International Journal of Sensor Networks and Data Communications

Chen et al., Sensor Netw Data Commun 2015, 4:2
DOI: 10.4172/2090-4886.1000124

Research Article Open Access

Data Encryption and Transmission Based on Personal ECG Signals

Ching-Kun Chen[1], Chun-Liang Lin[1]*, Shyan-Lung Lin[2] and Cheng-Tang Chiang[3]

[1]Department of Electrical Engineering, National Chung Hsing University, Taichung, Taiwan
[2]Department of Automatic Control Engineering, Feng Chia University, Taichung, Taiwan
[3]Boson Technology Co., LTD, Taichung, Taiwan

Abstract

ECG signal vary from person to person, making it difficult to be imitated and duplicated. Biometric identification based on ECG is therefore a useful application based on this feature. Synchronization of chaotic systems provides a rich mechanism which is noise-like and virtually impossible to guess or predict. This study intends to combine our previously proposed information encryption/decryption system with chaotic synchronization circuits to create private key masking. To implement the proposed secure communication system, a pair of Lorenz-based synchronized circuits is developed by using operational amplifiers, resistors, capacitors and multipliers. The verification presented involves numerical simulation and hardware implementation to demonstrate feasibility of the proposed method. High quality randomness in ECG signals results in a widely expanded key space, making it an ideal key generator for personalized data encryption. The experiments demonstrate the use of this approach in encrypting texts and images via secure communications.

Keywords: Communication security; Encryption; Chaos synchronization, Electrocardiogram

Introduction

Digital information is increasingly applied in real-world applications as multimedia and network technologies continue to develop. A specific encryption system is therefore required to protect the information during transmission [1-3]. Cryptography is a basic information security measure that encodes messages to make them non-readable. However, conventional block cipher algorithms such as data encryption standard (DES), triple data encryption standard (Triple-DES), and international data encryption algorithm (IDEA) are unsuitable for image encryption because of the special storage characteristics of images [4,5]. Conventional image encryption algorithms are primarily based on the position permutation, such as Arnold transform, magic square matrix, and fractal curve scan [6]. In addition, permutation only algorithms are weak against known text attacks because they cannot change the grayscale of the pixel. Recently, the close relationship between chaos and cryptography has played an active role in data encryption [7-13] because of its significant features, including sensitivity to initial conditions, non-periodicity, and randomness. These features make the chaotic system an ideal tool for communication security [14].

There are no models accounting for all cardiac electrical activities because the human heart is an extremely complex biological system, which makes ECG signals vary from person to person. Compared with common biometric-based systems, the biometric feature of ECG signals is extremely difficult to duplicate. Therefore, an ECG signal could be a biometric tool for individual identification [15-22]. The theory of chaotic dynamical systems has used several features, including the correlation dimension, Lyapunov exponents, and approximate entropy, to describe system dynamics. These key features can explain ECG behavior for diagnostic purposes [23-25].

In ordinary telecommunication system, a specific frequency sine wave carrier is modulated and transmitted with certain message. A receiver system must be tuned to the particular frequency of the carrier sine wave to recover the message. Synchronization of chaotic systems provides a rich mechanism forming another application to personalize secure communications, which are noise-like and impossible to be guessed or predicted. The application of chaotic synchronization to secret communication was previously suggested by Pecora and Carroll [26,27]. There were many control techniques to synchronized chaotic systems, such as fuzzy control [28,29], delayed neural networks [30,31], impulsive control [32], and nonlinear error feedback control [33]. The chaotic signals can also be used to mask information or serve as the modulating waveforms [34-37].

In this research, we use Lyapunov exponent's spectrum to extract the features of human ECG and use them as a secret key to encrypt images and text messages for secure data transmission. The proposed approach uses a chaotic cryptosystem based on the private feature of ECG signals and chaotic functions for information encryption. We combine the previously developed information encryption/decryption system [7-9] with chaotic synchronization circuits to facilitate private key masking. The chaotic synchronization system consists of a driver circuit and a response circuit. This concept of the private key transmission is based on chaotic signal masking and recovery. The transmitter adds a noise-like masking signal to the private key and the receiver removes it by using two synchronization circuits. This configuration forms an indecipherable scheme that is useful for personalized data transmission, in which extreme security is of primary concern.

To implement the proposed the secure communication system, a pair of Lorenz-based synchronized circuits are realized by operational amplifiers, resistors, capacitors and multipliers. The experimental results contain numerical and hardware verification which demonstrates applicability of the proposed design method.

***Corresponding author:** Chun-Liang Lin, Department of Electrical Engineering, National Chung Hsing University, Taichung, Taiwan 402, R.O.C, Tel: +886-4-22851549; Fax: +886-4-22851410; E-mail: chunlin@dragon.nchu.edu.tw

Received August 31, 2015; **Accepted** September 29, 2015; **Published** October 05, 2015

Citation: Chen CK, Lin CL, Lin SL, Chiang CT (2015) Data Encryption and Transmission Based on Personal ECG Signals. Sensor Netw Data Commun 4: 124. doi:10.4172/2090-4886.1000124

Description of Method

Phase-space reconstruction

A phase space or diagram is a space in which each point describes two or more states of a system variable. The number of states that can be displayed in the phase space is called the phase space dimension or reconstruction dimension. The phase space in d dimensions displays a number of points $\left\{\vec{Z}(n)\right\}$ of the system, where each point is given by

$$\vec{Z}(n) = \left[z(n), z(n+n_T), \cdots, z(n+(d-1)n_T)\right] \quad (1)$$

Where n is the moment in time of the state variables, n_T = T/Δ with Δ denoting the sampling period and T is the period between two consecutive measurements for constructing the phase plot. The trajectory in d dimensional space is a set of k consecutive points and $n=n_0$, n_0+n_T, L, $n0+(k-1)n_T$, where n_0 is the starting time (in terms of the number of sampling period) of observation.

Phase space reconstruction shows the state trajectories of $z(n)$ and $z(n+n_T)$ at the same time scale. Figure 1 shows the ECG signal from encryption person and the phase plot.

Calculation of the lyapunov exponents

The Lyapunov exponent is an important feature of chaotic systems which quantifies sensitivity of the system to the initial conditions. Sensitivity to initial conditions means that a small change in the state of a system will grow at an exponential rate and eventually dominate the overall system behavior. Lyapunov exponents are defined as the long-term average exponential rates of divergence of the nearby states. If a system has at least one positive Lyapunov exponent, the system is chaotic. The larger the positive exponent, the more chaotic the system becomes. The exponents are generally arranged such that $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$, where λ_1 and λ_n correspond to the most rapidly expanding and contracting principal axes, respectively. Therefore, λ_1 may be regarded as an estimator of the dominant chaotic behavior of the system. This study uses the largest Lyapunov exponent λ_1 as a measure of the ECG signal using the Wolf algorithm [38].

Logistic map

The logistic map is a polynomial mapping of the second order. Its chaotic behavior for different parameters was unveiled in [39]. The logistic map equation is given by the following equation and can be illustrated as in Figures 2 and 3:

$$L_{n+1} = A\, L_n (1 - L_n) \quad (2)$$

where n=0,1,2,…, $0 \leq L \leq 1$, $0 \leq A \leq 4$, A is a (positive) bifurcation parameter. Figure 2 shows the bifurcation diagram of the logistic map in the range $1 \leq A \leq 4$. When the vertical slice A=3.4, the iteration sequence splits into two periodic oscillations, which continues until A is slightly larger than 3.45. This is called periodic-doubling bifurcation in chaos theory.

Successive doublings of the period quickly occur in the range of $3.45<A<3.6$. When A increases to 3.6, the periodicity becomes chaotic in the dark area. Many new periodic orbits emerge as A continuously grows from 3.45 to 4. Figure 3 shows the property of the logistic map with different parameter A. The results converge on the same value after several iterations without any chaotic behavior when $A \in (0, 3)$, as shown in Figure 3(a). The system appears periodicity when $A \in [3, 3.6)$, as illustrated in Figure 3(b). The chaotic random-like behavior when $A \in [3.6, 4)$ is shown in Figure 3(c).

