stream mapping of 1D chaotic scrambler are granted to messages that can tolerate low level encryption but meet high speed encryption. It can be

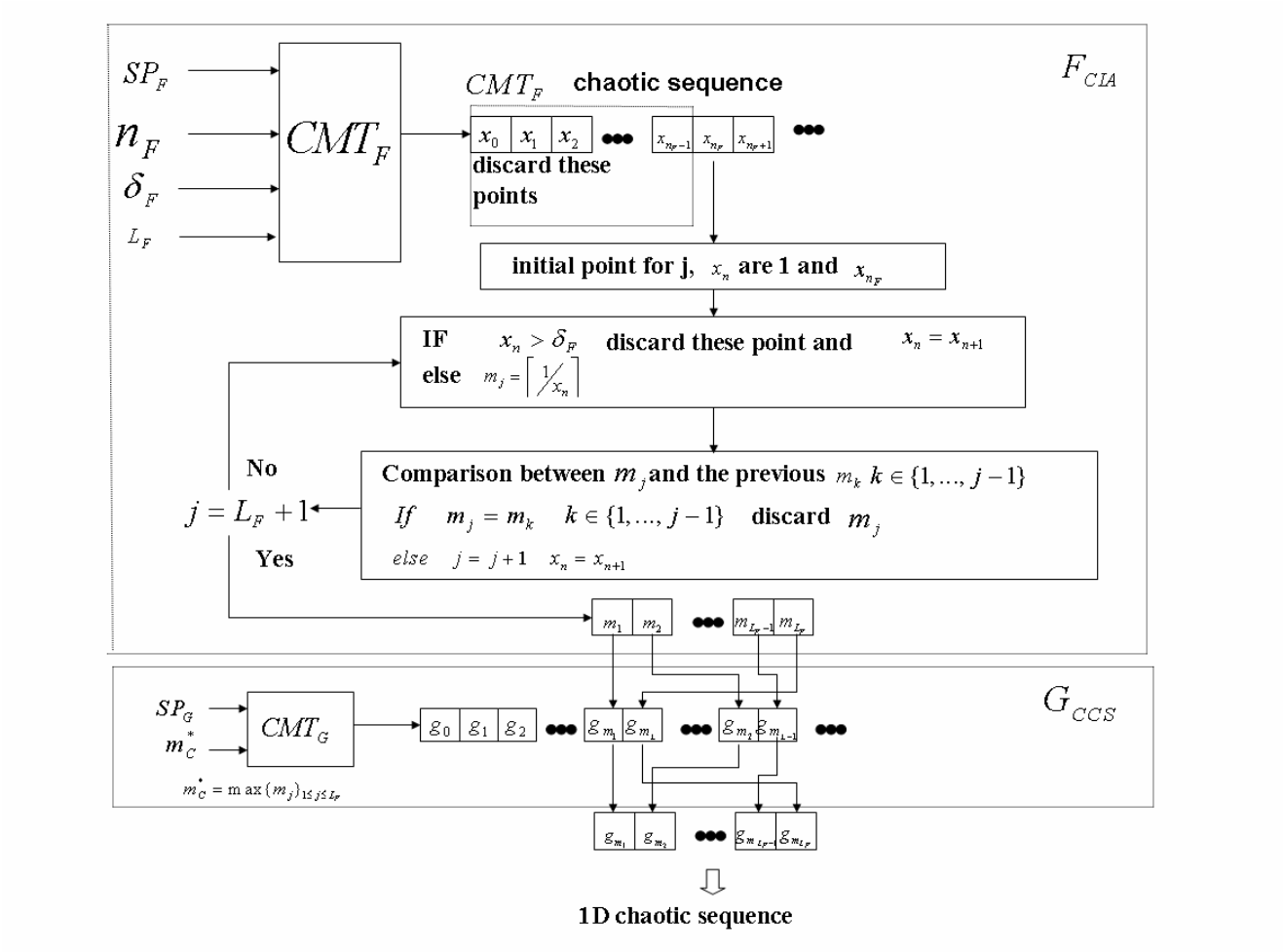

Fig. 1 The proposed 1D chaotic sequence scrambler.

applied in real time G.729 audio and MPEG-4 video signal. Simulation results show that it is a feasible encryption scheme in wireless telemedicine system with transmission bit error rate (BER) 10^{-3}, 10^{-4}, and 10^{-7} for audio, video, and data signal, respectively [1]. As long as there is an input parameter error, for example, with 0.00000001% initial point error, these signals will not be recovered.

