Journal of Marine Science and Technology

Volume 19 | Issue 6 Article 11

A 2D CHAOS-BASED VISUAL ENCRYPTION SCHEME FOR CLINICAL EEG SIGNALS

Chin-Feng Lin
Department of Electrical Engineering, National Taiwan Ocean University, Keelung, Taiwan, R.O.C., lcf1024@mail.ntou.edu.tw

Boa-Shun Wang
Department of Electrical Engineering, National Taiwan Ocean University, Keelung, Taiwan, R.O.C.

Recommended Citation
Lin, Chin-Feng and Wang, Boa-Shun (2011) "A 2D CHAOS-BASED VISUAL ENCRYPTION SCHEME FOR CLINICAL EEG SIGNALS," *Journal of Marine Science and Technology*: Vol. 19: Iss. 6, Article 11.
DOI: 10.51400/2709-6998.2209
Available at: https://jmstt.ntou.edu.tw/journal/vol19/iss6/11

A 2D CHAOS-BASED VISUAL ENCRYPTION SCHEME FOR CLINICAL EEG SIGNALS

Acknowledgements

The authors acknowledge the support of the teacher research project of National Taiwan Ocean University, 99B60201, Center for Marine Bioenvironment and Biotechnology, NSC 93-2218-E-019-024, and the valuable comments of the reviewers.

A 2D CHAOS-BASED VISUAL ENCRYPTION SCHEME FOR CLINICAL EEG SIGNALS

Chin-Feng Lin* and Boa-Shun Wang*

Key words: two dimensional (2D) chaos-based encryption scheme, clinical electroencephalography, transmission bit error rate, parallel processing, mobile telemedicine.

ABSTRACT

In this paper, we have developed a two-dimensional (2D) chaos-based encryption scheme that can be applied to signals with transmission bit errors in clinical electroencephalography (EEG) and mobile telemedicine. As opposed to one-dimensional (1D) chaos-based encryption, the proposed 2D schemes uses the concept of parallel processing to increase the encryption speed. An essential feature of the proposed scheme is that signals mapping of a 2D chaotic scrambler and a permutation scheme are used to obtain clinical EEG information that requires high-level encryption. Simulation results show that when the correct deciphering parameters are inputted, EEG signals with a transmission bit error rate (BER) of 10^{-7} are completely recovered. However, these signals can not be recovered if there is an error in the input parameters, for example, an initial point error of 0.00000001%.

I. INTRODUCTION

Chaos theory is an interesting branch of mathematics that has been widely applied in many engineering fields [2-31]. One application of this theory is chaos-based encryption, which is used for the encryption of data, audio, video, images, and biomedical signals. Unlike block encryption algorithms such as the data encryption standard (DES) algorithm, Rivest, Shamir, and Adleman (RSA) algorithm, and advanced encryption standard (AES) algorithm, a chaos sequence is continuous and suitable for data encryption in continuous media such as audio, video, electrocardiogram (ECG) and electroencephalography (EEG) signals, and in large block files such as image signals. Chaos-based encryption is sensitive to the starting point and type of the chaotic logistic map used; different starting points and chaotic logistic maps generate different chaotic sequences for encryption. Zhou *et al.* [31] identified several disadvantages of previous chaos-based encryption system: (i) the chaotic map may be analyzed easily if a few plaintext-ciphertext pairs are known; (ii) the self-synchronization subsystem is insensitive to the parameters used; and (iii) the signal to be encrypted is strongly correlated to the original signal. In [26], an efficient hierarchical chaotic image encryption algorithm has been developed on the basis of chaotic permutation and used for rearranging image blocks and for scrambling the pixels in each block. In [2, 3, 17, 20, 21, 24-26], chaos-based encryption schemes that can be applied to e-mail, voice, and video signals have been proposed. In these studies, chaos-based encryption algorithms have been adopted to generate encrypted bit streams. In these encryption algorithms, an exclusive-OR (XOR) gate is used to generate encryption e-mail, voice, and video bit streams. Chaos-based decryption carried out in the receiver by using the same parameters used for chaos-based encryption and decrypted e-mail, voice, and video bit streams are generated by carrying out an XOR operation. Chaos-based encryption is suitable for mobile telemedicine applications [11-14, 16], as it guarantees confidentiality of patient-related information by facilitating data protection. In [12], we carry out chaos-based pixel address (position) permutation and transformation of pixel values for the encrypt ion X-ray images. We use all-pass filtering to scramble the phase spectra of the most-important low-resolution sub-image in the following manner. In the pre-filtering step, we add 2D chaotic signals to randomize reference phase spectra; then, in the post-filtering step, we subtract the same reference phase spectra to recover the original phase spectra of the image. In [14], we proposed a one-dimensional (1D) chaos-based bit streams ciphers for use in mobile telemedicine systems. In [15], we scramble the signal values of the inputted EEG signals by a 1D chaotic signal to randomize the EEG signal values, and applied chaotic address scanning order encryption to achieve visual encryption. In this paper, we make improvements to 1D chaos-based encryption and propose a 2D chaos-based visual encryption scheme based on parallel processing for application to clinical EEG signals. The proposed 2D chaos-based cipher can simultaneously encrypt N clinical channels in a parallel architecture. An essential feature of the 2D encryption scheme is that signal mapping of 2D chaotic scrambler and a permutation scheme are used to obtain clinical EEG information that requires high-level encryption. The encryption speed in the case of 2D