Henon map

The Henon map is a 2-D iterated map with chaotic solutions proposed by M. Henon [40]. The Henon equation can be written as follows

$$\begin{cases} X_{n+1} = 1 - aX_n^2 + bY_n, \\ Y_{n+1} = X_n, \end{cases} \quad n = 1, 2, \ldots \quad (3)$$

where a and b are (positive) bifurcation parameters with b being a measure of the rate of area contraction. The Henon map is the most general 2-D quadratic map possessing the property that the contraction is independent of X and Y. Bounded solutions exist for the Henon map over the ranges of a and b, and some yield chaotic solutions. The demonstrative map was plotted for $a = 1.4$ and $b=0.3$. From which one can observe the chaotic behavior. Figure 4 shows the attractor of the Henon map on the X-Y space.

Lorenz system

The Lorenz system was originally developed as a simplified mathematical model of atmospheric by Edward Lorenz in 1963 [41], which is a 3-dimensional dynamical system described by

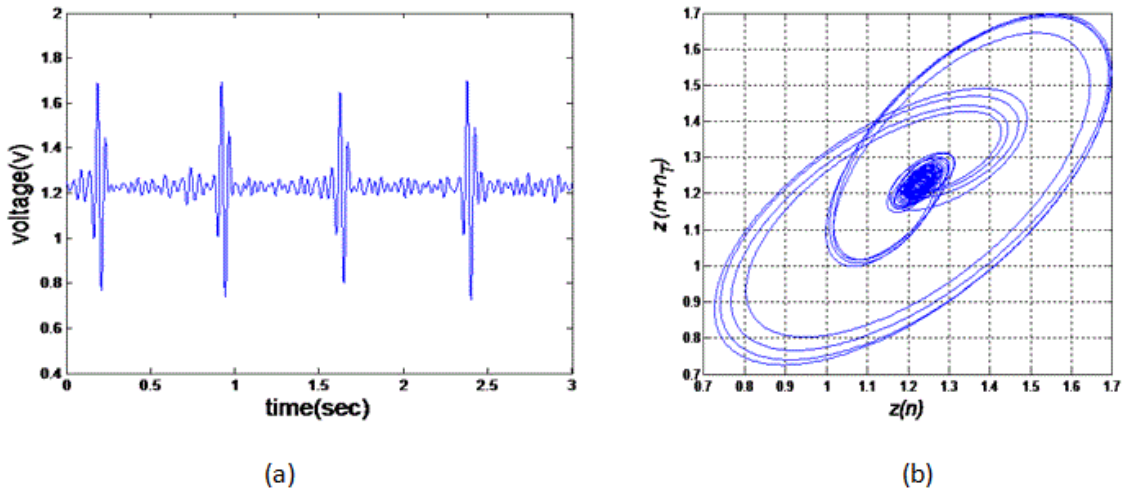


Figure 1: (a) ECG signal (b) phase plot taken from the encryption person.

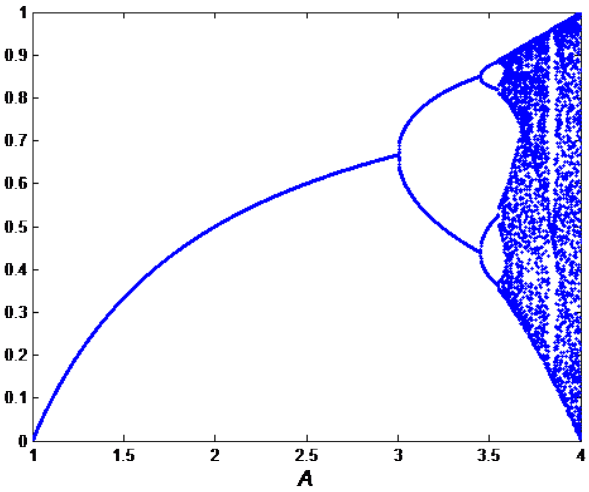


Figure 2: Bifurcation diagram of the logistic map.

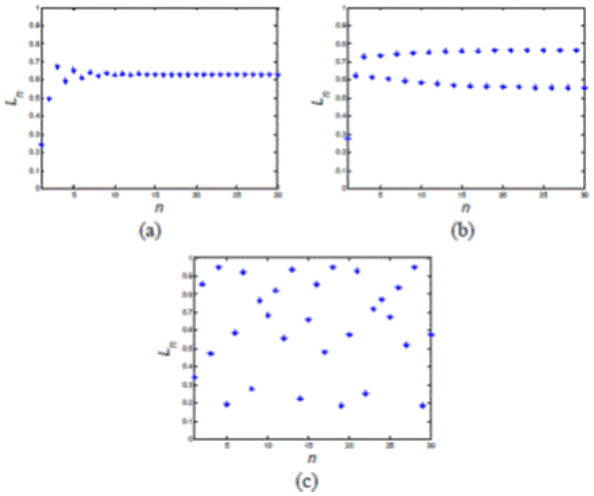


Figure 3: Property of logistic map with different bifurcation parameter with L0=0.1 (a) A=2.7 (b) A=3.1 (c) A=3.8.

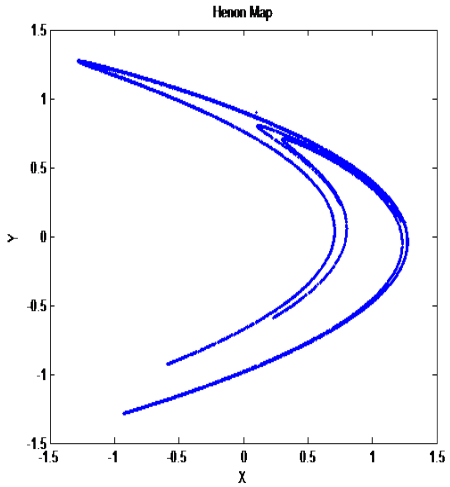


Figure 4: Attractors for the Henon map with a= 1.4 and b=0.3.

$$\begin{aligned}\dot{x} &= s(y - x)\\ \dot{y} &= rx - y - xz\\ \dot{z} &= xy - pz\end{aligned} \tag{4}$$

where *x,y*, and *z* are dynamic variables and *s, r*, and *p* are positive system parameters. The Lorenz system has a single positive Laypunov exponent, λ_1 = 1.069, while the other are λ_2 = 0 and λ_3 = -12.73 respectively. More detailed complex dynamics of the Lorenz system can be seen in [42]. For the typical values *s*=10, *r*=28, *p*=8/3 the time serials of the variables *X, Y* and *Z* are shown in Figure 5(a); the system has a 3-dimensional chaotic attractor as shown in Figure 5(b).

Synchronization of two identical lorenz systems

Consider the following linear coupling of two identical Lorenz systems:

$$\begin{aligned}\dot{x}_1 &= s(y_1 - x_1) + d_1(x_2 - x_1)\\ \dot{y}_1 &= rx_1 - y_1 - x_1z_1 + d_2(y_2 - y_1)\\ \dot{z}_1 &= x_1y_1 - pz_1 + d_3(z_2 - z_1)\end{aligned} \tag{5}$$

$$\begin{aligned}\dot{x}_2 &= s(y_2 - x_2) + d_1(x_1 - x_2)\\ \dot{y}_2 &= rx_2 - y_2 - x_2z_2 + d_2(y_1 - y_2)\\ \dot{z}_2 &= x_2y_2 - pz_2 + d_3(z_1 - z_2)\end{aligned} \tag{6}$$

Where $x_i,y_i,z_i(i=1,2)$ are state variables, and $d_j(j=1,2,3)$ are coupling coefficients. The driver system consists of x_1, y_1 and z_1. The response system is described by x_2, y_2 and z_2. In particular, when $d_1\neq0$, $d_2=0$, $d_3=0$ the coupled systems and are x-coupled. Similarly, the systems with $d_2\neq0$, $d_1=d_3=0$ are *y*-coupled, and the systems are *z*-coupled when $d_3\neq0$, $d_1=d_2=0$. We can define the synchronization errors $e_x(t)$, $e_y(t)$, $e_z(t)$ as

$$\begin{aligned}e_x &= x_1 - x_2,\\ e_y &= y_1 - y_2,\\ e_z &= z_1 - z_2,\end{aligned} \tag{7}$$

then

$$\begin{aligned}-x_1z_1 + x_2z_2 &= -z_1e_x - x_2e_z,\\ -x_1y_1 - x_2y_2 &= y_1e_x + x_2e_y\end{aligned} \tag{8}$$

From (5)-(8), the error dynamics is given by

$$\begin{aligned}\dot{e}_x &= -(s+2d_1)e_x + se_y\\ \dot{e}_y &= -(r-z_1)e_x - (1-2d_2)e_y - x_2e_z\\ \dot{e}_z &= y_1e_x + x_2e_y - (p+2d_3)e_z\end{aligned} \tag{9}$$

The coefficient matrix of this system is

$$A(t) = \begin{bmatrix} -(s+2d_1) & s & 0\\ r - z_1 & -(1+2d_2) & -x_2\\ y_1 & x_2 & -(p+2d_3)\end{bmatrix}, \tag{10}$$

Define

$$\begin{aligned}B(t) &= \frac{A(t) + A^T(t)}{2}\\ &= \begin{bmatrix} -(s+2d_1) & (r+s-z_1)/2 & y_1/2\\ (r+s-z_1)/2 & -(1+2d_2) & 0\\ y_1/2 & 0 & -(p+2d_3)\end{bmatrix}\end{aligned} \tag{11}$$

Let $\alpha(t)$ and $\beta(t)$ be the minimum and maximum eigenvalues of matrix $B(t)$ respectively. According to the result in [43], we have the following lemma.

