A Fast Chaos-based Visual Encryption Mechanism for Integrated ECG/EEG Medical Signals with Transmission Error

Chin-Feng Lin and Cheng-Hsing Chung
Department of Electrical Engineering
National Taiwan Ocean University
No.2 Beึงing Road, Keelung
Taiwan

invited paper by Prof. Nikos Mastorakis and Dr. T. Mihail

Abstract: - In this paper, we have developed a chaos-based visual encryption mechanism that can be applied for the integrated electrocardiogram (ECG)/electroencephalography (EEG) medical signals. The main reason for using chaos sequences is to increase the unpredictability as compared to other types of random sequences. Thus, we used a 1D chaotic scrambler and a permutation scheme to achieve integrated ECG/EEG visual encryption. One way for realizing the visual encryption mechanism is to scramble the signal values of the input integrated ECG/EEG signal by multiplying a 1D chaotic signal to randomize the ECG/EEG signal values, and then a chaotic address scanning order encryption is applied to the randomize reference values. Simulation results show that when the correct deciphering parameters are entered, the signal will be completely recovered, and the percent root-mean-square difference (PRD) values for ECG and EEG medical signals with channel transmission bit error rate (BER) $10^{-7}$ are $4.69 \times 10^{-15} \, \%$ and $4.33 \times 10^{-15} \, \%$, respectively.

Key-Words: - chaos, visual encryption, integrated ECG/EEG medical signals, fast, transmission error, percent root-mean-square difference values.

1 Introduction

The application of chaos theory in the field of cryptography was first discussed by Wheeler and Matthews [1–2]. In Dachselt et al. [3], the authors presented their opinions and described the research performed by them during 1990–2000 on the relation between chaos and cryptography. Kocarev et al. [4] discussed some issues concerning the application of chaos theory in the field of cryptography, and they inspired the design concept of chaos-based encryption. Yang et al. [5] summarized the similarities and differences between block-encryption algorithms (private-key algorithms), pseudo-random number stream ciphers, and chaos-based stream ciphers. Block-encryption algorithms include the data encryption standard (DES), Rivest, Shamir, Adleman (RSA), and advanced encryption standard (AES) algorithms. Chaos has potential applications in encryption. This is because the main motive for using chaos sequences is to increase the unpredictability as compared to other types of random sequences. In addition, chaos-based encryption algorithms have certain properties: sensitivity to changes in the initial conditions and parameters, random-like behavior and unstable periodic orbits with long periods. A robust encryption mechanism can be developed by using a large set of parameters.

The visual image encryption concept was proposed in 1994 by Naor et al. [6]. Its main principle is to use the susceptibility of human vision to encrypt the images in such a manner that privacy or confidentiality is maintained; such techniques make it impossible for people to clearly see the primitive image. Visual image encryption can be implemented by (i) pixel address (position) permutation, (ii) transformation of pixel values and, (iii) a combination of pixel address (position) permutation and transformation of pixel values. Friedrich [7] initially applied chaos theory to arrange the pixel addresses (positions) in order to make the images indistinguishable to human vision. Yen et al. [8] also utilized chaos to produce a binary digit array, thereby achieving a conversion of pixel values. However, Li et al. [9] proposed a chaos-derived binary digit decryption sequence that enables a brute-force search in order to decipher a sequence. A new video streams encryption algorithm for H.264 that uses a chaos pseudo sequence has been discussed in Li et al. [10]. However, they did not consider the use of a chaos-based encryption mechanism in
medical signals. The performance of 2D and 1D chaos-based visual encryption mechanisms that uses JPEG2000 X-ray medical images and electrocardiogram (ECG) medical signals, has been extensively studied in our earlier work [11]-[15]. In this paper, we extend our previous research [11] by considering the employment of 1D chaos-based visual encryption mechanisms in integrated ECG/electroencephalography (EEG) medical signals with transmission error. We realize integrated ECG/EEG visual encryption based on values resulting from the mapping of a 1D chaotic scrambler and a permutation scheme. One way to realize this type of visual encryption mechanism is to scramble the values of the input integrated ECG/EEG medical signals by multiplying the 1D chaotic signal to randomize integrated integrated ECG/EEG medical signal values, and then a chaotic address scanning order encryption is applied to the randomize the reference values. Simulation results show that when the correct deciphering parameters are entered, the signal can be completely recovered, and the percent root-mean-square difference (PRD) values are $15.10^{-69}\%$ and $4.3310^{-4.33}\%$ for ECG and EEG medical signals with channel transmission bit error rate (BER) $10^{-7}$, respectively.

