

Implementation of An Offline Chaos-based EEG Encryption Software

Chin-Feng Lin*, Shun-Han Shih*, Jin-De Zhu*, Sang-Hung Lee*

*Department of Electrical Engineering, National Taiwan Ocean University, Taiwan

lcf1024@mail.ntou.edu.tw

Abstract— In the paper, we use Microsoft visual studio development kit and C# programming to implement a chaos-based electroencephalogram (EEG) encryption software. A chaos logic map, and initial value of the chaos logic map are used to generate level I chaos-based EEG encryption bit streams. A chaos logic map, initial value, a bifurcation parameter of the chaos logic map, and two encryption level parameters are used to generate level II chaos-based EEG encryption bit streams. A chaos logic map, initial value, a bifurcation parameter of the chaos logic map, two encryption level parameters, and a permutation scheme are used to implement level III chaos-based EEG encryption software. 16 channel EEG Vue signals are tested using the encryption software. The encryption speed is the lowest, and most robust for the level III chaos-based EEG encryption software. Testing results show that the encryption effect is superior, and when a correct deciphering parameter is put in, the EEG signals will be completely recovered. However, if there is an input parameter error with, for example, a 0.00001% initial point error, it will lead to chaotic encryption bit streams and the 16 channel EEG signals will not be recovered.

Keywords— chaos, encryption, software, 16-channel EEG Vue signals, Microsoft visual studio development kit, C# programming.

I. INTRODUCTION

A chaos-based encryption mechanism is an interesting research topic [1-5]. This encryption method is suitable for encrypting audio, images, video, and clinical EEG signals with large block files. Unlike block encryption algorithms, such as the data encryption standard (DES) algorithm, Rivest, Shamir, and Adleman (RSA) algorithm, and the advanced encryption standard (AES) algorithm, a chaos sequence is continuous and sensitive to the starting point and type of chaotic logistic map; different starting points and chaotic logistic maps generate different chaotic sequences for encryption. In our previous studies [6-11], we discuss several chaos-based encryption mechanisms for application in mobile telemedicine, JPEG 2000 medical images, and EEG clinical signals. For this study, we use the Microsoft visual studio development kit and C# programming to implement offline chaos-based electroencephalogram (EEG) encryption software. The proposed software can be installed on personal computers with Window environment by click chaosencryption2 file as shown in Fig.1. The software implementation principle will

be presented in the conference. In the second section, we discuss the application of the software, the 16-channel EEG signals, and the performance of the offline chaos-based encryption. A brief conclusion is provided in the third section.

II. APPLICATION METHODS OF THE SOFTWARE AND THE TESTING ON ITS PERFORMANCE

Figure 2 shows a working window of the offline chaos-based EEG encryption software. Figure 3 shows the 16-channel EEG signals prior to encryption, which was observed using EEG Vue software for enabling medical observation of brainwaves developed by the Nicolet Company. This encryption software can be applied using the following steps.

- Step 1: Load the 16-channel EEG signals to the chaos-based encryption and decryption software “chaosencryption2” for testing.
- Step 2: Specify and save the path and file name of the encrypted file.
- Step 3: Select the encryption level and establish the encryption parameters r_1 , r_2 , x_1 , x_2 , nf , and df . The encryption parameters can be filled with real numbers within the following ranges:
 r_1 , r_2 : 3.6 to 4.0.
 x_1 , x_2 , df : 0 to 1.0
 nf : 10,000 to 10,000,000 The correct encryption parameters for this experiment are listed in the following:
Level of encryption: Level 3
 $r_1=3.965$;
 $x_1=0.321$;
 $r_2=3.811$;
 $x_2=0.124$;
 $nf=10000$;
 $df=0.2$
- Step 4: Click the ENC button to start encrypting; the encryption time is 127 s.
- Step 5: Use EEG Vue software to observe the encrypted 16-channel brainwave, as shown in Fig. 4.

