We are IntechOpen, the world’s leading publisher of Open Access books
Built by scientists, for scientists

3,900 Open access books available
116,000 International authors and editors
120M Downloads

154 Countries delivered to
TOP 1% Most cited scientists
12.2% Contributors from top 500 universities

WEB OF SCIENCE™
Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com
Implementation of a Multimaps Chaos-Based Encryption Software for EEG Signals

Chin-Feng Lin and Che-Wei Liu

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 $2.59 \times 10^{-11}$, 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:

![Figure 1. The proposed chaotic permutation address index approach.](http://dx.doi.org/10.5772/67721)
Step 1: Input the encryption parameters, $SP_F$, $r_F$, $L_F$, $n_F$, $\delta_F$, 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.

$\delta_F$: The level of parameter 2 of security.

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

$$ x_{n+1} = r_F x_n (1 - x_n) $$  \hspace{1cm} \text{(1)}

$x_o = SP_F$

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

Step 3: If $x_m < \delta_F$, discard $x_m$, $m \in \{n_F + 1, n_F + 2, \ldots\}$

else

$$ x_p = x_m \quad \text{initial} \quad p = 0 $$

Step 4:

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

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

$$ G_r = Z_p \quad r = p \neq 0 \quad \text{..................................................................................................} \text{(3)}$$

else discard $Z_p$.

Step 6: If $r = L_F$

$$ L_M = G_0, G_1, \ldots, G_{L_f - 1}$$

$LM$ is the chaotic permutation address index sequence.

else

$$ m = m + 1; \quad p = p + 1; \quad r = r + 1; \text{ and go to Step 3.}$$

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

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

$SP_G$: The initial value of the chaotic quadratic map.

$r_G$: The bifurcation parameter of the quadratic logic map.

$L_F$: The length of encryption clinical EEG signal.
The chaotic quadratic map was adopted in CCESGA, and described as follows:

\[ q_{n+1} = \frac{1}{C_0} r G_{Q(n)} \]

\[ q_0 = S P_G \]

The generation the chaotic quadratic map sequence was \( Q \),

\[ Q = q_0 \quad q_1 \quad \cdots \quad q_{L_F} \]

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

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

\[ E = e_0 \quad e_1 \quad \cdots \quad e_{L_F} \]

\[ E = Q(G_0) \quad Q(G_1) \quad \cdots \quad Q(G_{L_F}) \]

\[ E = q_{G_0} \quad q_{G_1} \quad \cdots \quad q_{G_{L_F}} \]

Step 4: Input the clinical EEG signal, \( eeg \).

\[ eeg = eeg_0 \quad eeg_1 \quad \cdots \quad eeg_{L_F} \]

Step 5: Generate the chaos-based encryption clinical EEG signal, \( eegE \).

\[ eegE = eeg \times E \]

\[ eegE = eeg_0 \quad eeg_1 \quad \cdots \quad eeg_{L_F} \]

Figure 2. The proposed chaotic clinical EEG signal generator approach.
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 $SP_F = x_1$, $r_F = R$, $SP_G = x_2$, $r_G = \alpha$, $n_F$, and $\delta_F$ 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 $SP_F = x_1$, $r_F = R$, $SP_G = x_2$, $r_G = \alpha$, $n_F$, and $\delta_F$ 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...
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

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

$EEG_{ori}$: 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 $3.87 \times 10^{-11}$. 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 $2.59 \times 10^{-11}$ 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 $SP_F = x_1$, $r_F = r$, $SP_C = x_2$, $r_C = \alpha$, $n_F$, and $\delta_F$ are 0.6, 4, 0.6, 1.4, 100, and
In addition, the decryption parameters $SP_F = x_1$, $r_F = r$, $SP_G = x_2$, $r_G = \alpha$, $n_F$, and $\delta_F$ 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

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

(9)

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

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

Figure 5. The encrypted chaotic multimaps visual one-channel 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

<table>
<thead>
<tr>
<th>Encryption</th>
<th>PRD</th>
<th>Encryption time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>$r$</td>
<td>$x_2$</td>
</tr>
<tr>
<td>0.6</td>
<td>4</td>
<td>0.6</td>
</tr>
<tr>
<td>0.60001</td>
<td>4</td>
<td>0.6</td>
</tr>
<tr>
<td>0.6</td>
<td>3.9999</td>
<td>0.6</td>
</tr>
<tr>
<td>0.6</td>
<td>4</td>
<td>0.601</td>
</tr>
<tr>
<td>0.6</td>
<td>4</td>
<td>0.6</td>
</tr>
<tr>
<td>0.6</td>
<td>4</td>
<td>0.6</td>
</tr>
<tr>
<td>0.6</td>
<td>4</td>
<td>0.6</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Encryption</th>
<th>PCC</th>
<th>Error decryption time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>r</td>
<td>xα</td>
</tr>
<tr>
<td>0.60001</td>
<td>4</td>
<td>0.6</td>
</tr>
<tr>
<td>0.6</td>
<td>3.9999</td>
<td>0.6</td>
</tr>
<tr>
<td>0.6</td>
<td>4</td>
<td>0.601</td>
</tr>
<tr>
<td>0.6</td>
<td>4</td>
<td>0.6</td>
</tr>
<tr>
<td>0.6</td>
<td>4</td>
<td>0.6</td>
</tr>
</tbody>
</table>

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


