Secure Communications Based on Dual Synchronization of Cross - Coupled Different Chaotic Oscillators

Fadhil Rahma Tahir
University of Basrah, College of Engineering,
Department of Electrical Engineering,
Basrah-Iraq

Abstract
The dual synchronization of two different pairs of chaotic oscillators: one pair of Duffing oscillators and one pair of Murali-Lakshmanan-Chua (ML-Chua) circuits, has been achieved by numerical simulations. The cross coupling method, where the difference in the voltage between the sum of the of the two master oscillators voltages and one of the slave oscillator voltage is injected to the other slave oscillator as an electrical current, for the dual synchronization has been used. The accuracy of synchronization of chaos is numerically obtained by calculating the root mean square error (RMSE). A communication scheme is presented, utilizing the chaotic masking (CMS) technique. Encoding and decoding of a message based on dual synchronization of chaos has been demonstrated.

Keywords: secure communications, synchronization of chaos, electronic circuits.

ألاتصالات المُحْكَمة على قاعِدة التزامن المزدوج لمذبذبات فوضوية مختلفة ذات ترابط متقاطع

فاضل رحمة طاهر
قسم الهندسة الكهربائية، كلية الهندسة، جامعة البصرة،
البصرة – العراق

الخلاصة:

تم انجاز المحاكاة العددية للتزامن المزدوج (dual synchronization) لزوجين مختلفين من المذبذبات الفوضوية (chaotic oscillators) : زوج لمذبذب دافنك (Duffing oscillator) وزوج لدائرة مورلي - لاكشمانان - جوا - (Murali Lakshmanan-Chua circuit). استخدمت طريقة الترابط المتقاطع (cross coupling) لانجاز التزامن المزدوج، حيث أن فرق الفولتيات بين المجموع لاخراج فولتيات مذبذبات المتبوع (master oscillators) واخراج احد مذبذبات التابع (slave oscillators) يُحقن إلى المذبذب التابع الآخر (slave oscillator) كتيار كهربائي. دقة التزامن للفوضى (accuracy of chaos synchronization)، حُررت عدديا بحساب جذر معدل التربيع للخطأ Root Mean Square Error (RMSE) . قُدم في هذا البحث نظام الاتصالات الذي استخدم تقنية القناع الفوضوي(chaotic masking). تم أظهار التشفير واعادة فك الشفرة لرسالة مُرسلة على أساس التزامن المزدوج للفوضى.

I-Introduction

Chaos synchronization has attracted interest for its potential applications to secure communications and spread spectrum communications [1-5]. Synchronization is process wherein two or more systems adjust a given property of their motion to common behavior, due to the coupling or forcing [6]. Chaos synchronization was initially focused in unidirectional coupled systems [1]. The reason beyond this fact could be that, for technical applications, it is interesting to reproduce the state of a certain chaotic system, no matter the distance or the number of the replica systems [7]. This kind of configuration is commonly known as master-slave configuration and is the most extended technique to synchronize chaotic systems [8-10].

However, in the most of previous works, the configuration of chaotic synchronization is limited to the single pair of one way – coupled chaotic systems. From the nonlinear dynamic point of view, synchronizing chaos in multiple pairs of one way – coupled oscillators is a very interesting topic, which is related to identification of chaos from mixed chaotic waveforms [11]. The synchronization of multiple pairs of one way – coupled chaotic oscillators offers advantage for application in the multi users communications. The multiple pairs of chaotic oscillators can be synchronized through single channel. To synchronize each pair of chaotic oscillators, all parameters values must be identical between the drive and response systems. The coupling signal is a sum of the waveforms from each of the drive oscillators. The response oscillators synchronize to their corresponding in the drive system. This form of synchronization becomes a multiplexing scheme when chaotic waveforms are information carrier [12].

This paper, discusses the dual synchronization of chaos based on two totally different pairs, one Duffing oscillator [13] pair and Murali-Lakshmanan-Chua (ML-Chua) circuit pair [14]. Numerical simulation of dual synchronization of the chaotic signals based on the two different systems are shown for demonstration. Also, this paper presents the communication scheme by using dual synchronization of chaos and its application for data transmission.

The paper is organized as follows: In section II the system configuration is described . In section III, the state equations that govern the whole system are derived. Also, the simulation results are given in section III. Section IV discuss the chaos communications. A brief conclusion is given in Section V.