Paper submitted 08/12/09; revised 02/23/10, 04/12/10; accepted 06/09/2010.
Author for correspondence: Chin-Feng Lin (e-mail: lcf1024@mail.ntou.edu.tw).
**Department of Electrical Engineering, National Taiwan Ocean University, Keelung, Taiwan, R.O.C.*

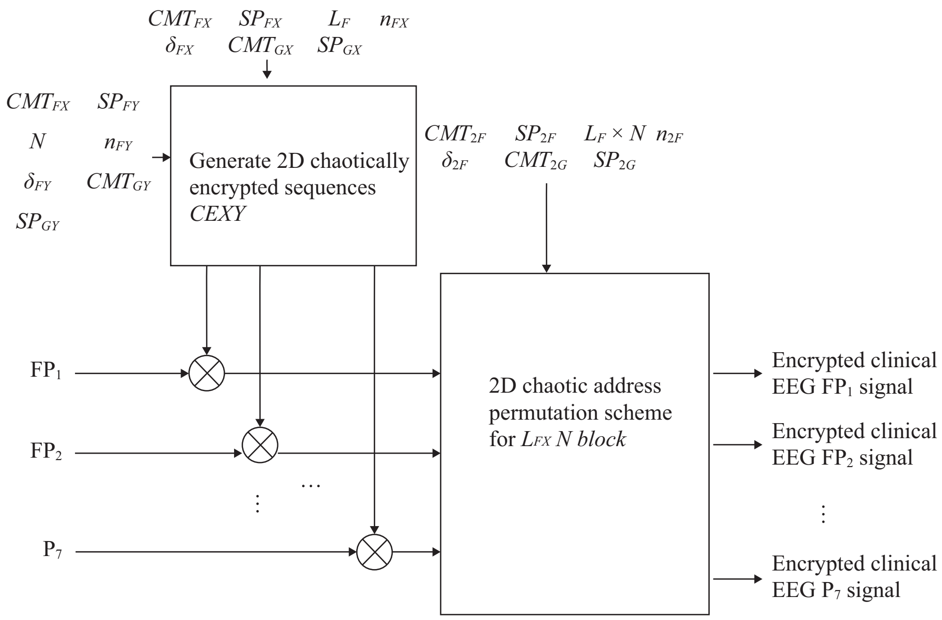

Fig. 1. Proposed 2D chaos-based encryption scheme for clinical EEG signals.

encryption is N times higher than that in the case of 1D chaos-based encryption; on the other hand, the hardware complexity in 2D encryption is N times lower than that in 1D encryption. This is because part of the hardware can be hardware shared in the proposed 2D chaos-based cipher. Simulation results show that when the correct deciphering parameters are inputted, signals with a transmission bit error rate (BER) of $10^{-7}$are completely recovered. However, signal recovery is not achieved if there is an error in the input parameters, for example, an input point error of 0.00000001%.

II. A 2D CHAOS-BASED ENCRYPTION SCHEME FOR CLINICAL EEG SIGNALS

Fig. 1 shows the architecture of the proposed 2D chaos-based encryption scheme to clinical EEG signals. In this scheme, a 2D chaos-based encryption scrambler and a 2D chaotic address permutation method are used. First, N multichannel clinical EEG signals are inputted to the 2D chaos-based cipher and processed by a 2D chaos-based encryption scrambler to generate 1st 2D chaotically encrypted EEG signals. In addition, 2D chaotically encrypted sequences are generated, and are multiplied by the N multichannel clinical EEG signals to obtain the 1st 2D chaotically encrypted EEG signals. Then, the 1st 2D chaotically encrypted EEG signals are processed by the 2D chaotic address permutation method to generate a 2nd 2D chaotically encrypted EEG signals. Fig. 2 shows the flow chart of the proposed 2D visual chaos-based encryption scheme for clinical EEG signals. In order to increase the robustness of the encryption system, we use chaotic index address assignment process F_{CIAX} and chaotic candidate point generator process G_{CCSX} to represent values in the x coordinate axis, and to generate 1D chaotically encrypted sequences (*CEX*) of length L_F. Similarly, the process is repeated to generate 1D chaotically encrypted sequences (*CEY*) of length N in the y coordinate axis. The vector inner product of *CEX* and *CEY* is obtained to generate 2D chaotically encrypted sequences *CEXY*. The 1st 2D chaotically encrypted signals *CEEG1* is generated from the vector inner product of *CEXY* and N channel clinical *EEG* signals. In order to decrease the correlation between the encrypted and original EEG signals, we use 2D chaotic address permutation encryption to generate 2nd 2D chaotically encrypted EEG signals *SGEEGN*. The parameters used in the scheme are listed in Table 2. The steps involved in the implementation of our 2D chaos-based encryption scrambler can be summarized as shown below.