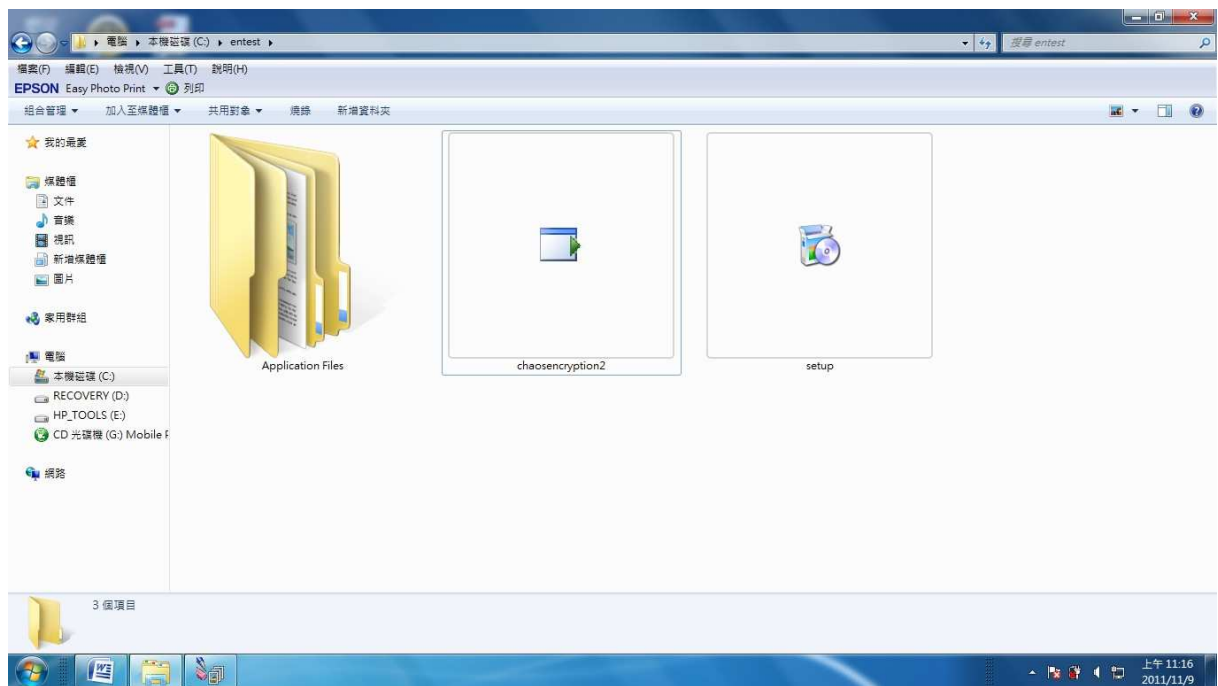


Fig.1 The proposed an offline chaos-based EEG encryption software.

