I.J. Mathematical Sciences and Computing, **2018, 1, 56-70**
Published Online January 2018 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijmsc.2018.01.04

Available online at http://www.mecs-press.net/ijmsc

A Secure Communication Scheme using Generalized Modified Projective Synchronization of Coupled Colpitts Oscillators

Kammogne Soup Tewa Alain[a*], Fotsin Hilaire Bertrand[a]

[a] *Laboratory of Condensed Matter-Electronics and Signal Processing (LAMACET), Department of Physics, Faculty of Sciences, University of Dschang, Cameroon. Tel: (+237) 675 52 25 59*

Received: 14 August 2017; Accepted: 16 October 2017; Published: 08 January 2018

Abstract

A new scheme for secure information transmission is proposed using the generalized modified projective synchronization (GMPS) method. The linear transformation of the modified Colpitts oscillator, first introduced in Cristinel and Radu (Low-Power Realizations of Secure Chaotic Communication Schemes. IEEE Asia Pacific Conference on Circuits and Systems, 2000) is investigated prior to the more detailed study by Kammogne et al. (Journal of chaos. (2014). doi: 10.1155/2014/659647). This circuit is employed to encrypt the information signal. In the receiver end, by designing the controllers and the parameter update rule, GMPS between the transmitter and receiver systems is achieved and the unknown parameters are estimated simultaneously. Based on the Lyapunov stability theory, the controllers and corresponding parameters update rule are constructed to achieve generalized modified projective synchronization between the transmitter and receiver system with uncertain parameters. The original information signal can be recovered successfully through some simple operations by the estimated parameter. The message signal can be finally recovered by the identified parameter and the corresponding demodulation method. Numerical simulations are performed to show the validity and feasibility of the presented secure communication scheme.

Index Terms: Chaotic system, Linear transformation, Generalized Modified Projective Synchronization (GMPS), Secure communication, Parameters estimation.

1. Introduction

The combination of synchronization and unpredictability leads to an interesting application: A secret message which is to be sent from a transmitter to a receiver (two identical MCO) is encoded in the chaotic

* Corresponding author. Tel.: (+237) 675 52 25 59
E-mail address: kouaneteoua@yahoo.fr

signal which is exchanged between these two partners. Since Pecora and Carroll [1] presented the conception of chaotic synchronization for two identical chaotic systems with different initial conditions, many synchronization methods have been proposed, such as complete synchronization (CS) [1], generalized synchronization [2], phase synchronization [3], impulse synchronization [4], lag synchronization [5], projective synchronization and fuzzy approach [6, 7, 8], etc. Amongst all kinds of chaos synchronization, projective synchronization, first reported by Mainieri and Rehacek [6], has been especially extensively studied because it can obtain faster communication with its proportional feature [9, 10, 11, 12].

Since the signal is chaotic, it is normally difficult even impossible to extract any message from it. This signal, however, synchronizes the transmitter system with the receiver which can immediately decode the message. Master-slave synchronization has many applications in technology such as in secured telecommunication [13-14]. It is well known that some researches today are most oriented to neural network synchronization [15-16] but the master-slave synchronization remains the benchmark of all methods encountered in the literature. So, it's not obvious to implement this scheme, but in fact communication by synchronized chaotic electronic circuits was demonstrated in 1993 by Cuomo and Oppenheim [17] and by Parlitz *et al*. [18]. These pioneering papers stimulated intensive research on communication with synchronized chaos which is still ongoing. The information signal is recovered through decoding in the synchronized receiver. The variables and the parameters of the response system can be the ciphered. We should note that a cryptosystem cannot exist without a key. The general hypothesis in telecommunication suppose that the cryptanalyst knows exactly the design and functioning of the cryptosystem under study, i.e., he knows every detail about the ciphering algorithm, but he does not possess any information about the secret key. This is an evident requirement in today's secure communications systems, usually referred to as *Kerckhoffs' principle* [19]. A typical assumption made by most chaotic cryptosystems' designers is that the system's parameters play the role of the key which is not efficient in many secure schemes. One way to handle this drawback is to design the controllers containing the key and the corresponding parameters update rule to achieve GMPS between the transmitter and receiver systems and estimate the unknown parameters simultaneously. Obviously, it is worthwhile to mention that some of these systems (master/receiver) have complex structure and require the knowledge of these parameters which may plays an important role in telecommunication. Therefore, parameters estimations remains a characteristic for an efficient secure scheme. Besides, it is obvious that practical controllers should have simple structures which is not the case of the controllers involving the projective method. In fact, the projective synchronization (PS) has been used in the research on secure communication because of the unpredictability of the scaling factor which may be a useful element (the key for example). In addition to our knowledge, in most of secure communication schemes [21], the message size is required to be sufficiently small, otherwise it may induce a chaotic system to be asymptotically stable or emanative, which may render the failure of recovering the emitted signal. So it's important to investigate how to transmit high amplitude message signals.

Recently, it has been shown that the modified Colpitts Oscillator (further called MCO) can exhibit complicated dynamics with reference to the classical Colpitts oscillator linked to its nonlinearity topology which is a great advantage in telecommunication. In general, the security of chaos-based communication systems is dependent on the complexity degree of master's dynamics, carrying signal as well as the encryption scheme used [22]. There are only a few studies in the synchronization of the MCO systems [23], though these systems are widely encountered in practice, in particular in communication. The experimental results presented by Ababai and Marculescu [24] performs much better compared to other implementations in terms of power dissipation, but at the present stage, it was be very difficult to estimated or to control the parameters of the Transmitter/Receiver. Specifically, motivated by the vulnerability to attacks of certain architectures and the role of the MCO in practice, the use of chaotic systems for data scrambling is thoroughly investigated using the GMPS.

In this paper, we will apply the adaptive control to design a secure communication scheme based on generalized modified projective synchronization. The message signal is added in the transmitted side. The scaling coefficient is taken as the parameter of the system to guarantee communication security.

The organization of this paper is as follows. In Section 2 we present the dynamical analysis linked to the transformation theory of the MCO. The section 3 is consecrated to the dynamical analysis of the system dynamic proposed. Problem formulation is relaxed. In section 4, a secure communication scheme via GMPS of the MCO system is proposed. The controllers and the parameter update rule are devised for obtaining the desired synchronization and identify the unknown parameter simultaneously. Numerical simulations are given to illustrate and validate the proposed communication scheme in section 5. Our conclusions are finally drawn in section 6.