Step 1: Select a chaotic logistic map type CMT_{FX} of F_{CIAX}, where the starting point is SP_{FX}, L_F is the length of an encrypted clinical EEG signal. The parameters n_{FX} and, δ_{FX} denote the security level.

Step 2: Generate a chaotic sequence of length n_{FX}.

$$x_{n+1} = CMT_{FX}(x_n);\ x_0 = SP_{FX} \quad n = \{1, 2, ..., n_{FX}\} \tag{1}$$

Step 3: Discard the previous n_{FX} chaotic sequence.

Step 4: Generate a new chaotic sequence

$$x_n = CMT(x_{n_{FX}+1});\ n = \{n_{FX}+1, ...\};$$

Step 5: If $x_n > \delta_{FX}$, discard x_n and go to step 4. Else, go to step 6.

Table 1. The performance of transmission error of the proposed 2D chaos-based clinical EEG signals.

	BER	10^{-7}	10^{-6}	10^{-5}	10^{-4}	10^{-3}	10^{-2}	10^{-1}
Correct encryption	PRD (%)	1.1285	1.1285	1.1744	1.2069	6.1534	20.0253	61.2303
	MSE	0.0056	0.0056	0.0061	0.0064	0.167	1.7691	16.5397
	r	0.9999	0.9999	0.9999	0.9999	0.9981	0.9804	0.8288
Error encryption	r	0.0272	0.0272	0.0272	0.0272	0.0276	0.0297	0.0341

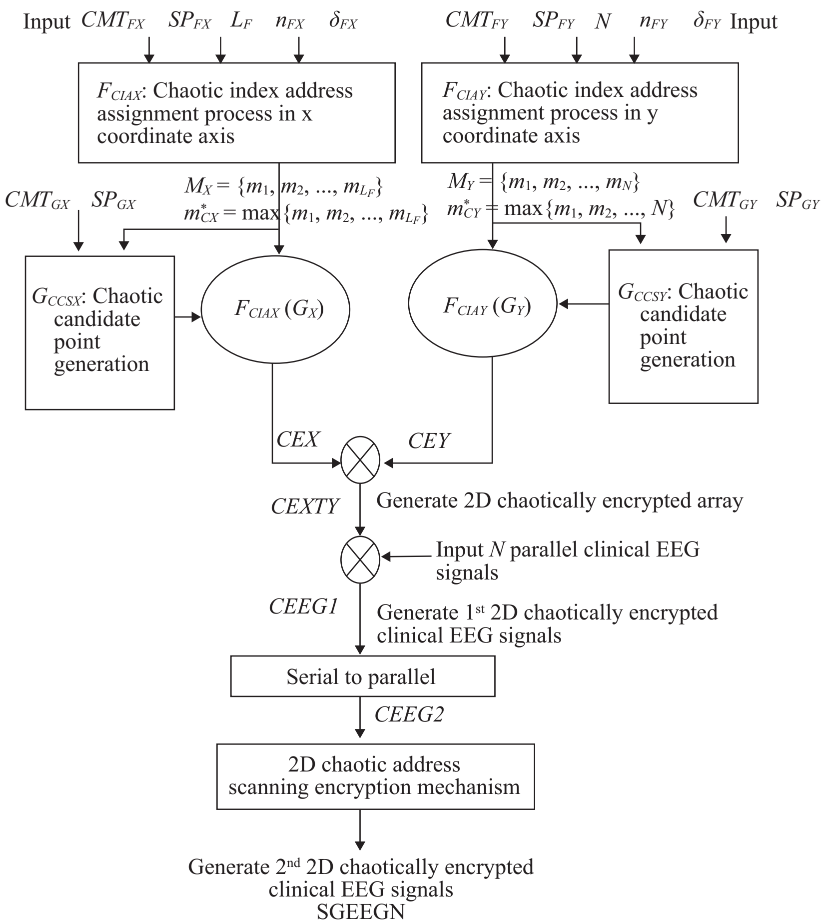

Fig. 2. Flow chart of the proposed 2D visual chaos-based encryption scheme for clinical EEG signals.

Step 6:

$$m_k = \left\lceil \frac{1}{x_n} \right\rceil \tag{2}$$

If $m_k \notin M_X$; $M_X = \{m_1, \ldots, m_{k-1}, m_k\}$, go to step 7. Else, go to step 4.

Step 7: If $k = L_F$;

$$M_X = \{m_1, m_2, ..., m_{L_F}\}; \quad m^*_{CX} = \max\{m_1, m_2, ..., m_{L_F}\}; \tag{3}$$

Else, go to step 4.

Step 8: Deliver m^*_{CX} to the chaotic candidate point generator G_{CCSX}.

Step 9: Deliver a chaotic logistic map of the type CMT_{GX} for G_{CCSX}, where the starting point is SP_{GX}.

