On observer synchronization of non-identical discrete-time hyperchaotic maps based on aggregation techniques and arrow form matrix

R.L. Filali M. Benrejeb and P. Borne

Rania Linda Filali1, Mohamed Benrejeb2, Pierre Borne3
1, 2 LARA. Ecole Nationale d’Ingénieurs de Tunis (ENIT)
BP 37, Le Belvédère, 1002 Tunis, Tunisia
1, 3 LAGIS. Ecole Centrale de Lille
Cité Scientifique BP 48, F 59651, Villeneuve d’Ascq Cedex, Lille, France
E-mail: 1 rania.filali@ec-lille.fr, 2 mohamed.benrejeb@enit.rnu.tn, 3 pierre.borne@ec-lille.fr

Abstract
In this paper, new sufficient conditions for synchronization of non-identical discrete-time hyperchaotic maps is proposed for hyperchaotic cryptosystem communication. They use aggregation techniques for stability study associated to the Benrejeb arrow form matrix for system description. In addition, suitable choice of outputs feedback brings the problem of synchronization of two non-identical hyperchaotic maps to two identical hyperchaotic maps one. The considered case of synchronization of third order hyperchaotic Hénon-Baier Klein maps shows the efficiency of the proposed approach to recover secure transmission of an image and a text.

Keywords: synchronization, discrete-time hyperchaotic maps, aggregation technique, arrow form matrix, secure communication.

1 Introduction

During the last decades, the problem of the synchronization of chaotic and hyperchaotic maps has gained a significant attention due to its potential applications, especially in the light of its application in secure communication area. Synchronization phenomena of chaotic systems makes the trajectories of the master system and the slave ones achieving synchronism after a transition time, starting from different initial conditions. Many effective methods have already been successfully applied to the problem since Pecora and Carrolls research works [1]. Recently, with the development of nonlinear control theory, various synchronization schemes have been proposed such as: adaptive control [3], observer-based control [14], backstepping control [4], active control [5] or nonlinear control [13]. However, most of the methods, mentioned above, are designed to synchronize two identical chaotic systems. In this paper, the proposed synchronization of two non-identical discrete-time chaotic systems which is well adapted with the secure communication is based on establishing new output feedback stabilizing conditions. With the
use of the Borne and Gentina practical criterion for stability study [7, 8] associated to
the Benrejeb arrow form matrix for system description [6, 10, 11], this approach consti-
tutes an extension of previous results on synchronization studies of identical discrete-time
chaotic processes [13, 14]. In Section 2, sufficient conditions leading to conclude to the
synchronization of non-identical discrete-time hyperchaotic maps are given for a secure
communication scheme combining conventional cryptographic methods and synchroniza-
tion of discrete-time hyperchaotic systems. In section 3, the proposed design of a complete
synchronous output feedback stabilizing controller of two non-identical Baier-Klein map-
Hénon maps is applied with success for secure transmission of signals as an image and a
text.

2 Design of observer synchronization for non-identical
chaotic maps using single channel transmission

In this section, the discrete-time hyperchaotic secure communication, called hyperchaotic
cryptosystem, figure 1, shows the efficiency of the proposed non-identical hyperchaotic
approach synchronization. This cryptosystem is a combination of a classical cryptographic
technique and of observer-based synchronization, allowing the receiver to recover the
information transmission without considering noise such that: \( y_m(k) = y_s(k) \).

\[
\begin{align*}
x_m(k+1) &= Ax_m(k) + f(x_m(k)) + E + \delta NV(k) \\
y_m(k) &= Cx_m(k)
\end{align*}
\]

\( N = [n_1 \ldots n_q]^T \) is a constant vector characterizing the way to mix the ciphertext \( V(k) \)
with the chaotic signal \( x_m(k) \), \( \delta \) a scaling factor chosen to allow the term \( \delta NV(k) \) to
belong to a compatible range with respect to the minimum and the maximum bounds of
states variables of master and slave chaotic signals [18].

Let consider a slave system in the receiver side described as:

\[
\begin{align*}
x_s(k+1) &= A_1x_s(k) + f_1(x_s(k)) + E_1 + Bu(k) \\
y_s(k) &= Cx_s(k)
\end{align*}
\]
with $x_m(k) = [x_{m1}(k) \ldots x_{mn}(k)]^T \in \mathbb{R}^n$, $x_s(k) = [x_{s1}(k) \ldots x_{sn}(k)]^T \in \mathbb{R}^n$.