2. Description of the MCO

The Colpitts circuit is easily modelled, easily realized and scalable in frequency. In 1994, the occurrence of chaos was first demonstrated in the Colpitts oscillator by [25]. Actually the chaotic dynamics produced by this oscillator is relatively well understood (see an interesting text in Ref. [22]).

An autonomous MCO chaotic system in Ref. [23] which is described by the following nonlinear differential equations:

$$\begin{aligned} \frac{dx}{d\tau} &= z - a_2 \exp(-az - by) \\ \frac{dy}{d\tau} &= -b_0 - b_0 y + z \\ \frac{dz}{d\tau} &= 1 - x - y - c_{11} z \end{aligned} \tag{1}$$

where x, y and z are state variables; and a, b, a_2, b_0, c_{11} are systems parameters. When $a = 2.251362,\ b = 192.3,\ b_0 = 0.1064814815, c_{11} = 0.934,\ a_2 = 8.518518.10^{-11}$, system (1) exhibits a chaotic behaviour. Its attractor is similar to Chen's attractor, as depicted in Fig. 1.

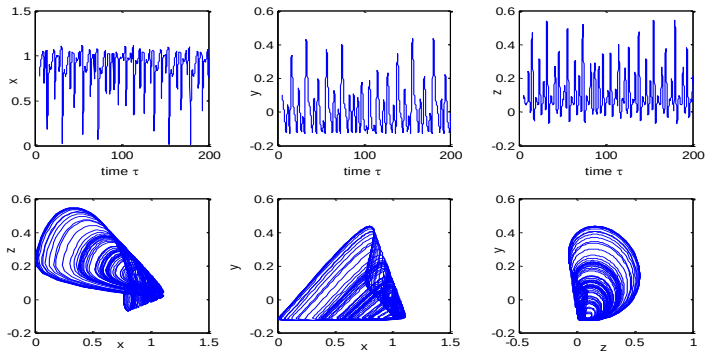


Fig.1. Trajectories and Chaotic Attractors of MCO.

3. Dynamical Approach of MCO

3.1. Transformation analysis of MCO

In order to quantify the parameters inside the exponential term argument, let introduce the coordinates change in state and output-space:

$$\left(z_1, z_2, z_3\right) = \left(x_1, e^{-bx_2}, e^{-ax_3}\right) \tag{2}$$

Derivatives in the considered space are given by

$$\left(\dot{x}_1, \dot{x}_2, \dot{x}_3\right) = \left(\dot{z}_1, -\frac{1}{b}\frac{\dot{z}_2}{z_2}, -\frac{1}{a}\frac{\dot{z}_3}{z_3}\right) \tag{3}$$

In these new coordinates, the system (1) takes the form

$$\begin{aligned} \dot{z}_1 &= -\sigma_1 \ln z_3 - \sigma_2 z_2 z_3 \\ \dot{z}_2 &= \sigma_3 z_2 - \sigma_4 z_2 \ln z_2 + \sigma_6 z_2 \ln z_3 \\ \dot{z}_3 &= \sigma_0 (z_1 - 1) z_3 - \sigma_7 z_3 \ln z_2 - \sigma_5 z_3 \ln z_3 \end{aligned} \tag{4}$$

with $\sigma_1 = \frac{1}{a}, \sigma_2 = a_1, \sigma_3 = bb_0, \sigma_4 = b_0, \sigma_5 = c_{11}, \sigma_0 = a$, $\sigma_6 = ba^{-1}, \sigma_7 = \sigma_6^{-1}$. The system (3) present five parameters as system (1) which confirms the linearity of transformation.

3.2. Existence and uniqueness of the solution

Let's defined a class of continuous $\psi(t)$ such that

$$C[0,T] \text{by } \|\psi\| = \sup_{t\in(0,T]} |\psi(t)|, \quad \psi(t) \in C[0,T] \tag{5}$$

System (4) can be written in the following form:

$$\dot{z} = \tilde{\phi}(z,\tau)\theta_1 + \tilde{\varepsilon}(z,\tau)\theta_2 + \sum_{i=1}^{p} \hat{\theta}_i \Omega_i \bar{\varepsilon}(z,\tau), \quad p = 2, \tag{6}$$

$$z(0) = z_0 \tag{7}$$

with

$$z = \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix}, \Omega_1 = \begin{bmatrix} 0 & 0 & -1 \\ 0 & -z_2 & 0 \\ 0 & 0 & -z_3 \end{bmatrix}, \Omega_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & z_2 \\ 0 & -z_3 & 0 \end{bmatrix}, \tilde{\phi}(z(\tau),\tau) = \begin{bmatrix} 0 \\ z_2 \\ -z_3 \end{bmatrix}, \bar{\varepsilon}(z(\tau),\tau) = \begin{bmatrix} \ln z_1 \\ \ln z_2 \\ \ln z_3 \end{bmatrix},$$
$$\tilde{\varepsilon}(z(\tau),\tau) = \begin{bmatrix} -z_2 z_3 \\ 0 \\ z_1 z_3 \end{bmatrix}, \theta_2 = \begin{bmatrix} \sigma_2 \\ 0 \\ \sigma_0 \end{bmatrix}, \theta_1 = \begin{bmatrix} 0 \\ \sigma_3 \\ \sigma_0 \end{bmatrix}, \hat{\theta}_1 = \begin{bmatrix} \sigma_1 \\ \sigma_4 \\ \sigma_7 \end{bmatrix}, \hat{\theta}_2 = \begin{bmatrix} 0 \\ \sigma_6 \\ \sigma_5 \end{bmatrix}$$

Theorem 1. *The sufficient condition for existence and uniqueness of the solution of system (6) with initial conditions* $z(0) = z_0$ in the region $\Omega \times J$ *is*

$$K = T_{\max}\left(\sigma_1 + \sigma_2, \sigma_3 + \sigma_4 + \sigma_6, \left(2\sigma_0 + \sigma_5 + \sigma_7\right)A^2\right)$$

Proof. The existence and uniqueness of the solution is studied in the region $\Omega \times J$ where $J = (0,T]$ and $\Omega = \left\{(z_1, z_2, z_3) : \max\left\{|z_1|, |z_2| \text{and } |z_3|\right\} \le A\right\}$ where A is a positive constant.