Step 10: Generate a chaotic sequence of length m^*_C.

$$g_{n+1} = CMT_{GX}(g_n); \quad g_0 = SP_{GX}; n = \{1, 2, \ldots, m^*_C\}; \quad G_X = \{g_1, \ldots, g_{m^*_C}\} \tag{4}$$

Step 11: Deliver M to the chaotic candidate point generator G_{CCSX}.

Step 12: Generate an encrypted chaotic signal CEX in the x coordinate axis.

$$M_X = \{m_1, m_2, ..., m_{L_F}\}; G_X = \{g_1, ..., g_{m_C^*}\};$$
$$CEX = \{g_{m_1}, g_{m2}, ..., g_{m_{L_F}}\} = \{cex_1, cex_2, ..., cex_{L_F}\} \quad (5)$$

Step 13: Repeat steps 1-12 to generate an encrypted chaotic signal *CEY* in the y coordinate axis. The length of the *CEY* signal is *N*.

Step 14: Generate a 2D chaotically encrypted sequence *CEXY*.

$$CEX = \{cex_1, cex_2, ..., cex_{L_F}\}$$

$$CEY = \{cey_1, cey_2, ..., cey_{L_F}\}$$

$$CEXY = \begin{bmatrix} cex_1 \times cey_1 & cex_2 \times cey_1 & \cdots & cex_{L_{FX}} \times cey_1 \\ cex_1 \times cey_2 & cex_1 \times cey_2 & \cdots & cex_{L_{FX}} \times cey_2 \\ \vdots & \vdots & \vdots & \vdots \\ cex_1 \times cey_N & cex_2 \times cey_N & \cdots & cex_{L_{FX}} \times cey_N \end{bmatrix} = \begin{bmatrix} cexy_{11} & cexy_{12} & \cdots & cexy_{1L_F} \\ cexy_{21} & cexy_{22} & \cdots & cexy_{2L_F} \\ \vdots & \vdots & \vdots & \vdots \\ cexy_{N1} & cexy_{N2} & \cdots & cexy_{NL_F} \end{bmatrix} \quad (6)$$

Step 15: Input *N* parallel clinical EEG signals. The length of the clinical EEG signal sequences is L_F. The *N* clinical EEG signals are defined as

$$EEG = \begin{bmatrix} eeg_{11} & eeg_{12} & \cdots & eeg_{1L_F} \\ eeg_{21} & eeg_{22} & \cdots & eeg_{2L_F} \\ \vdots & \vdots & \vdots & \vdots \\ eeg_{N1} & eeg_{N2} & \cdots & eeg_{NL_F} \end{bmatrix} \quad (7)$$

Step 16: Generate 1st 2D chaotic clinical EEG signals *CEEG1*, which are given as

$$CEEG1 = EEG \times CEXY = \begin{bmatrix} ceeg1_{11} & ceeg1_{12} & \cdots & ceeg1_{1L_F} \\ ceeg1_{21} & ceeg1_{22} & \cdots & ceeg1_{2L_F} \\ \vdots & \vdots & \vdots & \vdots \\ ceeg1_{N1} & ceeg1_{N2} & \cdots & ceeg1_{NL_F} \end{bmatrix} \quad (8)$$

Then, input the *N* parallel 1st 2D chaotic clinical EEG Signals *CEEG1* to a serial-to-parallel converter and generate an $N \times L_F$ chaotic clinical EEG signals *CEEG2*, which are given as

$$CEEG1 = \{ceeg1_{11} \;\; ceeg1_{12} \;\; \cdots \;\; ceeg1_{1L_F} \;\; \cdots \;\; ceeg1_{NL_F}\}$$
$$CEEG2 = \{ceeg2_1 \;\; ceeg2_2 \;\; \cdots \;\; ceeg2_{N \times L_F}\} \quad (9)$$

Process the chaotic clinical EEG signals *CEEG2* by using 2D chaotic address permutation method, and output the 2nd 2D chaotically encrypted clinical EEG signals.

The 2D chaotic address permutation encryption scheme is described as follows.

Steps 1 to 5 are the same as those described for the 1st 2D chaos-based encryption scheme.

Step 6:

$$m_{kl} = \left\lceil \frac{1}{x_n} \right\rceil \quad (10)$$

If $m_{k1} \le N \times L_F$; $m_{k1} \notin \{m_1, \ldots, m_{k-1}\}$;
$M = \{m_1, \ldots, m_{k1-1}, m_{k1}\}$; go to step 7.
Else, go to step 4;

Step 7: If $k1 = N \times L_F$
$M = \{m_1, m_2, \ldots, m_{N \times L_F}\}$; else, go to step 4.

Step 8: Deliver *M* to the output encrypted signal processor.

Step 9: Deliver the encrypted clinical EEG signals *CEEG2* to output the encrypted signals.