Lemma 1. The differential equation $\dot{X} = A(t)X$ has a solution X (t), then

$$\|X(0)\|\exp\left\{\int_0^t \alpha(t)dt\right\} \le \|X(t)\| \le \|X(0)\|\exp\left\{\int_0^t \beta(t)dt\right\} \tag{12}$$

It is easily proven by the following equation

$$\frac{d\|X(t)\|^2}{dt} = X^T(t)B(t)X(t)$$

Therefore, if $\exists\ \varepsilon>0$ such that $\beta(t)<-\varepsilon$, then for any initial state $X(0)$, one has $X(t) \to 0$ exponentially. Note that $B(t)$ is a symmetric matrix, thus all eigenvalues of $B(t)$ are real for all t. Let the eigenvalues be $\lambda_i(i=1,2,3)$ with $\lambda_1\le\lambda_2\le\lambda_3$. For the two identical Lorenz systems, if $(x_1(0), y_1(0), z_1(0) \neq (x_2(0), y_2(0), z_2(0))$, then the state trajectories of the two identical Lorenz systems will separate as time goes by and become unrelated. When $d_j(j=1,2,3)$ satisfy $F(d_1,d_2,d_3) > 0$, the two identical chaotic systems will travel at the same orbit simultaneously.

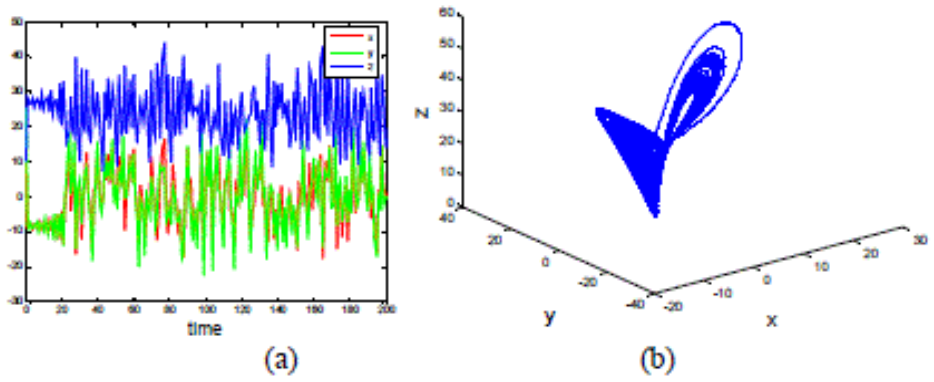


Figure 5: The Lorenz system (a) time profiles of the variables x, y and z (b) x-y-z phase trajectories.

That is, the two identical Lorenz systems with linear coupling will be synchronized. On the contrary, if the coupling coefficient $F(d_1,d_2,d_3) < 0$, the two identical chaotic systems will operate independently at their own orbits, i.e., they are not synchronized.

Theorem 1: Given the coupling coefficients $d_i>0$, i = 1, 2, 3 if d_1, d_2, d_3 satisfy the following condition

$$\gamma_0 = (s+2d_1)(1+2d_2)(p+2d_3) - \frac{p^2(s+r)}{16(p-1)}M > 0,$$

$$\sigma_0 = (s+2d_1)(1+2d_2)(1+s+2d_1+2d_2) + (p+2d_3)(1+s+2d_1+2d_2)(1+s+p+2(d_1+d_2+d_3)) - \frac{p^2(s+r)}{16(p-1)}(s+2d_1+M) > 0,$$

Where $M = \max\{1+2d_2, p+2d_3\}$ then for any $(x_1(0),y_1(0),z_1(0),x_2(0),y_2(0),z_2(0))$, the two coupled Lorenz systems will be synchronized as $t\to+\infty$, provided that the orbit is close enough to the basin of attraction.

Pf: See Appendix for the details.

For s=10, r=28, p=8/3, the initial states x_{10}=10, y_{10}=25, z_{10}=10, x_{20}=20, y_{20}=11, z_{20}=5, and the coupling coefficients d_1=1.2, d_2=0.8, d_3=2.1, the numerical simulation of the corresponding chaotic phase trajectories and state errors versus time are illustrated in Figures 6 and 7.

System Design and Secure Data Transmission

ECG acquisition

Traditionally, ECG signals are recorded through more than three electrodes attached to the human body and manipulated in a complex data management system. This is not suitable for the current purpose. Instead of the way, this research proposes to use a convenient handheld device, developed by our research team, to collect physiological signals from only two leads [44], as shown in Figure 8(a). Each lead is attached to an electrode. The required signals are acquired when two electrodes are simultaneously touched. Figure 8(b) shows the device's structure, which comprises two sensing electrodes. The two active sensor electrodes are connected to the pulse measurement device and the pulse measurement device comprises a negative feedback difference common mode signal and a buffer/balanced circuit for providing a circuit with a self-common point electrode potential. The first bio-potential signal is detected by the first active sensor electrode and the common

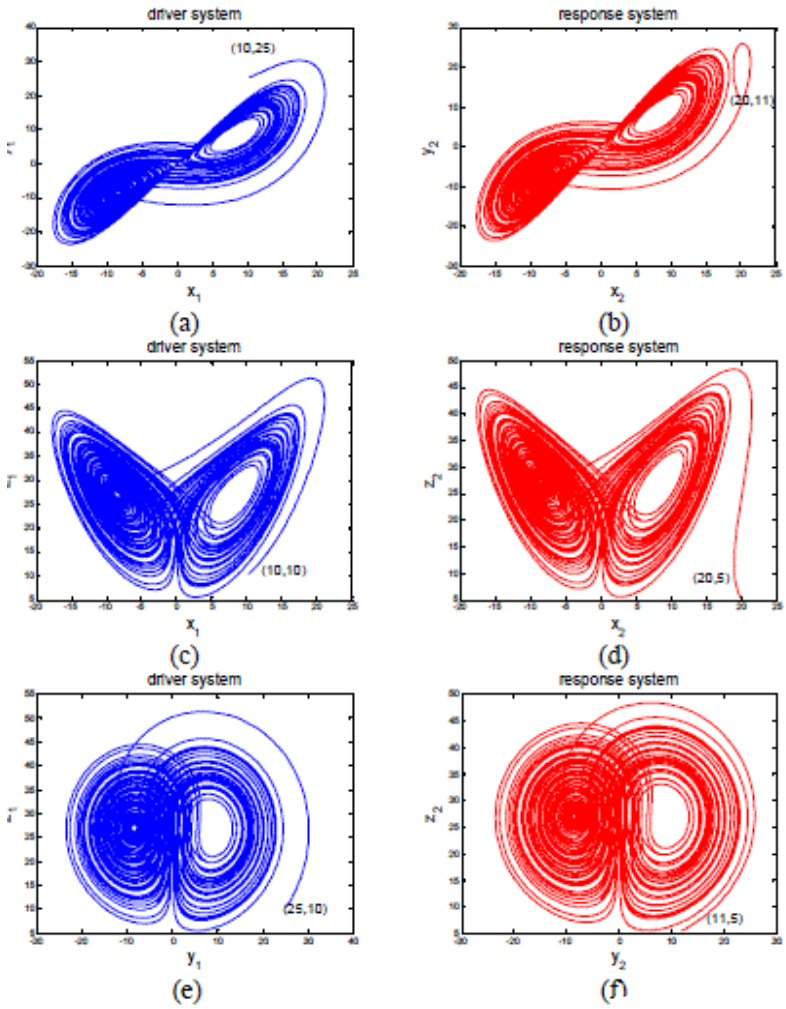


Figure 6: Chaotic phase trajectories for the two Lorenz systems (a) x_1-y_1 plane (b) x_2-y_2 plane (c) x_1-z_1 plane (d) x_2-y_2 plane (e) y_1-z_1 plane (f) y_2-z_2 plane.

