# E-Medicine: A Secure Transmission of Electrocardiograms Using Chaotic Oscillators Synchronization

Alain Tiedeu(✉), Yannick Abanda, and Gutenbert Kenfack

LAGEMES, National Advanced School of Engineering,
University of Yaoundé 1, Yaoundé, Cameroon
alain.tiedeu@polytechnique.cm

**Abstract.** Telemedicine is developing at high speed. In this context, patient's privacy and security is of great importance. Therefore any physiological signal, needs to be encrypted before their transmission over any channel. In this paper, we have developed an encryption system using chaotic synchronization to encrypt and decrypt information. The system was used for secure transmission of electrocardiograms signals as example.

**Keywords:** Electrocardiograms · Chaos synchronization · Secure transmission

## 1 Introduction

E-medicine uses information technologies to deliver health services. Its goal is to widen the access to medical services. As communication costs are growing cheap, e-medicine is becoming widely affordable (Moore 2002). Recently, advances in telecommunications networks have led to many successful e-medicine experiences around the world. Kontaxakis et al. (2000) developed an e-medicine workstation to acquire process and transmit ultrasonic images while Sachpazidis and Hohlfeld (2005) proposed a communication system for medical applications. The vast indian subcontinent has witnessed telemedicine success stories (Ayyaga et al. 2003; Pal et al. 2005; Deodhar 2001). Remote monitoring of patients is more and more common due either to an aging patient population, long distances to cover to find well equipped health centers or the need to decrease healthcare costs. These informations often transit through public channels with risk of being hijacked, intercepted, etc. This makes the need for encryption or other protection techniques crucial. Unfortunately, the works mentioned above and others in the field of telemedicine have not addressed the concern over protection of patient health information. We intend to do it in this paper.

Electrocardiograms (ECG) have a dual nature in the fact that they are used for both medical and identification purposes (Sufi et al. 2011; Almehmadi and Chatterjee 2015). A literature review on ECG encryption reveals methods including permutation encoding, wavelet anonymization, and noise-based obfuscation, just to name a few. Chaos-based encryption has an advantage over the other schemes because it is applicable to continuous signals, possesses a highly unpredictable nature, is sensitive to initial conditions and other key parameters.


C. M. F. Kebe et al. (Eds.): InterSol 2018, LNICST 249, pp. 83–89, 2018.
https://doi.org/10.1007/978-3-319-98878-8_8

To the best of our knowledge, secured ECG signal transmission with chaotic oscillators of different natures at emission and reception ends has not been studied. In this paper, we bridge this gap. Firstly, we develop an active control based strategy to synchronize a Colpitts and a Hartley oscillator. Secondly, we carry out encryption of ECG signal by the Colpitts oscillator, send it through the channel and decrypt it using the Hartley oscillator. The block diagram of the proposed system is given in Fig. 1.

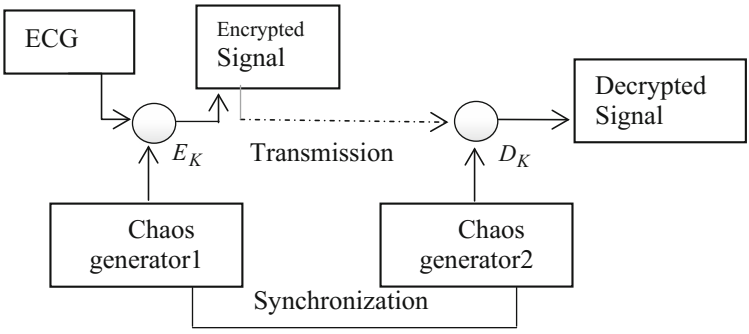


**Fig. 1.** ECG secured transmission system

### 1.1 Presentation of the Encryption System

The encryption/Decryption system is made of the ECG source, two chaotic generators and a transmission system (line). The signal from the ECG source is multiplied by the output of chaotic generator 1, modulated then transmitted. At the reception end, the output of chaotic generator 2 which is synchronized with chaotic generator 1 is used to decrypt the signal by simple division of received signal after it has undergone detection. The different elements of the system are described below.