Step 10: Perform chaotic address permutation of the encrypted clinical EEG signal *SGEEG*.

$$GEEG = \{geeg_1, ..., geeg_{N \times L_F}\};$$
$$M = \{m_1, m_2, ..., m_{N \times L_F}\}$$
$$SGEEG = \{geeg_{m_1}, geeg_{m_2} ..., geeg_{m_{N \times L_F}}\}$$
$$= \{sgeeg_1, sgeeg_2, ..., sgeeg_{N \times L_F}\} \quad (11)$$

Step 11: Input *SGEEG* to a serial-to-parallel converter, and generate 2nd 2D chaotically encrypted clinical EEG signals *SGEEGN*.

$$\text{SGEEGN} = \begin{bmatrix} sgeeg_1 & sgeeg_2 & \cdots & sgeeg_{L_F} \\ sgeeg_{L_{F+1}} & sgeeg_{L_F+2} & \cdots & sgeeg_{2L_F} \\ \vdots & \vdots & \vdots & \vdots \\ sgeeg_{(N-1)\times L_F+1} & sgeeg_{(N-1)\times L_F+2} & \cdots & sgeeg_{N \times L_F} \end{bmatrix} \quad (12)$$

If the abovementioned process is carried out in the reverse order, the *N* parallel clinical EEG signals are decrypted.

III. SIMULATION RESULTS

Fig. 3 shows the eight parallel clinical EEG signals FP1, FP2, …, P8, P7 in the EEG database [5]. The sampling rate of each clinical signal channel is 256 samples/s. The following are the parameters used in the proposed 2D chaos-based encryption scheme. The starting points are $SP_{GX} = 0.100011$, and $SP_{FX} = 0.200011$, $m_C^* = 256$, $N = 8$, $n_{FX} = n_{FY} = 25600$, and

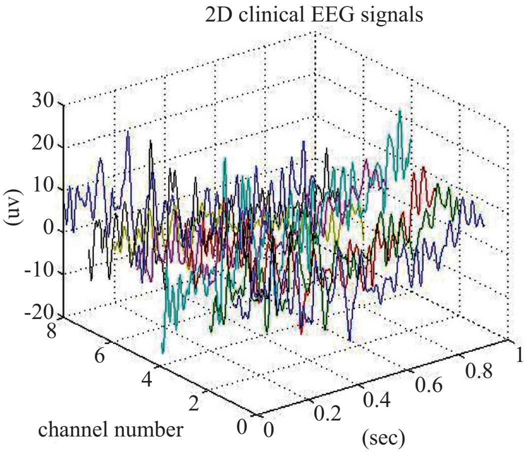

Fig. 3. Eight parallel clinical EEG signals.

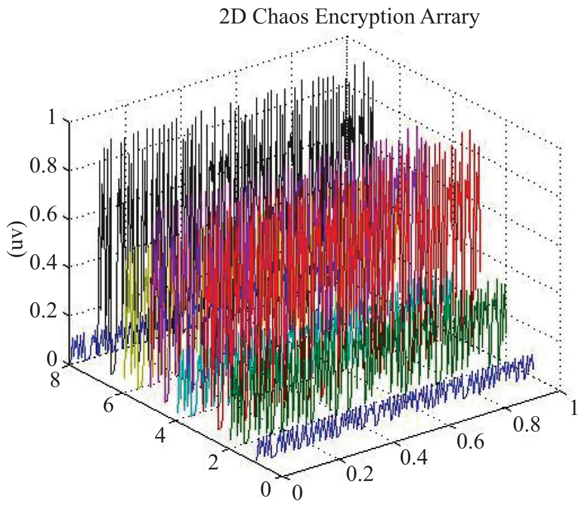

Fig. 4. 2D chaotically encrypted array.

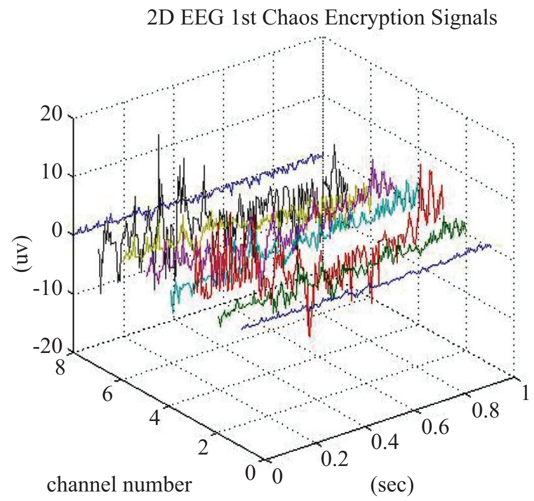

Fig. 5. The 1st 2D chaotically encrypted clinical EEG signals generated by using the proposed chaotic scrambler. (r = 0.11)