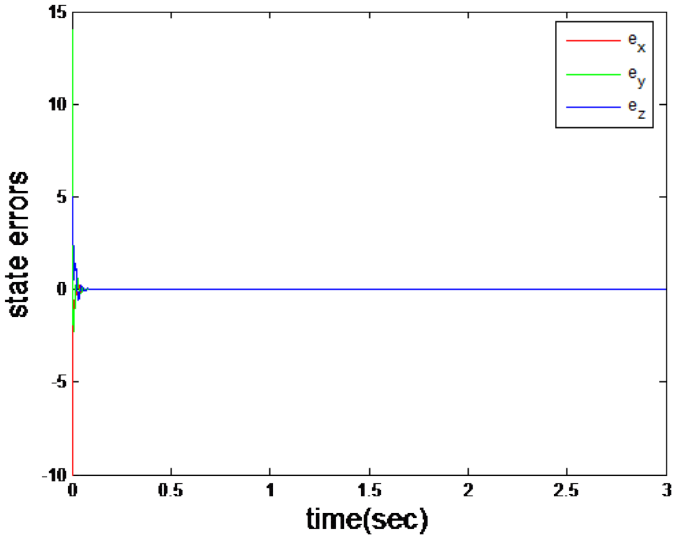
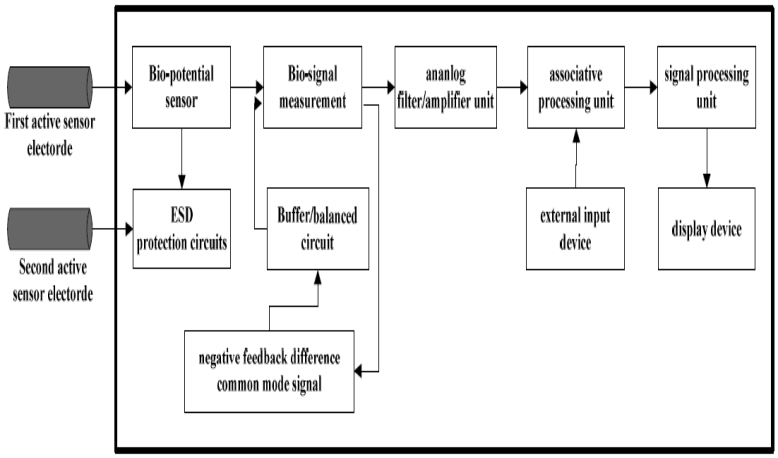


Figure 7: Synchronization errors $e_x(t)$, $e_y(t)$, $e_z(t)$ for the two Lorenz systems.

(a)



(b)

Figure 8: Self-developed handheld ECG acquisition device (a) measurement device (b) structure of the patented portable instrument ET-600.

point electrode. The second bio-potential signal, possesses the same magnitude, but with a different phase as the first bio-potential signal detected by the second active sensor electrode and the common point electrode. The associative processing unit receives the signal which is processed by an analog filter/amplifier unit with the operational frequency from 0.5 to 40Hz.

The self-developed ECG management device accompanied with a

digital signal processing unit (NI USB6211) and the ECG data acquisition in the LabVIEW environment. The signals measured are then used to reconstruct ECG signals and extract the features by our feature extraction program.

Secure data transmission

The structure of the proposed secure information transmission system based on the two Lorenz circuits is proposed in Figure 9. The encryption person's ECG data are collected and saved as a private key. The processed secret information is transmitted via the proposed chaotic encryption system, which is activated by the private key. To decrypt the secret information, the recipient should possess both of the ECG plot and the chaotic decryption algorithm. In addition, the ECG extraction program must be used to extract the features as the initial key for the proposed chaotic decryption algorithms.

Implementation of synchronization circuit for secure communication

An electric circuit is designed to realize the Lorenz-based synchronized circuit for secure data communication, as illustrated in Figure 10. The voltages at the nodes labeled x_1, y_1 and z_1 correspond to the states of and x_2, y_2 and z_2 to the states of, respectively. The operational amplifier LF412 and associated circuitry perform the basic operations of addition, subtraction, and integration. The nonlinear

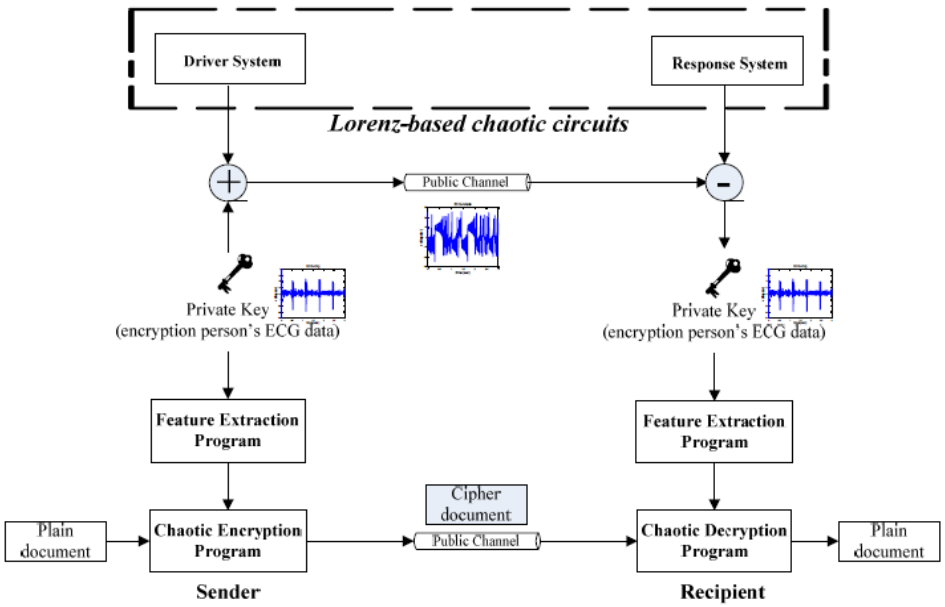


Figure 9: Structure of the secure information transmission based on the chaotic masking Lorenz circuits.

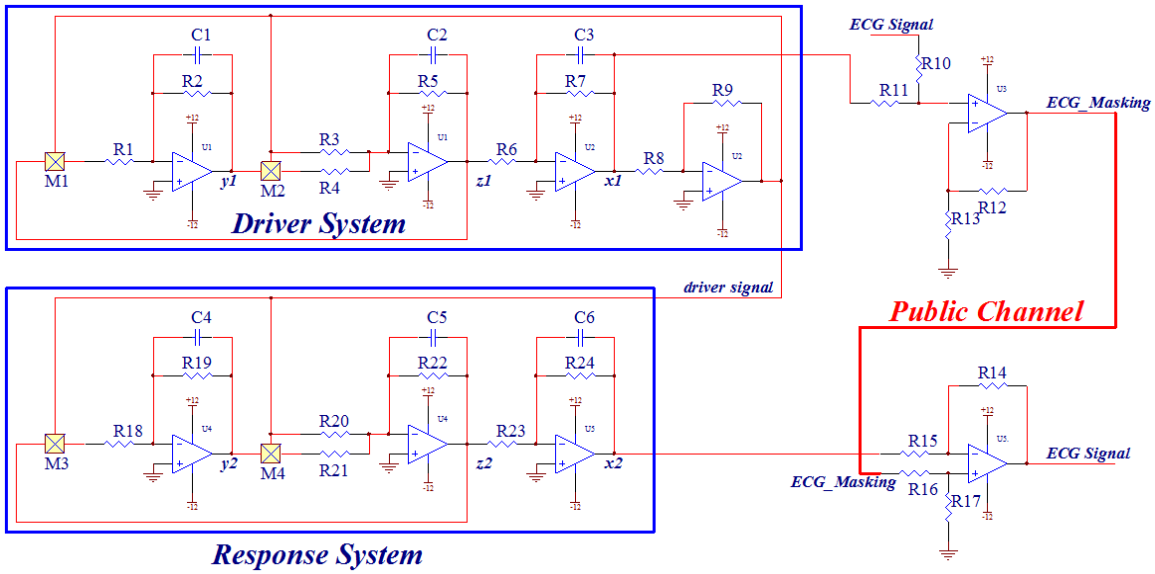


Figure 10: Lorenz-based chaotic masking communication circuit.