2. 1D chaotic sequence scrambler

In order to achieve secure medical communication, our 1D chaotic sequence scrambler is developed. Figure 1 shows this concept. The basic concept of the 1D chaotic signal scrambler is generated a 1D random sequence based on chaotic theory. Then the input media signal bit streams are to scramble the 1D chaotic random bit streams in order to achieve encryption effect. The encryption medical signal will loss patient's medical information and make the medical signal illegible. The procedure generating the 1D chaotic random sequences are described as following. First, generate the index address that is required for each chaotic candidate random values by using chaotic index address assignment process which is denoted as F_{CIA}. Using the chaotic candidate point generator which is denoted as G_{CCS} generates the corresponding random value. In other words, generate a sequence of chaotic numbers with a finite length based on chaotic candidate point generator G_{CCS}, then find out the corresponding value in the sequence based on the address value generated by chaotic index address assignment process F_{CIA} as the random value and use these chaotic random sequences to scramble media signal bit streams. The encryption procedure could be described as

E(P,K)=C, where P is the original signal, E is the encryption algorithm, K is the encryption key, and C is the scrambled signal. Our chaotic index address assignment process, F_{CIA} is described in the following:

Step 0: Select chaotic logistic map type CMT_F of F_{CIA}.

Step 1: inputs SP_F, L_F, n_F, δ_F.

Where SP_F is the starting point of F_{CIA}. L_F is the length of in the input ECG bit streams, n_F is the number of discarded initial chaotic index points and δ_F is for the level of security.

Step 2:(a) If $\delta_F > 1$, then terminate the procedure; otherwise do the next step.

(b) $x_0 = SP_F$

(c)Generate n_F chaotic points:

$$x_n = CMT_F(x_{n-1}) \quad (1)$$

and then discard those points

Step 3: (a) $x_{n_F+1} = CMT_F(x_{n_F})$

(b) If $x_n > \delta_F$ then discard this point and go to step 2; otherwise do the next step.

$$\text{(c) } m_j = \left\lceil 1 \Big/ x_{n_F+1} \right\rceil \quad (2)$$

where the initial value for index j is 1,and j=j+1;

Step 4: [comparson between m_j and the previous m_k, $1 \le k \le j-1$]

If $m_j \in \{m_k, 1 \le k \le j-1\}$, then discard this point and go to step 2; Otherwise do the next step.

Step 5: If $j \ge L_F$, terminate the procedure and then output m_j, $1 \le j \le L_F$.

In addition, the procedure for chaotic candidate point generator G_{CCS} is described as follows:

Step 0: Select chaotic logistic map type CMT_G of G_{CCS}.

Step 1: inputs SP_G, where is the starting point of G_{CCS}

Step 2: Generate a sequence of chaotic numbers with a finite length of m_C^* by performing the iterative algorithm

$$x_n = CMT_G(x_{n-1}),$$

$$x_0 = SP_G \; x_0 = SP_{CCS,C}, \; 1 \le n \le m_C^* \quad (3)$$

Step 3: Output x_n, $1 \le n \le m_C^*$.

Thus, the procedure for 1D chaotic media signal scrambler is summarized as follows:

Step 1: [generated chaotic index address sequence]

(a) $1 \le j \le L_F$, $m_j \in N$,

$$F_{CIA}\{m_1, ..., m_{L_F}\} \to N \quad (4)$$

(b) m_C^* = maximum index address=

$$= \max_{1 \le j \le L_F} m_j$$

Step 2: [generated chaotic candidate points in stage 1]

Generate a chaotic candidate point sequence with a finite length of m_C^* by performing $G_{CCS}: x_n$, $1 \le n \le m_C^*$.