$E$ and $E_1$ are constant vectors of systems (1) and (2), respectively.

$$B = I_{n \times n}$$

$(x_m(0), x_s(0)) = ((1, 0.1, 0), (-0.5, 0, 0.3))$ initial conditions, $A = \{a_{ij}\}$ and $A_1 = \{a_{1_{ij}}\}$ constant matrices and $f(x_m(k))$ and $f_1(x_s(k))$ nonlinear vectors.

The key $K_e(k)$ in the transmitter side is defined by:

$$K_e(k) = \text{int} \left( A \sqrt{x_{m1}^4 + \cdots + x_{mn}^4} \right) \mod 256$$

and the key $K_d(k)$ in the receiver side as following:

$$K_d(k) = \text{int} \left( A \sqrt{x_{s1}^4 + \cdots + x_{sn}^4} \right) \mod 256$$

The function $\text{int}(x)$ gives the integer part of $x$.

The used encryption $e(.)$ is an XOR algorithm:

$$V(k) = e(m(k), K_e(k)) = m(k) \oplus K_e(k)$$

and the decryption function $d(.)$ is as following:

$$m_r(k) = d(V(k), K_d(k)) = V(k) \oplus K_d(k)$$

$m_r(k)$ is the recovered encrypted signal, $d(.)$ the corresponding decryption function. If the chaotic systems of the receiver and transmitter are synchronized, the receiver side can find the same $K_d(k)$, as in the encrypter, $K_e(k)$. The goal now is to synchronize master and slave systems and, at the same time, to design a Luenberger-like discrete observer depending on gain based on a suitable choice of the control law $u(k)$ designed to make two non-identical chaotic systems achieving the complete state synchronization.

The evolution of the error vector $e(k)$ between the master and the slave systems:

$$e(k) = x_s(k) - x_m(k)$$

can also be described by the following:

$$e(k + 1) = A_1 x_s(k) + f_1(x_s(k)) - A x_m(k) + f(x_m(k)) + E_1 - E + B u(k) + N \delta V(k)$$

The following vector controllers $u(k)$, retained in this case, is by outputs feedback control design and by the introduction of an additional compensation term:

$$u(k) = (A - A_1) x_s(k) + f(x_s(k)) - f_1(x_s(k)) - E_1 + E + L (y_m(k) - y_s(k))$$

where:

- $L(.) = \{l_i(.)\} \in \mathbb{R}^n$ is an unknown vector gain of observer to be determined,

- $u(k)$ is chosen as (10) to bring the synchronization study of non-identical discrete-time hyperchaotic systems (1) and (2) to synchronization study of two identical hyperchaotic systems, described as (1).
The substitution of (10) into (9) yields the error system as following:

\[ e(k+1) = A e(k) + f(x_s(k)) - f(x_m(k)) + N\delta V(k) - BL(Cx_m(k) + \delta V(k) - Cx_s(k)) \]

\[ e(k+1) = (A - BL) e(k) + \delta V(k) (N - BL) + f(x_m(k)) - f(x_s(k)) \]

(11)

If the considered

\[ N = BL \]

(13)

is satisfied, it comes:

\[ e(k+1) = (A - BL) e(k) + f(x_m(k)) - f(x_s(k)) \]

(14)

Once can observe that by the choice of the output control law \( u(k) \) as (10), it brings the study of synchronizing of two non-identical hyperchaotic systems to the study of two identical ones.

For several chaotic systems, \( f(x_s(k)) - f(x_m(k)) \) can be, as shown in [17], factorized as following:

\[ f(x_s(k)) - f(x_m(k)) = Q(x_m(k), x_s(k)) e(k) \]

(15)

where matrix \( Q(x_s(k), x_m(k)) \) is a bounded matrix whose elements depend on \( x_m(k) \) and \( x_s(k) \).