Device	Description	Value	Tolerance
U1~U5	Op Amp (LF412)		
R_1,R_4,R_8~R_{18},R_{21},R_{23}	1/4W Resistor	10 KΩ	±0.05%
R_2,R_{19}	1/4W Resistor	374 KΩ	±0.05%
R_3,R_{20}	1/4W Resistor	35.7 KΩ	±0.05%
R_5,R_{22}	1/4W Resistor	1 MΩ	±0.05%
R_6,R_7,R_{23},R_{24}	1/4W Resistor	100 KΩ	±0.05%
C1~C6	Capacitor	0.1μF	±0.1%
M1~M4	Analog multiplier		

Table 1: Components of the chaotic masking communication circuits.

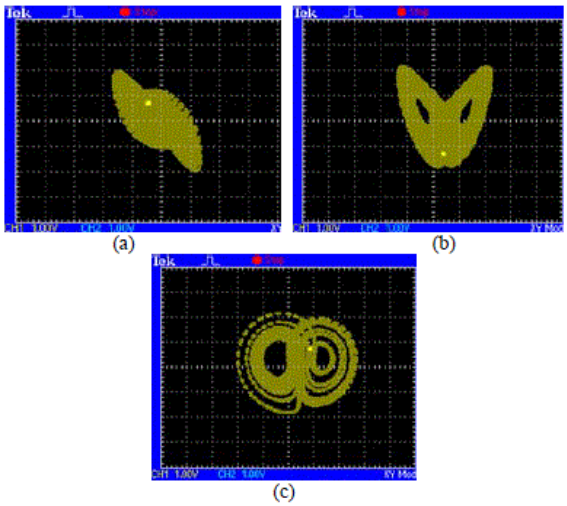


Figure 11: Phase portraits of the Lorenz oscillator (a) *x-y* plane (b) *x-z* plane (c) *y-z* plane.

terms in the system and are implemented with the analog multiplier AD633. The component list of the Lorenz-based chaotic masking communication circuit is given in Table 1. The system parameters *s, r,* and *p* can be implemented by resistors R_2,R_3,R_5 *and* R_7 as follows

$$s = \frac{R_5}{R_7}, \quad r \approx \frac{R_5}{R_3}, \quad p \approx \frac{R_5}{R_2} \tag{13}$$

The private key ECG signal was masked by chaotic signal of the driver system and is presented as ECG_masking, which is sent out through a public channel. On the other side, the ECG_masking signal is received and the private key is recovered by synchronized chaotic signal of the response system.

Experimental results for synchronization and secure communication are given to demonstrate the performance of the proposed scheme. Figure 11 shows the Lorenz-based circuit's attractor projected onto the x-y plane, x-z plane, and y-z plane, respectively. Figure 12 shows the phase portrait in x_1-x_2 plane illustrating synchronization of the Lorenz-based circuits. Figure 13(a) shows practical implementation of the proposed secure data communication system. Figure 13(b) depicts the scrambled private key ECG signal, the transmitted chaotic signal ECG_masking, and the recovered private key ECG_signal in the response system.

Encryption/decryption algorithms

We now explain the procedure of the proposed information encryption/decryption system using ECG signals with a chaotic logistic map for text encryption and chaotic Henon map for image encryption. Figure 14 presents the block diagram of the information encryption/decryption scheme. The chaotic functions depicted in Section 2 are employed in the information encryption/decryption algorithm using the logistic map, Henon map, ECG extraction program, and Wolf algorithm. The ECG extraction program extracts the individual features of the users as the initial key (λ_1) for the logistic map and Henon map, and subsequently uses these chaotic functions to generate an unpredictable random orbit. The unpredictable random orbit is used as a private encryption key serial to replace pixel values, images coordinates, and ASCII codes. Conversely, the chaotic decryption algorithm fulfills the inverse operation.

Figure 15 shows the flow chart of the chaotic encryption algorithm for the document with blended Figure and text. First, text and images of the encrypted document are separated. Set the encrypted grayscale image to be S, whose size is M×N and the pixel related to the coordinates (i, j) is denoted $I(i,j)$, $1 \le i \le M$ and $1 \le j \le N$. The new coordinates of the pixel $I(i,j)$, after replacement, denoted (i', j') with I'(i,j) representing the replaced $I(i,j)$. To enhance undetectability, the new coordinates and the pixel $I'(i', j')$ are produced using the chaotic Henon map . The format of encrypted text is transformed into Text file (T.txt). We obtain the strings with the line terminators and convert characters into ASCII codes until the end of the file (T.text), and then the ciphertext (T_mask. text) is converted into ASCII codes by using the chaotic logistic map and the converted ASCII codes into characters accordingly.

Experimental Results

Table 2 lists key parameters of logistic map and Henon map for testing the encryption and decryption algorithms.

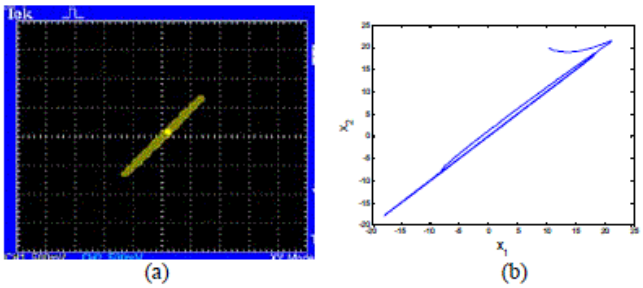


Figure 12: Synchronization of the driver signal x_1 and response signal x_2 (a) experimental result (b) numerical plot.

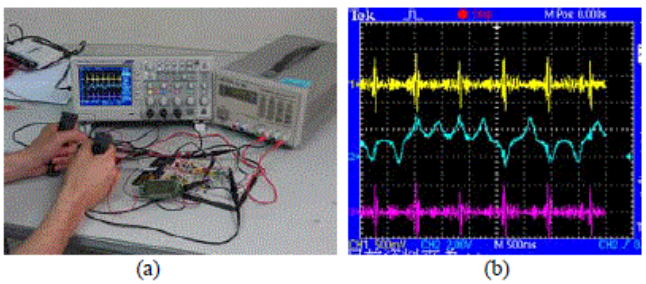


Figure 13: Practical implementation of the proposed secure communication system (a) the testing scene (b) Channel 1: private key ECG_signal, Channel 2: transmitted chaotic signal ECG_masking, Channel 3: recovered private key ECG_signal in the response system.

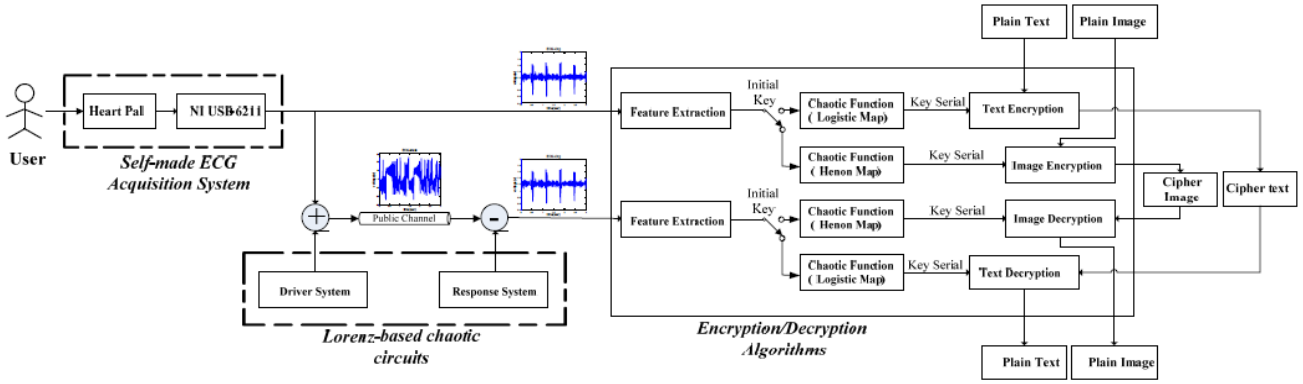


Figure 14: Block diagram of the proposed information encryption/decryption scheme.