Step 3: [generated chaotic random scramble sequences]

$$G(i) = x_{m_i} \quad (5)$$

$1 \le i \le L_F$, $x_{m_i} = G_{CCS}: x_n$, $n = m_j$

$$S(i) = s_i = \begin{cases} 1 & if \quad x_{m_i} \ge 0.5 \\ 0 & if \quad x_{m_i} < 0.5 \end{cases} \quad (6)$$

$1 \le i \le L_F$

Then the media signal is scrambled the 1D chaotic random sequence to achieve encryption.

3. Chaotic Scanning Encryption

A chaotic permutation in medical signal locations is used to increase secure telemedicine communication. It is similar to chaotic index address assignment F_{CIA}

and is described as follow. By using chaotic permutation process, those orders are scanned. Then those orders are re-scanning via chaotic de-permutation to reconstruct L_F medical signal bit streams in the receiver. The chaotic permutation a process F_{CP} is described as follows:

Step 0: Select chaotic logistic map type $CMT_{F_{CP}}$ of F_{CP}.

Step 1: inputs $SP_{F_{CP}}$ and L_F

Where SP_F is the starting point of $F_{CIA} \cdot L_F$ is the length of in the input signal bit streams

Step 2: $x_0 = SP_2$

Step 3: (a) Generate a chaotic address index corresponding to "j", $1 \le j \le L_F$:

$$x_n = CMT_{F_{CP}}(x_{n-1}) \qquad (7)$$
$$m_j \leftarrow \lceil 1/x_n \rceil$$

If $m_j > L_F$, discard m_j, and go to setp 2. Otherwise do the next step.

Step 4:[Comparson between m_j and the previous m_k, $1 \le m_k \le j-1$]

If $m_j \in m_k, 1 \le k \le j-1$, then discard this point and go to step 2. Otherwise do the next step.

Step 5: If $j \ge L_F$, terminate the procedure and then output m_j, $1 \le j \le L_F$. Otherwise do the next steps.

(a) $n \leftarrow n+1$

(b) $j \leftarrow j+1$

(c) go to step2

4. Simulation Results

We have carried out a simulation to demonstrate proper functionality of the proposed unequal encryption in wireless telemedicine system. In the simulation, we use a two-layer highest security chaotic encryption mechanism and applied to the EEG medical signal bit streams and JPEG2000 x-ray medical signal bit streams. This two-layer security protection mechanism includes (1) 1D chaotic random sequence scrambler and (2) chaotic EEG bit streams address scanning order encryption. In addition, a 1D fast chaotic random sequence scrambler is used in audio signal bit streams as well as MPEG-4 video signal bit streams. The design parameters and performance verification is described as follows. The parameters δ_F is 0.1 for input medical signal, n_F is equal to 10^6. CMT_F, CMT_G, and $CMT_{F_{CP}}$ have the same simple chaotic map $C(x,r)$ is given by