The solution of (6) and (7) is given by

$$z = z_0 + \int_0^t \left[\tilde{\phi}(z,s)\theta_1 + \tilde{\varepsilon}(z,s)\theta_2 + \sum_{i=1}^{p} \hat{\theta}_i \Omega_i \bar{\varepsilon}(z,s) \right] ds \tag{8}$$

From the equivalence of the integral equation (11) and the system (6)-(7), denoting the right hand side of (8) by *G(z)*, then

$$\begin{aligned} G(z') - G(z'') &= \int_0^t \left[\tilde{\phi}(z',s)\theta_1 + \tilde{\varepsilon}(z',s)\theta_2 + \sum_{i=1}^{p} \hat{\theta}_i \Omega_i \bar{\varepsilon}(z',s) \right] ds - \int_0^t \left[\tilde{\phi}(z'',s)\theta_1 + \tilde{\varepsilon}(z'',s)\theta_2 + \sum_{i=1}^{p} \hat{\theta}_i \Omega_i \bar{\varepsilon}(z'',s) \right] ds \\ &= \int_0^t \left[\left(\tilde{\phi}(z',s) - \tilde{\phi}(z'',s)\right)\theta_1 + \left(\tilde{\varepsilon}(z',s) - \tilde{\varepsilon}(z'',s)\right)\theta_2 + \sum_{i=1}^{p} \hat{\theta}_i \Omega_i \left(\bar{\varepsilon}(z',s) - \bar{\varepsilon}(z'',s)\right) \right] ds \\ &\le h_0 \|z' - z''\| \theta_1 + h_1 \|z' - z''\| \theta_2 + \sum_{i=1}^{p} \hat{\theta}_i \Omega_i \|z' - z''\| \\ &= \left(h_0\theta_1 + h_1\theta_2 + \sum_{i=1}^{p} \hat{\theta}_i \Omega_i \right) \|z' - z''\| \\ &= K \|z' - z''\| \end{aligned}$$

After some calculations, it's obvious that

$$K = T_{\max}\left(\sigma_1 + \sigma_2, \sigma_3 + \sigma_4 + \sigma_6, \left(2\sigma_0 + \sigma_5 + \sigma_7\right) A^2\right) \tag{9}$$

The following consideration can be made if $K > 1$, then then mapping (6) is a contraction mapping. The proof of *theorem 1* is complete.

3.3. Dissipation and existence of attractors

Preliminary insights concerning the existence of attractive sets that might coexist in the system could be gained by evaluating the volume contraction/expansion rate $\left(\Gamma = V^{-1} dV/d\tau\right)$ of the oscillator modelled by (1) at any given point $(z_1, z_2, z_3)^T$ of the space. The following expression can be derived:

$$\begin{aligned} \Gamma &= \frac{\partial \dot{z}_1}{\partial z_1} + \frac{\partial \dot{z}_2}{\partial z_2} + \frac{\partial \dot{z}_3}{\partial z_3} \\ &= \sigma_3 - \sigma_4 - \sigma_5 - \sigma_0 + \sigma_0 z_1 - \ln\left(z_2^{\sigma_4 + \sigma_7} z_3^{\sigma_5 - \sigma_6}\right) \\ &= \sigma_0 z_1 - \ln\left(\frac{z_2^{\sigma_4 + \sigma_7} z_3^{\sigma_5}}{\delta z_3^{\sigma_6}}\right) \end{aligned}$$

where $\ln\delta = \sigma_3 - \sigma_4 - \sigma_5 - \sigma_0$ and $\dot{z} = (\dot{z}_1, \dot{z}_2, \dot{z}_3)$.

Consider the fact that the system (4) is dissipative which is expressed as follows:

$$div(\dot{z}) = \sigma_0 z_1 - \ln\left(\frac{z_2^{\sigma_4+\sigma_7} z_3^{\sigma_5}}{\delta z_3^{\sigma_6}}\right) < 0 \tag{10}$$

This condition implies that the solutions of the new system are bounded as $\tau \to \infty$. We may rewrite the condition (10) as follows:

$$z_1 < \frac{1}{\sigma_0} \ln\left(\frac{z_2^{\sigma_4+\sigma_7} z_3^{\sigma_5}}{\delta z_3^{\sigma_6}}\right) \tag{11}$$

In fact, an infinitesimal deviation of the initial conditions will eventually result in the divergence of nearby starting orbits. After a while, the system initially unstable becomes dissipative and stays unchanged with respect to its dynamical variables which strongly justify the synchronization process of MCO in the space considered. Fig. 2 and 3 depicts the divergence of the flow (4) and the phase portrait in the new space.

