On discrete-time chaotic multimodels synchronization using aggregation techniques for encryption

Ameni Dridi1[†], Rania Linda Filali2[††], Mohamed Benrejeb3[†††]

LA.R.A, Automatique, ENIT, BP 37, Le Belvédère, 1002 Tunis, Tunisia.

Summary
This paper deals with observer-based synchronization of new discrete-time chaotic multimodels and its application to secured communication. Based on Borne and Gentina practical criterion for the stability study associated to the arrow form matrix for systems description, sufficient conditions for the synchronization between a chaotic multimodel considered as a transmitter and a chaotic multi-observer designed as a receiver, are proposed . A new hyperchaotic multimodel, designed from two 3D Hénon maps is considered as an illustrative example of the proposed approach. The bifurcation diagrams show that the new multimodel has a larger range of parameters values that generates chaotic behavior as compared to the 3D Hénon map. This enlarges the key space and thus enhances the robustness of the communication scheme. The obtained results are applied with success to a two-channel communication scheme.

Key words:
discrete-time chaotic multimodel; synchronization; aggregation techniques; arrow form matrix, secure communication scheme

1. Introduction

During the last decades, chaos-based techniques have been widely used to perform secure communication schemes [1-4]. In fact, chaotic systems are considered as a very promising solution for cryptosystem designers due to their specific features, such as the noise-like time series, the sensitive dependence on initial conditions and parameters and the ergodicity [5, 6].

Pecora and Caroll have theoretically and experimentally shown that the synchronization of such systems is actually possible under certain conditions. [7]

Their pioneering work has received a great deal of attention, especially in the secure communication field [8-13].

In [14], it was shown that the synchronization problem can be reduced to a standard non-linear state estimation problem where the slave system is designed as an observer of the master system and the synchronization is achieved by stabilizing the error dynamics between the master and the slave systems.

However, chaos-based communication schemes are still vulnerable to many attack techniques despite the motivating results. It has been shown that chaotic attractors can be identified and approximately reconstructed due to their characteristic shapes [15- 19].

This reconstruction can give information about the family of the chaotic systems and the corresponding dynamic models, thus allowing the parameters to be easily identified.

As a solution to this problem, in [20], is proposed a class of continuous nonlinear multimodels designed from two or more chaotic systems. The authors showed that the resulting multimodel has one more bifurcation parameter that can be used as a key for encryption to extend the key space and enhance the robustness of the communication scheme.[21].

In this paper, the multimodel approach, proposed in [20], is extended to the case of discrete-time chaotic systems. The mutimodel described by (1) is built from p discrete-time chaotic sub-models, such that

$$\begin{cases} x(k+1) = \sum_{i=1}^{p} \mu_i(\zeta(k))(A_i x(k) + f_i(x(k))) \\ y(k+1) = Cx(k) \end{cases} \quad (1)$$

where $x(k)$ is the state vector, $x \in R^n$, $y(k)$ is the output vector, $y \in R^q$, A_i and C are constant matrices with appropriate sizes, f_i are nonlinear discrete-time functions and μ_i , $i = 1, ..., p$ are weighting functions that ensure a kind of mixing between the p sub-models defined such that

Manuscript received February 5, 2018
Manuscript revised February 20, 2018

$$\begin{cases} \sum_{i=1}^{p} \mu_i(\zeta) = 1? \\ 0 \le \mu_i(\zeta) \le \quad \forall i = 1, \dots, p? \end{cases} \tag{2}$$

ζ is a state vector that may be measurable or non-measurable.

The obtained multimodel is then used as a transmitter in a communication scheme and the receiver is a multi-observer designed to achieve synchronization by using the Borne and Gentina criterion for stability study [22- 24] associated to the arrow form for systems description [25-27, 37, 38].

After the design of the multimodel using two hyperchaotic systems in Section II, sufficient stabilization conditions are proposed to achieve the observer-based synchronization between two identical discrete-time chaotic multimodels. In section III, a cryptographic system is considered as an application to secured communication using a new multimodel designed from two 3D Hyper-chaotic Hénon maps to illustrate the efficiency of the proposed approach.

2. Proposed discrete-time chaotic multimodels synchronization method: basic idea

In this section, the multimodel approach is used to define a new class of chaotic systems built from two or more discrete –time chaotic attractors. Then, synchronization conditions between a master chaotic multimodel and a slave multi-observer are obtained using the practical stability criterion of Borne and Gentina study [22- 24] associated to the specific Benrejeb arrow form matrix [25-30, 37, 38]. After achieving the synchronization, a secure communication scheme is considered to test the efficiency of the proposed approach.

2.1 Considered discrete-time chaotic multimodels

Let consider the two n-dimensional discrete-time chaotic sub-systems in Lurie form described in state space for p=2, by

$$x(k+1) = A_i x(k) + f_i(x(k)),\ i = 1, 2 \tag{3}$$

It comes the system (4), proposed as a multimodel [31], such that

$$\begin{cases} x_m(k+1) = \mu_1(y_m)(A_1 x_m(k) + f_1(x_m(k))) \\ \qquad + \mu_2(y_m)(A_2 x_m(k) + f_2(x_m(k))) \\ y_m(k) = C x_m(k) \end{cases} \tag{4}$$

and $\mu_2(.) = 1 - \mu_1(.)$.

$x_m(k)$ and $y_m(k)$ are respectively the state and output vectors,. A_i, $i = 1, 2,$ are $(n \times n)$ constant matrices, C is a constant matrix with appropriate sizes and f_i, $i = 1, 2,$ are nonlinear discrete-time functions chosen such that each sub-system has a chaotic behavior. The multimodel (4) is integrated as a master system in a transmission scheme based on chaotic synchronization.