$$C(x,r) = rx(1-x), \quad 0 < x < 1 \qquad (8)$$

and the recursive form is expressed as

$$x_{n+1} = rx_n(1-x_n) \qquad (9)$$

where the starting point $x_0 = SP_F = SP_G = SP_{F_{CP}}$ is equal to 0.1. The transmission BER for encrypted audio, video, and data are 10^{-3}, 10^{-4}, and 10^{-7}, respectively. Figure 2 shows decrypted audio signal with transmission BER 10^{-3} and 0.00000001% initial point error. Figure 3 shows decrypted audio signal with transmission BER 10^{-3}. It is seen that the decrypted audio signal 0.00000001% initial point error is not clear. Figure 4 shows the decrypted JPEG2000 X-ray medical signal with transmission BER 10^{-4} and 0.00000001% initial point error. Figure 5 shows the decrypted JPEG2000 X-ray medical signal with transmission BER 10^{-4}. Figure 6 shows the PSNR values for decrypted MPEG-4 video signal with transmission BER 10^{-4}. Figure 7 shows the PSNR values for decrypted MPEG-4 video signal with transmission BER 10^{-4} and 0.00000001% initial point error. Figure 8 shows the decrypted EEG medial signal with transmission BER 10^{-7} and 0.00000001% initial point error. Figure 9 shows decrypted EEG medial signal with transmission BER 10^{-7}. From these simulation results, it is found that the chaos-based encryption mechanism is very superior. When correct deciphering parameters are put in, the signal will be completely recovered; but, when there is an input parameter error, for example, with 0.00000001% initial point error, these signals will not be recovered. The mean square error of the original and the decrypted audio is 0.0169. The percent root-mean-

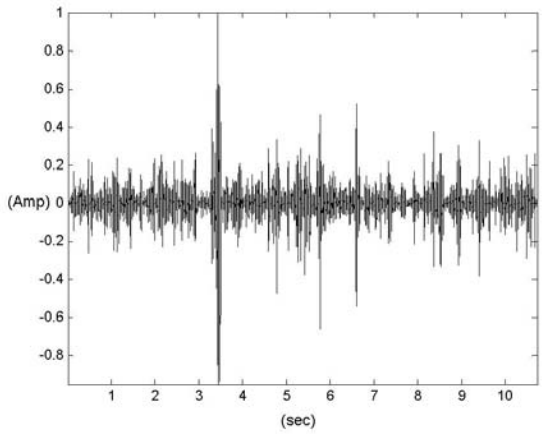

Figure 2 The decrypted audio signal with transmission BER 10^{-3} and 0.00000001% initial point error.(r=0.0033)

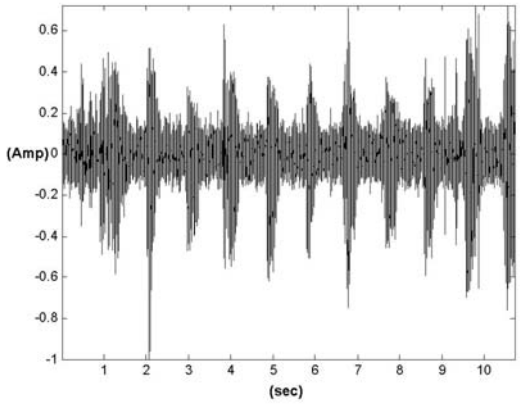

Figure 3 The decrypted audio signal with transmission BER 10^{-3} . (MSE=0.0169)

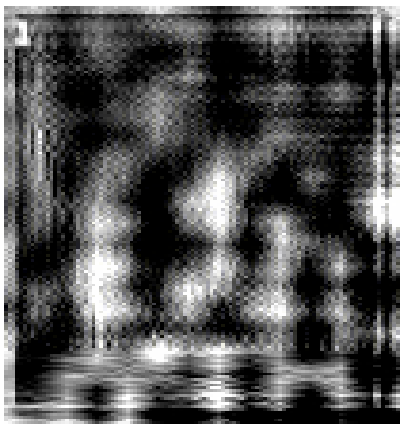

Figure 4. The decrypted JPEG2000 X-ray medical signal with transmission BER 10^{-4} and 0.00000001% initial point error.

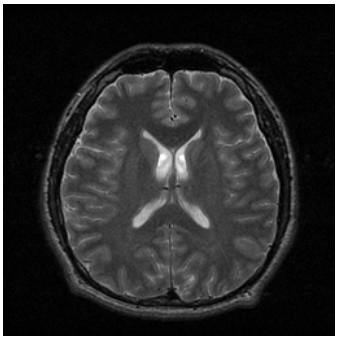

Figure 5 The decrypted JPEG2000 X-ray medical signal with transmission BER 10^{-4} . (PSNR = 30.31dB)

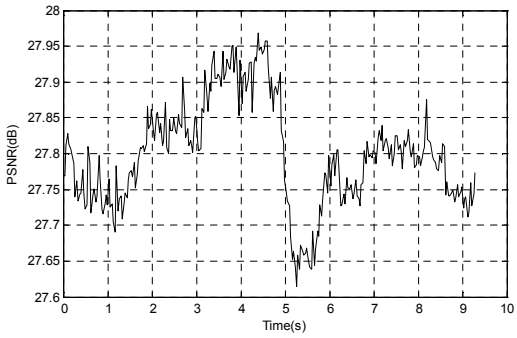

Figure 6. The PSNR values for decrypted H.264 video signal.