II-Dual Synchronization Configuration

The block diagram for the dual synchronization configuration of one Duffing oscillators pair and one ML-Chua circuits pair are plotted in fig.(1a). One Duffing oscillator and one ML-Chua circuit used as master oscillators, which are referred as for master1 and master2, respectively. The other Duffing oscillator and ML-Chua circuit are used as slave oscillators (slave1 and slave2). The cross coupling method is used. The voltages in two master oscillators are combined as a transmission signal, $V_{m1}+V_{m2}$, and the signal is transmitted through a channel to the slave oscillators. In the front of the one oscillator, the transmitted signal is subtracted by the voltage of the other salve oscillators. The injection signal is written as $V_{m1}+V_{m2}-V_{s2}$ for slave1 oscillator, and $V_{m1}+V_{m2}-V_{s1}$ for the slave2 oscillator. For slave1, The injection signal is equal to V_{m1} under the condition of the synchronization between master2 and slave2, because V_{s2} component cancels the V_{m2} component from the mixed signal $V_{m1}+V_{m2}$. This

[11]D. L. Donoho and I. M. Johnstone, " Adapting to Unknown Smoothness via Wavelet Shrinkage", *Journal of American Statistical Association*, 90(432): 1200 -1224, December 1995.

[12]A. Antoniadis and J. Bigot, "Wavelet Estimators in Nonparametric Regression: A Comparative Simulation Study", *Journal of Statistical Software*, Vol.6, 2001.

[13]R. Rangarajan, R. Venkataramanan and S. Shah, " Image Denoising Using Wavelets ", December 16,2002.
http://www.personal.engin.umich.edu/~rvenkata/551_code/Report.pdf

[14]S. G. Chang, B. Yu and M. Vetterli, "Adaptive Wavelet Thresholding for Image Denoising and Compression", *IEEE Trans. Image Processing*, Vol. 9, No. 9, pp. 1532-1546, September 2000.

[15]F. Zhe Ren and H. Zhou, "The Fixed –Phase Iterative Algorithm Recovery of Blurred Image", ICSP, 2000.

[16]H. A. Jwad, " A Novel Approach for Restoration of Blurred Images ", M. Sc. Thesis Submitted to The Department of The Computer Engineering, University of Basrah ,May 2004.

[17]"Digital Image Processing in Natural Sciences and Medicine"
http://as.ch/DIP/Manual/1WinterSemester/DIP-Part-01(6-11).pdf.

[18]J. G. Brankov, J. Djordjeric, M. N. Wernick and N. P. Galatsanos, " Tomographic Image Reconstruction for System with Partially-Known Blur", Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, USA, 1999.

[19]P. G. Nikolas, " Multichannel Regularized Iterative Restoration of Motion Compensated Image Sequences", M. Sc. Thesis Submitted to The Department of Electrical and Computer Engineering, University of Northwestern, March 1995.

[20]X.Miao,"Image Restoration:Removal of Blur Caused by Uniform Linear Motion", University of California at Berkeley , 2000.
http://www.cnr.berkeley.edu/~miaoxin/research/deblurring/Deblurring.htm

[21]K. K. Aggelos, "Iterative Image Restoration Algorithm", Optical Engineering, Vol. 28, No. 7, pp. 735-748, July 1989.

[22]H. H. Abdul Zahrah, " Encryption Using Wavelet Coded Image Data ", M. Sc. Thesis Submitted to The Department of The Computer Engineering, University of Basrah, June 2004.

equivalent to one - pair system and the dual synchronization can be achieved.

Figure(1b) shows the schematic of the four chaotic circuits used in present simulation of the dual synchronization configuration. The subscripts m1, m2, s1, s2 of the parameters indicate the master1 , master2, slave1, and slave2 oscillators, respectively. The combined signal is injected to subtractor, through an ideal channel, in order to subtract a voltage V_{s1} and V_{s2} in front of slave2 and slave1 circuits, respectively. The electrical current is injected into the capacitor of each slave circuit through the coupling resistor $R_{c.du}$ and $R_{c.ch}$, respectively. The amount of current can be controlled by coupling resistor R_c.

