Chapter 8

Implementation of a Multimaps Chaos-Based Encryption Software for EEG Signals

Chin-Feng Lin and Che-Wei Liu

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/67721

Abstract

In the chapter, we adopted a chaos logic map and a quadratic map to develop the chaos-based multi-maps EEG encryption software. The encryption performances of the chaos-based software were studied. The percent root-mean-square difference (PRD) is used to estimate the accuracy of a correctly decrypted EEG signal with respect to the original EEG signal. Pearson correlation coefficient (PCC) is used to estimate the correlation between the original EEG signal and an incorrectly decrypted EEG signal. The seven encryption aspects were testing, the average PRD value of the original and correctly decrypted EEG signals for the chaos-based multi-maps software is 2.59 x 10^{-11}, and the average encryption time is 113.2857 ms. The five error decryption aspects were testing, the average PCC value of the original and error decrypted EEG signals for the chaos-based multi-maps software is 0.0026, and the average error decryption time is 113.4000 ms. These results indicate that the chaos-based multimaps EEG encryption software can be applied to clinical EEG diagnosis.

Keywords: EEG encryption software, multiple chaotic maps, logic map, quadratic map

1. Introduction

Chaos-based encryption is an important research topic in the field of multimedia information communication and storage [1–8]. Compared to the advanced encryption standard (AES), data encryption standard (DES), and the Rivest, Shamir, & Adleman (RSA) algorithm, chaos-based cryptography can exhibit higher levels of security and strong anti-attack ability [7, 8]. The use of chaos-based encryption schemes has expanded steadily over the last few years. Sankpal and Vijaya [9] provided the insights on chaos-based image encryption. Chaotic encryption mechanisms with infinite precision and unpredictability are sensitive to initial conditions and chaotic parameters. Complex chaotic maps have higher levels of security. Chaos-based multimedia encryption can be used in an open access network, and the internet. Zhou et al. [10] proposed a cascade chaotic system using two one-dimension (1-D) chaotic maps in series. The 1-D chaotic maps included logistic, tent, and sine maps. Compared to the use of one 1-D chaotic map, the simulation results showed that the proposed cascade chaotic system had higher robustness and randomness, more unpredictable parameters, and improved chaotic properties and chaotic performance.

Babu and Ilango [11] integrated chaos-based look-up tables using a higher-dimensional Arnold's cat map (ACM) to achieve high encryption sensitivity with respect to the secret key space for audio encryption. The coefficients of the original and encrypted audio signals were employed to evaluate encryption robustness. Mostaghim and Boostani [12] proposed a chaotic visual cryptography (CVC) algorithm to increase steganography in security applications. The key space, key sensitivity, and correlation coefficient of the proposed CVC encryption method were demonstrated. Munir [13] proposed a chaos-based image encryption method using discrete cosine transform (DCT) in the frequency domain. The size of the encrypted image block was 8×8. The ACM was used to permute the encrypted image block and achieve visual image encryption. The 2D Henon chaotic map and skew tent map play a significant role in the design of permutation and diffusion image encryption mechanisms [14]. The Henon chaotic map generates two different chaotic addresses to permute the row and column of encrypted values in the shuffling process. Furthermore, the unimodal skew tent map was used to scramble the pixel values of the encrypted image using exclusive or (XOR) operations in the diffusion process. Liu et al. [15] proposed a pseudorandom bit generator (PRBG) using parameter-varying logistic map. The change mechanism of the parameters was designed, and the proposed PRBG displayed non-stationary behavior. The parameter-varying logistic map disrupted the phase space of the chaotic system, and could overcome phase space reconstruction to withstand attacks.

Awad et al. [16] investigated chaos-based encryption and transformation approaches using fuzzy keyword search for a mobile cloud storage system. The comprehensive tests showed that the proposed technology obtained a significantly more efficient solution to the searchable encryption problem compared to existing solutions. Huang et al. [17] developed an image cryptosystem using permutation architecture with block and stream ciphers. Ricardo and Alejandro [18] modified a 32-bit chaotic Bernoulli map PRBG using an 8-bit microcontroller. The multiplication, accommodation, addition, and shifting operations were integrated. Jolfaei et al. [19] indicated that permutation-only image ciphers have been used to protect multimedia information in recent years. In the permutation-only image encryption algorithm, the multimedia information is scrambled using a permutation mapping matrix generated by a PRBG. In previous studies [20–23], a chaos-based visual encryption mechanism, 2D chaos-based visual encryption scheme, C# based chaotic single map encryption system, and chaotic visual cryptosystem using empirical mode decomposition algorithm for clinical electroencephalogram (EEG) signals have been proposed. In the chapter, chaotic multimaps of one-channel clinical

EEG encryption software were developed to enhance the encryption robustness. The rest of this paper is organized as follows. The encryption algorithm focusing on the encryption software is investigated in Section 2. Section 3 provides implementation and experimental results of chaotic multimaps of visual clinical EEG encryption software. The conclusion and future work are presented in Section 4.

