OBSERVABILITY PROPERTIES AND STATISTICAL ANALYSIS OF A CHAOTIC "JOUNCE" CRYPTOSYSTEM

Octaviana DATCU[1], Mihai STANCIU[2]

Hyperchaos is considered to improve security, when compared to chaos, by providing more complex and less vulnerable temporal signals for secret communications. One of the simplest jounce hyperchaotic systems is analyzed to decide upon the possibility to reconstruct all four states, at the receiving end, when over the communication channel only one of the four states is sent. A very simple secret communication scheme, with the first state of the transmitter as its output, is proposed. The distributions of the estimation errors are investigated. The recovery of the secret message is tested under changes of the secret key.

Keywords: hyperchaos, synchronization, error distribution, cryptosystem, observer

1. Introduction

Variables such as position, velocity and acceleration are well known in the study of the dynamics of a point. Less known are the jerk and the jounce, its changing rate defined by (1), where $\vec{a},\vec{v},\vec{d}$ are the acceleration, velocity and distance. Vectors $\vec{j}$ and $\vec{s}$ correspond to the jerk and the jounce, also known as spasm, sprite, surge or snap [13].

$$\vec{j}=\frac{d\vec{a}}{dt}=\frac{d^2\vec{v}}{dt^2}=\frac{d^3\vec{d}}{dt^3};\qquad \vec{s}=\frac{d\vec{j}}{dt}=\frac{d^2\vec{a}}{dt^2}=\frac{d^3\vec{v}}{dt^3}=\frac{d^4\vec{d}}{dt^4} \tag{1}$$

A chaotic system has one positive Lyapunov exponent, *i.e.* a direction in which it obeys a positive reaction, being unstable. It must also possess a null exponent along the flow and one negative exponent to ensure the evolution of the solution in a bounded space. Consequently, a continuous chaotic system must have at least three dimensions [14]. The hyperchaotic behavior is stated as being the dynamics with at least two positive Lyapunov exponents, thus having at least four coordinates [12]. This corresponds to the jounce, the fourth derivative of position, thus being a hyperjerk. One of the simplest hyperjerks is described by equation (2) [1]:

[1] Lecturer, Dept.of Telecommunications, University POLITEHNICA of Bucharest, Romania, e-mail: od@elcom.pub.ro

[2] Associate Professor, Dept.of Telecommunications, University POLITEHNICA of Bucharest, Romania, e-mail: ms@elcom.pub.ro

$$\frac{d^4x}{dt^4}+\frac{d^3x}{dt^3}+A\frac{d^2x}{dt^2}+\left(\frac{dx}{dt}\right)^2+x=0\rightarrow\begin{cases}\dot{x}_1=x_2\\ \dot{x}_2=x_3\\ \dot{x}_3=x_4\\ \dot{x}_4=-(x_1+x_2^2+Ax_3+x_4)\end{cases} \tag{2}$$

where $\dot{x}_k=dx_k(t)/dt, k=\{1,2,3,4\}$ and A is the bifurcation parameter of the system. [1] contains the bifurcation diagram corresponding to the number of solutions the system (2) has, when varying the parameter A in the interval [3.3;4.6].

Due to their properties, chaotic signals can be used to mask the secret message in secure communications [9]. Pecora [10] highlighted that the extraction of the message masked by a chaotic signal pointed out by Pérez and Cerdeira [11] can be overcome by using hyperchaotic systems, manifesting increased randomness and higher unpredictability compared to chaos. Hyperchaos improves security by providing more complex and less vulnerable temporal signals [2].

One of the simplest jounce (hyperjerk) systems is analyzed to decide upon the possibility to reconstruct all four states, at the receiving end, when a transmitter sends over the communication channel only one of the four state variables it possesses. A simple secret communication scheme, with the output of the transmitter being is its first state, is proposed. This choice leads to an identity between the original state space and the estimates obtained by a properly tuned higher order sliding-mode observer, thus the message being easily recovered by the receiver. The distributions of the estimation errors are taken into account for identical initialization of the transmitter and the receiver, and for different starting point for the latter. The recovery of the secret message is tested under changes of the values of the control parameter and those of the initial conditions. The larger frame of the present work is defined in [5] and [6].

2. Main results

A. The first state of the hyperjerk as output of an encryption scheme

The transform induced by choosing $z_1=y=x_1$ as the output of the transmitter (2), and successively deriving it, to reveal the unknown states, is in:

$$\begin{cases}z_1=x_1\\ z_2=x_2\\ z_3=x_3\\ z_4=x_4\end{cases} \tag{3}$$

Following, a secret message is added to the dynamics of the hyperjerk (2) by using the inclusion method belonging to the third generation of chaotic secure communication [15]. Consequently, the unknown message denoted m, is added to the fourth equation of system (2). The coordinate change (3) becomes (4), a new derivative of the data series being needed, in order to retrieve the message.

$$\begin{cases} z_1 = x_1 \\ z_2 = x_2 \\ z_3 = x_3 \\ z_4 = x_4 \\ z_5 = -(x_1 + x_2^2 + Ax_3 + x_4) + m \end{cases} \tag{4}$$