2 A Fast 1D Chaos-based Integrated ECG/EEG Medical Signal Scrambler

We use an unpredictable chaos sequence against a chaos map of relatively sensitive initial values when designing the 1D chaotic integrated ECG/EEG medical signal scrambler. Since the front sequence of a chaos sequence is more predictable, we delete the preceding $n_F$ chaos sequences in order to improve the encryption strength, further we delete the chaos sequence value greater than $\delta_F$ in the chaos sequence to increase the unpredictability of the chaos sequence. The 1D chaotic integrated ECG/EEG medical signal scrambler developed by us is as shown in Figure 1. First, the chaotic index address assignment process $F_{CIA}$ is performed, followed by the chaotic candidate point generator process $G_{CCS}$; this results in the generation of a chaos encrypted ECG/EEG medical signal. The encryption process shown in Figure 2 is given as follows:

Step 1: selected a chaotic logistic map type $CMT_F$ of $F_{CIA}$, the starting point $SP_F$ of $CMT_F$, the length $L_F$ for an encrypted ECG/EEG medical signal, the parameters $n_F$ and, $\delta_F$ for the security level.

Step 2: generated a chaotic sequence with length $n_F$.

\[ x_{n+1} = CMT(x_n) \]

\[ x_0 = SP_F \]
\( n = \{1, 2, \ldots, n_F\} \)

Step 3: discard previous \( n_F \) chaotic sequence.

Step 4: generate a chaotic sequence

\[
x_n = CMT(x_{n+1})
\]

\[
n = \{n_F + 1, \ldots\}
\]

Step 5: if \( x_n > \delta_F \)
discard \( x_n \) and go to step 4.
else go to step 6. end.

Step 6:

\[
m_k = \left[ \frac{1}{x_n} \right]
\]

if \( m_k \not\in \{m_1, \ldots, m_{k-1}\} \)
\[
M = \{m_1, \ldots, m_{k-1}, m_k\} \text{ go to step 7.}
\]
else go to step 4. end

Step 7: if \( k = L_F \)
\[
M = \{m_1, m_2, \ldots, m_{L_F}\}
\]
\[
m^*_C = \max\{m_1, m_2, \ldots, m_{L_F}\}
\]
else go to step 4. end

Step 8: deliver \( m^*_C \) to the chaotic candidate point generator process \( G_{CCS} \).

Step 9: deliver a chaotic logistic map type \( CMT_G \) of \( G_{CCS} \), the starting point \( SP_G \) of \( CMT_G \).

Step 10: generated a chaotic sequence with length \( m^*_C \).

\[
g_{n+1} = CMT_G(g_n)
\]

\[
g_0 = SP_G, \quad n = \{1, 2, \ldots, m^*_C\}
\]

\[
G = \{g_1, \ldots, g_{m^*_C}\}
\]

Step 11: deliver \( M \) to the chaotic candidate point generator process \( G_{CCS} \).

Step 12: generate encrypted chaotic signal \( CE \).

\[
M = \{m_1, m_2, \ldots, m_{L_F}\}
\]

\[
G = \{g_1, \ldots, g_{m^*_C}\}
\]

\[
CE = \{g_{m^*_C}, \ldots, g_{m_{L_F}}\}
\]

Step 13: deliver ECG/EEG medical signal \( EECGS \) with length \( L_F \) to \( G_{CCS} \).

\[
EECGS = \{eeeg_1, \ldots, eeg_{L_F}\}
\]

Step 14: deliver encrypted chaotic signal \( CE \) to \( G_{CCS} \).

Step 15: generate encrypted EECG medical signal \( GEECG \).

\[
EECGS = \{eeeg_1, \ldots, eeg_{L_F}\}
\]

Figure 2 Process of the 1D chaotic ECG/EEG medical signal scrambler.

\[
CE = \{g_{m^*_C}, g_{m_{L_F}}, \ldots, g_{m_{L_F}}\}
\]

\[
GEECG = EECGS \cdot CE = \{eeeg_1, \cdot g_{m^*_C}, \cdot eeg_{L_F}, \cdot g_{m_{L_F}}\}
\]

\[
= \{\text{geeg}, \ldots, \text{geeg}_{L_F}\}
\]

3 A Chaotic Scanning Encryption Mechanism

We further increase the encryption strength in further via scanning strategy. With regard to the encrypted ECG/EEG medical signal \( GEECG \) generated in section II, we perform address rearrangement. The chaotic scanning encryption mechanism \( S_{csem} \) developed by us, shown in Figure 3, is given as follows:

Step 1 to 5 are the same as those in section II.

Step 6: \( m_k = \left[ \frac{1}{x_n} \right] \)

if \( m_k \leq L_F \)
\[
m_k \not\in \{m_1, \ldots, m_{k-1}\} \quad M = \{m_1, \ldots, m_{k-1}, m_k\}
\]
go to step 7. else go to step 4. end

Step 7: if \( k = L_F \)
\[
M = \{m_1, m_2, \ldots, m_{L_F}\}
\]
else go to step 4. end
Step 8: deliver $M$ to the output encrypted signal process.

Step 9: deliver encrypted ECG/EEG medical signal $GEECG$ to output encrypted signal process.