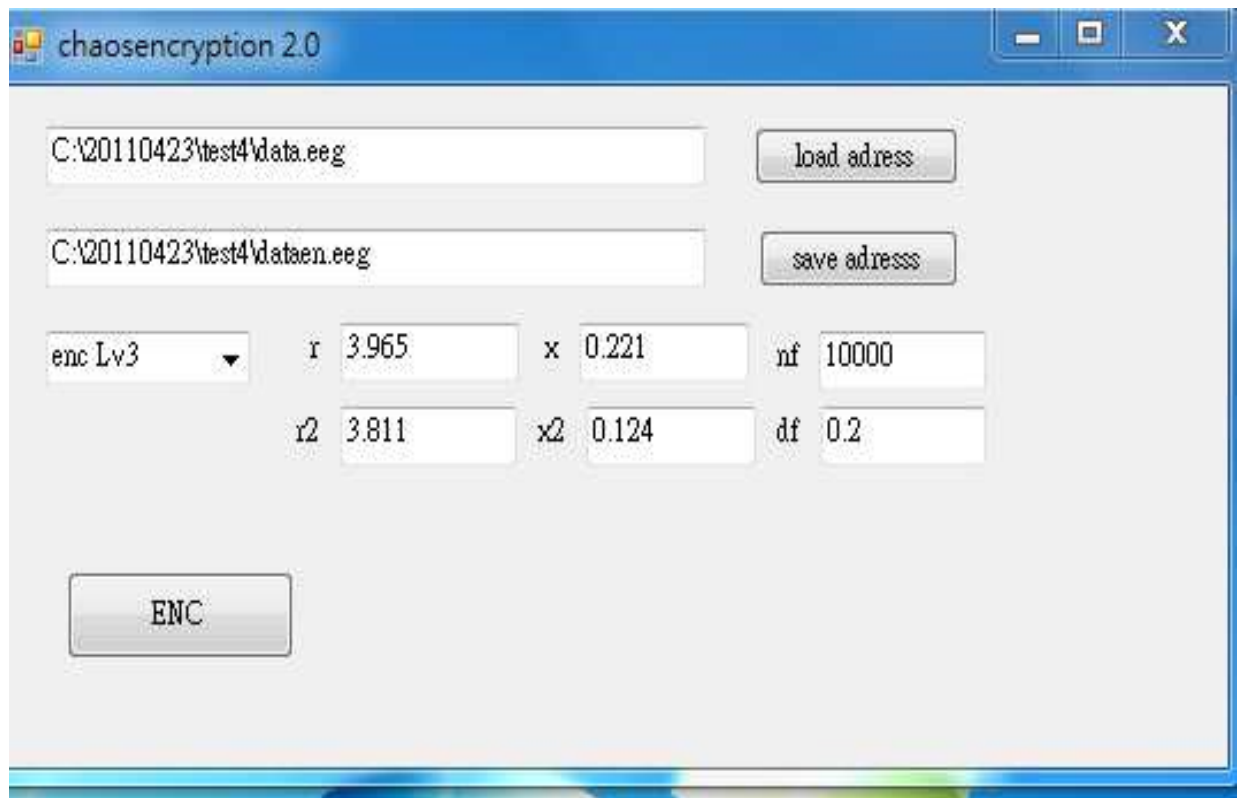


Figure 2 shows a working window of the offline chaos-based EEG encryption software

ACKNOWLEDGMENTS

THE AUTHORS ACKNOWLEDGE THE SUPPORT OF THE NSC 100-2221-E-019-019, AND THE VALUABLE COMMENTS OF THE REVIEWERS.

REFERENCES

- [1] F. Dachsel and W. Schwarz, "Chaos and cryptography," *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications*, pp.1498-1509, 2001.
- [2] L. Kocarev, "Chaos-based cryptography : A brief overview," *IEEE Circuits and System Magazine*, pp.6-21, 2001.
- [3] M. Yan, N. Bourbakis, and S. Li, "Data, image, video encryption, " *IEEE Potentials*, pp.28-34, 2004.
- [4] M. Naoki, J. Goce, A. Kazuyuki, and K. Ljupco, "Chaotic Block Ciphers: From Theory to Practical Algorithms," *IEEE Trans. Circuits and Systems I*, pp. 1341-1352, 2006.
- [5] C. M. Ou, "Design of Block Ciphers by Simple Chaotic Functions," *IEEE Computational Intelligence Magazine*, pp.54-59, 2009.
- [6] C. F. Lin, C. H. Chung, Z. L. Chen, C. J. Song, and Z. X. Wang, "A chaos-based unequal encryption mechanism in wireless telemedicine with error decryption," *WSEAS Transactions on Systems*, pp.49-55 , 2008.
- [7] C. F. Lin, W. T. Chang, and C. Y. Li, "A chaos-based visual encryption mechanism in JPEG2000 medical images," *J. of Medical and Biological Engineering*, pp.144-149, 2007.
- [8] C. F. Lin, C. H. Chung, and j. H. Lin, "A Chaos-based Visual Encryption Mechanism for EEG Clinical Signals," *Medical & Biological Engineering & Computing*, pp.757-762, 2009.
- [9] C. F. Lin, and B. S. H. Wang, "A 2D Chaos-based Visual Encryption Scheme for Clinical EEG Signals," *appear to Journal of Marine Science and Technology*.
- [10] C. F. Lin, and C. H. Chung, "A Chaos-based ECG/EEG Visual Encryption Methods and Devices," Taiwan, R.O.C. patent, I 338845.
- [11] C. F. Lin, "An Chaos-based Unequal Encryption Devices for Mobile Telemedicine," Taiwan, R.O.C. patent, M339162.