To estimate the coordinates $\hat{z}_k, k = \{1,2,3,4,5\}$, the receiver uses a high order sliding-mode observer (HOSMO) [7]:

$$\begin{cases} \dot{\hat{z}}_1 = v_1 = \hat{z}_2 - 8 \cdot L^{1/5} \cdot \left|\hat{z}_1 - y\right|^{4/5} \cdot sign[K \cdot (\hat{z}_1 - y)] \\ \dot{\hat{z}}_2 = v_2 = \hat{z}_3 - 5 \cdot L^{1/4} \cdot \left|\hat{z}_2 - v_1\right|^{3/4} \cdot sign[K \cdot (\hat{z}_2 - v_1)] \\ \dot{\hat{z}}_3 = v_3 = \hat{z}_4 - 3 \cdot L^{1/3} \cdot \left|\hat{z}_3 - v_2\right|^{2/3} \cdot sign[K \cdot (\hat{z}_3 - v_2)] \\ \dot{\hat{z}}_4 = v_4 = \hat{z}_5 - 1.5 \cdot L^{1/2} \cdot \left|\hat{z}_4 - v_3\right|^{1/2} \cdot sign[K \cdot (\hat{z}_4 - v_3)] \\ \dot{\hat{z}}_5 = v_5 = -(\hat{z}_2 + 2\hat{z}_2\hat{z}_3 + A_2\hat{z}_4 + \hat{z}_5) - 1.1 \cdot L \cdot sign[K \cdot (\hat{z}_5 - v_4)] \end{cases} \tag{5}$$

Once the $\hat{z}_k, k = \{1,2,3,4,5\}$ coordinates are accurately estimated, the states $\hat{x}_k, k = \{1,2,3,4\}$ and the message $\hat{m}$ are given by:

$$\begin{cases} \hat{x}_1 = \hat{z}_1 \\ \hat{x}_2 = \hat{z}_2 \\ \hat{x}_3 = \hat{z}_3 \\ \hat{x}_4 = \hat{z}_4 \\ \hat{m} = \hat{z}_5 + (\hat{z}_1 + \hat{z}_2^2 + A_2\hat{z}_3 + \hat{z}_4) \end{cases} \tag{6}$$

The Euler method is used in Matlab-Simulink, being the only that is reliable with sliding-mode simulation, according to [7]. The fixed step used is $T_s = 10^{-5}$. The transmitter is initialized with $(x_1, x_2, x_3, x_4)\big|_{t=0} =$ $(0.85, 0.26, 0.48, 0.18)$. Its parameter is $A = 3.48$, for hyperchaotic behavior [1].

To tune the HOSMO (5), its parameters K and L should be chosen such that the estimation is done accurately and subject to as less chattering as possible, *i.e.* the effect induced by the high frequency control switching, which can be dangerous in applications [7]. The observer (5) has initial conditions

$(z_1, z_2, z_3, z_4, z_5)\big|_{t=0} = ((x_1, x_2, x_3, x_4)\big|_{t=0}, 0.63)$, where $z_5\,|_{t=0}$ was randomly chosen from a uniform distribution in [0,1]. The parameter $A_2 = A = 3.48$. The recovery of the states of the transmitter and the secret message, with (5) and (6), for parameters $(K, L) = (10^{20}, 200)$ for the HOSMO are given in Fig. 1. More details and values can be found at http://www.elcom.pub.ro/~od/.