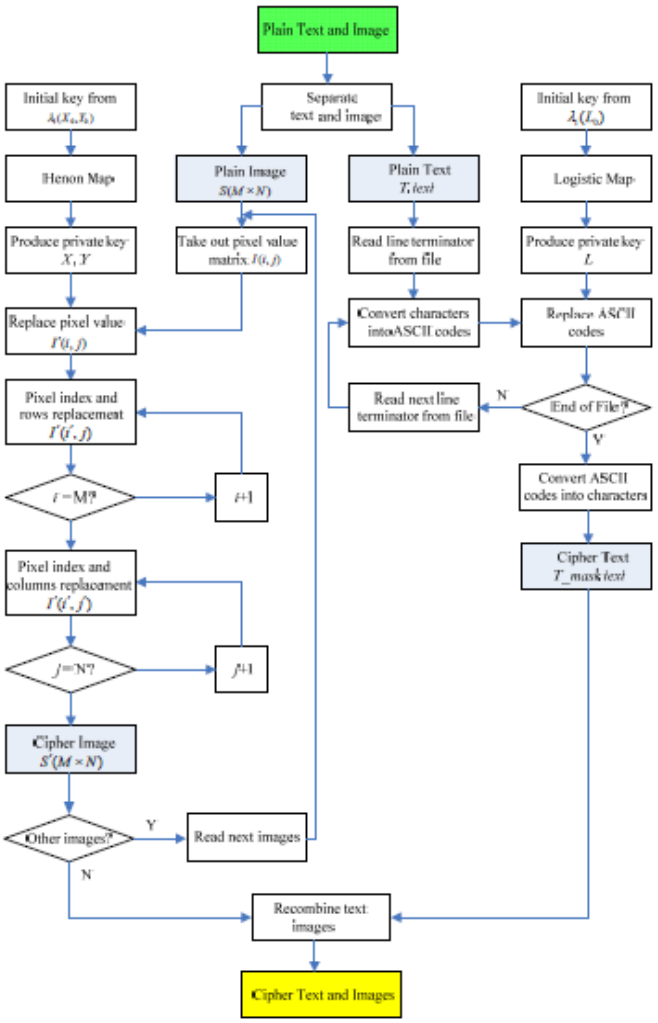


Figure 15: Flow chart of the chaotic encryption algorithm.

Case 1: Figureure encryption and decryption

The physiological signals of the users were collected from the self-made portable instrument accompanied with a digital signal processing unit and analyzed in the LabView environment. For a qualified encryption system, the key serial should be able to Figureht against the brute-force attack. It should also be sensitive to the private key. A variety of simulation studies were conducted to test robustness of the proposed encryption system. Table 3 lists three representative images supported in the MATLAB image processing toolbox. Table 4 reveals

Items	Value	Description
N	1500	number of iterations
$\lambda_1(X_0, Y_0, L_0)$	0.01573	initial value formed by λ_1 of the encryption person
a	1.4	system parameter of Henon map
b	0.3	system parameter of Henon map
A	4	system parameter of logistic map

Table 2: Parameters of the chaotic functions for encryption and decryption.

Filename	Size	Color type
Liftingbody.png	512 × 512	8 bits grayscale
Canoe.tif	346 × 207	8 bits indexed
pears.png	732 × 486	24 bits RGB

Table 3: Different kinds of images.

Items	Value	Description
n	1500	number of iterations
$\lambda_1(X_0, Y_0, L_0)$	0.01487	initial value formed by λ_1 of the non-encryption person
a	1.4	system parameter Henon map
b	0.3	system parameter Henon map
A	4	system parameter of Logistic map

Table 4: Parameters of chaotic functions for decryption.

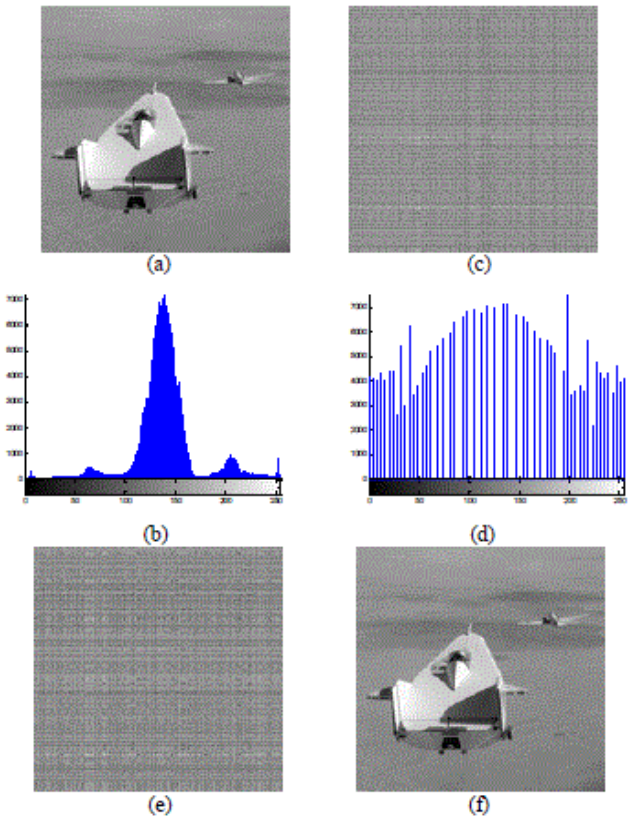


Figure 16: Encryption and decryption for Case 1 (a) original image (b) histograms of original image (c) encrypted image (d) histograms of encrypted image (e) incorrect decrypted image (f) correct decrypted image.

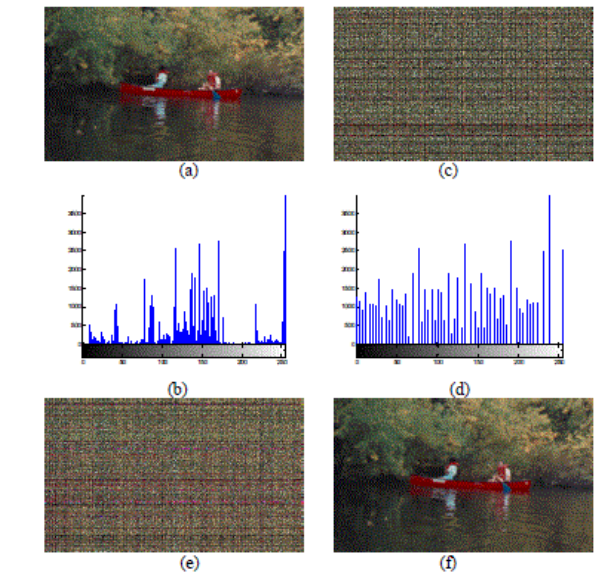


Figure 17: Encryption and decryption for Case 2 (a) original image (b) histograms of the original image (c) encrypted image (d) histograms of the encrypted image (e) incorrect decrypted image (f) correct decrypted image.

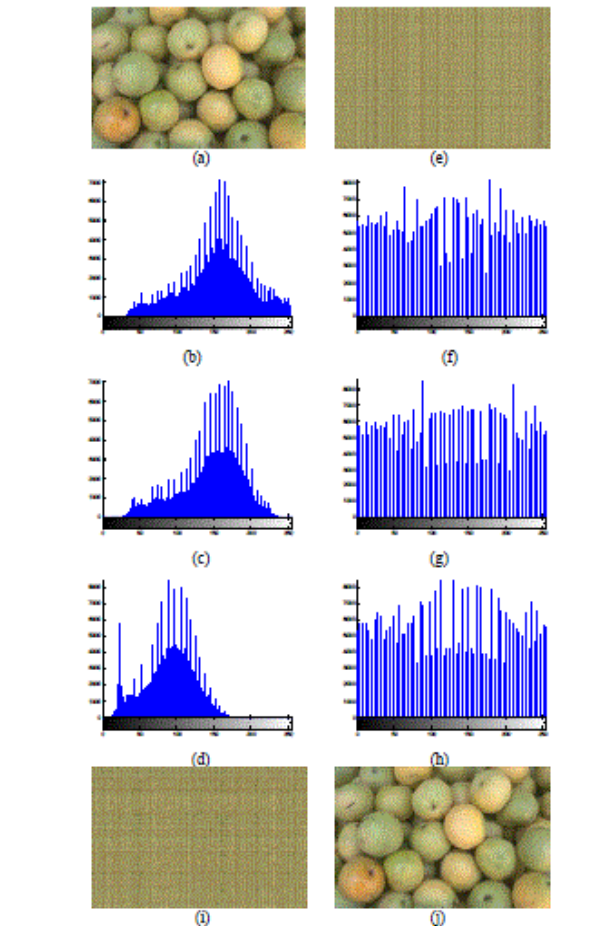


Figure 18: Encryption and decryption for Case 3 (a) original image (b)(c)(d) the histograms of red, green and blue channels of the original image respectively (e) encrypted image (f)(g)(h) histograms of red, green and blue colors of the encrypted image respectively (i) incorrect decryption (j)correct decryption.

that when the initial values changed to λ_1 for the non-encryption person, the decryption scheme generated a completely different decrypted result. Figures 16-18 display simulation results and histograms for three kinds of images. The image histogram illustrates how pixels in an image are distributed by graphing the number of pixels at the intensity level of color. The results of histogram analysis show an extremely different content in the original and encrypted images.