- Step 6: Load the encrypted EEG signals to the chaos-based encryption and decryption software "chaosencryption2.0."
- Step 7: Specify and save the path and file name of the decrypted file.
- Step 8: Select the appropriate decryption level and enter the decryption parameters r1, r2, x1, x2, nf, and df.
- Step 9: Use the EEG Vue software to observe the correctly decrypted 16-channel EEG signals.
- Step 10: Select the appropriate decryption level and enter the correct decryption parameters r2, x1, x2, nf, and df, and wrong decryption parameter r1 with a 0.00001% initial error.
- Step 11: Use the EEG Vue software to observe the incorrectly decrypted 16-channel EEG signals.

The data sizes of the testing 16-channel EEG signals are 28.538 Kbytes, 14.493 Kbytes, and 17.277 Kbytes, respectively; the length of the 16-channel brainwave was recorded as 42 min 42 s, 13 min 18 s, and 11 min 11 s, respectively. Level 3 encryption was used for encryption, with an encryption time of 127 s, 97 s, and 103 s, respectively. The percent root-mean-square Difference (PRD) values of the correct decryption of the three EEG signals and the original EEG signal were zero. The PRD value is defined as

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

where X_{ori} is the original clinical EEG signal and X_{dec} is the decrypted clinical EEG signal. PRD is the similar mean square-error (MSE) used to define signal distortion. The PRD of signals A and B is 0, which implies that signals A and B are identical.

III.CONCLUSIONS

Based on the results of our previous studies on chaos-based encryption, we developed offline chaos-based 16-channel brainwave encryption and decryption software using the Microsoft Visual Studio development kit and C# programming. Additionally, we also provide recommendations and advice regarding its application and encryption and decryption performance. The results of tests on the actual files indicate that the offline chaos-based 16-channel EEG signals encryption and decryption software developed in this study performs outstandingly. In future studies, we will devote greater effort to developing more robust chaos-based brainwave encryption software and a simpler interface for encryption parameter input.