Step 10: generate chaotic scanning encrypted ECG/EEG medical signal $SGEEG$.

$$GEECG = \{geecg_1, ..., geecg_{L_F}\}$$

$$M = \{m_1, m_2, ..., m_{L_F}\}$$

$$SGEECG = \{sgeecg_1, sgeecg_2, ..., sgeecg_{L_F}\}$$

4 Simulation Results

We use a simulation method to discuss the application of a chaos-based visual encryption mechanism to ECG/EEG medical signals. The 360 samples/sec ECG signal and 256 samples/sec EEG signal are up-sampled to perform a 720 samples/sec integrated ECG/EEG signal as shown in Fig. 4. Then a encrypted ECG/EEG medical signal is shown in Figure 5. A two-layer highest security chaotic visual encryption mechanism is applied to the ECG/EEG medical signal. This two-layer security protection mechanism includes (1) 1D chaotic random values scrambler and (2) chaotic ECG/EEG signal address scanning order encryption. Our development security parameters include a chaotic logistic map type $CMT_F$ of $F_{CIA}$, the starting point $SP_F$ of $CMT_F$, the length $L_F$ for an encrypted ECG/EEG medical signal, the parameters $n_F$, $\delta_F$ for security level of $F_{CIA}$, a chaotic logistic map type $CMT_G$ of $G_{CCS}$, the starting point $SP_G$ of $CMT_G$, a chaotic logistic map type $CMT_S$ of $S_{csem}$, the starting point $SP_S$ of $CMT_S$, and the parameters $n_S$, $\delta_S$ for the security level of $S_{csem}$. The greater the value of parameters $n_F$, the greater is the number of chaos sequences deleted, and the harder is the prediction of the chaos encrypted sequence generated. The smaller the value of parameters $\delta_F$, the more the chaos sequence deleted, the greater is the number of chaos sequences deleted, and the harder is the prediction of the chaos encrypted sequence generated. We could achieve different levels of encryption by varying the parameters $n_F$ and $\delta_F$. The design parameters and performance verification are described as follows.

$$CMT_F = CMT_G = CMT_S = r\times(1 - x), \quad r = 4 \quad 0 < x < 1$$

$$SP_F = SP_G = SP_S = 0.1$$

The percent root-mean-square difference (PRD) parameter and the Pearson correlation coefficient are used to discuss the distortion of decrypted signals and robustness of encrypted signals. The PRD value is defined as

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

where $X_{ori}$ is the original ECG or EEG medical signal and $X_{dec}$ is the decrypted ECG or EEG medial signal. The Pearson correlation coefficient is given by

$$r = \frac{\sum_{i=1}^{N}XY - \sum_{i=1}^{N}X\sum_{i=1}^{N}Y}{\sqrt{(\sum_{i=1}^{N}X^2 - (\sum_{i=1}^{N}X)^2/N)(\sum_{i=1}^{N}Y^2 - (\sum_{i=1}^{N}Y)^2/N)}}$$

where X and Y are the intensities of values in the original ECG/EEG signal and encrypted ECG/EEG signals, respectively. N is the total number of values.
Figure 4 The original integrated ECG/EEG medical signals.

Figure 5 The encrypted ECG/EEG medical signals.

Figure 6 When correct deciphering parameters are put in, the ECG signal with transmission BER $10^{-7}$ will be completely recovered, and the PRD value is $15.43 \times 10^{-6}$%.

Figure 7 When correct deciphering parameters are put in, the EEG signal with transmission BER $10^{-7}$ will be completely recovered, and the PRD value is $4.33 \times 10^{-15}$%.
in the EEG signal. Figure 5 shows the ECG/EEG medical signal obtained by multiplying a 1D chaotic signal to randomize the ECG/EEG signal values and a chaotic address scanning order encryption in the encrypted a chaotic address scanning order encryption in the encrypted medical signal. The Pearson correlation coefficient is \( r = 0.03 \), which corresponds to a low correlation (\( r = 0 \) represents the case where the images are completely uncorrelated). The encrypted a chaotic address scanning order encryption in the encrypted medical signal is unreadable and there is some loss of medical information. Figure 6 and Figure 7 shows that when correct deciphering parameters are used, the ECG and EEG signal with transmission BER \( 10^{-7} \) will be completely recovered, and the PRD value are \( 4.69 \times 10^{-15}% \) and \( 4.33 \times 10^{-15}% \), respectively. From these figures, we observe that the chaos-based visual encryption mechanism is superior with regard to applications to ECG and EEG medical signals.

5 Conclusion

Considering the popularity of E-hospitals and M-hospitals, it is necessary to encrypt EEG medical signals. In this paper, we develop a chaos-based visual encryption mechanism for applications to ECG/EEG medical signals. This chaos-based visual encryption mechanism includes two-layer security protection, namely, (1) a 1D chaotic random value scrambler and (2) chaotic ECG/EEG signal address scanning order encryption. Simulation results show that the ECG/EEG medical signal visual encryption mechanism is very superior and, it can lead to the EEG and ECG medical signal will be unreadable and loss medical information. The detailed discussion will be presented in 12th WSEAS Int. conf. on systems as well as extended paper.

Reference