2. Encryption algorithm

The encryption algorithm consists of two main components: chaotic permutation address index approach (CPAIA) and chaotic clinical EEG signal generator approach (CCESGA) for the proposed encryption software. The encryption parameters are inputted to CPAIA, and the chaotic permutation address index sequence is generated. The chaotic permutation address index sequence is integrated to CCESGA, and the chaos-based encryption clinical EEG signal is generated. The proposed CPAIA is shown in **Figure 1**. The CPAIA algorithm proceeds as follows:

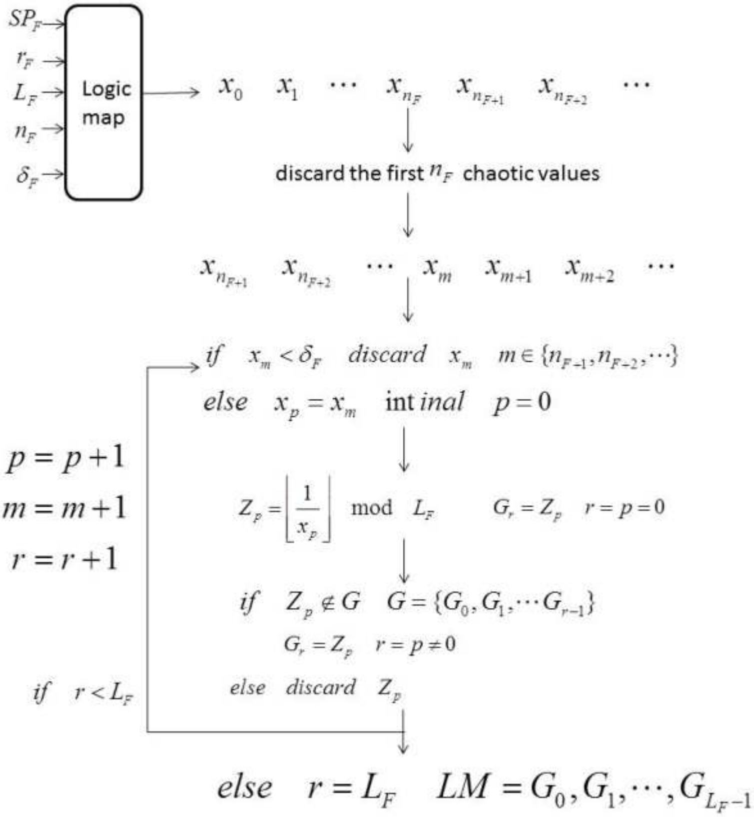

SP_F
r_F
L_F
n_F
δ_F
Logic map
$x_0 \quad x_1 \quad \cdots \quad x_{n_F} \quad x_{n_{F+1}} \quad x_{n_{F+2}} \quad \cdots$
discard the first n_F chaotic values
$x_{n_{F+1}} \quad x_{n_{F+2}} \quad \cdots \quad x_m \quad x_{m+1} \quad x_{m+2} \quad \cdots$
$if \quad x_m < \delta_F \quad discard \quad x_m \quad m \in \{n_{F+1}, n_{F+2}, \cdots\}$
$else \quad x_p = x_m \quad \text{int}\,inal \quad p = 0$
$p = p+1$
$m = m+1$
$r = r+1$
$Z_p = \left\lfloor \frac{1}{x_p} \right\rfloor \bmod L_F \qquad G_r = Z_p \quad r = p = 0$
$if \quad Z_p \notin G \quad G = \{G_0, G_1, \cdots G_{r-1}\}$
$G_r = Z_p \quad r = p \neq 0$
$else \quad discard \quad Z_p$
$if \quad r < L_F$
$else \quad r = L_F \quad LM = G_0, G_1, \cdots, G_{L_F - 1}$

Figure 1. The proposed chaotic permutation address index approach.

Step 1: Input the encryption parameters, $SP_F \quad r_F \quad L_F \quad n_F \quad \delta_F$, into the CPAIA.

SP_F: The initial value of the chaotic logic map.

r_F: The bifurcation parameter of the chaotic logic map.

L_F: The length of encryption clinical EEG signal.

n_F: The level of parameter 1 of security.

δ_F: The level of parameter 2 of security.

The chaotic logic map was adopted in CPAIA, described as following.

$x_{n+1} = r_F x_n(1 - x_n)$……………………………………………………………(1)

$x_o = SP_F$

Step 2: Discard the first n_F chaotic logic map values; the chaotic logic map sequence is $x_{n_F+1} \quad x_{n_F+2} \quad \cdots \quad x_m \quad x_{m+1} \quad \cdots$.

Step 3: If $x_m < \delta_F$, discard x_m, $m \in \{n_{F+1}, n_{F+2}, \cdots\}$

else

$x_p = x_m \quad initinal \quad p = 0$

Step 4:

$$Z_p = \left\lfloor \frac{1}{x_p} \right\rfloor \quad \text{mod} \quad L_F \quad G_r = Z_p \quad r = p = 0 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

Step 5: If $Z_p \notin G \quad G = \{G_0, G_1, \cdots, G_{r-1}\}$

$G_r = Z_p \quad r = p \neq 0$……………………………………………………………(3)

else discard Z_p.

Step 6: If $r = L_F \quad LM = G_0, G_1, \cdots, G_{L_F-1}$

LM is the chaotic permutation address index sequence.

else

m = m + 1;

p = p + 1;

r = r + 1; and go to Step 3.

The proposed CCESGA is shown in **Figure 2**. The CCESGA algorithm proceeds as follows:

Step 1: Input the encryption parameters, $SP_G \quad r_G \quad L_F$, into the CCESGA.

SP_G: The initial value of the chaotic quadratic map.

r_F: The bifurcation parameter of the quadratic logic map.

L_F: The length of encryption clinical EEG signal.