### 1.2 Chaotic Oscillators

In this work, we use two different chaotic oscillators, namely, Colpitts (generator 1) and Hartley (generator 2) oscillators. These are drawn in Figs. 2 and 3 below.

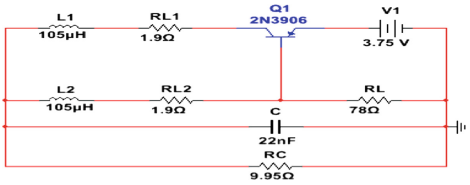


**Fig. 2.** Hartley oscillator

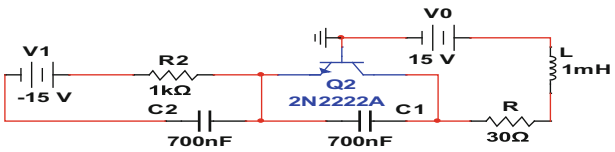


**Fig. 3.** Colpitts oscillator

### 1.3 Oscillators Dynamics

Applying Kirchoff voltage law to the circuit in Fig. 2 and changing variables, we obtain dimensionless equations:

$$\begin{cases} \dot{x}_1 = y_1 - z_1 - ax_1, \\ \dot{y}_1 = q - x_1 - by_1 - F(z_1), \\ \dot{z}_1 = dx_1 - ez_1 + F^*(z_1). \end{cases} \tag{1}$$

with

$$F(z_1) = \begin{cases} -\frac{1}{V_{TH}}(h + m \times z_1), z_1 \geq lamda \\ s, z_1 < lamda \end{cases} \quad \text{and} \quad F^*(z_1) = \begin{cases} 0, z_1 \geq lamda \\ f(g + a_1 z_1), z_1 < lamda \end{cases}$$

Then, when we apply the Kirchhoff voltage law to the circuit in Fig. 3 and carry out a change of variables, we obtain the following:

$$\begin{cases} \dot{x} = y - a_2\vartheta(z), \\ \dot{y} = c - x - z - b_1 y, \\ \dot{z} = \varepsilon(y - d_1). \end{cases} \tag{2}$$

where

$$\vartheta(z) = \begin{cases} -(1+z) & z < -1, \\ 0 & z \geq -1. \end{cases}$$

Solving (1) and (2) numerically using 4$^{th}$ order Runge-Kutta, yields the dynamics of the oscillators. The phase portraits obtained are shown in Figs. 4 and 5.

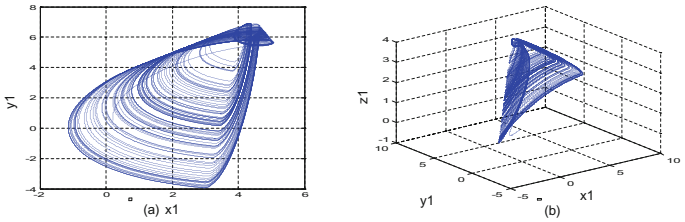


**Fig. 4.** (a) 2D phase portrait for Hartley oscillator. (b) 3D phase portrait for Hartley oscillator.

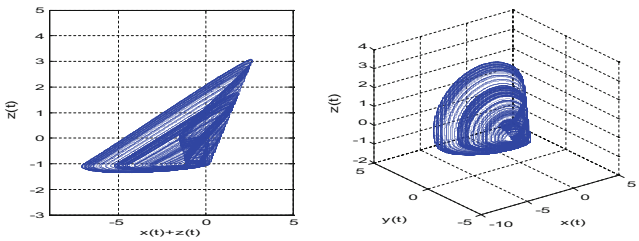


**Fig. 5.** (a) 2D phase portrait for Colpitts oscillator. (b) 3D phase portrait for Colpitts oscillator.

The phase portraits of Figs. 4 and 5 are strange attractors and indicate the possibility of chaotic behavior. A common method to confirm chaotic dynamics is to compute Maximum Lyapunov Exponent (MLE). The dynamics of MLE below (Figs. 6 and 7) confirm the chaotic nature of the oscillators.