Figure 7 The decrypted MPEG-4 video signal with transmission BER 10^{-4} and 0.00000001% initial point error.

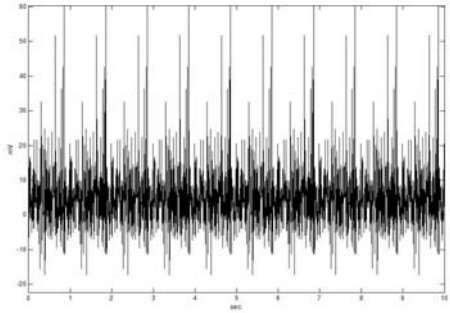

Figure 8 the decrypted ECG medial signal with transmission BER 10^{-7} and 0.00000001% initial point error.(r=0.055)

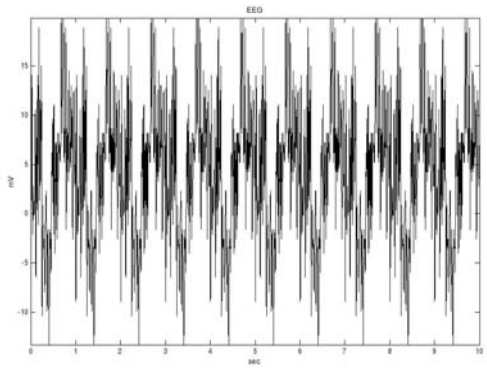

Figure 9 The decrypted EEG medial signal with transmission BER 10^{-7}. (PRD =0.12146%)

square difference (PRD) for original and the decrypted EEG signal is 0.12146%. The PRD value is defined as

$$PRD = 100 \times \sqrt{\frac{\sum_{i=1}^{L}(X_{ori}(i) - X_{dec}(i))^2}{\sum_{i=1}^{L} X_{ori}^2(i)}} \quad (10)$$

Where X_{ori} is original EEG medical signal. X_{dec} is the decrypted EEG medial signal with transmission BER 10^{-7}. The EEG medical signal is clear and can be applied in medicine. In order to compare the initial and the decrypted EEG medical signal with 0.00000001% initial point error, we use the Pearson correlation coefficient given by

$$r = \frac{\sum XY - \frac{\sum X \sum Y}{N}}{\sqrt{(\sum X^2 - \frac{(\sum X)^2}{N})(\sum Y^2 - \frac{(\sum Y)^2}{N})}} \quad (11)$$

where X and Y are the intensities of values in original EEG signal and encryption EEG signal, respectively. N is the total number of values in the EEG signal. Pearson correlation coefficient between the original and the encryption EEG signal is r=0.05. It corresponds to a low correlation (r = 0 represents the case where the images are completely uncorrelated). The decrypted EEG medical signal with 0.00000001% initial point error is unreadable and lost medical information. The peak signal to noise ratio (PSNR) of the original and the decrypted JPEG2000 X-ray image with lossless compression is 30.31dB as well as the original and the decrypted MPEG-4 video signal is 27.3 dB. These audio and video signals are clear and can be applied in wireless telemedicine.