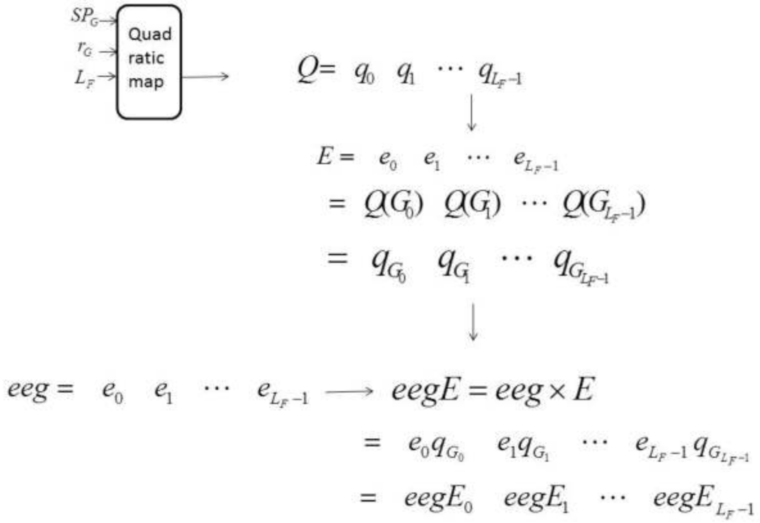

SP_G
r_G
L_F
Quad ratic map
$Q= q_0 \; q_1 \; \cdots \; q_{L_F-1}$
$E= e_0 \; e_1 \; \cdots \; e_{L_F-1}$
$= Q(G_0) \; Q(G_1) \; \cdots \; Q(G_{L_F-1})$
$= q_{G_0} \; q_{G_1} \; \cdots \; q_{G_{L_F-1}}$
$eeg= e_0 \; e_1 \; \cdots \; e_{L_F-1}$
$eegE = eeg \times E$
$= e_0 q_{G_0} \; e_1 q_{G_1} \; \cdots \; e_{L_F-1} q_{G_{L_F-1}}$
$= eegE_0 \; eegE_1 \; \cdots \; eegE_{L_F-1}$

Figure 2. The proposed chaotic clinical EEG signal generator approach.

The chaotic quadratic map was adopted in CCESGA, and described as follows:

$q_{n+1} = 1 - r_G \cdot q_n^2$……………………………………………… …………(4)

$q_o = SP_G$

The generation the chaotic quadratic map sequence was Q,

$Q = q_0 \quad q_1 \quad \cdots \quad q_{L_F-1}$

Step 2: Input the chaotic permutation address index sequence, LM.

Step 3: Generate the chaos-based encryption sequence, E.

$E = e_0 \quad e_1 \quad \cdots \quad e_{L_F-1}$ …………………………… …………(5)

$= Q(G_0) \quad Q(G_1) \quad \cdots \quad Q(G_{L_F-1})$

$= q_{G_0} \quad q_{G_1} \quad \cdots \quad q_{G_{L_F}-1}$

Step 4: Input the clinical EEG signal, eeg.

$eeg = eeg_0 \quad eeg_1 \quad \cdots \quad eeg_{L_F-1}$ ……………………………………………..(6)

Step 5: Generate the chaos-based encryption clinical EEG signal, $eegE$.

$eegE = eeg \times E$…………………………………………………………………....(7)

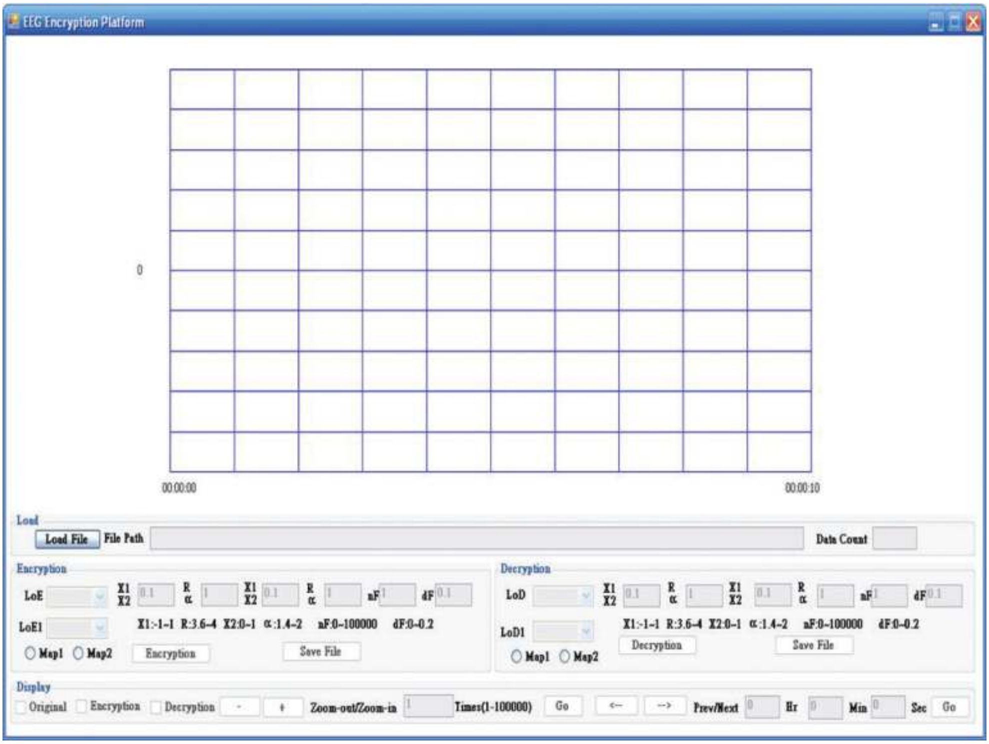
$= e_0 q_{G_0} \quad e_1 q_{G_1} \quad \cdots \quad e_{L_F-1} q_{G_{L_F}-1}$