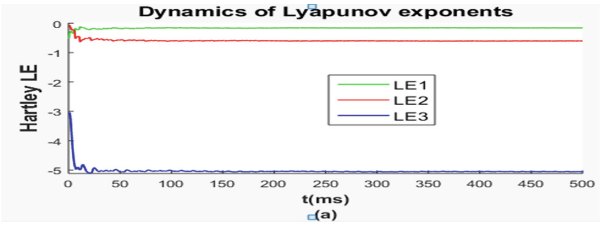


**Fig. 6.** Dynamics of Lyapunov exponents for Hartley oscillator

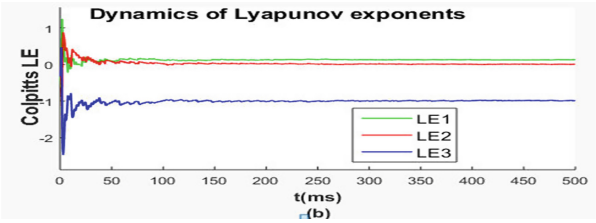


**Fig. 7.** Dynamics of Lyapunov exponents for Colpitts oscillator

## 2 Synchronization

Simply put, synchronizing the two oscillators is making sure that their output have the same values with time. Ideally, the difference should be zero. But practically, a "very small" error is enough. The first oscillator is the drive, while the second is the response. The controller U is the system that ensures the synchronization while the synchronization error is e.

$$\text{For the drive system:} \quad \begin{cases} \dot{x} = y - a_2\vartheta(z), \\ \dot{y} = c - x - z - b_1 y, \\ \dot{z} = \varepsilon(y - d_1). \end{cases} \tag{3}$$

$$\text{And the response system:} \begin{cases} \dot{x}_1 = y_1 - z_1 - ax_1 + U_1(t), \\ \dot{y}_1 = q - x_1 - by_1 - F(z_1) + U_2(t), \\ \dot{z}_1 = dx_1 - ez_1 + F^*(z_1) + U_3(t). \end{cases} \tag{4}$$

$U(t) = [U_1(t), U_2(t), U_3(t)]^T$ being the controller.

The synchronization error is: $e_1 = x_1 - x, e_2 = y_1 - y, e_3 = z_1 - z$.

Let's choose the controller described by Eq. (5)

$$\begin{cases} U_1(t) = -e_2 + z_1 + ax - a_2\vartheta(z) \\ U_2(t) = -y(b_1 - b) + e_1 - z + F(z_1) \\ U_3(t) = -dx_1 + ez + \varepsilon(y - d_1) + F^*(z_1) \end{cases} \tag{5}$$

Simulations were then carried out based on this controller and the state variables for drive and response respectively. The error was evaluated and the system was finally used to encrypt then decrypt the ECG signal, when the computed error converged towards zero. The following section presents some results yielded by the system.

## 3 Results and Discussion

In this section we shall present results from the synchronization, encryption and finally decryption.

### 3.1 Synchronization

The decrypted signal will be as close to the original one as far as the synchronization is accurate.