The corresponding slave system, designed as a multi-observer, is defined by

$$\begin{cases} x_s(k+1) = \mu_1(y_m)(A_1 x_s(k) + f_1(x_s(k)) \\ \qquad + L_1(.)(y_m(k) - C x_m(k))) + (1 - \mu_1(y_m))(A_2 x_s(k) \\ \qquad + f_2(x_s(k)) + L_2(.)(y_m - C x_m(k))) \\ y_s(k) = C x_s(k) \end{cases} \tag{5}$$

$x_s(k)$ and $y_s(k)$ are the state and output vectors of the slave system, respectively. $L_i(.) = \left[l_{i1}(.), \dots, l_{in}(.) \right]$, i=1, 2, are the Luenberger discrete-time mutli-observer gain matrices satisfying the master-slave chaotic system's synchronization conditions [8, 32, 28-30].

2.2 Synchronization conditions of coupled chaotic multimodels

For the error vector $e(k)$ defined by

$$e(k) = x_m(k) - x_s(k) \tag{6}$$

the error system description can be rewritten, as follows

$$e(k+1) = \begin{cases} \mu_1(y_m)((A_1 - L_1(.)C)e(k) + f_1(x_m) - f_1(x_s)) \\ +(1 - \mu_1(y_m))((A_2 - L_2(.)C)e(k) + f_2(x_m) - f_2(x_s)) \end{cases} \tag{7}$$

To simplify the error system formulation, (7) is rewritten as following

$$e(k+1) = \begin{cases} (A-KC)e(k) + (\mu_1(y_m)(f_1(x_m(k) - f_1(x_s(k)) \\ +(1-\mu_1(y_m))(f_2(x_m) - f_2(x_s)))e(k) \end{cases} \quad (8)$$

with

$$K = \mu_1(y_m)L_1(.) + (1-\mu_1(y_m))L_2(.) \quad (9)$$

and

$$A = \mu_1(y_m)A_1 + (1-\mu_1(y_m))A_2 \quad (10)$$

In [36], it is showed that the non-linearity term for several chaotic systems expressed by

$$\mu(y_m)(f_1(x_m) - f_1(x_s)) + (1-\mu_1(y_m))(f_2(x_m) - f_2(x_s))$$

can be factorized, as follows

$$Q(x_m(k), x_s(k))e(k) \quad (11)$$

where $Q(.)$ is an $(n \times n)$ matrix with non-linear elements.

In this case, the error system can be rewritten, as follows

$$e\left(k ?+\text{刭}\right) = ?A_c\left(x_m\left(k\right) ?x_s\left(k\right)\right)e\left(k\right) \quad (12)$$

with

$$A_c\left(x_m\left(k\right), \text{刭}_s\left(k\right)\right) = A - KC + ?Q\left(x_m\left(k\right) ?x_s\left(k\right)\right) \quad (13)$$

The following theorem, based on the use of Borne and Gentina stability criterion [Borne et al., 1976, 1987, Gentina et al., 1976] associated to the specific canonical Benrejeb arrow form matrix [22-24] gives sufficient synchronization conditions between the slave system (5) and the master system (4) [11, 25-30, 37, 38].

To apply the theorem, the Luenberger discrete-time mutli-observer gain matrices must be chosen such that the matrix $A_c\left(x_m\left(k\right), ?x_s\left(k\right)\right)$ be in the arrow form as follows

$$A_e\left(x_m\left(k\right), ?x_s\left(k\right)\right) = \begin{pmatrix} a_{e_{11}} & a_{e_{12}} & \cdots & a_{e_{11}} \\ a_{e_{11}} & a_{e_{22}} & & \\ \vdots & & \ddots & \\ a_{e_{11}} & & & a_{e_{11}} \end{pmatrix} \quad (14)$$

Theorem: The error vector defined by (6) and introduced in (12) converges towards zero, if the matrix (13) is in the arrow form (14), such that [28-30]

(i) the non-linear elements of the matrix $A_e(.)$ are isolated in one row,

(ii) the diagonal elements, $a_{e_{ii}}(.)$, $i = 2, \ldots, n$ of the matrix $A_e(.)$ are expressed, such that

$$1 - \left|a_{e_{ii}}(.)\right| > 0 \quad (15)$$

(iii) there exists ε , $\varepsilon > 0$, such that

$$1 - \left|a_{e_{11}}(.)\right| - \sum_{i=2}^{n} \begin{pmatrix} \left|a_{e_{i1}}(.)a_{e_{1i}}(.)\right| \\ \times\left(1 - \left|a_{e_{ii}}(.)\right|\right)^{-1} \end{pmatrix} > \varepsilon \quad (16)$$

Proof: The overvaluing system based on the use of the vectorial norm [23]

$$p(z(k))[|z_1(k)|, ..., |z_n(k)|]^T, \; z(k) = [z_1(k), ..., z_n(k)]^T \quad (17)$$

is defined by

$$z(k+1) = M(A_e(.))z(k) \quad (18)$$

with

$$M\left(.\right) = \left\{m_{ij}(.)\right\}, \text{刭}m_{ij} = \left|a_{e_{ij}}(.)\right| \forall i, j = 1, ..., n \quad (19)$$

The error system (12) is stabilized by the multi-observer (5) if the appropriate multi-observer gains L_i, $i = 1, 2$ are chosen such that the matrix $\left(I - M(A_e(.))\right)$ is an M matrix; i.e if, by the application of the stability criterion of Borne and Gentina, there exists an ε , ε >0, such that the condition (15) is satisfied and

$$\det(I - M(A_e(.))) > \varepsilon \quad (20)$$

The computation of the first member of this inequality leads to the following expression

$$det(I - M\left(A_e\left(.\right)\right)) = \begin{pmatrix} 1 - \left|a_{e_{11}}\left(.\right)\right| \\ -\sum_{i=2}^{n} \begin{pmatrix} \left|a_{e_{i1}}(.)a_{e_{1i}}(.)\right| \\ \times\left(1 - \left|a_{e_{ii}}\left(.\right)\right|\right)^{-1} ? \end{pmatrix} \end{pmatrix} \times \left(\prod_{j=2}^{n}\left(1 - \left|a_{e_{jj}}(.)\right|\right)\right) \quad (21)$$

which helps to easily achieve the proof of the theorem.