$= eegE_0 \quad eegE_1 \quad \cdots \quad eegE_{L_F-1}$

3. Chaotic multimaps visual clinical EEG encryption software

Figure 3 shows the developed chaotic multimaps visual clinical EEG signal encryption software. The software was developed using C# language and Microsoft Visual Studio integrated development environment (IDE). The software includes input, encryption, decryption, storage, and display modules. One-channel clinical EEG signals were inputted in the software through an input module, and were encrypted using an encryption module; these encrypted clinical EEG signals were decrypted using a decryption module. Furthermore, the encryptions and decryptions were stored and displayed using storage and display modules, respectively. The ranges of encryption parameters SP_F = $x1$, r_F = R, SP_G = $x2$, r_G = α, n_F, and δ_F are 0-1 real numbers (RNs), 3.6-4 RNs, 0-1 RNs, 1.4-2 RNs, 0-100000 integrate number, and 0-0.2 RNs, respectively. **Figure 4** displays the original one-channel clinical EEG signal, whose length is 10 s, and sample rate is 256 samples/s.

Figure 5 shows the encrypted chaotic multimaps visual one-channel clinical EEG signal. The medical features of the encrypted EEG signal were visually unrecognizable and could not be applied to clinical EEG diagnosis. The encryption parameters $SP_F = x1$, $r_F = R$, $SP_G = x2$, $r_G = \alpha$, n_F, and δ_F are 0.6, 4, 0.6, 1.4, 100, and 0.05, respectively. The robustness of the developed visual chaotic multimaps encryption software was excellent. **Figure 6** shows the correctly decrypted



Encryption: X1 X2 0.1 R α 1 X1 X2 0.1 R α 1 nF 1 dF 0.1

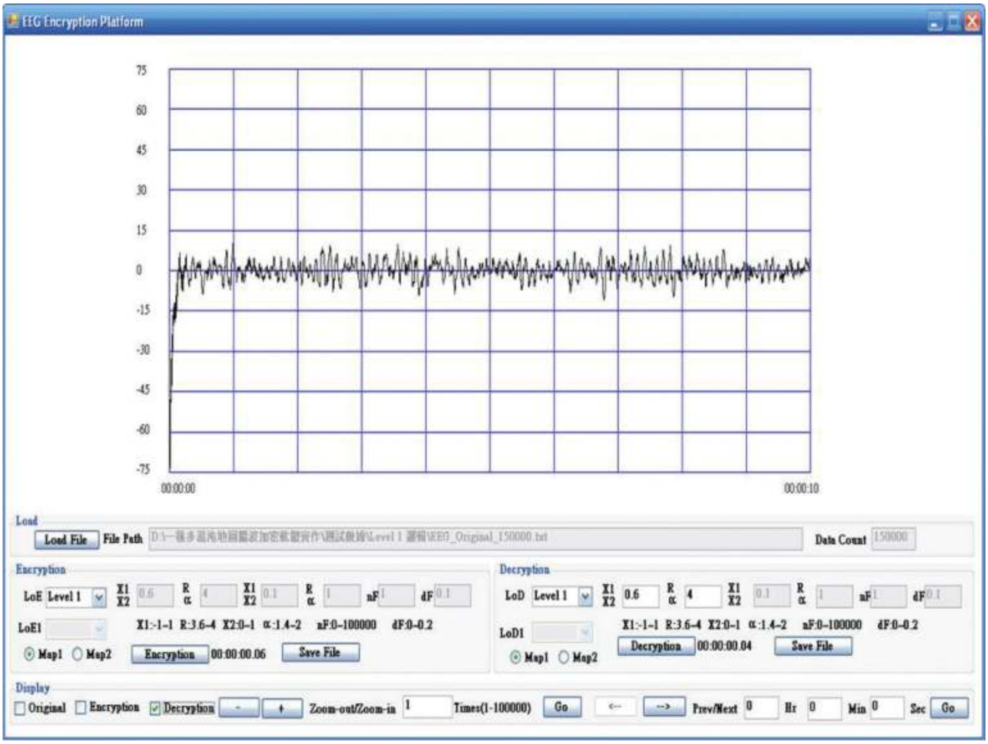
X1:-1-1 R:3.6-4 X2:0-1 α:1.4-2 nF:0-100000 dF:0-0.2

Decryption: X1 X2 0.1 R α 1 X1 X2 0.1 R α 1 nF 1 dF 0.1

X1:-1-1 R:3.6-4 X2:0-1 α:1.4-2 nF:0-100000 dF:0-0.2

Zoom-out/Zoom-in 1 Times(1-100000) Prev/Next 0 Hr 0 Min 0 Sec

Figure 3. The developed chaotic multimaps visual clinical EEG signal encryption software.