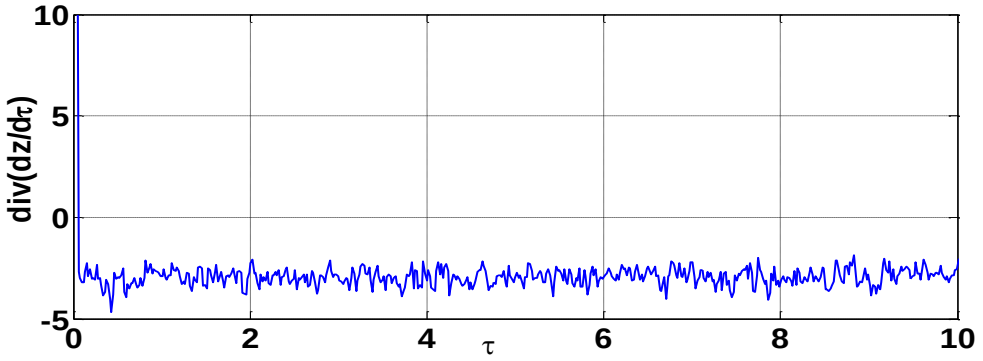


Fig.2. Divergence of the Flow of MCO in the New Space

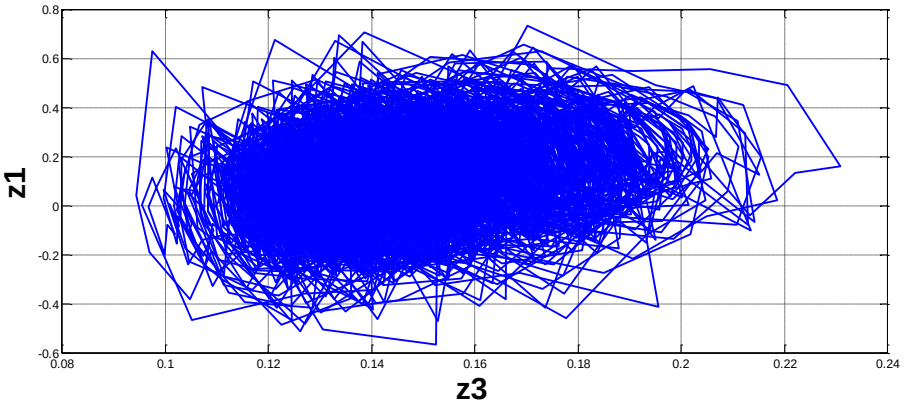


Fig.3. Phase Portrait of MCO in the New Space in the Presence of Artificial Pertubation.

4. A New Secure Communication Scheme via GMPS of the MCO

Consider the following driving system

$$\begin{aligned}\dot{z}_1(\tau) &= -\sigma_1 \ln z_3(\tau) - \sigma_2 z_2(\tau) z_3(\tau) + m(\tau)\\ \dot{z}_2(\tau) &= \sigma_3 z_2(\tau) - \sigma_4 z_2(\tau) \ln z_2(\tau) + \sigma_6 z_2(\tau) \ln z_3(\tau)\\ \dot{z}_3(\tau) &= \sigma_0 (z_1(\tau) - 1) z_3(\tau) - \sigma_7 z_3(\tau) \ln z_2(\tau) - \sigma_5 z_3(\tau) \ln z_3(\tau)\end{aligned} \tag{12}$$

$m(\tau)$ is the plaintext that is modulated into the chaotic driving system. Select the output $z_1(\tau)$ of the driving system (12) as the transmitted signal, then constructs the receiver as follows:

$$\begin{aligned}\dot{s}_1(\tau) &= -\sigma_1' \ln z_3(\tau) - \sigma_2' s_2(\tau) z_3(\tau) + p(\tau) + u_1\\ \dot{s}_2(\tau) &= \sigma_3' s_2(\tau) - \sigma_4' s_2(\tau) \ln s_2(\tau) + \sigma_6' s_2(\tau) \ln z_3(\tau) + u_2\\ \dot{p} &= -\beta(\alpha_1 s_1 - z_1)\end{aligned} \tag{13}$$

where β is the positive constant parameter.

The overall transmission scheme is presented below on Fig. 4.

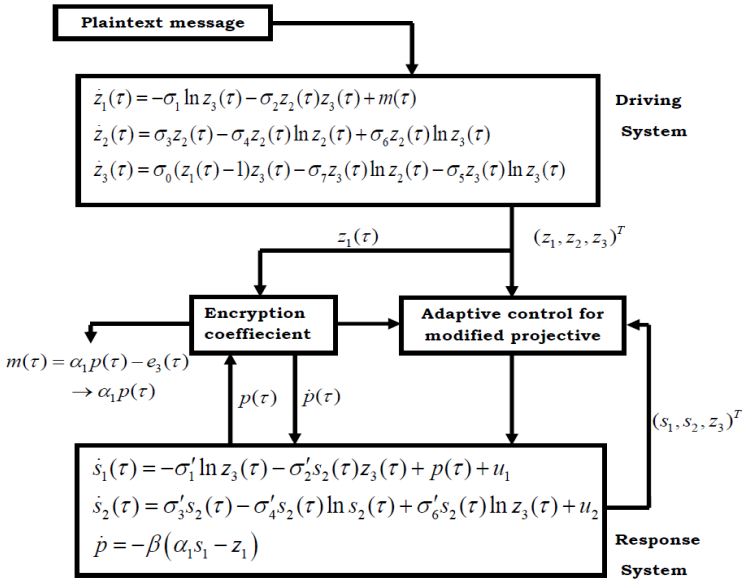


Fig.4 Block Diagram Illustrating the Proposed Secure Communications Scheme using GMPS

Let us consider the following state derivative errors.

$$\begin{cases} e_1 = \alpha_1 s_1 - z_1, \\ e_2 = \alpha_2 s_2 - z_2, \\ e_3 = \alpha_1 p - m \end{cases} \tag{14}$$

Then the derivative of the error system can be described as

$$\begin{aligned}\dot{e}_1(\tau) &= \alpha_1\dot{s}_1(\tau) - \dot{z}_1(\tau)\\ \dot{e}_2(\tau) &= \alpha_2\dot{s}_2(\tau) - \dot{z}_2(\tau)\\ \dot{e}_3(\tau) &= \alpha_1\dot{p}(\tau) - \frac{dm}{d\tau}\end{aligned} \tag{15}$$

The controllers and adaptive laws are designed by

$$\begin{aligned}u_1 &= \frac{1}{\alpha_1}\left(\alpha_1\sigma_1'\ln s_3 + \alpha_1\sigma_2' s_2 z_3 + \sigma_1'\ln z_3(\tau) - \sigma_2' z_2(\tau) z_3(\tau) + \alpha_1 p(\tau) - m(\tau) - k_1 e_1\right)\\ u_2 &= \frac{1}{\alpha_2}\begin{pmatrix}\sigma_3' z_2(\tau) + \sigma_4' z_2(\tau)\ln z_2(\tau) - \sigma_6' z_2(\tau)\ln z_3(\tau) - \alpha_2\sigma_3' s_2 + \\ -\alpha_2\sigma_4' s_2 \ln s_2 - \alpha_2 s_2 \ln z_3 - k_2 e_2\end{pmatrix}\end{aligned} \tag{16}$$

where $\dot{k}_n = \left(\alpha_n z_n - s_n\right)^2$ for $n = 1, 2$

One advantage of this type of controller is that it can be easily constructed through time varying resistors, capacitors or operational amplifier and their combinations, or using a digital signal processor together with the appropriate converters. Consequently,

$$\begin{aligned}\dot{e}_1 &= e_3(\tau) + (\sigma_1 - \sigma_1')\ln z_3(\tau) + (\sigma_2 - \sigma_2')z_2(\tau)z_3(\tau) - k_1 e_1\\ \dot{e}_2 &= -(\sigma_3 - \sigma_3')z_2(\tau) + (\sigma_4 - \sigma_4')z_2(\tau)\ln z_2(\tau) - (\sigma_6 - \sigma_6')z_2(\tau)\ln z_3(\tau) - k_2 e_2\\ \dot{e}_3 &= -\beta\alpha_1 e_1 + \frac{dm}{d\tau}\\ \dot{k}_1 &= e_1^2,\ \dot{k}_2 = e_2^2\end{aligned} \tag{17}$$