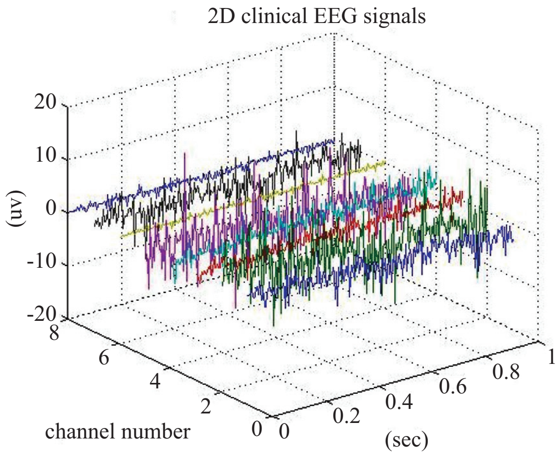

Fig. 6. The 2nd 2D chaotically encrypted clinical EEG signals generated by using the proposed chaotic scrambler and 2D chaotic address permutation method. (r = 0.016)

$\delta_{FX} = \delta_{FY} = 0.1$. The chaotic equation $x_{n+1} = rx_n(1 - x_n)$ is applied to all types of chaotic logistic maps. Figs. 4 and 5 show the 2D chaotically encrypted array and the 2D chaotically encrypted EEG signals, respectively. We discuss the difference between the original and chaotically encrypted EEG signals by using the Pearson correlation coefficient γ, which is given by

$$r = \frac{\sum XY - \frac{\sum X \sum Y}{Z}}{\sqrt{(\sum X^2 - \frac{(\sum X)^2}{Z})(\sum Y^2 - \frac{(\sum Y)^2}{Z})}} \tag{13}$$

Here, X and Y are the amplitudes of the original and encrypted EEG signals, respectively. Z is the total number of sampled EEG signals. The r value of signals A and B is 1, which indicates that these signals A and B are identical and completely correlated. The r value is 0.11 for the original clinical EEG signals and the chaotically encrypted signal (transmission BER of 10^{-7}) generated by using the proposed chaos-based encryption scrambler. Fig. 6 shows the 2D EEG signals that are chaotically encrypted by the proposed encryption scrambler and the 2D chaotic address permutation method. The transmission BER is 10^{-7}. The r value of the original clinical EEG signals and those encrypted using the proposed encryption scheme is 0.0272. In this case, the encrypted clinical EEG signal are unreadable. The percent root-mean-square difference (PRD) is used to evaluate the distortion of the decrypted signals. The PRD value [1] is obtained using the equation

$$PRD = 100 \times \sqrt{\frac{\sum_{i=1}^{L} (X_{ori}(i) - X_{dec}(i))^2}{\sum_{i=1}^{L} X_{ori}^2(i)}} \tag{14}$$

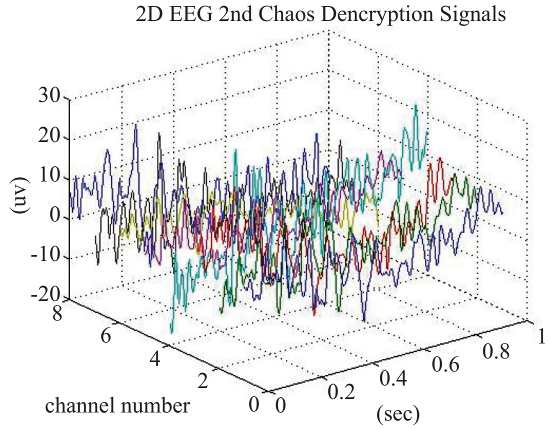

Fig. 7. 2D EEG chaos decrypted signals. (BER = 10^{-7} and PRD = 1.1285%).

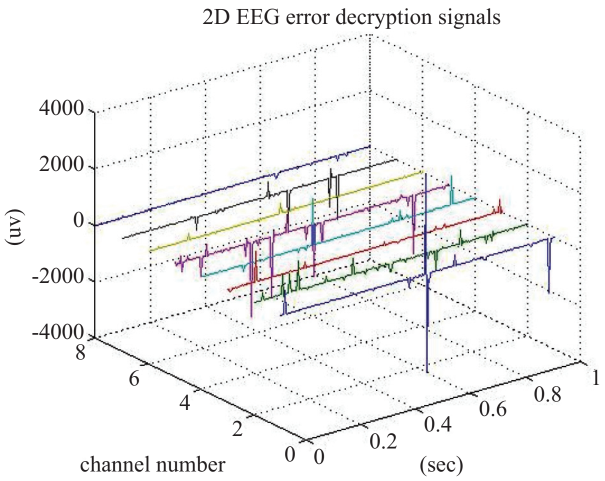

Fig. 8. 2D decrypted EEG signals with error decryption parameter.

where X_{ori} and X_{dec} are the original and decrypted clinical EEG signals, respectively. The correct decrypted clinical EEG signals are shown in Fig. 7. We assume that the received EEG signals with a transmission BER of 10^{-7}. The PRD value of the correct decrypted EEG signals and the original EEG signals is 1.1285%. Fig. 8 shows that the error in the decrypted EEG signals and the decrypted parameter at the starting point is 10^{-6}. From the values shown in Table 1, we can discuss the effect of the transmission BERs in the EEG signals that are encrypted by using the proposed scheme. The *PRD* and *r* values of the correct encrypted signals are the same for BER = 10^{-7} and 10^{-6}. The decrypted EEG signals are distorted when the transmission BER exceeds 10^{-3}. From theses simulation results, we conclude that the proposed chaos-based 2D encryption is a superior scheme that is well suited for application to clinical EEG signals.