III-Numerical Simulations

A-Model

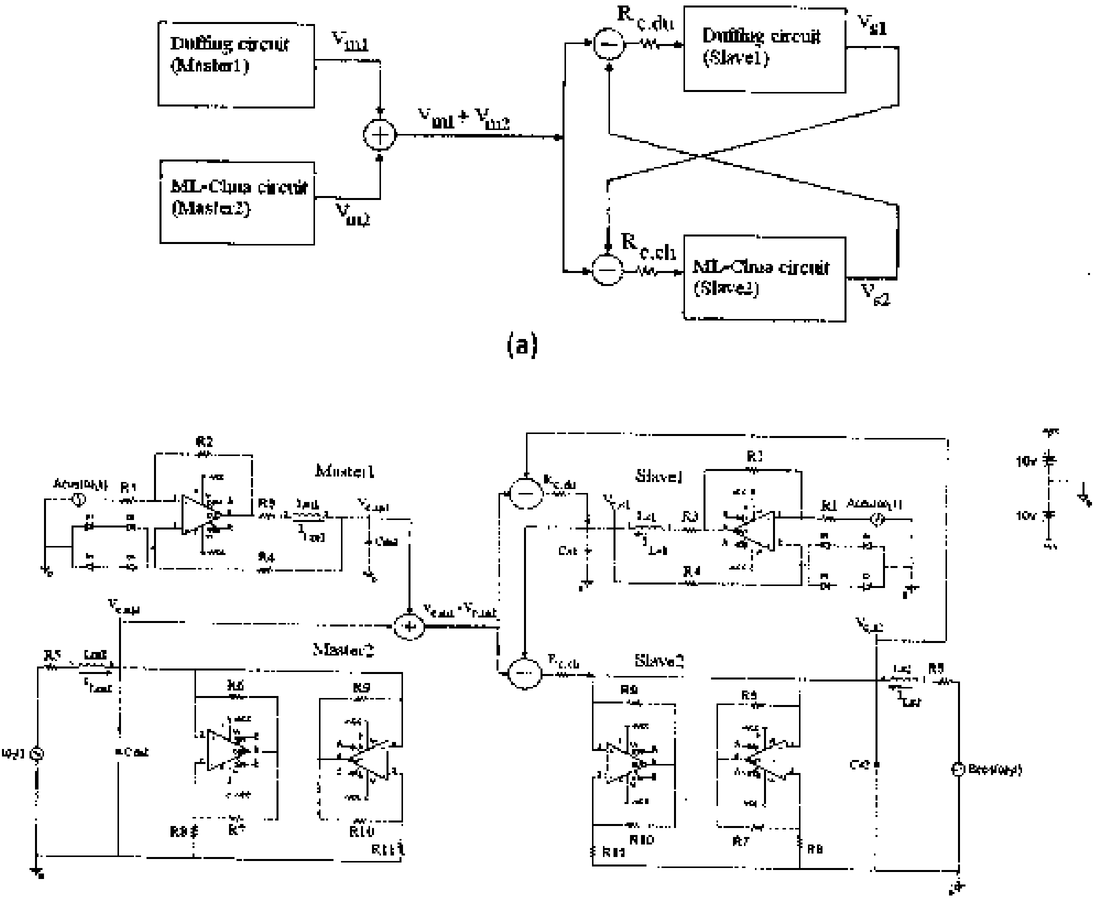
The four circuits shown in fig.(1b), can be described by the nonautonomous state equations as follows:

- Duffing Oscillator [13]

-Master1:

$$Cm1\frac{dV_{c,m1}}{dt} = I_{L,m1}$$

$$Lm1\frac{dI_{L,m1}}{dt} = f\left(V_{c,m1}\right) - R_3 I_{L,m1} + \frac{R_2}{R_1}A\cos(\omega_1 t - \pi) \qquad (1)$$



(a)

(b)

Figure 1.(a) Block diagram and (b) Schematic of dual synchronization of chaos in one Duffing circuit pair and one ML-Chua circuit pair.

-Slave1:

$$Cs1\frac{dV_{c,s1}}{dt}=I_{L,s1}+\frac{(V_{c,m1}+V_{c,m2}-V_{c,s1}-V_{c,s2})}{R_{c,du}}$$

$$Ls1\frac{dI_{L,s1}}{dt}= f(V_{c,s1})-R_3I_{L,s1}+\frac{R_2}{R_1}A\cos(\omega_1t-\pi) \quad (2)$$

In (1) and (2), the nonlinear function f(.) can be given by a piecewise linear approximation:

$$f(V_c)=\begin{cases}-\left(1+\frac{R_2}{R_1}\right)(V_c-2V_\gamma) & ,V_c>2V_\gamma\\ \frac{R_2}{R_1}V_c & ,-2V_\gamma\le V_c\le 2V_\gamma\\ -\left(1+\frac{R_2}{R_1}\right)(V_c+2V_\gamma) & ,V_c<-2V_\gamma\end{cases} \quad (3)$$

- ML-Chua Circuit [14]:

-Master2:

$$Cm2\frac{dV_{c,m2}}{dt}=I_{L,m2}-g(V_{c,m2})$$

$$Lm2\frac{dI_{L,m2}}{dt}=-R_5I_{L,m2}-V_{c,m2}+B\cos(\omega_2t) \quad (4)$$

-Slave2:

$$Cs2\frac{dV_{c,s2}}{dt}=I_{L,s2}-g+\frac{(V_{c,m1}+V_{c,m2}-V_{c,s1}-V_{c,s2})}{R_{c,ch}}$$

$$Ls2\frac{dI_{L,s2}}{dt}=-R_5I_{L,s2}-V_{c,s2}+B\cos(\omega_2t) \quad (5)$$

In (4) and (5), the function g(.) is the nonlinear current-voltage characteristic of the negative resistor (NR) in the ML-Chua circuit and is given by the following piecewise linear approximation [15]:

$$g(V_c)=G_bV_c+\frac{1}{2}(G_a-G_b)[|V_c+E|-|V_c-E|] \quad (6)$$

B- Results

In the present simulation, the master and slave systems of each pair have identical values for circuits parameters. For the Duffing oscillators pair, the values of circuit parameters used in the simulation are Cm1=Cs1=47nf, Lm1=Ls1=35mH, $R_1=R_2=R_4=10k\Omega$, $R_3=20\Omega$, A=0.38V, $\omega_1=2\pi(1000)$ rad.s^{-1}, $V_\gamma=0.5$. For ML-Chua circuits pair: Cm2=Cs2=10nf, Lm2=Ls2=18mH, $R_5=1.34k\Omega$, B=0.2V, $\omega_2=2\pi(6300)$rad.s^{-1}. The values of the parameters for negative resistor (NR) in are: $R_9=R_{10}=220\Omega$, $R_{11}=2.2k\Omega$, $R_6=R_7=22k$, $R_8=3.3k\Omega$, $G_a=-7.6*10^{-4}$, $G_b=4.1*10^{4}$, and E=1.

The initial conditions for the whole system are listed as follows:

Master1: $(V_{c,m1}(0),I_{L,m1}(0))=(1,1,0)$

Slave1: $(V_{c,s1}(0),I_{L,s1}(0))=(1,0)$

Master2: $(V_{c,m2}(0),I_{L,m2}(0))=(0.3,0)$

Slave2: $(V_{c,s2}(0),I_{L,s2}(0))=(0.1,0)$.

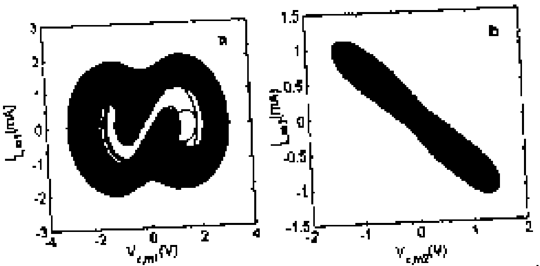


Figure 2. Double band chaotic attractor of (a) Duffing circuit and (b) ML-Chua circuit.

The fourth order Runge-Kutta method with variable step size is used to simulate the system. Without coupling between the master and slave oscillators, the Duffing oscillator and ML-Chua circuit, exhibit chaotic oscillations. In fig.(2), the phase portrait chaotic attractors generated by the tow circuits are reported. Figure(2a) refers to Duffing oscillator, while fig.(2b) refers to ML-Chua circuit.

With coupling between the master and slave oscillators, to investigate the accuracy of chaos synchronization, the root mean square error (RMSE) is obtained by the simulation of the following equation:

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(V_{c,mi} - V_{c,si}\right)^2} \qquad (7)$$

Where N is the number of the sample of the temporal waveforms $V_{c,mi}$ and $V_{c,si}$ of the corresponding master and slave oscillators at the i_{th} sampling point. The investigation of the accuracy of the synchronization achieved when the value of the coupling resistor R_c is varied. Figure(3) shows the RMSE for the pairs master1 - slave1 and master2 - slave2 as a function of R_c. The RMSE decreased with decreases R_c from 700Ω. The minimum RMSE is obtained at $R_c = R_{c,du} = 172.5Ω$ and $R_c = R_{c,ch} = 270Ω$ for the slave1 (Duffing circuit) and slave2 (ML-Chua circuit), respectively.