EEG Encryption Platform

Load

Load File File Path D:\一種多混沌映射腦波加密軟體實作\測試數據\Level 1 邏輯\EEG_Original_150000.txt Data Count 150000

Encryption

LoE Level 1 X1/X2 0.6 R/α 4 X1/X2 0.1 R/α 1 nF 1 dF 0.1

LoE1

X1:-1-1 R:3.6-4 X2:0-1 α:1.4-2 nF:0-100000 dF:0-0.2

● Map1 ○ Map2 Encryption 00:00:00.06 Save File

Decryption

LoD Level 1 X1/X2 0.6 R/α 4 X1/X2 0.1 R/α 1 nF 1 dF 0.1

LoD1

X1:-1-1 R:3.6-4 X2:0-1 α:1.4-2 nF:0-100000 dF:0-0.2

● Map1 ○ Map2 Decryption 00:00:00.04 Save File

Display

□ Original □ Encryption ☑ Decryption - + Zoom-out/Zoom-in 1 Times(1-100000) Go <-- --> Prev/Next 0 Hr 0 Min 0 Sec Go

Figure 4. The original one-channel clinical EEG signal.

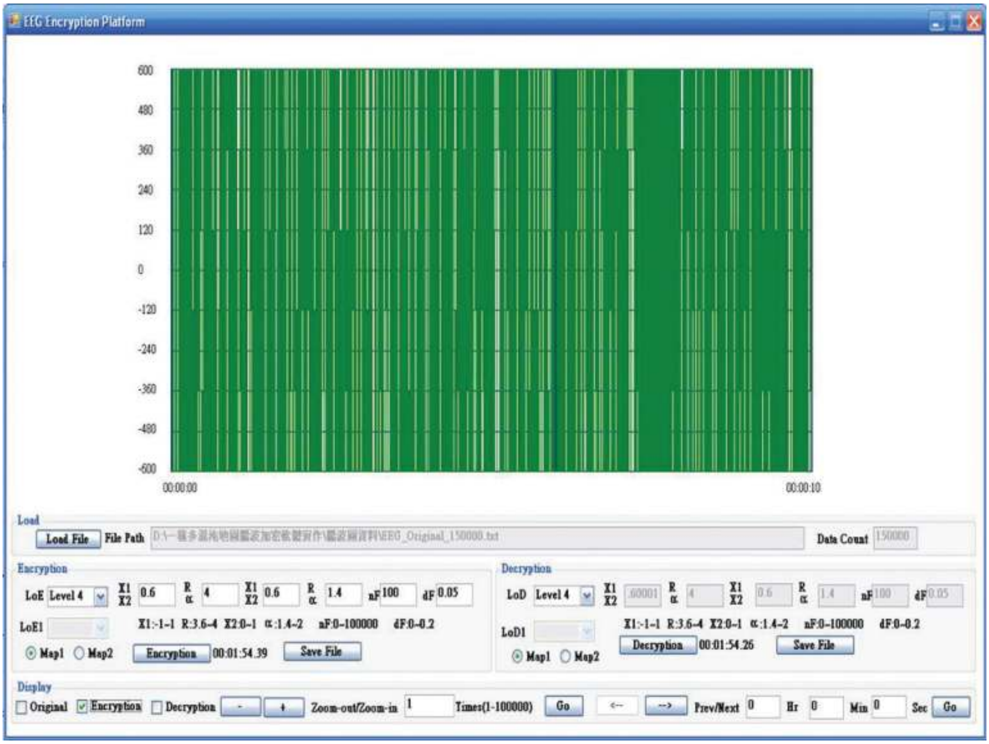
one-channel clinical EEG signal. The percent root difference (PRD) value is adopted to evaluate the difference between the original and correctly decrypted clinical EEG signals and is defined as

$$PRD = 100 \times \sqrt{\frac{\sum_{i=1}^{L_F} (EEG_{ori}(i) - EEG_{dec}(i))^2}{\sum_{i=1}^{L_F} EEG_{ori}^2(i)}} \tag{8}$$

EEG_{ori}: amplitudes of original clinical EEG signal.

EEG_{dec}: amplitudes of decrypted clinical EEG signal.

The parameter L_F is 2560. The PRD value of the original and correctly decrypted clinical EEG signals is 3.87×10^{-11}. **Table 1** lists the encryption parameters, PRD values of correct decryption, and encryption time of the proposed chaotic multimaps visual encryption mechanism for a clinical EEG signal. Seven encryption aspects were tested, and the average PRD value of original and correctly decrypted clinical EEG signal is obtained as 2.59×10^{-11} and with the encryption time as 113.2857 ms. From **Figure 6** and **Table 1**, the accuracy of a correctly decrypted EEG signal was excellent, and the correct decryption speed was acceptable. **Figure 7** shows the decrypted one-channel clinical EEG signal with error decryption parameters; the encryption parameters $SP_F = x1$, $r_F = r$, $SP_G = x2$, $r_G = \alpha$, n_F, and δ_F are 0.6, 4, 0.6, 1.4, 100, and



Load
Load File File Path D:\[illegible]\EEG_Original_150000.txt Data Count 150000

Encryption
LoE Level 4 X1/X2 0.6 R/α 4 X1/X2 0.6 R/α 1.4 nF 100 dF 0.05
LoE1
X1:-1~1 R:3.6~4 X2:0~1 α:1.4~2 nF:0~100000 dF:0~0.2
● Map1 ○ Map2 Encryption 00:01:54.39 Save File

Decryption
LoD Level 4 X1/X2 .60001 R/α 4 X1/X2 0.6 R/α 1.4 nF 100 dF 0.05
LoD1
X1:-1~1 R:3.6~4 X2:0~1 α:1.4~2 nF:0~100000 dF:0~0.2
Decryption 00:01:54.26 Save File
● Map1 ○ Map2

Display
□ Original ☑ Encryption □ Decryption - + Zoom-out/Zoom-in 1 Times(1-100000) Go <-- --> Prev/Next 0 Hr 0 Min 0 Sec Go