2.3 Application to a secure communication scheme

The theoretical results of the synchronization approach, introduced in the previous section, are applied to a secure communication scheme. A message is transmitted using a chaotic multimodel as a transmitter and a multi-observer as a receiver designed using the proposed synchronization conditions. The two-channel transmission scheme is considered for the purpose to obtain fast synchronization dynamics and high security [29, 33].

As shown in Fig.1, the transmission process uses a channel different from that of the synchronization one. The chaotic multimodel, proposed as the transmitter, generates the output $y(k)$ and the key $K_c(k)$, used to encrypt the original message $m(k)$ with an encryption rule$v_c(.)$. The encrypted message $V(k)$ is transmitted to the receiver designed as an observer via channel 1. The ouptput $y(k)$ is transmitted via channel2 to ensure the synchronization with the receiver. Once the synchronization between the master and the slave systems is obtained, the key generated by the chaotic receiver, $K_d(k)$, gets the same values as the key $K_c(k)$ at the transmitter. Using an appropriate decrypting function v_d (.), the information $m_r(k)$ can be recovered.

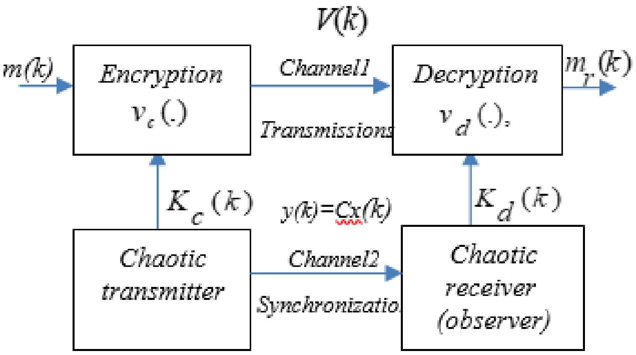

Fig. 1 A two-channel hyperchaotic secure-communication system

3. Case of a new 3D Generaliezd chaotic Hénon multimodel

Two different sets of parameters, corresponding to two different chaotic behaviors of Hénon maps [34, 33], are used with appropriate activation functions to build the multimodel, proposed as the transmitter. The receiver is designed using the proposed synchronization method. Numerical simulations, based on the proposed transmission scheme Fig.1, are performed in this section.

3.1 Master 3D Hénon chaotic multimodel design

The considered discrete-time hyperchaotic Hénon map is described by [34, 33]

$$\begin{cases} x_1(k+1) = a_i - x_2^2(k) - b_i x_3(k) \\ x_2(k+1) = x_1(k) \\ x_3(k+1) = x_2(k) \end{cases} \tag{22}$$

Two sets of parameters a_i and b_i corresponding to two different chaotic behaviours of (22), are chosen as follows

Set1: $a_1 = 1.76;\ b_1 = 0.1$

Set2: $a_2 = 1.5;\ b_2 = 0.15$

The attractors corresponding to set 1 with initial conditions fixed to $x(0) = (0.1, 0.2, 1)$ and set 2 with intial conditions fixed to $x(0) = (0.1, 0.2, 1)$ have two different shapes as shown in Fig.2 and Fig.3, respectively.

The activation function μ_1 satisfying the constraints (2) is chosen such that transition between the two sub-models is achieved to avoid synchronization problems [20]. It is expressed as follows

$$\mu_1(y) = (1 + \tanh(\gamma y))/2 \tag{23}$$

where $\gamma \in [0, 1]$ is an arbitrary parameter chosen to get a real transition.

Fig.4 shows how μ_1 function can ensure transition for different values of γ .

The multimodel mixing the two corresponding sub-models, considered as a master system is described by

$$\begin{cases} x_1(k+1) = \mu_1(y)(a_1 - x_2^2(k) - b_1 x_3(k)) \\ \qquad + (1-\mu_1(y))(a_2 - x_2^2(k) \\ \qquad - b_2 x_3(k)) \\ x_2(k+1) = \mu_1(y)x_1(k) + (1-\mu_1(y))x_1(k) \\ x_3(k+1) = \mu_1(y)x_2(k) + (1-\mu_1(y))x_2(k) \\ y(k) \quad = x_1(k) + x_2(k) \end{cases} \tag{24}$$

Fig. 5a and Fig. 5.b show the state variables evolution and the attractor of the resulting multimodel for $\gamma = 0.5$, respectively. The bifurcation diagrams, presented in Fig.6.a and Fig. 6.b, illustrate the chaotic behavior of the multimodel for b_1=0.1, a_2 =1.5, b_2=0.15 when a_1 is variable and for a_1 =1.5, b_1=0.1, b_2=0.15 when a_2 is variable, respectively. The security of the communication scheme strongly depends on the size of the key space which contains the possible parameters generating the chaotic behavior [5].

As shown in Fig.6.a and Fig.6.b, it may be noted that the multimodel gets a chaotic behavior for $a_1 \in [-0.1,\ 0.8] \cup [1.25,\ 1.8]$ and $a_2 \in [-0.2,\ 0.58] \cup [0.9,\ 1.6]$. However, the chaotic behaviors of Hénon map1 and Hénon map 2 represented by the bifurcation diagrams of Fig. 7.a and Fig. 7.b, are obtained for $a_1 \in [0.8,\ 1.09] \cup [1.39,\ 1.76]$ and $a_2 \in [0.8,\ 1.25] \cup [1.38,\ 1.55]$, respectively.