Case 2: Document blended with figures and text

We take Page 2 of this paper as the object of experiment, which contains text and Figures to be encrypted. We transform the formats of text and Figures into Text (.txt) file and Image (.png) file simultaneously. Figures. 19-21 show the demonstration that it incorporates the text encryption algorithm with Logistic map and the image encryption

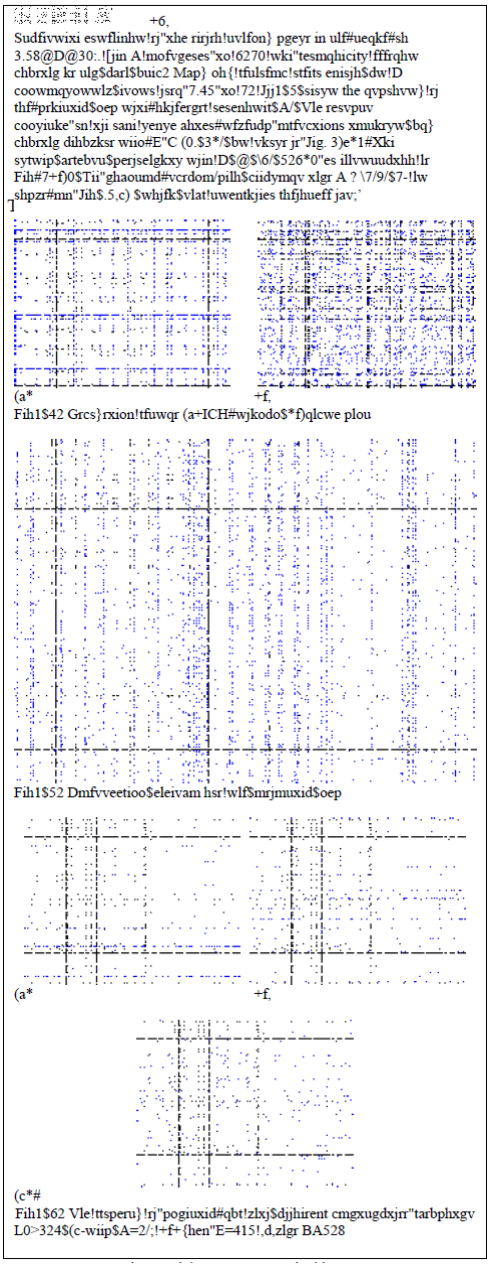


Figure 19: Ciphertext of Page 2 in this paper.

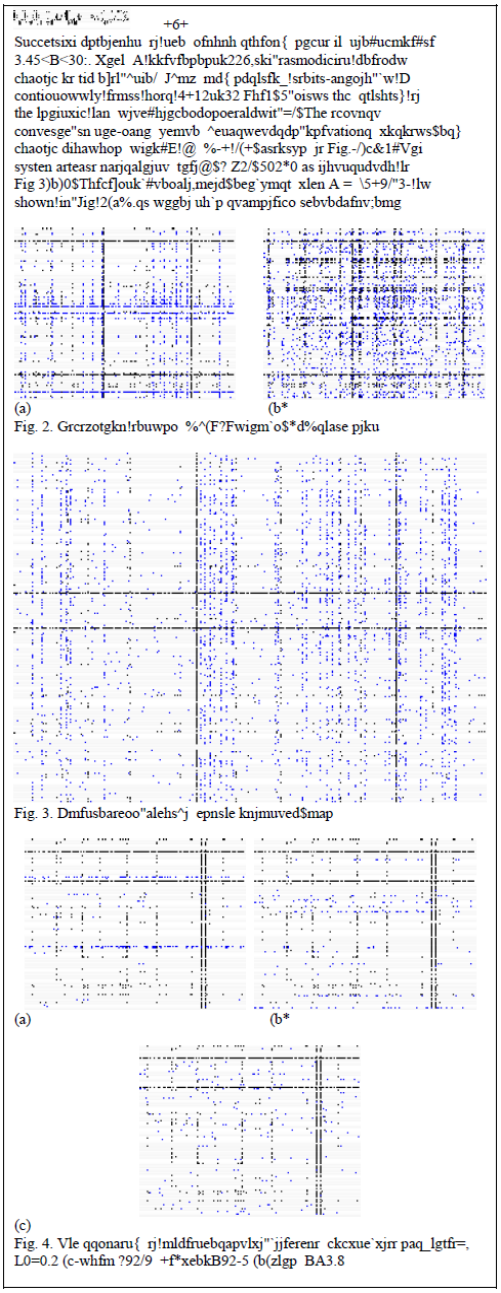


Figure 20: Wrong decrypted plaintext.

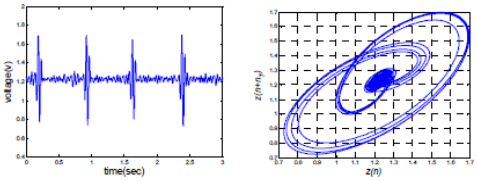
algorithm with Henon map. The encrypted plaintext is obviously non-readable, as shown in Figure 19. To compare the decrypted result of the chaotic encryption system, we chose an incorrect key and a correct one to activate the decryption algorithm. Figures. 20 and 21 show the results of decryption indicating that the proposed encryption system is quite sensitive to the key chosen and thus is appropriate for secure communication.

Conclusions

This paper has presented theoretical and experimental studies on chaos synchronization and masking of data communication using electronic devices that are described by the Lorenz equations, and showed

$L_{n+1} = AL_n(1-L_n)$ (2)

where n=0,1,2,…, $0 \le L \le 1$, $0 \le A \le 4$, A is a (positive) bifurcation parameter. Fig. 2 shows the bifurcation diagram of the logistic map in the range $1 \le A \le 4$ .When the vertical slice A=3.4, the iteration sequence splits into two periodic oscillations, which continues until A is slightly larger than 3.45. This is called periodic-doubling bifurcation in chaos theory. Successive doublings of the period quickly occur in the range of $3.45<A<3.6$. When A increases to 3.6, the periodicity becomes chaotic in the dark area. Many new periodic orbits emerge as A continuously grows from 3.45 to 4. Fig. 3 shows the property of



(a) (b)

Fig. 1. Encryption person (a)ECG signal (b)phase plot

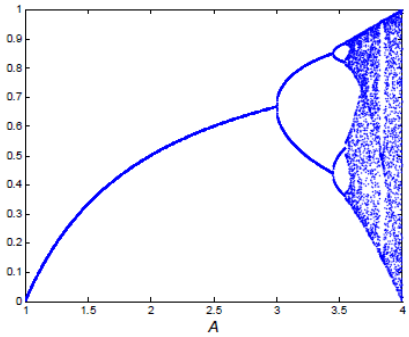
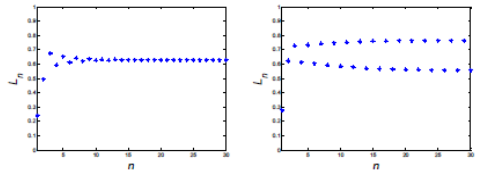
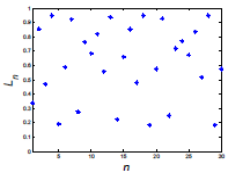


Fig. 2. Bifurcation diagram for the logistic map



(a) (b)



(c)

Fig. 3. The property of logistic map with different bifurcation parameter A, L0=0.1 (a)when A=2.7 (b)when A=3.1 (c)when A=3.8

Figure 21: Resulting (correct) decrypted plain text.

that the private key created by ECG signals can be recovered from a chaotic carrier using a response system whose chaotic dynamics is synchronized with a driver system. The use of ECG signal's features from nonlinear dynamic modeling for information encryption is investigated. A personalized encryption scheme based on the individual-specific features of ECG as a personal key is proposed. To decrypt the encrypted message that one needs a specific ECG message accompanied with our proposed encryption algorithm. The blended functionality yields a doubly encrypted scheme, which is extremely hard to be decrypted. Unlike traditional cryptographic algorithms, the presented approach features an infinite key space. This makes it an ideal key generator for encryption algorithms. Experimental results have proved feasibility and effectiveness of the proposed design. Moreover, the encryption time shows its potential applicability in real-time applications.