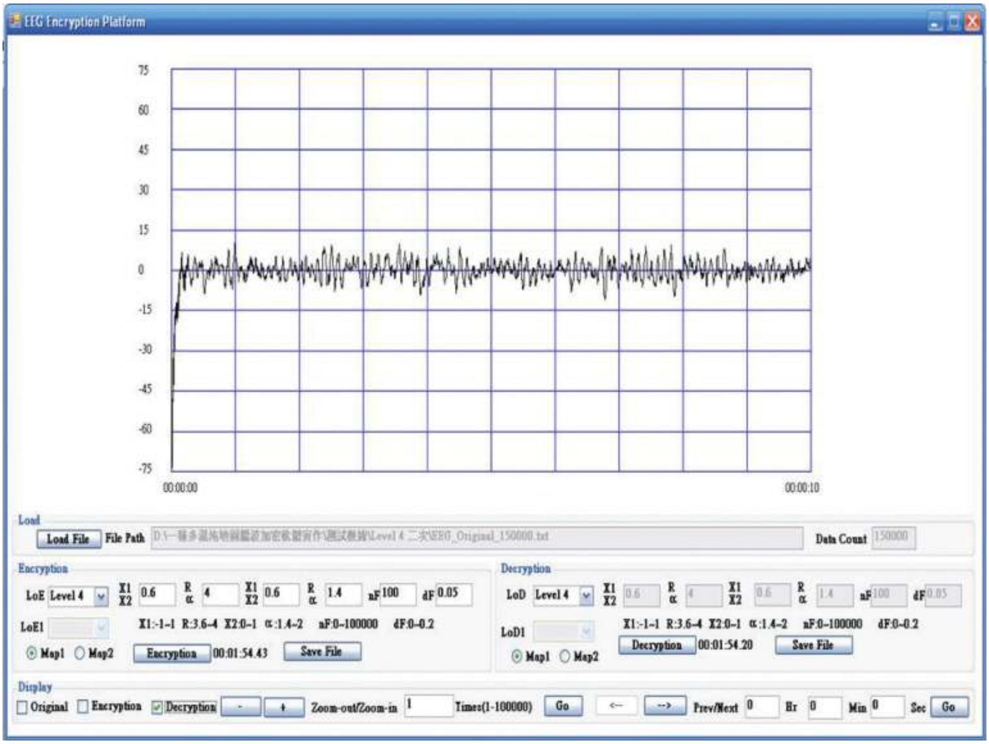
Figure 5. The encrypted chaotic multimaps visual one-channel clinical EEG signal.

0.05, respectively. In addition, the decryption parameters $SP_F = x1$, $r_F = r$, $SP_G = x2$, $r_G = \alpha$, n_F, and δ_F are 0.6, 4, 0.60001, 1.4, 100, and 0.05, respectively. The Pearson correlation coefficient (PCC) was adopted to evaluate the difference between the original and error decryption clinical EEG signals and is defined as

$$r = \frac{\sum_{i=1}^{L_F} EEG_{ori}(i) EEG_{errdec}(i) - \frac{\sum_{i=1}^{L_F} EEG_{ori}(i) \sum_{i=1}^{L_F} EEG_{errdec}(i)}{L_F}}{\sqrt{\left(\sum_{i=1}^{L_F} EEG_{ori}^2(i) - \frac{\left(\sum_{i=1}^{L_F} EEG_{ori}(i) \right)^2}{L_F} \right) \left(\sum_{i=1}^{L_F} EEG_{errdec}^2(i) - \frac{\left(\sum_{i=1}^{L_F} EEG_{errdec}(i) \right)^2}{L_F} \right)}} \quad (9)$$

EEG_{ori}: amplitudes of the original clinical EEG signal.

EEG_{errdec}: amplitudes of error decrypted clinical EEG signal.



File Path D:\一種多混沌映射腦波加密軟體實作\測試數據\Level 4 二次\EEG_Original_150000.txt Data Count 150000

Encryption: LoE Level 4 X1 0.6 R 4 X2 0.6 α 1.4 nF 100 dF 0.05
LoE1
X1:-1~1 R:3.6~4 X2:0~1 α:1.4~2 nF:0~100000 dF:0~0.2
● Map1 ○ Map2 Encryption 00:01:54.43

Decryption: LoD Level 4 X1 0.6 R 4 X2 0.6 α 1.4 nF 100 dF 0.05
LoD1
X1:-1~1 R:3.6~4 X2:0~1 α:1.4~2 nF:0~100000 dF:0~0.2
● Map1 ○ Map2 Decryption 00:01:54.20