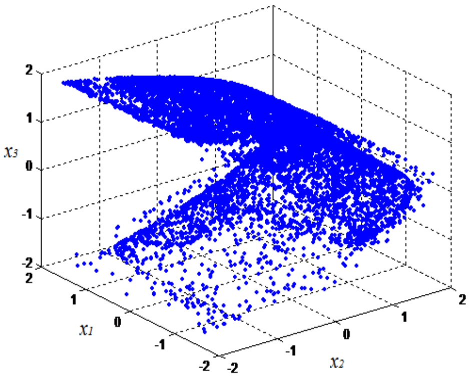

Fig. 2 Hypercahotic Hénon map 1 for set 1

The comparison of the different possible values of a_1 and a_2 generating chaotic behaviors shows that our chaotic multimodel has larger possible values than Hénon maps 1 and 2, which means a much larger key space.

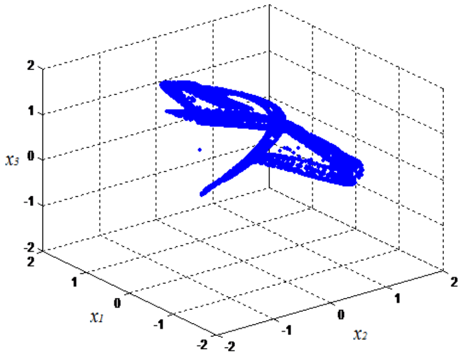

Fig. 3 Hypercahotic Hénon map 2 for set 2

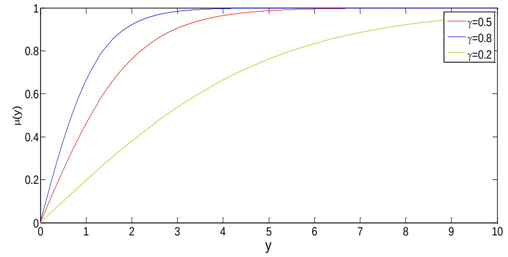

Fig. 4 Activation function for different values of γ

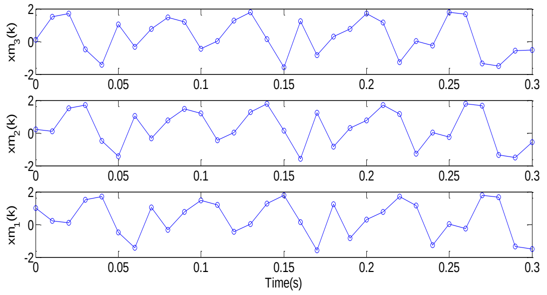

Fig. 5.a States variables of the hyperchaotic multimodels

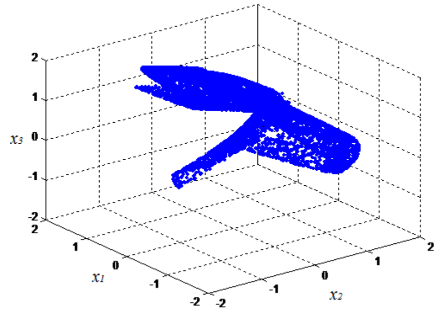

Fig. 5.b Hyperchaotic multimodel based on Hénon maps 1 and 2

3.2 Proposed coupled chaotic Hénon multimodels synchronization

Consider the following chaotic multimodel (23) as the master system

$$\begin{cases} x_{m1}(k+1) = \mu_1(y_{m2})(a_1 - x_{m2}^2(k) - b_1 x_{m3}(k)) \\ \qquad + (1-\mu_1(y_{m2}))(a_2 - x_{m2}^2(k) - b_2 x_{m3}(k)) \\ x_{m2}(k+1) = \mu_1(y_{m2}) x_{m1}(k) + (1-\mu_1(y_{m2})) x_{m1}(k) \\ x_{m3}(k+1) = \mu_1(y_{m2}) x_{m2}(k) + (1-\mu_1(y_{m2})) x_{m2}(k) \\ y_m(k) \quad = c_1 x_{m1}(k) + c_2 x_{m2}(k) + c_3 x_{m3}(k) \\ \end{cases} \tag{25}$$

The associated Lugenberger multi-observer receiver is given by the following equations

$$\begin{cases} x_{s1}(k+1) = \mu_1(y_{m2})((a_1 - x_{s2}^2(k) - b_1 x_{s3}(k)) \\ \qquad + L_{11}(y_{m1}(k) - y_{s1}(k))) \\ \qquad + (1-\mu_1(y_{m2}))((a_2 - x_{s2}^2(k) - b_2 x_{s3}(k)) \\ \qquad + L_{21}(y_m(k) - y_s(k))) \\ x_{s2}(k+1) = \mu_1(y_{m2})\left[x_{s1}(k) + L_{12}(y_{m1}(k) - y_{s1}(k))\right] \\ \qquad + (1-\mu_1(y_{m2}))\left[x_{s1}(k) + L_{22}(y_m(k) - y_s(k))\right] \\ x_{s3}(k+1) = \mu_1(y_{m2})\left[x_{s2}(k) + L_{13}(y_{m1}(k) - y_{s1}(k))\right] \\ \qquad + (1-\mu_1(y_{m2}))\left[x_{s2}(k) + L_{23}(y_m(k) - y_s(k))\right] \\ y_{s1}(k) \quad = c_1 x_{s1}(k) + c_2 x_{s2}(k) + c_3 x_{s3}(k) \end{cases} \tag{26}$$

where $x_m(k)$ and $y_m(k)$ are the master state vectors and the output vector, $x_s(k)$ and $y_s(k)$ are the slave state vectors and $L_i = \left[l_{i1} \quad l_{i2} \quad l_{i3}\right]^T$, $i = 1, 2$, are the observer gain matrices.