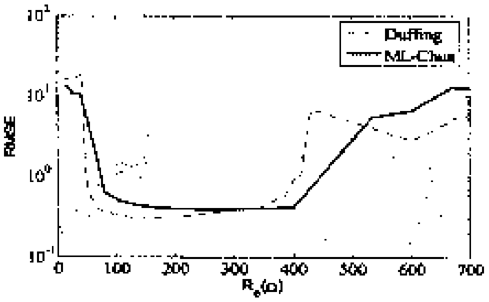
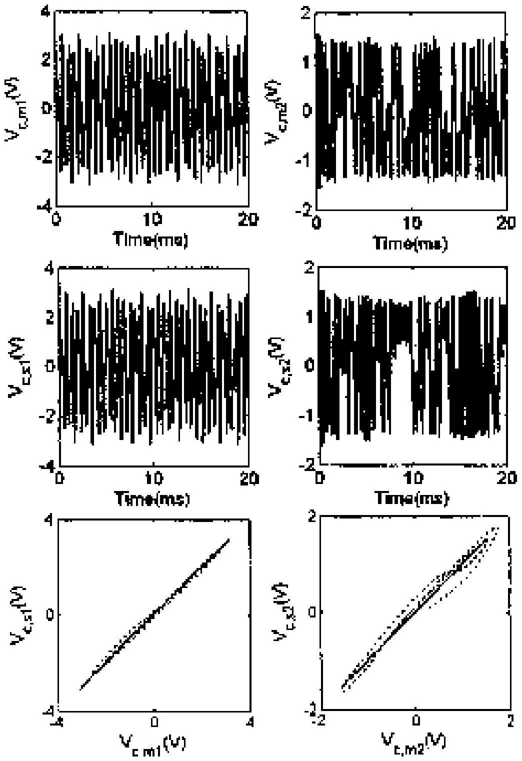


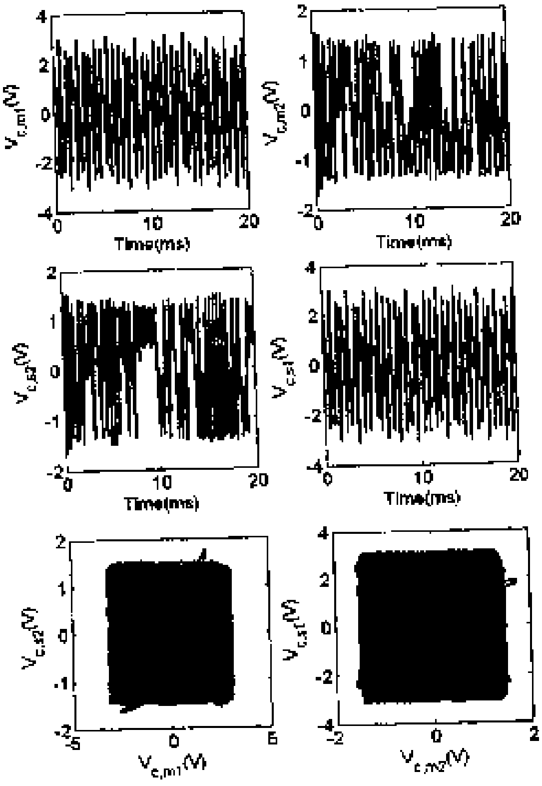
Figure 3. Root mean square error (RMSE) for the pairs master1-slave1 (Duffing) and master2-slave2 (ML-Chua) as a function of coupling resistor.

Dual synchronization of the chaotic oscillator is achieved for the pairs master1-slave1 and master2-slave2 as shown in figs.((4a)and (4b)). Conversely, the different pairs of circuits for master1-slave2 and master2-slave1 are not synchronized to each other as shown in figs.((4c)and(4d)). Figure(5) shows the temporal waveforms of the synchronization error within each pair. Also, the results confirmed that the current I_L in the eqns.(1) and (2) are also synchronized between the two corresponding circuits as shown fig.((5b) and(5d)).Although the systems are initially desynchronized, the synchronization



(a) (b)

Figure 4. Temporal waveforms and their correlation plots of V_c for: (a) the pair master1-slave1 and (b) the pair master2-slave2.



(c) (d)

Figure 4. Continue: (c) the different pair master1-slave2 and (d) the different pair master2-slave1.

is rapidly achieved with a settling time of about 1.5 ms. Figure (6) reveal that the temporal waveform of the transmission signal $V_{m1}+V_{m2}$ and their correlation plots with the output of slave1 and slave2, respectively. No linear correlation is observed between the transmission signal and the output signals of slave1 and slave2 as shown in figs.((6b)and (6c)), respectively.