VI. CONCLUSION

In this paper, we have developed a high-speed encryption scheme based on the chaos theory for application to clinical EEG signals. Signals mapping of a 2D chaotic scrambler and a permutation scheme are used to obtain clinical EEG information that requires high-level encryption. Simulation results show that when the correct deciphering parameters are inputted, the signals are completely recovered. This 2D encryption scheme can also be applied to mobile telemedicine systems in which the EEG signals have a transmission BER of 10^{-7}. However, signal recovery is not achieved if there is an appreciable error in the input parameters, for example, when the

Table 2. The parameters of the proposed 2D chaos-based visual clinical EEG signals.

F_{CIAX}	chaotic index address assignment process in x coordinate axis
CMT_{FX}	a chaotic logistic map type of F_{CIAX}
SP_{FX}	a initial value of chaotic logistic map CMT_{FX}
x_n	chaotic sequences which was generated by chaotic logistic map type CMT_{FX} and initial value SP_{FX}
n_{FX}	security level parameter discard previous n_{FX} chaotic sequences (x_n) to increase encryption robustness.
δ_{FX}	security level parameter If x_n is larger than δ_{FX}, discard the chaotic point x_n to increase encryption robustness.
G_{CCSX}	chaotic candidate point generation in x coordinate axis
CMT_{GX}	a chaotic logistic map type of G_{CCSX}
SP_{GX}	a initial value of chaotic logistic map CMT_{GX}
G_X	chaotic sequences which was generated by chaotic logistic map type CMT_{GX} and initial value SP_{GX}
F_{CIAY}	chaotic index address assignment process in y coordinate axis
CMT_{FY}	a chaotic logistic map type of F_{CIAY}
SP_{FY}	a initial value of chaotic logistic map CMT_{FY}
y_n	chaotic sequences which was generated by chaotic logistic map type CMT_{FY} and initial value SP_{FY}
n_{FY}	security level parameter discard previous n_{FY} chaotic sequences (y_n) to increase encryption robustness.
δ_{FY}	security level parameter If y_n is larger than δ_{FY}, discard the chaotic point y_n to increase encryption robustness.
G_{CCSY}	chaotic candidate point generation in y coordinate axis
CMT_{GY}	a chaotic logistic map type of G_{CCSY}
SP_{GY}	a initial value of chaotic logistic map CMT_{GY}
G_Y	chaotic sequences which was generated by chaotic logistic map type CMT_{GY} and initial value SP_{GY}
L_F	the number of input clinical EEG samples per channel
N	the number of input parallel clinical EEG channels
CEX	1D chaotically encrypted sequence in the x coordinate axis
CEY	1D chaotically encrypted sequence in the y coordinate axis
$CEXY$	2D chaotically encrypted array
$CEEG1$	1^{st} 2D chaotically encrypted clinical EEG signals
$SGEEGN$	2^{nd} 2D chaotically encrypted clinical EEG signals
γ	Pearson correlation coefficient

initial point error is 0.00000001%. The proposed encryption scheme can be used for the encryption of E-health and M-health biomedical signals.

ACKNOWLEDGMENTS

The authors acknowledge the support of the teacher research project of National Taiwan Ocean University, 99B60201, Center for Marine Bioenvironment and Biotechnology, NSC 93-2218-E-019-024, and the valuable comments of the reviewers.