5. Conclusion

In this paper, we have developed a new unequal encryption mechanism based on theory of chaos. A bit stream mapping of 1D chaotic scrambler and a permutation scheme are allocated to the EEG and JPEG2000 X-ray image medical information that requires higher encryption. In addition, a bit stream mapping of 1D chaotic scrambler are granted to G.729 audio, and MPEG-4 video signals that can tolerate low encryption level but meet high speed encryption. Simulation results show when correct deciphering parameters are put in, the signal will be completely recovered. It is a feasible encryption scheme in wireless telemedicine system with transmission BER 10^{-3}, 10^{-4}, and 10^{-7} for audio, video, and data signal, respectively. However, it there is existed with an input parameter error, for example, with 0.00000001% initial point error, these signals will not be recovered. The unequal encryption mechanism can be applied in E-health and M-health. In addition, current optimization techniques like genetic algorithm (GA) can apply in the unequal encryption mechanism to increase encryption and decryption speeds.

References

[1] Cabral J. E. and Kim Y., "Multimedia Systems for Telemedicine and Their Communications Requirement," *IEEE Commun. Magazine,* vol. 34, 1996, pp. 20-27.

[2] Cypher D., Chevrollier N., Montavont N., and Golmie N., "Preailing over Wires in Healthcare Environments: Benefits and Challenges," *IEEE Communications Magazine*, 2006, pp.56-63.

[3] Kocarev L., "Chaos-Based Cryptography: A Brief Overview," *IEEE Circuits and System Magazine,* 2001, pp.6-21.

[4] Yang M., Bourbakis N. and Li S., "Data, image, video encryption," *IEEE Potentials*, August/September, 2004, pp.28-34.

[5] Li Y., Liang L., Su Z., and Jiang J., " A New video Encryption Algorithm for H.264, " *IEEE ICICS 2005 ,* pp.1121-1124.

[6] Rao K. D. , "A Robust and Secure Scheme for Image Communication Over Wireless Channels," *IEEE 7th CAS Symposium on Emerging Technologies:Circuits and Systems for 4G mobile Communication, 2005*.

[7] Tang, K. W. ,"A Chaos-based Secure Voice Communication system," *IEEE International Conference on Industrial Technology*, 2005, pp.571-576.

[8] Volos Ch. K., Kyprianidis I. M., and Stouboulos I. N., " Chaotic Cryptosystem based on Inverse Duffing Circuit, " *Proc. of the 5th WSEAS Int. Conf. on Non-Linear Analysis, Non-Linear Systems and Chaos, Bacharest, Romania*, pp.92-97.

[9] Grigoras V. and Grigoras C., " Chaos Encryption Method Based on Large Signal Modulation in Additive Nonlinear Discrete-Time System", *Proc. of the 5th WSEAS Int. Conf. on Non-Linear Analysis, Non-Linear Systems and Chaos, Bacharest, Romania*, pp.98-103.

[10] Lin C. F., Chang W. T., and Li C. Y., " Design of A Chaos Base Visual Encryption Mechanism in JPEG2000 Medical Image," *IEEE International Conference On Systems & Signals 2005*, pp.277~282, Taiwan.

[11] Lin C. F. and Chung C. S., "A Chaos Base Visual Encryption Mechanism in ECG Medical Signal, "*World Congress on Medical Physics and Biomedical Engineering 2006,* pp.2250~2253, Korea.

[12] Lin C. F., Chang W. T., and Li C. Y., "A Chaos-based Visual Encryption Mechanism in JPEG2000 Medical Images," *J. of Medical and Biological Engineering*, 27(3), 2007, pp.144-149.

[13] Lin C. F., and Chung C. H. , "A chaos-based visual encryption mechanism in integrated ECG/EEG medical signals," *appear in IEEE the 10th International Conference on Advanced Communication Technique 2008, Korea*

[14] Burnett R. , Brunstrom A., and Nilsson A. G., "Perspectives on Multimedia Communication, Media, and Information Technology," *John Wiley & Sons, Ltd, 2003*.

[15] Lin C. F. , Chung C. H. , Chen Z. L., Song C. J., and Wang Z. X., "A Chaos Based Unequal Encryption Mechanism in Mobile Medicine System, "*appear in IEEE Intelligent Information Hiding and Multimedia Signal Processing 2007*, pp.233-236, Taiwan.