Acknowledgment

This research was sponsored by Ministry of Science and Technology, Taiwan, ROC under the grant 104-2622-E-005-011.

References

1. Chen TH, Wu CS (2010) Compression-unimpaired batch-image encryption combining vector quantization and index compression. Information Science 180: 1690-1701.
2. Kao YW, Huang KY, Gu HZ, Yuan SM (2013) uCloud: a user-centric key management scheme for cloud data protection. IET Information Security 7: 144-154.
3. Lu J, Wei Y, Fouque PA, Kim J (2012) Cryptanalysis of reduced versions of the Camellia block cipher, IET Information Security 6: 228-238.
4. Salleh M, Ibrahim S, Isnin IF (2003) Image encryption algorithm based on chaotic mapping, Journal Teknologi 39: 1-12.
5. Usama M, Khan MK (2008) Classical and chaotic encryption techniques for the security of satellite image. Proceedings of IEEE International Conference Biometrics and Security Technologies.
6. Alexopulos C, Bourbakis NG, Ioannou N (1995) Image encryption method using a class of fractals. Journal Electronic Imaging 4: 251-259.
7. Chen CK, Lin CL, Chiang CT, Lin SL (2012) Personalized information encryption using ECG signals with chaotic functions. Information Science 193: 125-140.
8. Chen CK, Lin CL (2010) Text encryption using ECG signals with chaotic logistic map. Proceedings of IEEE Conference Industrial Electronics and Applications.
9. Chen CK, Lin CL, Chiu YM (2010) Data encryption using ECG signals with chaotic Henon map. Proceedings of IEEE Conference Industrial Electronics and Applications.
10. Behnia S, Akhshani A, Mahmodi H (2008) A novel algorithm for image encryption based on mixture of chaotic maps. Chaos, Solitons and Fractals 35: 446-471.
11. Oliveira LPL, Sobottka M (2008) Cryptography with chaotic mixing. Chaos, Solitons and Fractals 35: 408-419.
12. Solak E, Cokal C (2011) Algebraic break of image ciphers based on discretized chaotic map lattices. Information Science 181: 227-233.
13. Zhu ZL, Zhang W, Wong KW, Yu H (2011) A chaos-based symmetric image encryption scheme using a bit-level permutation. Information Science 181: 1171-1186.
14. Jakimoski G, Kocarev L (2001) Chaos and cryptography: block encryption ciphers based on chaotic maps. IEEE Trans. Circuit and Systems-I: Fundamental Theory and Applications 48: 163-169.
15. Chen CK, Lin CL, Lin SL, Chiu YM, Chiang CT, et al. (2014) A chaotic theoretical approach to ECG-Based identity recognition. IEEE Computational Intelligence Magazine? 9: 53-63.
16. Lin SL, Chen CK, Lin CL, Yang WC, ChiangC T, et al. (2014) Individual identification based on chaotic electrocardiogram signals during muscular exercise. IET Biometrics 3: 257-266.
17. Biel L, Pattrsson O, Philipson L, Wide P (2001) ECG analysis: a new approach in human identification. IEEE Trans. Instrumentation and Measurement 50: 808-81.
18. Chiu CC, Chuang CM, Hsu CY (2009) A novel personal identity verification approach using a discrete wavelet transform of the ECG signal. International Journal of Wavelets, Multi-resolution and Information Process. 7: 341-355.
19. Israel SA, Irvine JM, Cheng A, Wiederhold MD, Wiederhold B K, et al. (2005) ECG to identify individuals, Pattern Recognition. 38: 133-142.
20. Singla SK, Sharma A (2010) ECG as biometric in the automated world. International Journal of Computer Science & Communication. 1: 281-283.

21. Loong J L C, Subari K S, Besar R, Abdullah M K (2010) A new approach to ECG biometric systems: a comparative study between LPC and WPD systems. Word Academy of Science, Engineering and Technology 68: 759-764.

22. Chen CK, Lin CL, Chiu YM (2011) Individual identification based on chaotic electrocardiogram signals. Proceedings of IEEE International Conference on Industrial Electronics and Applications.

23. Casalegio A, Braiotta S (1997) Estimation of Lyapunov exponents of ECG time series-the influence of parameters. Chaos, Solitons, and Fractals 8: 1591-1599.

24. Jovic A, Bogunovic N (2007) Feature extraction for ECG time-series mining based on chaos theory. Proceedings of International Conference Information Technology Interfaces.

25. Owis MI1, Abou-Zied AH, Youssef AB, Kadah YM (2002) Study of features based on nonlinear dynamical modeling in ECG arrhythmia detection and classification. See comment in PubMed Commons below IEEE Trans Biomed Eng 49: 733-736.

26. Pecora LM, Carroll TL (1990) Synchronization in chaotic systems. See comment in PubMed Commons below Phys Rev Lett 64: 821-824.

27. Pecora LM, Carroll TL (1991) Driving systems with chaotic signals. See comment in PubMed Commons below Phys Rev A 44: 2374-2383.

28. Lian KY1, Chiang TS, Chiu CS, Liu P (2001) Synthesis of fuzzy model-based designs to synchronization and secure communications for chaotic systems. See comment in PubMed Commons below IEEE Trans Syst Man Cybern B Cybern 31: 66-83.

29. Shih-Yu Li, Zheng-Ming Ge (2011) Fuzzy Modeling and Synchronization of Two Totally Different Chaotic Systems via Novel Fuzzy Model. See comment in PubMed Commons below IEEE Trans Syst Man Cybern B Cybern 41: 1015-1026.

30. Cheng CJ, Liao TL, Yan JJ, Hwang CC (2006) Exponential synchronization of a class of neural networks with time-varying delays. See comment in PubMed Commons below IEEE Trans Syst Man Cybern B Cybern 36: 209-215.

31. Cao J1, Chen G, Li P (2008) Global synchronization in an array of delayed neural networks with hybrid coupling. See comment in PubMed Commons below IEEE Trans Syst Man Cybern B Cybern 38: 488-498.

32. Xu WG, Shen HZ, Hu DP, Lei AZ (2005) Impulse tuning of Chua chaos. International Journal of Engineering Science 43: 831-844.

33. Kunin, I., Chemykh, G., Kunin, B: Optimal chaos control and discretization algorithms, Int. J. Eng. Sci. 44, 59-66 (2006).

34. Tsay SC, Huang C K, Qiu D L, Chen W T (2004) Implementation of bidirectional chaotic communication systems based on Lorenz circuits. Chaos, Solitons, and Fractals 20: 567-579.

35. Nana B, Woafo P, Domngang S (2009) Chaotic synchronization with experimental application to secure communications. Communications Nonlinear Science Numerical Simulation 14: 2266-2276.

36. Pehlivan I, Uyaroglu Y, Yogun M (2010) Chaotic oscillator design and realizations of the Rucklidge attractor and its synchronization and masking simulation. Scientific Research and Essays 5: 2210-2219.

37. Nana B, Woafo P (2011) Synchronized states in a ring of four mutually coupled oscillators and experimental application to secure communications. Communications Nonlinear Science Numerical Simulation 16: 1725-1733.

38. Wolf A, Swift J B, Swinney H L, Vastano J A (1985) Determining Lyapunov exponents from a time series. Physics Letter 16: 285-317.

39. May RM (1976) Simple mathematical models with very complicated dynamics. See comment in PubMed Commons below Nature 261: 459-467.

40. Henon M (1976) A two-dimensional mapping with a strange attractor. Communication in Mathematical Physics 50: 69-77.

41. Lorenz EN (1963) Deterministic nonperiodic flow. Journal of Atmospheric Sciences 20: 130-141.

42. Ge ZM, Tsen PC (2008) Chaos synchronization by variable strength linear coupling and Lyapunov function derivative in series form. Nonlinear Analysis 69: 4604-4613.

43. Dialecii JL, Krein MG (1974) Stability of differential equations in Banach space, AMS, New York.

44. Chiang CT (2005) Contact Type Pulse Measurement Device. USA Patent NO. US6945940B1.

45. Leonov G, Bunin A, Koksch N (1987) Attractor localization of the Lorenz system. ZAMM 67: 649-56.