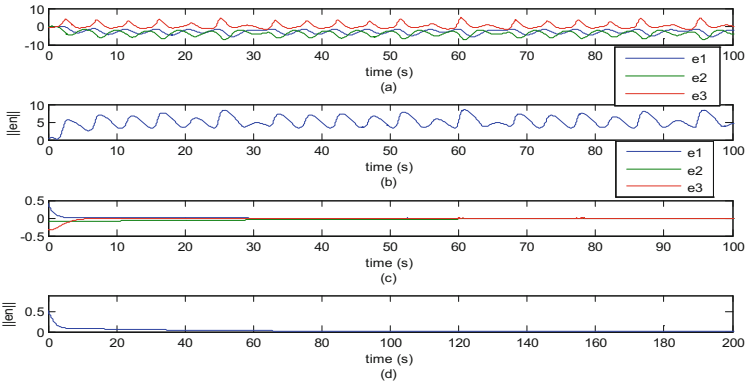


**Fig. 8.** (a) Synchronization error $e_1$, $e_2$, $e_3$ when the controller U is not activated, (b) the error's norm $\|e_n\|$ when the controller U is not activated (c) synchronization error $e_1$, $e_2$, $e_3$ with the controller U activated, (d) the error's norm $\|e_n\|$ with the controller U activated.

Figure 8 is a plot of the variable, the error when there is no controller and then the error when the oscillators are synchronized. We can see the error converging towards zero in event of synchronization.

### 3.2 Encrypted and Decrypted Signals

Figures 9 displays a visual example of encrypted, then decrypted signals.

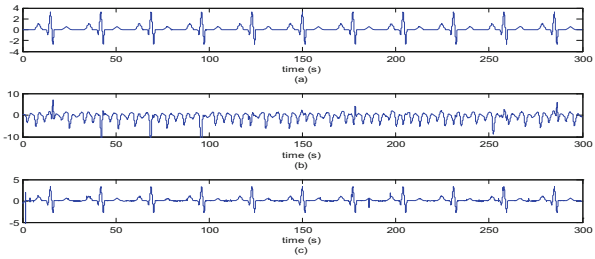


**Fig. 9.** (a) Original ECG signal (b) encrypted ECG signal, (c) decrypted ECG

We can see from Fig. 9 that the ECG signals are first encrypted, then decrypted correctly by the proposed system. Visually, these first results are satisfactory but will need in future works to be confirmed by some metrics like signal over noise ratio or/and mean square error.

## 4 Conclusion

In this work, we have designed and proposed an encryption and decryption system based on synchronization of chaotic oscillators. This was applied to the secured transmission of ECG signal. Results yielded by our system are encouraging and we hope to implement the experimental version in our future works.

## References

Moore, S.K.: Extending health care reach. IEEE Spectr. **39**(1), 66–71 (2002)

Kontaxakis, G., Walter, S., Sakas, G.: EU-TeleInViVo: an integrated portable telemedicine workstation featuring acquisition, processing and transmission over low-bandwidth lines of 3D ultrasound volume images. In: Proceedings of IEEE EMBS International Conference on Information Technology Applications in Biomedicine, pp. 158–163 (2000)

Sachpazidis, I., Hohlfeld, O.: Instant messaging communication gateway for medical applications. In: IASTED International Conference on Telehealth, Banff, Canada, 19–21 July 2005, pp. 12–16 (2005)

Ayyagari, A., et al.: Use of telemedicine in evading cholera outbreak in Mahakumbh Mela, Prayag UP India: an encouraging experience. Telemed. J. E. Health **9**, 89–94 (2003)

Pal, A., Mbarika, V.W., Cobb-Payton, F., Datta, P., McCoy, S.: Telemedicine diffusion in a developing country: the case of India (March 2004). IEEE Trans. Inf Technol. Biomed. **9**(1), 59–65 (2005)

Deodhar, J.: Telemedicine by email—experience in neonatal care at a primary care facility in rural India. J. Telemed. Telecare **8**, 20–21 (2001)

Sufi, F., Han, F., Khalil, I., Hu, J.: A chaos-based encryption technique to protect ECG packets for time critical telecardiology applications. J. Netw. Comput. Appl. **4**, 515–524 (2011)

Almehmadi, F.S., Chatterjee, M.R.: Secure chaotic transmission of electrocardiography signals with acousto-optic modulation under profiled beam propagation. Appl. Opt. **54**(2), 195–203 (2015)