The error system between (25) and (26) chaotic systems in the form (8) is expressed, such that

$$A = \begin{bmatrix} 0 & 0 & -(\mu_1 0.1 + (1-\mu_1)0.15) \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{27}$$

$$C = \left[c_1 \quad c_2 \quad c_3\right] \tag{28}$$

and

$$f_i(x_m(k)) = \left[-x_{m2}^2(k) \quad 0 \quad 0\right]^T, \ i = 1, 2 \tag{29}$$

$$f_i(x_s(k)) = \left[-x_{s2}^2(k) \quad 0 \quad 0\right]^T, \ i = 1, 2 \tag{30}$$

The matrix Q is such that

$$Q = \begin{bmatrix} 0 & \text{-}x_{m2}(k)\text{-}x_{s2}(k) & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{31}$$

I It comes the following matrix characterizing the error system introduced in (13).

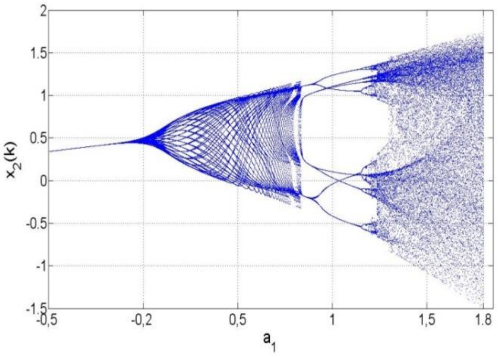

Fig. 6.a Bifurcation diagram of the hyperchaotic multimodel for a_1 being variable

$$A_c\ (x_m\ (k)\ ,\ x_s\ (k))\ =$$

$$\begin{bmatrix} \begin{cases} \mu_1(-l_{11}c_1) \\ +(1-\mu)(-l_{21}c_1) \end{cases} & \begin{cases} \mu_1(-x_{m2}-x_{s2}-l_{11}c_2) \\ +(1-\mu_1) \\ \times(-x_{m2}-x_{s2}-l_{21}c_2)) \end{cases} & \begin{cases} -\mu_1(0.1-l_{11}c_3) \\ \quad -(1-\mu_1)(0.15-l_{21}c_3) \end{cases} \\ \begin{cases} \mu_1(1-l_{12}c_1) \\ +(1-\mu_1)(1-l_{22}c_1) \end{cases} & \begin{cases} \mu_1(-l_{12}c_2) \\ +(1-\mu_1)(-l_{22}c_2)) \end{cases} & \begin{cases} \mu_1(-l_{12}c_3) \\ \quad +(1-\mu_1)(-l_{22}c_3)) \end{cases} \\ \begin{cases} \mu_1(-l_{13}c_1) \\ +(1-\mu_1)(-l_{23}c_1) \end{cases} & \begin{cases} \mu_1(1-l_{13}c_2) \\ +(1-\mu_1)(1-l_{23}c_2)) \end{cases} & \begin{cases} \mu_1(-l_{13}c_3) \\ +(1-\mu_1)(-l_{23}c_3) \end{cases} \end{bmatrix} \tag{32}$$

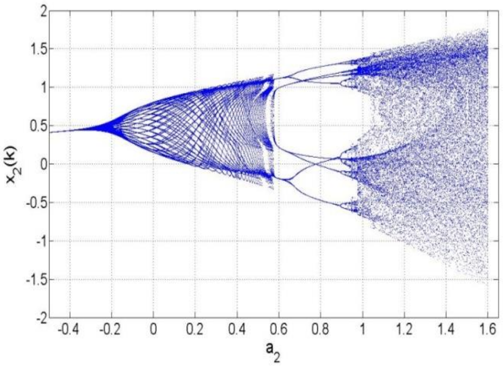

Fig 6.b Bifurcation diagram of the hyperchaotic multimodel for a_2 being variable

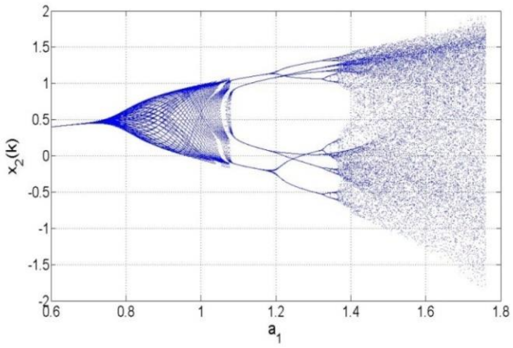

Fig 7.a Bifurcation diagram of Hénon map 1

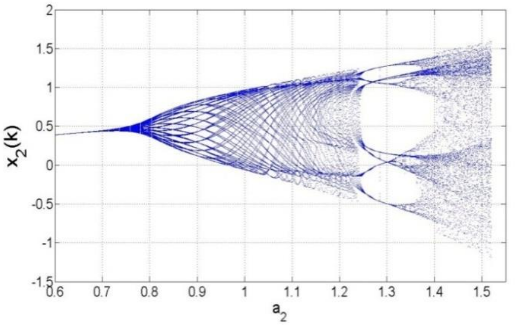

Fig 7.b Bifurcation diagram of Hénon map 2

To put it simply, the multi-observer gains are chosen, such that $l_{13} = l_{23}$, $l_{12} = l_{22}$, $l_{11} = l_{21}$. Then, we set $c_3 = 0$, $c_2 = \frac{1}{l_{13}}$ to get the the matrix $A_e(.)$ in the arrow form.