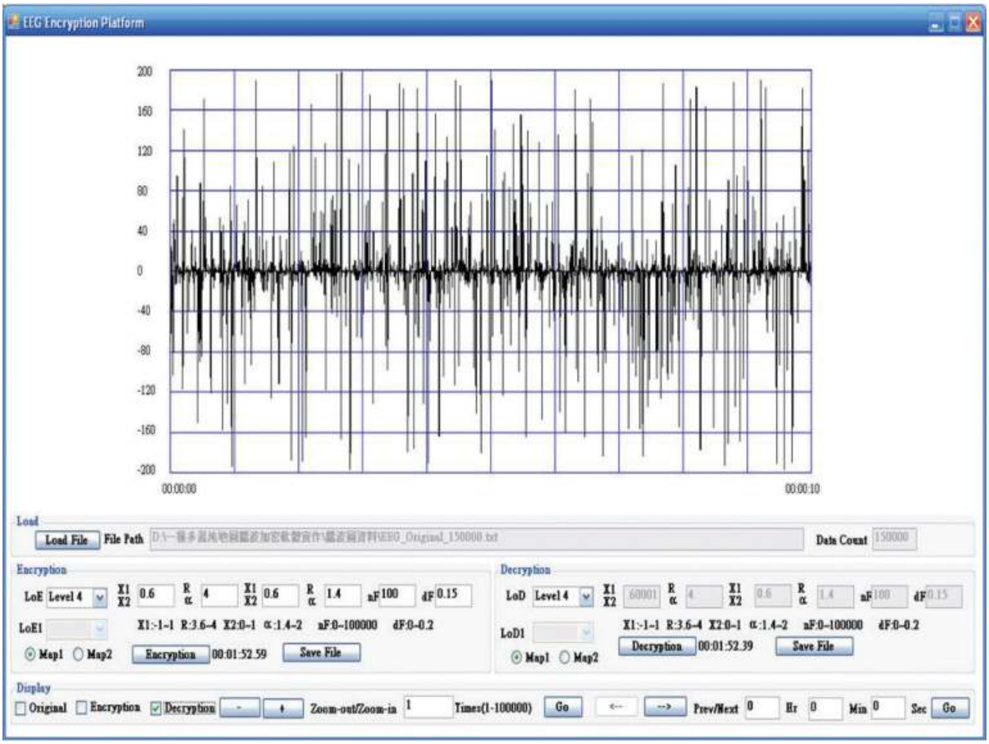
Display: □ Original □ Encryption ☑ Decryption Zoom-out/Zoom-in 1 Times(1-100000) Prev/Next 0 Hr 0 Min 0 Sec

Figure 6. The correctly decrypted one-channel clinical EEG signal.

Encryption						PRD	Encryption time (ms)
x_1	r	x_2	α	n_F	δ_F		
0.6	4	0.6	1.4	100	0.05	3.8734×10^{-11}	113
0.60001	4	0.6	1.4	100	0.05	1.2630×10^{-11}	113
0.6	3.9999	0.6	1.4	100	0.05	1.2362×10^{-11}	115
0.6	4	0.601	1.4	100	0.05	3.3033×10^{-11}	114
0.6	4	0.6	1.399	100	0.05	1.1655×10^{-10}	113
0.6	4	0.6	1.4	200	0.05	3.2141×10^{-11}	113
0.6	4	0.6	1.4	100	0.15	4.0856×10^{-11}	112

Table 1. The encryption parameters, PRD values of correct decryption, and encryption time of the proposed chaotic multimaps visual encryption mechanism for clinical EEG signal.

Table 2 lists the decryption parameters, PCC values of error decryption, and error encryption time of the proposed chaotic multimaps visual encryption mechanism for the clinical EEG signal. For this, five error decryption aspects were tested, the average PCC value of original



File Path D:\一種多混沌地圖腦波加密軟體著作\腦波資料\EEG_Original_150000.txt
Data Count 150000

Encryption
LoE Level 4 X1 X2 0.6 R α 4 X1 X2 0.6 R α 1.4 nF 100 dF 0.15
LoE1
X1:-1~1 R:3.6~4 X2:0~1 α:1.4~2 nF:0~100000 dF:0~0.2
● Map1 ○ Map2 Encryption 00:01:52.59 Save File

Decryption
LoD Level 4 X1 X2 60001 R α 4 X1 X2 0.6 R α 1.4 nF 100 dF 0.15
LoD1
X1:-1~1 R:3.6~4 X2:0~1 α:1.4~2 nF:0~100000 dF:0~0.2
● Map1 ○ Map2 Decryption 00:01:52.39 Save File

Display
□ Original □ Encryption ☑ Decryption - + Zoom-out/Zoom-in 1 Times(1-100000) Go <-- --> Prev/Next 0 Hr 0 Min 0 Sec Go

Figure 7. The decrypted one-channel clinical EEG signal with error decryption parameters.

and error decrypted clinical EEG signal was obtained as 0.0026, and the error decryption time was 113.4000 ms. From **Figure 7** and **Table 2**, the original and error decrypted clinical EEG signal was extremely uncorrelated, and the error decryption time was accepted.

Encryption						**PCC**	**Error decryption time (ms)**
x	r	x_n	α	n_F	δ_F		
0.60001	4	0.6	1.4	100	0.05	0.0020	112
0.6	3.9999	0.6	1.4	100	0.05	0.0061	113
0.6	4	0.601	1.4	100	0.05	0.0020	114
0.6	4	0.6	1.4	200	0.05	0.0015	114
0.6	4	0.6	1.4	100	0.15	0.0015	114

Table 2. The decryption parameters, PCC values of error decryption, and error encryption time of the proposed chaotic multimaps visual encryption mechanism for clinical EEG signal.

4. Conclusion

This chapter described the proposed chaotic multimaps visual encryption mechanism for one-channel clinical EEG signals. Chaotic logic and chaotic quadratic maps were employed in CPAIA and CCESGA, respectively. The proposed software was implemented using C# language and Microsoft Visual Studio IDE. The PRD and PCC values were used to evaluate the accuracy of the correctly decrypted clinical EEG signals and the robustness of error decryption clinical EEG signals, respectively. The testing results showed that the proposed chaotic multimaps visual encryption software is an excellent encryption software. In the future, the chaotic maps with 2-D, i.e., Henon map, can be adopted to enhance the encryption robustness.