The GMPS between master and slave systems will occur by the control law (16) and the following update rules for five unknown parameters $\sigma_1', \sigma_2', \sigma_3', \sigma_4'$ and σ_6':

$$\begin{aligned}\dot{\sigma}_1' &= e_1\ln z_3(\tau) - (\sigma_1' - \sigma_1)\\ \dot{\sigma}_2' &= e_1 z_2(\tau) z_3(\tau) - (\sigma_2' - \sigma_2)\\ \dot{\sigma}_3' &= -z_2(\tau)e_2 - (\sigma_3' - \sigma_3)\\ \dot{\sigma}_4' &= z_2(\tau)e_2\ln z_2(\tau) - (\sigma_4' - \sigma_4)\\ \dot{\sigma}_6' &= -z_2(\tau)e_2\ln z_3(\tau) - (\sigma_6' - \sigma_6)\end{aligned} \tag{18}$$

Theorem 2. *For given nonzero scaling functions $\alpha_i(t)$ (i=1,2), GFPS between the transmitter (12) and the receiver system (13) can be achieved, and all the uncertain parameters of the transmitter can be estimated under the conditions (16) et (18).*

Proof. Let define a Lyapunov candidate

$$V = \frac{1}{2}\sum_{j=1}^{3} e_j^2 + \frac{1}{2}\sum_{k=1}^{5}(\sigma_k - \sigma_k')^2 + \frac{1}{2}\sum_{n=1}^{2}(k_n - L_n)^2 \tag{19}$$

where L_1 and L_2 are sufficiently large positive constants compared to β. It is clear that the Lyapunov function *V(e)* is a positive definite function. Now, taking the time derivative of equation (19), we then get

$$\frac{dV}{d\tau} = \sum_{j=1}^{3} e_j \dot{e}_j + \sum_{k=1}^{5} (\sigma_k - \sigma_k')\dot{\sigma}_k + \sum_{n=1}^{2} (k_n - L_n)\dot{k}_n \tag{20}$$

Using solutions (17) and (18) one obtains:

$$\begin{aligned}
\frac{dV}{d\tau} &= e\dot{e} + \dot{\sigma}_1(\sigma_1 - \sigma_1') + \dot{\sigma}_2(\sigma_2 - \sigma_2') + \dot{\sigma}_3(\sigma_3 - \sigma_3') + \dot{\sigma}_4(\sigma_4 - \sigma_4') + \dot{\sigma}_5(\sigma_5 - \sigma_5') - \sum_{n=1}^{3}(k_n - L_n)\dot{k}_n \\
&= e_1 e_3 - k_1 e_1^2 - k_2 e_2^2 - e_1(\sigma_1 - \sigma_1')\ln z_3(\tau) - (\sigma_2 - \sigma_2')z_2(\tau)e_1 z_3(\tau) + \beta e_1 e_3 - \alpha_1 e_3 \frac{dm}{d\tau} \\
&\quad + (\sigma_3 - \sigma_3')z_2(\tau)e_2(\sigma_4 - \sigma_4') - z_2(\tau)e_2 \ln z_2(\tau) + (\sigma_5 - \sigma_5')z_3(\tau)e_3 \ln z_3(\tau) - \sum_{k=1}^{5}(\sigma_k - \sigma_k')^2 \\
&= e_1 e_3 - k_1 e_1^2 - k_2 e_2^2 + (k_1 - L_1)e_1^2 + (k_2 - L_2)e_2^2 + \beta e_1 e_3 - \alpha_1 e_3 \frac{dm}{d\tau} - \sum_{k=1}^{5}(\sigma_k - \sigma_k')^2 \\
&= -L_1 e_1^2 - L_2 e_2^2 + (1+\beta)e_1 e_3 - \alpha_1 e_3 \frac{dm}{d\tau} - \sum_{k=1}^{5}(\sigma_k - \sigma_k')^2 \\
&\le \left[-\frac{(1+\beta)^2}{2} + \frac{1}{2} - L_1 \right] e_1^2 - L_2 e_2^2 - \alpha_1 e_3 \frac{dm}{d\tau} - \sum_{k=1}^{5}(\sigma_k - \sigma_k')^2
\end{aligned} \tag{21}$$

Since the eigen frequency of the message signal *m* is much less than the oscillating frequency of the chaotic system, in practice we consider $\frac{dm}{dt} \approx 0$. Then

$$\frac{dV}{d\tau} \le \left[-\frac{(1+\beta)^2}{2} + \frac{1}{2} - L_1 \right] e_1^2 - L_2 e_2^2 - \sum_{k=1}^{5}(\sigma_k - \sigma_k')^2 \tag{22}$$

Let $L_1 = \max\left\{1 - \frac{(1+\beta)^2}{2}\right\}$. One then has

$$\frac{dV}{d\tau} \le -L_1 e_1^2 - L_2 e_2^2 - \sum_{k=1}^{5}(\sigma_k - \sigma_k')^2 \tag{23}$$

Since the Lyapunov function V is a positive definite and its time derivative $dV/d\tau$ is negative definite in the neighborhood of the zero solution for the system (17), the dynamical system error can converge asymptotically to the origin. This complete the proof.

5. Numerical Simulations

The plaintext message can bounded or unbounded with an oscillatory frequency less than the frequency of

the chaotic system. For our case we choose a square message for two reasons: (1) the square waves when we the medium is exclusive, such as our own cables. For example, the USB cable uses near-square waves that are more easily (and less costly) associated with the binary 1 and 0. (2) The each frequency propagates differently near objects and the ground. Also the antenna designs are frequency dependent. Note that the non-sinusoidal waves with base frequency have *f* multiple harmonics which are additional sine-waves at 2*f*, 3*f*, 4*f*...