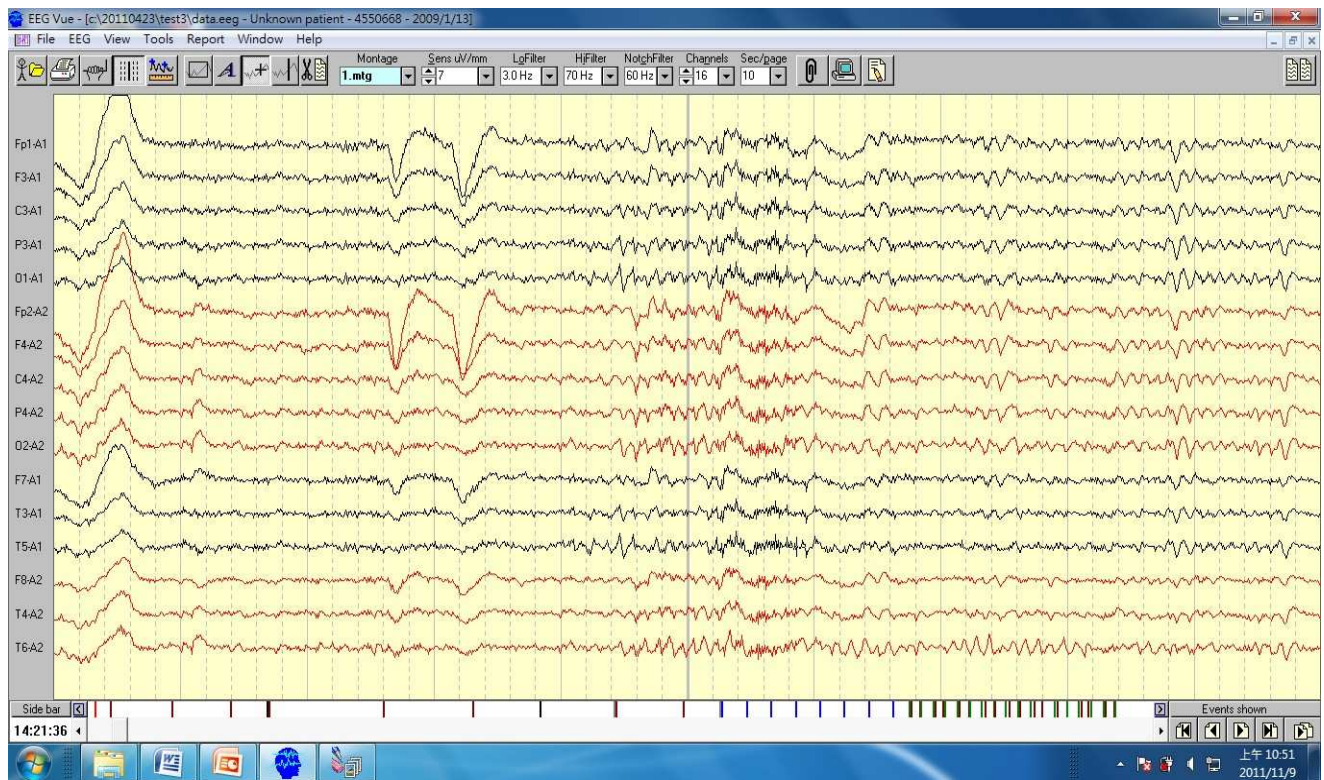


Figure 3 shows the 16-channel EEG signals prior to encryption.

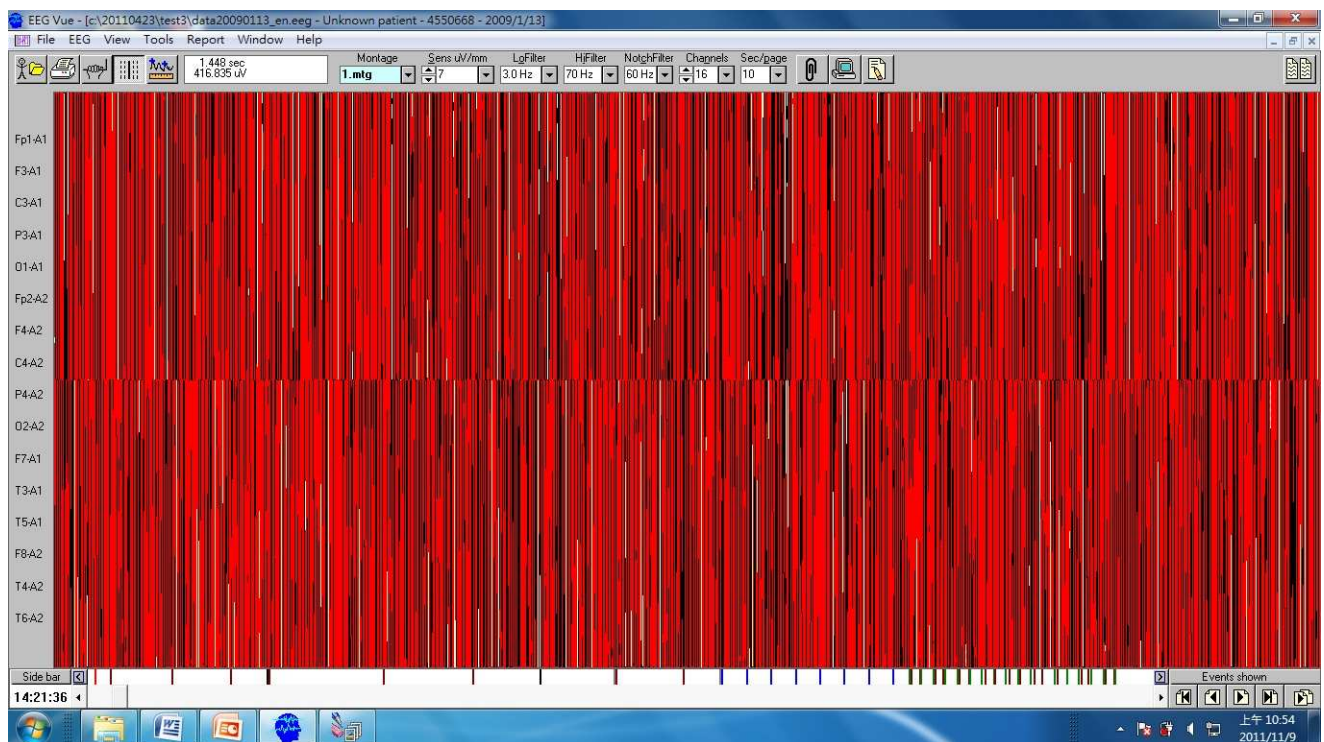


Figure 4 Use EEG Vue software to observe the encrypted 16-channel EEG signals

I