REFERENCES

1. Alfaouri, M., Daqrouq, K., Abu-Isbeih, I. N., and Khalaf, E. F., "Quality evaluation of reconstructed biological signals," *American Journal of Applied Science*, Vol. 5, No. 1, pp. 187-193 (2009).
2. Andrew, T. P. and Kevin, M. S., "Reconstructing the keystrem from a chaotic encryption scheme," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 48, No. 5, pp. 624-630 (2001).
3. Curiac, D. I., Dranga, O., Dragan, F., and Banias, O., "Chaos-based cryptography: End of the road?" *Proceeding of IEEE The International Conference on Emerging Security Information, Systems, and Technologies*, Spain, pp. 71-76 (2007).
4. Dachselt, F. and Schwarz, W., "Chaos and cryptography," *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications,* Vol. 48, No. 12, pp. 1498-1509 (2001).
5. EEG Database, from http://kdd.ics.uci.edu/database/eeg/eeg.html.
6. Frank, D., Kristina, K., and Wolfgang, S., "Discrete-time chaotic encryption systems-Part III: Cryptographical analysis," *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications*, Vol. 45, No. 9, pp. 983-988 (1998).
7. Jakimoski, G. and Kocarev, L., "Analysis of some recently proposed chaos-based encryption algorithms," *Physics Letters A*, Vol. 291, No. 6, pp. 381-384 (2001).
8. Kocarev, L., "Chaos-based cryptography: A brief overview," *IEEE Circuits and System Magazine*, Vol. 1, No. 3, pp. 6-21 (2001).
9. Li, Y., Liang, L., Su, Z., and Jiang, J., "A new video encryption algorithm for H.264," *IEEE International Conference on Information Communications, and Signal Processing*, Bangkok, Thailand, pp. 1121-1124 (2005).
10. Lin, C. F. and Chang, K. T., "A power assignment mechanism in Ka band OFDM-based multi-satellites mobile telemedicine," *Journal of Medical and Biological Engineering,* Vol. 28, No. 1, pp. 17-22 (2008).
11. Lin, C. F., Chang, W. T., Lee, H. W., and Hung, S. I., "Downlink power control in multi-code CDMA mobile medicine system," *Medical & Biological Engineering & Computing*, Vol. 44, No. 5, pp. 437-444 (2006).
12. Lin, C. F., Chang, W. T., and Li, C. Y., "A chaos-based visual encryption mechanism in JPEG2000 medical images," *Journal of Medical and Biological Engineering*, Vol. 27, No. 3, pp. 144-149 (2007).
13. Lin, C. F., Chen, J. Y., Shiu, R. H., and Chang, S. H., "A Ka band WCDMA-based LEO transport architecture in mobile telemedicine," in: Martinez, L. and Gomez, C. (Eds.), *Telemedicine in the 21st Century*, Nova Science Publishers, Inc, USA, pp. 187-201 (2008).
14. Lin, C. F., Chung, C. H., Chen, Z. L., Song, C. J., and Wang, Z. X., "A chaos-based unequal encryption mechanism in wireless telemedicine with error decryption," *WSEAS Transactions on Systems,* Vol. 7, No. 2, pp. 49-55 (2008).
15. Lin, C. F., Chung, C. H., and Lin, J. H., "A chaos-based visual encryption mechanism for EEG clinical signals," *Medical & Biological Engineering & Computing*, Vol. 47, No. 7, pp. 757-762 (2009).
16. Lin, C. F. and Li, C. Y., "A DS UWB transmission system for wireless telemedicine," *WSEAS Transactions on Systems*, Vol. 7, No. 7, pp. 578-588 (2008).
17. Man, K. P., Wong, K. W., and Man, K. F., "Security enhancement on VoIP using chaotic cryptography," *IEEE Conference on Industrial Electronics*, Paris, France, pp. 3703-3708 (2006).
18. Marco, G., Kristina, K., and Wolfgang, S., "Discrete-time chaotic encryption systems-Part I: Statistical design approach," *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications*, Vol. 44, No. 10, pp. 963-970 (1997).
19. Matthews, R., "On the derivation of a chaotic encryption algorithm," *Cryptologia*, Vol. 8, No. 1, pp. 29-41 (1989).
20. Murali, K., Yu, H., Varadan, V., and Leung, H., "Secure communication using a chaos based signal encryption scheme," *IEEE Transactions on Consumer Electronics*, Vol. 47, No. 4, pp. 709-714 (2001).
21. Naoki, M., Goce, J., Kazuyuki, A., and Ljupco, K., "Chaotic block ciphers: from theory to practical algorithms," *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications*, Vol. 53, No. 6, pp. 1341-1352 (2006).
22. Naor, M. and Shamir, A., "Visual cryptography," *Advances in Cryptography Eurocrypt Conference*, Perugia, Italy, pp. 1-12 (1994).
23. Ou, C. M., "Design of block ciphers by simple chaotic functions," *IEEE Computational Intelligence Magazine*, Vol. 3, No. 2, pp. 54-59 (2009).
24. Pareek, N., Patidar, V., and Sud, K., "Discrete chaotic cryptography using external key," *Physics Letter A*, Vol. 309, No. 1, pp. 75-82 (2003).
25. Ranjan, B. and Saumitr, P., "Novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system," *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications*, Vol. 53, No. 4, pp. 848-857 (2006).
26. Sobhy, M. I. and Shehata, A. E. D., "Secure e-mail and databases using chaotic encryption," *Electronics Letters*, Vol. 36, No. 10, pp. 875-876 (2000).
27. Wheeler, D. D., "Problems with chaotic cryptosystems," *Cryptologia*, Vol. 13, No. 3, pp. 243-250 (1989).
28. Yan, M., Bourbakis, N., and Li, S., "Data, image, video encryption," *IEEE Potentials*, Vol. 23, No. 3, pp. 28-34 (2004).
29. Yang, T., Wu, C. W., and Chua, L. O., "Cryptography based on chaotic systems," *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications*, Vol. 44, No. 5, pp. 268-271 (1997).
30. Yen, J. C. and Guo, J. I., "Efficient hierarchical chaotic image encryption algorithm and its VLSI realisation," *IEE Proceedings Vision, Image, and Signal Processing*, Vol. 147, No. 2, pp. 167-175 (2000).
31. Zhou, H. and Ling, X. T., "Problems with the chaotic inverse system encryption approach," *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications*, Vol. 44, No. 3, pp. 268-271 (1997).