Numerical simulations are given to show the feasibility and effectiveness of the controllers (16), choose the scaling factor $\alpha_1 = \alpha_3 = 0.001, \alpha_2 = 0.2$, $k_1(0) = 0.012, k_2(0) = 0.0024$. The fourth-order Runge-Kutta method is used to solve the systems with time step size 0.001. Let's consider the following audio message $m(\tau) = 0.0013 sign\left(\sin(1.2\tau)\right)$. The initial conditions of the drive system and response system are $z_1(0) = 2\times10^{-5}, z_2(0) = 5\times10^{-7}, z_3(0) = 4\times10^{-1}$, $s_1(0) = 2\times10^{-2}, s_2(0) = 1\times10^{-2}, s_3(0) = 3\times10^{-3}$ respectively. The Fig. 5 depicts a chaotic attractor at the output of the transmitted showing that the information signal is well hidden and cannot be retrieved by unauthorized agent. Synchronization of the system (12) and (13) is presented in Fig. 7. We remark that after a transient period ($\tau = 4$), the errors defined as $\|e(\tau)\| = \sqrt{e_1^2 + e_2^2 + e_3^2}$ $\to 0$ as $\tau \to \infty$ implying that all the state variables tend to be synchronized in a proportional. This fact is also reported in Fig. 6 which shown the evolution of the adaptive control gains. It's important to note here the amplitude of the gains which are low (k_{max}=*0.65*). It point out that the scheme provide a good test in term of energy consumption. We select the following parameters $p(0) = 10^{-4}, \beta = 1.34\times10^{-3}$, using the simple mathematical formulas (See parameters expressions of Eqs. 4), we derived the unknown parameters of the overall system (1).

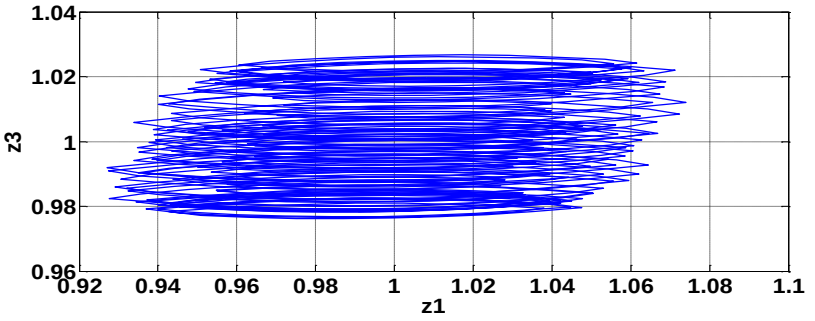
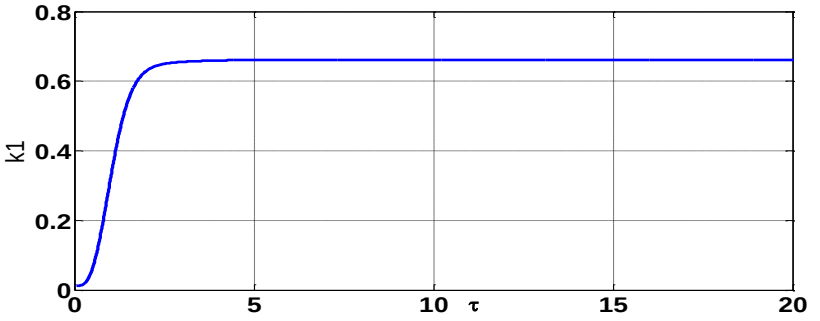
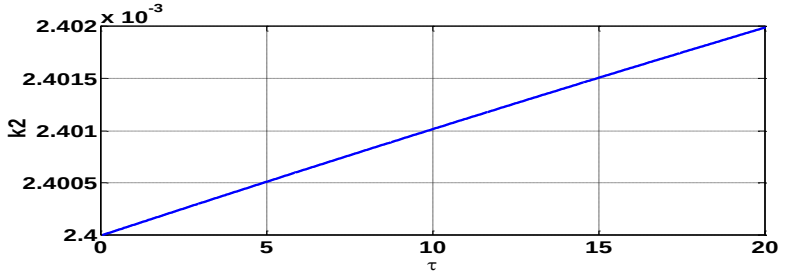


Fig.5. Attractor to the output of the transmitter.



(a)



(b)