The overvaluing system introduced in (16) and characterized by $M(A_e)$ can be represented as follows

$$M(A_e(x_m(k), x_s(k))) =$$

$$\begin{bmatrix} |l_{11}c_1| & |x_{m2} + x_{s2} + l_{11}c_2| & |0.1\mu_1 + 0.15(1-\mu_1) - l_{11}c_3)| \\ |1 - l_{12}c_1| & |l_{12}c_2| & 0 \\ |l_{13}c_1| & 0 & |l_{13}c_3| \end{bmatrix} \quad (33)$$

Fig.5.b shows that the state variables of the chaotic multi-models (22) are such as: $|x_{m2}| < 2$ and $|x_{s2}| < 2$ so we have $|-(x_{m2}+x_{s2}) - l_{11}c_2| < 4 + |l_{11}c_2|$.

By the application of the practical Borne and Gentina stability criterion, the characteristic matrix (32) of the error system in the form of (13) make the state systems variables converge to zero if the following conditions are satisfied:

i. $$1 - |l_{12}c_2| > 0 \quad (34)$$

ii. $$1 - |l_{11}c_1| - \frac{(4 + |l_{11}c_2|)\ (|1 - l_{12}c_1|)}{1 - |l_{12}c_2|}$$
$$- \left(\frac{|(\mu_1 0.1) + (1-\mu)_1 0.15 - l_{11}c_3|}{1 - |l_{13}c_3|} |l_{13}c_1| \right) > 0$$
$$(35)$$

As shown in Fig.8, the synchronization of the coupled hyperchaotic multimodels is completely achieved at nearly

$t = 0.08\ s$

for $C = [1.8, 0.9, 0]^T$, $L_2 = [-0.2, 0.6, 1.11]^T$

$x_m(0) =$ (0.1, 0.2, 1) and $x_s(0) =$ (0.5,0.3, 0.1).

3.3 Secure communication scheme based on chaotic multimodels

After the synchronization of two discrete-time chaotic Hénon multimodels, the results obtained in the previous section are applied to the proposed secure communication scheme presented in Fig.1.

The master and slave chaotic multimodels are used as key generators for encrypting and decrypting the original message $m(k)$ and the encrypted message V(k),

respectively. The encryption $v_c(.)$ used as a r-shift cipher algorithm [29, 35], is expressed such as

$$\begin{aligned} V(k) &= v_c(m(k), K_c(k)) \\ &= f_1(...f_1(f_1(f_1(m(k), K_c(k)), K_c(k))), \\ &\quad K_c(k)), ..., K_c(k)) \end{aligned} \quad (36)$$

mr(k) can be recovered at the receiver using a decryption rule given by the following expression

$$\begin{aligned} m_r(k) &= v_d(V(k), K_d(k)) \\ &= f_1(...f_1(f_1(f_1(V(k), -K_d(k)), -K_d(k))), \\ &\quad -K_d(k)), ..., -K_d(k)) \end{aligned} \quad (37)$$

with

$$K_c(k)=\sqrt{\left|x_{m1}(k)+x_{m2}(k)+x_{m3}(k)\right|} \qquad (38)$$

$$K_d(k)=\sqrt{\left|x_{s1}(k)+x_{s2}(k)+x_{s3}(k)\right|} \qquad (39)$$

$f_1(.)$ is a non-linear function defined such that

$$f_1(m(k),K_c(k))=\begin{cases} s(k)+2h, for: -2h\le s(k)\le -h \\ s(k), for\ -h<s(k)<h \\ s(k)-2h, for\ h\le s(k)\le 2h \end{cases} \qquad (40)$$

and

$$s(k)=m(k)+K_c(k) \qquad (41)$$

h is an encryption parameter chosen such that the transmitted message m(k) and the key $K_c(k)$ lies within the interval [-h,h].

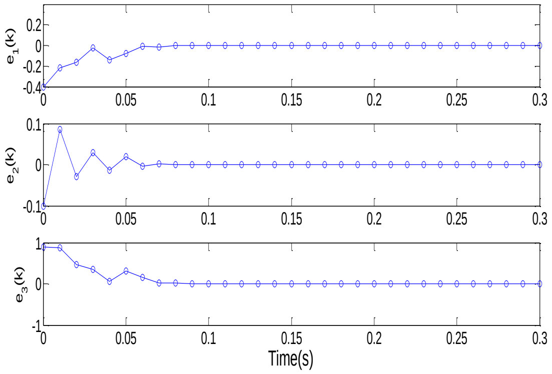

Fig. 8 Error dynamics of coupled 3D Hénon multimodels

The numerical results are given in Fig. 9, Fig. 10, and Fig. 11. The encryption parameters are h =2, r=5 and the sampling time is T=0.01s. Once the chaotic multimodels in (23) and (24) are synchronized, the key $K_d(k)$ in the receiver gets the same values as the $K_c(k)$ in the transmitter, as presented in Fig.10.

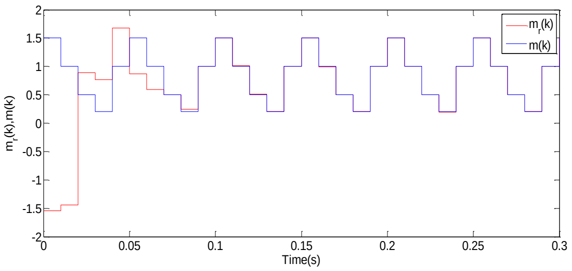

Fig. 9 Original message $m(k)$ and recovered message $m_r(k)$

The message $m_r(k)$ is completely recovered, as shown in Fig.8 and Fig.9 shows the encrypted message sent in channel2.