IV- Application In Communications

Many strategies of chaos communication schemes has been proposed, such as chaotic masking scheme (CMS), chaotic shift keying (CSK), and chaotic modulation (CM). The chaotic masking scheme consists of two identical chaotic systems in both the transmitter and receiver, a chaotic signal added to the message to obtain the coded message and the synchronized receiver can recover the original message by simply subtracting the chaotic masking signal [16].

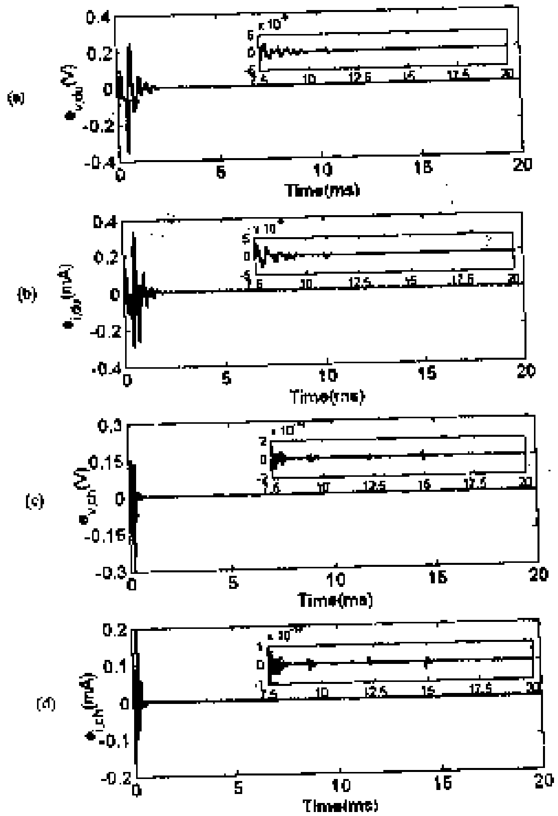


Figure 5. Temporal waveform of the error in the pair of Duffing circuits ((a) and (b)) and in the pair of ML-Chua circuits ((c) and (d)). $e_{v,du}=V_{c,m1}-V_{c,s1}$, $e_{i,du}=I_{L,m1}-I_{L,s1}$, $e_{v,ch}=V_{c,m2}-V_{c,s2}$, and $e_{i,ch}=I_{L,m2}-I_{L,s2}$.

Figure (7) demonstrates a communication scheme using the chaotic masking based on the dual synchronization of chaos. A message is coded by externally adding on each chaotic carrier of master1 (V_{m1}) or master2 (V_{m2}) independently. The coded message of each pair is delivering in additional transmission line. Also, the mixture of two chaotic waveforms between master1 and master2 is delivering

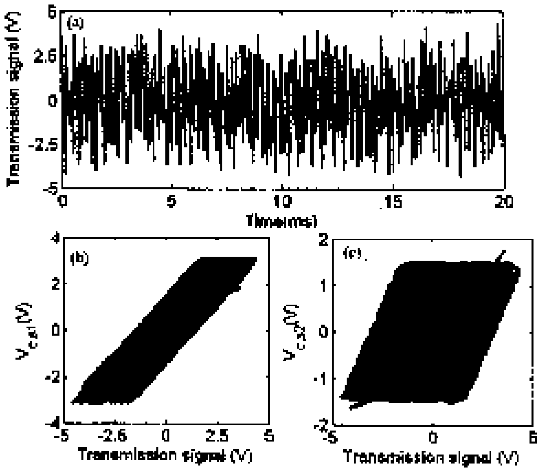


Figure6. (a)Temporal waveform of transmission signal $V_{m1}+V_{m2}$. (b) and (c) the correlation plots of transmission signal $V_{m1}+V_{m2}$ with the output of slave1 and slave2, respectively.

in additional transmission line in order to achieve the dual synchronization. Although all the transmission channels are accessibly by stealthier, the original message cannot be decoded without separating the two chaotic waveforms between master1 and master2.