Fig.6. Adaptive gains. (a) k_1, (b) k_2

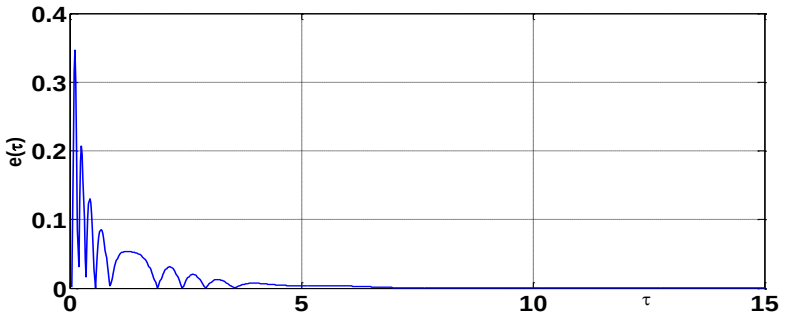


Fig.7. Synchronization Errors

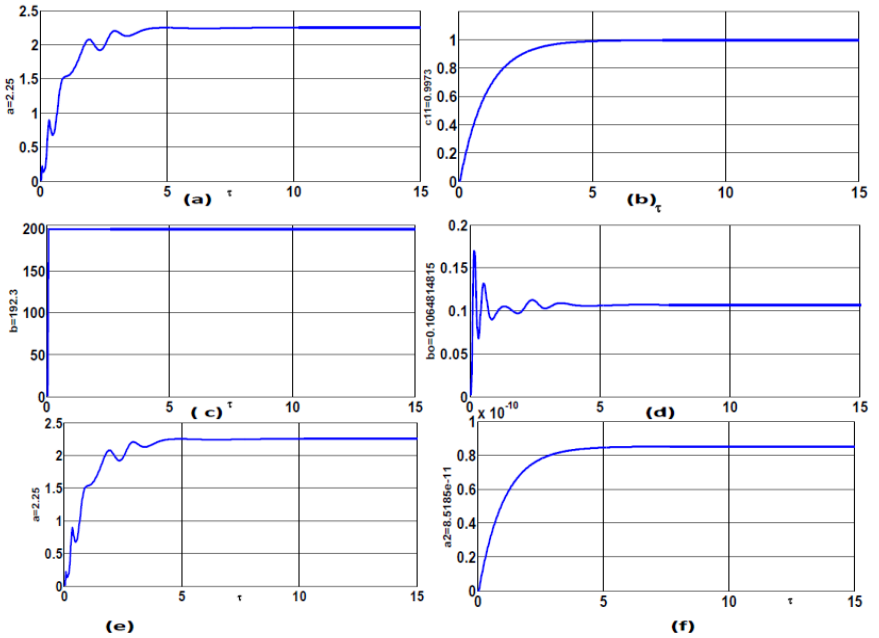


Fig.8. Estimated Values for Unknown Parameters (*a*,*b*,*c*,*d*,*e*,*f*)

Fig.9 shows the secret message communication of an audio message (in blue): the private signal information to be hidden and the recovered audio message $\hat{m}(\tau)$ at the receiver end (in red) which is obtained after a short transient behavior. Fig. 10 displays the evolution of the parameter *p(τ).* From (9) we can derive $e_3(\tau) = \alpha_1 p(\tau) - m(\tau) \to 0$ as $\tau \to \infty$ that is $\alpha_1 p(\tau)$ can recover the message signal $m(\tau)$.

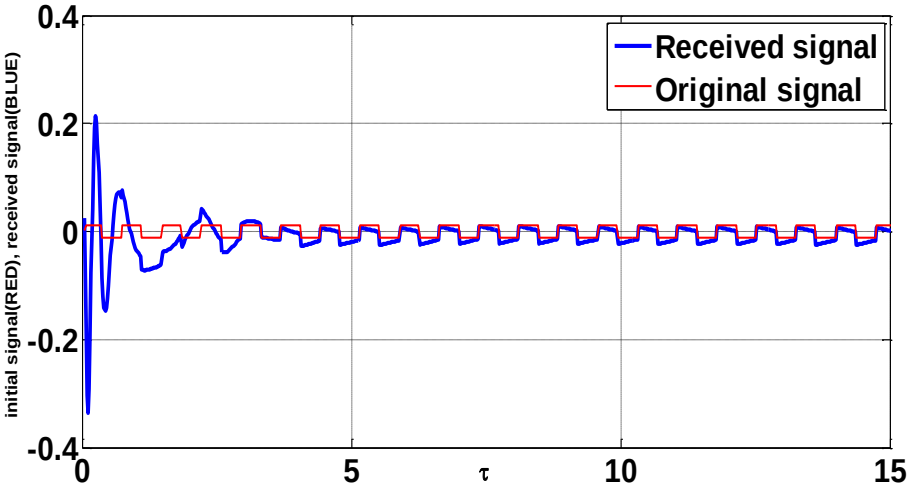


Fig.9. Original message (Red); Received message (Blue) for h1=0.001.

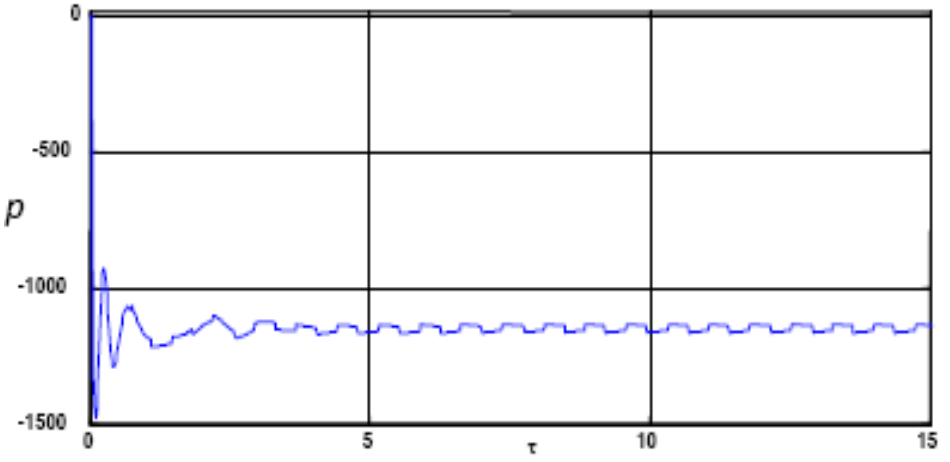


Fig.10. Time Evolution of the Parameter p(τ) for h1=0.001.

6. Conclusions and Remarks

In this paper, we have studied the generalized modified projective synchronization of the modified Colpitts oscillator. A reliable mathematical transformation is proposed in order to handle all the parameters of the

receiver. We remark that the proposed scheme is applicable to various other dynamical systems to efficiently estimate unknown parameters which could be arguments of some other nonlinear functions. The knowledge of all system parameters by estimation theory presented above is meaningful in practice. By the numerical simulation on the MCO in the new space, choosing suitable scale factor and controllers, we can achieve GMPS precision in a very short time. This could meet the challenge of many existing chaotic systems. Finally, based on this method, a novel secure communication project is designed. Under this structure, the message signal can successfully and secretly be transmitted through four main functions, i.e., modulation, chaotic transmitter, chaotic receiver and demodulation. Therefore, our secure communication has certain significance in practical applications. As a result, our study is of significances both in theory and in application.