Then, the error system can be rewritten as:

\[ e(k+1) = A_a(x_m(k), x_s(k)) e(k) \]

(16)

with:

\[ A_a(x_m(k), x_s(k)) = (A + Q(x_s(k), x_m(k)) - BL) \]

(17)

The error process, described by (16), is stabilized by the a choice of suitable control law of (10), making the matrix \( A_a(x_m(k), x_s(k)) \), defined by (17), in the arrow form. For this purpose, the following theorem can be established, based on the use of Borne and Gentina criterion [7, 8] associated to the canonical Benrejeb arrow form matrix \( A_a(.) = \{a_{aij}(.)\} = (A + Q(x_s(k), x_m(k)) - BL) \) [6,10], such that:

\[ A_a(.) = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ a_{n1} & & & a_{nn} \end{bmatrix} \]

(18)

gives sufficient conditions of synchronization of slave (1) with master (2) systems [9,12].

**Theorem 1.** The synchronization error, described by (16) converges towards zero, if the matrix \( A_a(.) \), defined by (17) and (18), is in the arrow form such that:

i. the nonlinear elements are isolated in one row of the matrix \( A_a(.) \);

ii. the diagonal elements, \( a_{aii}(.) \) of the matrix \( A_a(.) \) are such that:

\[ 1 - |a_{aii}(.)| > 0, \forall i = 2, \ldots, n \]

(19)
iii. there exist $\varepsilon > 0$ such that:

$$1 - |a_{a_11}(\cdot)| - \sum_{i=2}^{n} \left( |a_{a_11}(\cdot)a_{a_11}(\cdot)| \times (1 - |a_{a_i}(\cdot)|)^{-1} \right) > \varepsilon$$

(20)

Proof. The comparison system [8] of the error system (17), associated to the vectorial norm $p(z(k)) = [z_1(k) \ldots z_n(k)]^T$, $z(k) = [z_1(k) \ldots z_n(k)]^T$, is defined by the following equation:

$$z(k + 1) = M(A_a(\cdot))z(k)$$

(21)

with $M(\cdot) = \{m_{ij}(\cdot)\}$ such that $m_{ij}(\cdot) = |a_{a_{ij}}(\cdot)| \forall i,j = 1,2,\ldots,n$.

The error system (16) is stabilized by the output feedback law (10) if we make an appropriate choice of vectors gains $L$ and $C$ such as the matrix $(I - M(A_a(\cdot)))$ is an $M$-matrix [15] i.e if, by application of the practical stability criterion of Borne and Gentina [7,8], we have:

$$\begin{align*}
1 - |a_{a_i}(\cdot)| > 0, \forall i = 2,\ldots,n \\
det(I - M(A_a(\cdot))) > \varepsilon
\end{align*}$$

(22)

The computation of the first member of the last inequality, led as following:

$$det(I - M(A_a(\cdot))) = \left(1 - |a_{a_11}(\cdot)|\right) \times \left(\sum_{i=2}^{n} \left( |a_{a_11}(\cdot)a_{a_11}(\cdot)| \times (1 - |a_{a_i}(\cdot)|)^{-1} \right) \right) \times \left(\prod_{j=2}^{n} (1 - |a_{a_{ij}}(\cdot)|) \right)$$

(23)

achieves easily the proof of the theorem.

By the design of suitable output feedback and the above theorem, synchronisation of non-identical hyperchaotic maps is satisfied.

3 Synchronization of two non-identical hyperchaotic 3D generalized Hénon map and 3D Baier-Klein map

In this section, a proposed synchronization approach for a class of two non-identical discrete-time hyperchaotic systems is applied for the case of Baier-Klein/ Hénon.

Consider the following 3D discrete-time Baier-Klein map [16] which can be described as:

$$\begin{align*}
x_{m1}(k + 1) &= b - x_{m2}^2(k) - a.x_{m3}(k) + \delta l_1 V(k) \\
x_{m2}(k + 1) &= x_{m1}(k) + \delta l_2 V(k) \\
x_{m3}(k + 1) &= x_{m2}(k) + \delta l_3 V(k) \\
y_m(k) &= c_1 x_{m1}(k) + c_2 x_{m2}(k) + c_3 x_{m3}(k)
\end{align*}$$

(24)
For the parameters $a$ and $b$ such that $a = 0.1$ and $b = 1.76$, the system (24) is hyperchaotic as shown in figure 2.