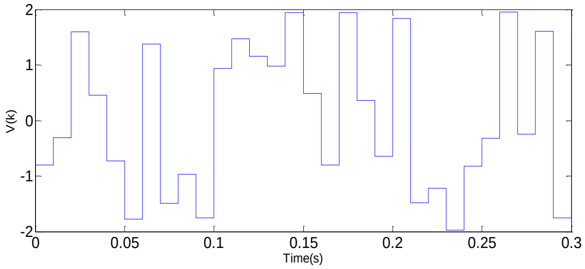

Fig. 10 Encrypted message $V(k)$

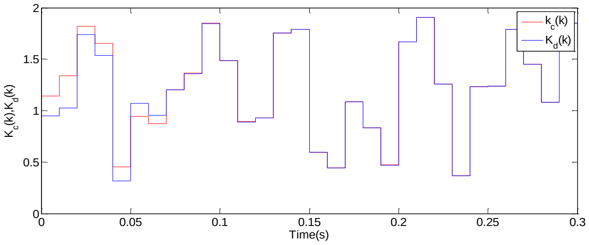

Fig. 11 The Key emitter key $K_c(k)$ and thereceiver key $K_d(k)$

4. Conclusion

In this paper, the multimodel approach is used to build a chaotic multi-model from two hyper-chaotic systems and suitable stabilization conditions are proposed for observer-based synchronization. The obtained results show that a combination of two chaotic systems can give more advantageous chaotic features to the resulting one, which enhances its performances in secure communication. Also, results show that the synchronization can be achieved between master and slave chaotic multimodels by the use of Borne and Gentina criterion associated to the arrow form matrix. The proposed approach is successfully applied to a secure communication scheme based on two transmission channels and 3D Hénon maps.

Acknowledgments

We would like to present our thanks to the reviewers for their eventual suggestions

References

[1] Oppenheim, A.V., Cuomo, K.M. and Strogatz, S. (1993) 'Synchronization of lorenz-based chaotic circuits with applications to communications', IEEE Transactions on Circuits and Systems II:Fundamental Theory and Applications, Vol. 40, No. 10, pp. 626–633.

[2] Dedieu, H,. Kennedy, M. P and Hasler, M. (1993) 'Chaos shift keying modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits', IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, Vol. 40, No. 10, pp. 634–642.

[3] Parlitz, U., Chua, L., Kocarev, Lj., Halle, K.S. and Shang, A. (1992) 'Transmission of digital signals by chaotic synchronization', International Journal of Bifurcation and Chaos, Vol. 2, No. 4, pp. 973–977.

[4] Khodadadzadeh, M and Gholizadeh, N.H. (2015) 'Improvement of chaotic secure communication scheme based on steganographic method and multimodal dynamic maps', International Journal of systems Control and Communications, Vol. 6 No.4, pp. 305-320.

[5] Alvarez, G. and Li, S. (2006) 'Some basic cryptographic requirements for chaos-based cryptosystems', International Journal of Bifurcation and Chaos, Vol. 16, No. 8, pp. 2129–2151.

[6] Zhen, P., Zhao, G., Min, L. and Li, X. (2014) 'A survey of chaos- based cryptography', Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC 2014), Guangdong, pp. 237–244.

[7] Pecora, L.M., Carroll, T.L. (1990) 'Synchronization in chaotic systems', Physics Review Letters, Vol. 64, No. 8, pp. 821-824.

[8] Liao, T.L. and Huang, N. (1999) 'An observer-based approach for chaotic synchronization with applications to secure communications', IEEE Transactions on Circuits and Syst.ems I: Fundamental Theory and Applications, Vol. 46 No. 9, pp. 1144–1150.

[9] Filali, R.L., Hammami, S. Benrejeb, M and Borne, P. (2012) 'Synchronization of discrete-time hyperchaotic maps based on aggregation technique for encryption', Systems, Signals and Devices, Chemnitz, Germany, pp. 1-6.

[10] Yau, H.T., Pu, Chi, Y. and Li, S,C. (2012) 'Application of a Chaotic Synchronization System to Secure Communication', Information Technology and Control, Vol. 41, No. 3, pp. 274-282.

[11] Khalifa, N. Filali, R.L. and Benrejeb, M. (2016) 'A Fast Selective Image Encryption Using Discrete Wavelet Transform and Chaotic Systems Synchronization', Information Technology and Control, Vol. 45, No. 3, pp. 235-242.

[12] Vaidyanathan, S., Sampath, S and Azar A.T. (2015) 'Global chaos synchronisation of identical chaotic systems via novel sliding mode control method and its application to Zhu system', International Journal of Modelling, Identification and Control, Vol 27, No.1, pp 3-13.

[13] We, Y., America M. and Guillermo F 'Robust chaotic communication via high gain observer', International Journal of systems, control and communications, Vol. 1, No. 2, pp.179 –192

[14] Nijmeijer, H. and Mareels, I. (1997) 'An observer looks at synchronization', IEEE. Transactions on Circuits and Systems I: Fundamental Theory and Applications, Vol. 44, No. 10, pp. 882–890.

[15] Short, K.M. (1994) 'Steps towards unmasking secure communications', International Journal of Bifurcation and Chaos, Vol. 4, No. 4, pp. 959–977.

[16] Short, K.M. (1996) 'Unmasking a modulated chaotic communications scheme', International Journal of Bifurcation and Chaos, Vol. 6 No. 2, pp. 367–375.

[17] Yang, T., Yang, L.B. and Yang, C. M.(1998) 'Cryptanalyzing chaotic secure communications using return maps', Physics Letters A, Vol. 245, No 6, pp. 495–510

[18] Alvarez, G. Montoya and F. Pastor, G. (2004) 'Breaking secure communication scheme based on the phase synchronization of chaotic systems' Chaos, Vol 14, No. 2, pp. 274-278.

[19] Li, S. and Chen, G. (2005) 'Breaking a chaos-based secure communication scheme designed by an improved modulation method', Chaos, Solutions and Fractals, Vol. 25, No. 1, pp.109-120.