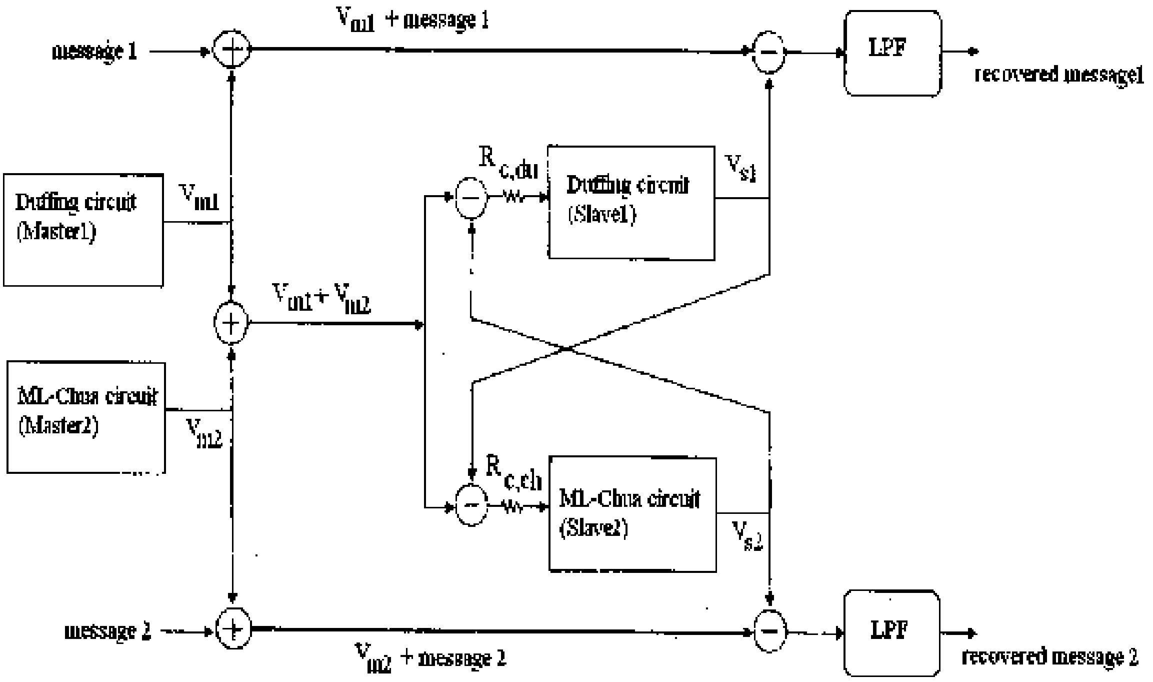
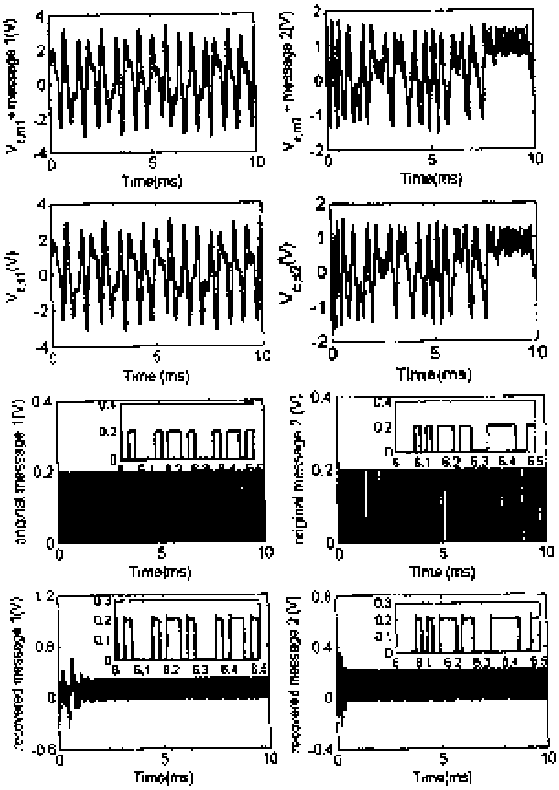


Figure 7. Block diagram of communication scheme (CMS) based on dual synchronization of chaos.



(a) (b)

Figure8. Message encoding and decoding. Top to bottom: Temporal waveforms of Master output + message, salve output, original message, and recovered message after filtering for the pair of : (a) Duffing oscillators and (b) ML-Chua circuits.

Figure (8) depicts the simulation results of encoding and decoding the message for two pairs (Duffing and ML-Chua). The message 1 was a $2^7 - 1$ (1001001) pseudo – random (PN) code, about of 6% from chaotic carrier ($V_{c,m1}$), at 40 Kbits/s. The message 2 was $2^6 - 1$ (101001) pseudo – random (PN) code, about of 13% from chaotic carrier ($V_{c,m2}$), at 50 Kbits/s. The top trace is the transmitted coded message. The second trace is the slave output , which is due to the dual synchronization and equal to the master output before the addition of the message. The third trace is the original message. The message is decoded by subtracting the salve output (second trace) from the received coded signal (first trace). The quality of the subtracted signal can be improved by the application of a fifth – order Butterworth low pass filter, and the original message can be recovered (bottom trace).