In state space, (24) becomes as (1), with:

$$
A = \begin{bmatrix}
0 & 0 & -0.1 \\
1 & 0 & 0 \\
0 & 1 & 0
\end{bmatrix}
$$  \hspace{1cm} (25)

$$
f (x_m (k)) = \begin{bmatrix} -x_{m2}^2 (k) & 0 & 0 \end{bmatrix}^T
$$  \hspace{1cm} (26)

and:

$$
E = \begin{bmatrix} 1.76 & 0 & 0 \end{bmatrix}^T
$$  \hspace{1cm} (27)

Consider the following 3D generalized Hénon map [2] as the slave system:

$$
\begin{cases}
x_{s1} (k + 1) = -b_{1} x_{s2} (k) + u_{1} (k) \\
x_{s2} (k + 1) = 1 + x_{s3} (k) - a_{1} x_{s2}^2 (k) + u_{2} (k) \\
x_{s3} (k + 1) = b_{1} x_{s2} (k) + x_{s1} (k) + u_{3} (k) \\
y_{s} (k) = c_{1} x_{s1} (k) + c_{2} x_{s2} (k) + c_{3} x_{s3} (k)
\end{cases}
$$  \hspace{1cm} (28)

The 3D generalized Hénon map (28), for the parameters $a_1 = 1.07$ and $b_1 = 0.3$, exhibits a hyperchaotic attractor as shown in figure 3.

In state space, (28) becomes as (2), with:

$$
A_1 (x_s (k)) = \begin{bmatrix}
0 & -0.3 & 0 \\
0 & 0 & 1 \\
1 & 0.3 & 0
\end{bmatrix}
$$  \hspace{1cm} (29)

$$
f_1 (x_s (k)) = \begin{bmatrix} 0 & -1.07 x_{s2}^2 (k) & 0 \end{bmatrix}^T
$$  \hspace{1cm} (30)

and:

$$
E_1 = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}^T
$$  \hspace{1cm} (31)

The figure 4 shows the error states between systems (24) and (28), with the following initial conditions $(x_m (0), x_s (0)) = ((1, 0.1, 0), (0.1, 0.2, -0.31))$, when the control law is turned off. It is obvious that the error grows chaotically with time.

Let consider the synchronization error between systems (24) and (28) described by:

$$
e_i (k) = x_{si} (k) - x_{mi} (k), \ i = 1, 2, 3
$$  \hspace{1cm} (32)
Applying (10), $u(k)$ can be written as:

\[
\begin{align*}
  u_1(k) &= 0.3x_{s2}(k) - 0.1x_{s3}(k) + 1.76 - x_{s2}^2(k) - \sum_{j=1}^{3} l_1 c_j e_j(k) \\
  u_2(k) &= x_{s1}(k) - x_{s3}(k) - 1 + 1.07x_{s2}^2 - \sum_{j=1}^{3} l_2 c_j e_j(k) \\
  u_3(k) &= -x_{s1}(k) + 0.7x_{s2}(k) - \sum_{j=1}^{3} l_3 c_j e_j(k)
\end{align*}
\] (33)

The choice of the control law (33), transforms the synchronization of the two non-identical 3D hyperchaotic Baier-Klein and 3D generalized Hénon maps problem to two identical 3D hyperchaotic Baier-Klein hyperchaotic maps one.

In the state space, the error system is as (16) and (17), with:

\[
Q(x_m(k), x_s(k)) = \begin{bmatrix}
0 & -(x_{s2}(k) + x_{m2}(k)) & 0 \\
0 & 0 & 0 \\
0 & 0 & 0
\end{bmatrix}
\] (34)

\[
B = I_{3 \times 3}
\] (35)

\[
C = \begin{bmatrix}
c_1 & c_2 & c_3
\end{bmatrix}
\] (36)

and:

\[
L = \begin{bmatrix}
l_1 & l_2 & l_3
\end{bmatrix}^T
\] (37)

The matrix, $A_a(x(k))$ can be rewritten as:

\[
A_a(.) = \begin{bmatrix}
-l_1(.)c_1(.) & -(l_1(.)c_2(.) + x_{m2}(k) + x_{s2}(k)) & -0.1 - l_1(.)c_3(.) \\
1 - l_2(.)c_1(.) & -l_2(.)c_2(.) & -l_2(.)c_3(.) \\
-l_3(.)c_1(.) & 1 - l_3(.)c_2(.) & -l_3(.)c_3(.)
\end{bmatrix}
\] (38)