Acknowledgements

The authors acknowledge the support of the NTOU Center for Teaching and Learning, Maritime Telemedicine Teaching and Learning Project, the support of the Union Teaching of the Ministry of Education for Medical Electronics in Taiwan, and the valuable comments of the reviewers.

Author details

Chin-Feng Lin* and Che-Wei Liu

*Address all correspondence to: lcf1024@mail.ntou.edu.tw

Department of Electrical Engineering, National Taiwan Ocean University, Taiwan, Republic of China

References

[1] Kotulski Z, Szczepanski J. Discrete chaotic cryptography. Ann. Physik. 1997; 6:381–394. DOI: 10.1002/andp.19975090504.

[2] Yang T, Wu W, Chua LO. Cryptography based on chaotic systems. IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications. 1997; 44:469–472. DOI: 10.1109/81.572346.

[3] Baptista MS. Cryptography with chaos. Physics Letters A. 1998; 240:50–54. DOI: 10.1016/S0375-9601(98)00086-3.

[4] Kocarev L. Chaos-based cryptography: a brief overview. IEEE Circuits and System Magazine. 2001; 1:6–21. DOI: 10.1109/7384.963463.

[5] Dachselt F, Schwarz W. Chaos and cryptography. IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications. 2001; 48:1498–1509. DOI: 10.1109/TCSI.2001.972857.

[6] Jakimoski G, Kocarev L. Chaos and cryptography: block encryption ciphers based on chaotic maps. IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications. 2001; 48:163–169. DOI: 10.1109/81.904880.

[7] Yan M, Bourbakis N, Li S. Data, image, video encryption. IEEE Potentials. 2004; 23:28–34. DOI: 10.1109/MP.2004.1341784.

[8] Ou CM. Design of block ciphers by simple chaotic functions. IEEE Computational Intelligence Magazine. 2009; 3:54–59. DOI: 10.1109/MCI.2008.919074.

[9] Sankpal PR, Vijaya PA. Image encryption using chaotic maps: a survey. Proceeding of 2014 Fifth International Conference on Signals and Image Processing. 2013; 102–107. DOI: 10.1109/ICSIP.2014.80.

[10] Zhou Y, Hua Z, Pun CM, Chen CL. Cascade chaotic system with applications. IEEE Transactions on Cybernetics. 2015; 45(9):2001–2012. DOI: 10.1109/TCYB.2014.2363168.

[11] Babu SG, Ilango P. Higher dimensional chaos for Audio encryption. Proceeding of Computational Intelligence in Cyber Security (CICS). 2013; pp. 52–58. DOI: 10.1109/CICYBS.2013.6597206.

[12] Mostaghim M, Boostani R. CVC: chaotic visual cryptography to enhance steganography. Proceeding of Information Security and Cryptology. 2014; pp. 44–48. DOI: 10.1109/ISCISC.2014.6994020.

[13] Munir R. A block-based image encryption algorithm in frequency domain using chaotic permutation. Proceeding of Telecommunication Systems Services and Applications. 2014; DOI: 10.1109/TSSA.2014.7065906.

[14] Khan J, Ahmad J, Hwang SO. An efficient image encryption scheme based on: Henon map, skew tent map and S-Box. Proceeding of Modeling, Simulation, and Applied Optimization. 2015; DOI: 10.1109/ICMSAO.2015.7152261.

[15] Liu L, Miao S, Hu H, Deng Y. Pseudorandom bit generator based on non-stationary logistic maps. IET Information Security. 2016; 10(2):87–94. DOI: 10.1049/iet-ifs.2014.0192.

[16] Awad A, Matthews A, Qiao Y, Lee B. Chaotic searchable encryption for mobile cloud storage. IEEE Transactions on Cloud Computing. IEEE Early Access Articles. pp. 1–14. DOI: 10.1109/TCC.2015.2511747.

[17] Huang C, Cheng H, Song Y, Ding Q. Permutation of image encryption system based on block cipher and stream cipher encryption algorithm. Proceeding of Third International Conference on Robot, Vision and Signal Processing. 2015; pp. 163–166. DOI: 10.1109/RVSP.2015.46.

[18] Ricardo FM, Alejandro DM. Algorithm for implementing 32-bits represented Bernoulli map using an 8-bits microcontroller. Proceeding of International Engineering Summit. 2016. DOI: 10.1109/IESummit.2016.7459773.

[19] Jolfaei A, Wu XW, Muthukkumarasamy V. On the security of permutation-only image encryption schemes. IEEE Transactions on Information Forensics and Security. 2016; 11 (2):235–246. DOI: 10.1109/TIFS.2015.2489178.

[20] Lin CF, Chung CH, Lin JH. A chaos-based visual encryption mechanism for clinical EEG signals. Medical & Biological Engineering & Computing. 2009; 47(7):757–762. DOI: 10.1007/s11517-009-0458-8.

[21] Lin CF, Wang BSH. A 2D chaos-based visual encryption scheme for clinical EEG signals. Journal of Marine Science and Technology. 2011; 19(6):666–672. DOI: 10.6119/JMST.

[22] Lin CF, Shih SH, Zhu JD. Chaos based encryption system for encrypting electroencephalogram signals. Journal of Medical Systems. 2014; 38:49. DOI: 10.1007/s10916-014-0049-6.

[23] Lin CF. Chaotic visual cryptosystem using empirical mode decomposition algorithm for clinical EEG signals. Journal of Medical Systems. 2016; 40:52. DOI: 10.1007/s10916-015-0414-0.