V-Conclusion

The dual synchronization of chaos in two totally different pairs one pair of Duffing oscillators and one pair of ML-Chua circuits is achieved simultaneously. The dual synchronization has been achieved by using one way – coupling between master and slave systems. The cross coupling method is used, where the difference in the voltage between the sum of the two master circuits and one slave circuit is injected into other slave circuit as an electrical current , for dual synchronization of chaos. The accuracy of the synchronization is investigated, and the results give the values of the coupling resistor that required for achieving dual synchronization of chaos. Also, the communication scheme using dual synchronization of chaos has been demonstrated. It has been shown by numerical simulations that the message encoding and decoding can be performed by using chaotic masking technique. A message (pseudo-random: PN code) is successfully recovered when dual synchronization of chaos is achieved.

References

[1]L. Pecora and T. L. Carrol, "Synchronization in Chaotic Systems", Phys. Rev. Lett. 64,821 (1990).

[2]N. Shibasaki, A. Uchida, S. Yoshimori, and P. Davis, " Characteristic Of Chaos Synchronization in Semiconductor Lasers Subject to Polarization Rotated Optical Feedback" ,IEEE Journal of Quantum Electronics, Vol.42, No. 3, 342-350,2006.

[3] G. Àlvarez, S. Li, F. Montoya, G. Pastor, And M. Romera," Breaking Projective Chaos Synchronization Secure Communication Using

Filtering and Generalized Synchronization", Chaos Silton and Fractals 24, 775-783, 2005.

[4] F. Lau,C. Tse, M. Ye, and S. Hua, " Coexitance of Chaos Based on Convential Digital Communication Systems of Eqial Bit Rate ", IEEE Transactions on Circuit and Systems-I, Regulars Papers, Vol.51, No. 2, 2004.

[5] C. Robilliard, E. H. Huntington, and M. R. Frater, " Digital Transmission for Improved Synchronization of Analog Chaos Generator in Communication Systems", Chaos 17, 023130(1-7), (2007).

[6] A. Caneco, C. Gràcio, and J. Rocha, " Symbolic Dynamics and Chaotic Synchronization in Coupled Duffing Oscillators", Journal of Nonlinear Mathematical Physics, Vol. 15, Supplement 3, 102-111, 2008.

[7] A. Wagemaker, J. M. Buldú, and M. A. Sanjuán," Isochronous Synchronization in Mutually Coupled Chaotic Circuits", Chaos 17, 023128(1-7), (2007).

[8] D. Huang, "Multiparameter Estimation Using only A Chaotic Time Series and Its Applications", Chaos 17, 023118(1-9) (2007).

[9] C. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos, " Synchronization of Two Mutually Coupled Duffing-Type Circuits", International Journal of Circuits, Systems and Signal Processing, Issue 3, Vol 1,274-281, 2007.

[10] Y. Xiao, W. Xu, X. Li, and S. Tang, "Adaptive Complete Synchronization of Chaotic Dynamical Network With Unknown and Mismatched Parameters", Chaos 17, 033118(1-8), (2007).

[11]A. Uchida, M. Kawano, and S. Yoshimori, "Dual Synchronization of Chaos in Colpitts Electronic Oscillators and Its Applications for Communications", Physical Review E- 68, 056207(1-11), 2003.

[12]J. Blakely and N. Corron, " Multiplexing Symbolic Dynamics-Based Chaos Communications and Synchronization ", Journal of Physics: Conference Series 23, 259-266, 2005.

[13] E. Tamaševičiūte, A. Tamaševičius, G.Mykolaitis, S. Bumeliene, and E. Lindberg," Analogue Electrical Circuit for Simulation of The Duffing-Holmes Equation", Nonlinear Analysis: Modelling and Control, Vol. 13, No. 2, 241-252, 2008.

[14]S.Parthasarathy and K. Manikandakumar, " Multiple Period-Doubling Bifurcation Route to Chaos in Periodically Pulsed Murali – Lakshmanan - Chua Circuit-Controlling and Synchronization of Chaos" , Chaos 17, 043120(1-9), 2007.

[15]L. Chua and G. Lin, "Canonical Realization of Chua's Circuit Family", Ieee Transactions on Circuit and Systems, Vol.37, No. 7, 1990.

[16] W. Yu, J. Cao, K. Wong, and J. Lü, " New Communication Schemes Based on Adaptive Synchronization" , Chaos(17), 033114(1-13), 2007.