[20] Cherrier, E., Boutayeb, M., Ragot, J and Aziz-Alaoui, M. (2007) 'Observer-based exponential synchronization of chaotic multimodels', European Control Conference (ECC'07), Kos, pp. 2635 – 2641.

[21] Li, S. Alvarez, G., Li, G. and Halag, W. A. (2007) 'Analog Chaos-based Secure Communications and Cryptanalysis: A Brief Survey', PysCon 2007.

[22] Borne, P., Gentina, J. C and Laurent, F. (1976) 'Sur la stabilité des systèmes échantillonnés non linéaires", RAIRO Revue Jaune, AFCET, J2, pp. 96–105,.

[23] Borne, P. (1987) 'Nonlinear systems stability: vector norm approach', Systems and Control Encyclopedia, Pergamon Press, pp. 3402–3406.

[24] [Borne et al., 2007] Borne, P. Vanheeghe, P and Duflos, E. (2007) 'Automatisation des processus dans l'espace d'état', Ed. Technip, Paris.

[25] Benrejeb, M and Borne, P. (1978) 'On an algebraic stability criterion for nonlinear process interpretation in the frequency domain', in Proceedings of the International Symposium on Advances in Measurement and Control, MECO, Acta Press, Athens, pp. 678–682,

[26] Benrejeb, M., Borne, P and Laurent, F. (1982) 'Sur une application de la représentation en flèche à l'analyse des processus', RAIRO Aut./Sys. Analysis and Control, Vol.16, No. 2, pp. 133–146.

[27] Benrejeb, M. and Hammami, S., (2008) 'New approach of stabilization of nonlinear continuous monovariable

processes characterized by an arrow form matrix', 1st International Conference Systems Engineering Design and Applications, SENDA 2008, Monastir, Tunisia.

[28] Filali, R.L., (2013) 'Sur la synchronisation et le cryptage de systèmes chaotiques à temps discret utilisant les techniques d'agrégation et la représentation en flèche des matrices', doctoral thesis, Université de Tunis el Manar et Ecole centrale de Lille, Tunisia, pp. 60-62.

[29] Filali, R.L., Benrejeb, M and Borne, P. (2014) 'On observer-based secure communication design using discrete-time hyperchaotic systems', Communications in Nonlinear Science and Numerical Simulation, Vol. 19, No. 5, pp. 1424-1432.

[30] Filali, R.L., Benrejeb, M and Borne, P. 'On observer synchronization of non-identical Discrete-time hyperchaotic maps using arrow form matrix', International Journal of Computers Communications and Control, Vol. 10, No. 3, pp.308-317.

[31] Dridi, A., Filali, RL, Benrejeb, M (2016) 'A discret time chaotic multimodel based on 2D Hénon maps', ASECS, Hammamet, pp.271-276.

[32] Miller, G and Grassi, D. A. (2002) 'Theory and experimental realization of observer based discrete-time hyperchaos synchronization', IEEE Transactions on Circuits and Systems .I: Fundamental Theory and Applications, Vol. 49, No. 3, pp. 373-378.

[33] Filali, R.L., Hammami, S., Benrejeb, M. and Borne, P. (2012) 'On synchronization, anti-synchronization and hybrid-synchronization of 3D discrete generalized Hénon map', Nonlinear Dynamics and Systems Theory, Vol. 12, No. 1, pp. 81–95.

[34] Baier, G and Klein, M. (1999) 'Maximum hyperchaos in generalized Hénon maps', Physics Letters A, Vol. 151, No. 6-7, pp. 281–284.

[35] Filali, R.L., Hammami, S., Benrejeb, M. and Borne, P. (2012) 'On synchronization, anti-synchronization and hybrid-synchronization of 3D discrete generalized Hénon map', Nonlinear Dynamics and Systems Theory, Vol. 12, No. 1, pp. 81–95.

[36] Jiang Z.P. , Tang W.K.S and Chen G. (2003) 'A simple global synchronization criterion for coupled chaotic systems', Chaos Solitons Fract, Vol. 15, No.5, pp. 925–935.

[37] Benrejb, M., Gasmi, M. (2001) "On the use of an arrow form matrix for modeling and stability analysis of singularly perturbed non-linear systems" Systems Analysis-Modelling-Simulation Vol. 40, No. 4, pp. 509

[38] M Benrejeb, M Gasmi, P Borne "New stability conditions for TS fuzzy continuous nonlinear models" Nonlinear Dynamics and Systems Theor, Vol. 5, No.4, pp. 369-379.

Ameni DRIDI was born in Tunisia in 1989. She obtained the Diploma of National enfineer from "Ecole Nationale des ingéneiurs de Tunis" ENIT in 2013, Currently a Phd student in ENIT. Her research interests are in the area of chaotic systems synchronization and secured communication.

Rania Linda FILALI was born in Tunisia in 1985. She obtained the Diploma of National engineer from "Ecole Nationale des ingéneiurs de Tunis" ENIT in 2008, The Master degree of Automatic control in 2010 from ENIT, the PhD in Automatic Control from "Ecole Nationale des ingéneiurs de Tunis and "Ecole Centrale de Lille" . Her research interests are in the area of chaotic systems synchronization and secured communication.

Pr. Mohamed BENRAJEB was born in Tunisia in 1950. He obtained the Diploma of "Ingénieur IDN" (French "Grande Ecole") in 1973, The Master degree of Automatic Control in 1974, the PhD in Automatic Control of the University of Lille in 1976 and the DSc of the same University in 1980. Full Professor at "Ecole Nationale d'Ingénieurs de Tunis" since 1985 and at "Ecole Centrale de Lille" since 2003, his research interests are in the area of analysis and synthesis of complex systems based on classical and non conventional approaches.