References

[1] Pecora LM, Carroll TL: Synchronization in chaotic systems. Phys Rev Lett1990, 64(8):821-824. 10.1103/PhysRevLett.64.821.
[2] Ge Z, Chang C: Generalized synchronization of chaotic systems by pure error dynamics and elaborate Lyapunov function. Nonlinear Anal Theory Methods Appl2009, 71(11):5301-5312. 10.1016/j.na.2009.04.020
[3] Breve FA, Zhao L, Quiles MG, Macau EEN: Chaotic phase synchronization and desynchronization in an oscillator network for object selection. Neural Netw2009, 22(5-6):728-737. 10.1016/j.neunet.2009.06.027
[4] Ren Q, Zhao J: Impulsive synchronization of coupled chaotic systems via adaptive feedback approach. Phys Lett A 2006, 355(4-5):342-347. 10.1016/j.physleta.2006.02.053
[5] Li C, Liao X, Wong K: Chaotic lag synchronization of coupled time-delayed systems and its applications in secure communication. Physica D Nonlinear Phenom 2004, 194(3-4):187-202. 10.1016/j.physd.2004.02.005
[6] Mainieri R, Rehacek J: Projective synchronization in three-dimensional chaotic systems. Phys Rev Lett 1999, 82(15):3042-3045. 10.1103/PhysRevLett.82.3042
[7] Xu D: Control of projective synchronization in chaotic systems. Phys Rev E 2001, 63: 27201-27204.
[8] Deepa B. Patil, Yashwant V. Dongre. A Fuzzy Approach for Text Mining. International Journal of Mathematical Sciences and Computing (IJMSC), Vol.1, No.4, pp.34-43, 2015.DOI: 10.5815/ijmsc.2015.04.04
[9] Chee CY, Xu D: Secure digital communication using controlled projective synchronization of chaos. Chaos Soliton Fract 2005, 23(3):1063-1070.
[10] Chen J, Jiao L, Wu J, Wang X: Projective synchronization with different scale factors in a driven-response complex network and its application in image encryption. Nonlinear Anal Real World Appl 2010, 11(4):3045-3058. 10.1016/j.nonrwa.2009.11.003.
[11] Hoang TM, Nakagawa M: A secure communication system using projective-lag and/or projective anticipating synchronizations of coupled multidelay feedback systems. Chaos Soliton Fract 2008, 38(5):1423-1438. 10.1016/j.chaos.2008.02.008.
[12] Li Z, Xu D: A secure communication scheme using projective chaos synchronization. Chaos Soliton Fract 2004, 22(2):477-481. 10.1016/j.chaos.2004.02.019.
[13] Xiangjun Wu1, Zhengye Fu and Jürgen Kurths: A secure communication scheme based generalized function projective synchronization of a new 5D hyperchaotic system. Phys. Scr. 90 (2015) 045210 (12pp).
[14] Chou H.G, Chuang C.F, Wang W.J, Lin J.C: A fuzzy-model-based chaotic synchronization and Its implementation on a secure communication system. IEEE Trans. Signal processing society 2013, 8: 2177–2185.
[15] Skardal P.S, Taylor D, Sun J: Optimal synchronization of directed complex networks, Chaos 2016, 26: 094807.

[16] Kammogne S.T, Kengne R., Fotsin H.B: Dynamics and Robust Adaptive Control Strategy for the Finite Time Synchronization of Uncertain Nonlinear Systems. International Journal of System Dynamics Applications, **6**(4), 34-62 2017, DOI: 10.4018/IJSDA.2017100103
[17] Cuomo K.M, Oppenheim A.V: Chaotic signals and systems for communications. Proc. of International Conference on Acoustics, Speech, and Signal Processing, Minneapolis, (1993).
[18] Parlitz U, Kocarev L, Stojanovski T, Preckel H: Encoding messages using chaotic synchronization. Phys. Rev. 1996, E53: 4351.
[19] Alvarez G, Li S. Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos, 2006, 16:2129–2151.
[20] Ritu Goyal, Mehak Khurana: Cryptographic Security using Various Encryption and Decryption Method. International Journal of Mathematical Sciences and Computing (IJMSC), Vol.3, No.3, pp. 1-11, 2017.DOI: 10.5815/ijmsc.2017.03.01
[21] Megam N, Fotsin H.B, Louodop P: Implementing a memristive Van der Pol oscillator coupled to a linear oscillator: synchronization and application to secure communication Phys. 2014, Scr. 89.
[22] Kammogne S.T, Fotsin H. B: Adaptive control for modified projective synchronization-based approach for estimating all parameters of a class of uncertain systems: Case of modified colpitts oscillators, Journal of Chaos 2014, 2014:1-13.
[23] Kammogne S.T, Fotsin H.B: Synchronization of modified Colpitts oscillator with structural perturbations. 2011; Physica scripta 83:65011-65018.
[24] Ababei C, Marculescu R: Low-Power Realizations of Secure Chaotic Communication Schemes". University of Minnesota, *IEEE*. (2000), 30-33.
[25] Kennedy M.P: Chaos in the Colpitts Oscillator. Fundamental Theory and Applications, 1994, 41(11): 771-778.

Authors' Profiles

Kammogne Soup Tewa Alain received the BSc degree in Physics from the University of Dschang, Cameroon, in 2005, the MSc in electronics from the same university in 2008 and the PhD degree in electronic and control theory in 2014. In 2012, he was awarded the DIPES II from the High Teacher College of Bambili, Cameroon. He is currently an Assistant Lecturer at the University of Dschang and National Polytechnic of Bamenda. His research interests are in the areas of nonlinear systems, focusing on chaos control, robust control, noises analysis and their potential applications to secure communication, biological systems and power electronics.

Fotsin Hilaire Bertrand is a Professor of physics and electronics at the University of Dschang, Cameroon, where he is the Deputy Head of the Condensed Matter, Electronics, and Signal Processing Laboratory. He was awarded the "Doctorat de Troisième Cycle" degree in physics (electronics) from the University of Yaoundé I (Cameroon) in 2000. In 2005, he was awarded the "Doctorat d'Etat" degree from the University of Yaoundé I, Cameroon. He served as an Assistant Lecturer at the Physics Department, Faculty of Science, University of Dschang, Cameroon, from 1996 to 2000. From 2000 to 2009 he worked as a Lecturer in the same Department. From 2004 to 2005 he was a Visiting Scientist at the Centre de Recherche en Automatique de Nancy (CRAN) in France. In 2009, he became an associate professor. In 2016, he became a full professor of Physics. His research interests include nonlinear dynamics, focusing on chaos control and synchronization in electronic circuits. Professor Fotsin is the author and coauthor of more than 80 scientific articles in the area of nonlinear

dynamics, chaos control and chaos synchronization, and renewable energies.

How to cite this paper: Kammogne Soup Tewa Alain, Fotsin Hilaire Bertrand,"A Secure Communication Scheme using Generalized Modified Projective Synchronization of Coupled Colpitts Oscillators", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.4, No.1, pp.56-70, 2018.DOI: 10.5815/ijmsc.2018.01.04