The choice of correction parameters $c_3$ and $l_3$ constant and satisfying the constrains:

\[
\begin{align*}
  l_2c_3 &= 0 \\
  1 - l_3c_2 &= 0
\end{align*}
\] (39)

makes this matrix $A_a(x(k))$ in Benrejeb arrow form, such that:

\[
A_a(.) = \begin{bmatrix}
-l_1(.)c_1(.) & -(l_1(.)c_2(.) + x_{m2}(k) + x_{s2}(k)) & -0.1 \\
1 - l_2(.)c_1(.) & -l_2(.)c_2(.) & 0 \\
-l_3(.)c_1(.) & 0 & 0
\end{bmatrix}
\] (40)
The system characterized by (16) is asymptotically stable, if the control gains $l_i$ and $c_j$, $i, j = 1, 2, 3$, are chosen so that the following conditions are satisfied:

i. the nonlinear elements are isolated in one row of the matrix $A_a(x(k))$;

ii. the diagonal element of the matrix $A_a(x(k))$ is such that:

$$1 - |l_2c_2| > 0$$

(41)

iii. there exist $\varepsilon > 0$ such that:

$$1 - |l_1c_1| - \frac{(x_{m2}(k) + x_{s2}(k) + |l_1c_2|)(|1 - l_2c_1|)}{1 - |l_2c_2|} - \frac{0.1c_1}{c_2} \geq \varepsilon$$

(42)

**Boundedness property**

The solutions $x_m(k)$ respectively $x_s(k)$ of the hyperchaotic attractor of systems (24) and (28) are forward completely and uniformly bounded. Boundedness is a common assumption for many physical systems such as oscillators and, more particularly, chaotic oscillators. The boundedness property of (24) and (28) allows us to perform the following transformation: $|x_{mu}| < 2$ and $|x_{su}| < 2$; thus, we have:

$$|x_{m2} + x_{s2} + l_1c_2| < 4 + |l_1c_2|$$

The condition (iii) of the above theorem can be rewritten as follows:

$$1 - |l_1c_1| - \frac{(4 + |l_1c_2|)(|1 - l_2c_1|)}{1 - |l_2c_2|} - \frac{0.1c_1}{c_2} > 0$$

(43)

Then, instantaneous gains $l_i$ and $c_j$, $\forall i, j = 1, 2, 3$, satisfying inequalities (41) and (43) such as:

$$C = \begin{bmatrix} 1.73 & 0.91 & 0 \end{bmatrix}$$

(44)

$$L = \begin{bmatrix} -0.20 & 0.55 & 1.10 \end{bmatrix}^T$$

(45)

 guaranty the synchronization of systems (24) and (28), as shown in figures 5 and 6.

![Figure 5: Time responses of master (Baier-Klein map) (——) and slave (Henon map)(——) outputs.](image)

![Figure 6: Error dynamics of the two diffrents hyperchaotic maps for activated controller](image)

The transmitted messages used in this paper, to show the efficiency of the proposed output control law, are exemples of a text and of a photography of Lena.

The figures 7 and 8 show that the synchronization between two discrete-time hyperchaotic systems is achieved via an output feedback law using the proposed approach. One can see that the generalized Hénon system is controlled to become Baier-Klein system. We can conclude that the proposed approach is applied with success to recover messages, as it is shown in figures 9 and 10.
Stabilization conditions are proposed for 3D chaotic discrete-time systems synchronization.

Figure 9: A single channel transmission: (α) original text $m(k)$, (β) crypted text $\delta^{-1}y_m(k)$, (γ) recovered text $m_r(k)$

Figure 10: A single channel transmission: (α) original Lena photo $m(k)$, (β) crypted Lena photo $\delta^{-1}y_m(k)$, (γ) recovered Lena photo $m_r(k)$

4 Conclusion

In this paper, new suitable output feedback stabilizing conditions is proposed between two non-identical hyperchaotic discrete-time systems, for the case of image and text transmission. Numerical simulations illustrate the efficiency of the above stabilization conditions for the exemple of 3D generalized hyperchaotic Hénon and 3D Baier-Klein maps bringed in two identical Baier-Klein ones.

References