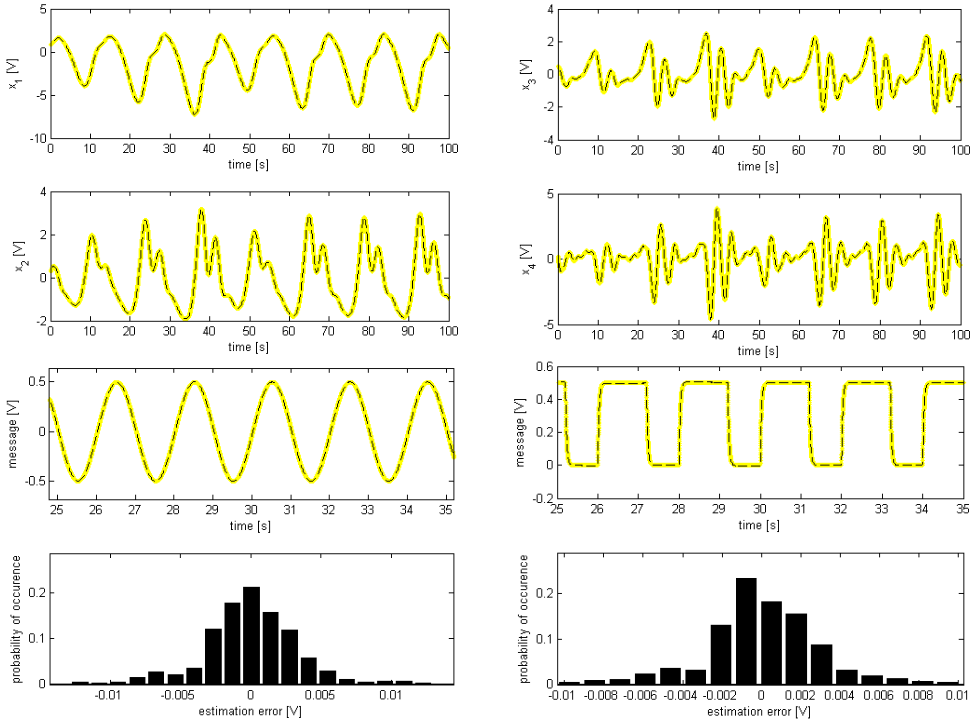

Fig. 1. Reconstruction of the states of the transmitter and of the secret message for parameters $(K, L) = (10^{20}, 200)$ and identical initialization of the transmitter and the receiver. Originals in solid bold line, estimated in dashed line.

The message was chosen to be a sine wave (left), respectively a rectangular wave (right), both with amplitude $A = 0.5V$ and frequency $f = 0.5Hz$. The maximum error between the estimated message and the original one, included in the dynamics of the transmitter (2), is about 25 mV, with a very low probability, as observed from Fig. 1. After applying the formula in the fifth equation in (6), a first order Butterworth low pass filter with cutting frequency $f_{-3dB} = 11 \cdot f$ is used, to filter high frequency noise from the estimated message. For better comparison of the signals, the original message was also filtered.

The states x_1, x_2, x_3, x_4 are accurately estimated with errors of order $10^{-16}, 10^{-10}, 10^{-7}, 10^{-3}$, respectively, as exemplified in Fig. 2, for a rectangular wave as message.

The recovered message and the probability distribution function of the estimation error are portrayed in Fig. 3 for different parameters K and L.

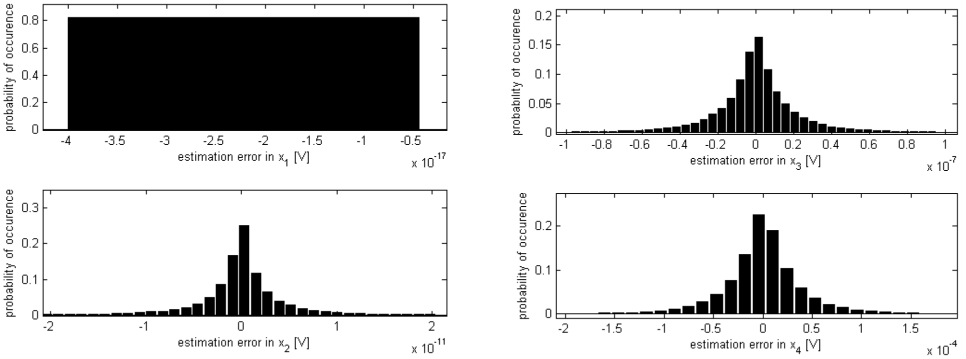

Fig. 2. Estimation errors for parameters $(K, L) = (10^{20}, 2 \cdot 10^3)$ and identical initialization of the transmitter and the receiver, for rectangular wave as message.

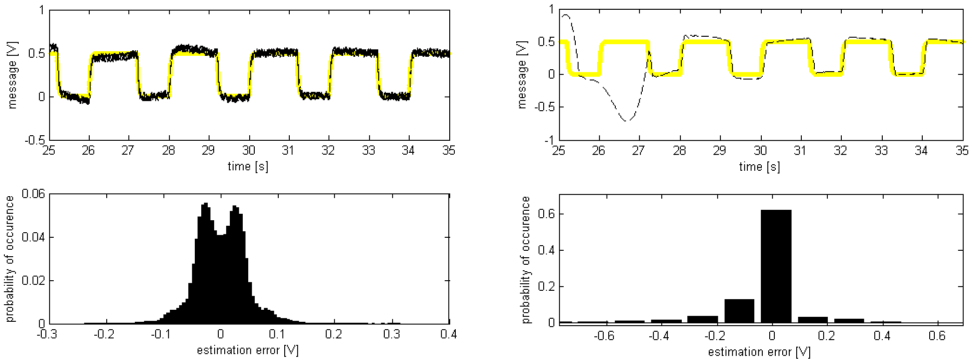

Fig. 3. Reconstruction of the secret message for parameters $(K, L) = (10^{10}, 2 \cdot 10^3)$ (left) and $(K, L) = (10^{10}, 5)$ (right); identical initialization of the transmitter and the receiver.

Once the observer is tuned, one must verify the sensitivity of the encryption scheme to a change in the key $E = \{A, (x_1, x_2, x_3, x_4)|_{t=0}\}$. Thus, the initial conditions for the observer are chosen from random standard normal distributions, $(z_1, z_2, z_3, z_4, z_5)|_{t=0} = (0.54, 1.83, -2.26, 0.86, 0.32)$, whilst the transmitter remains initialized at $(x_1, x_2, x_3, x_4)\big|_{t=0} = (0.85, 0.26, 0.48, 0.18)$. The observer converges to original states and the message is obtained without difficulty, when the receiver has exact knowledge of the transmitter’s parameter,

$A_2 = A,$ but with inacceptable error when the receiver introduces a truncated value of A for the parameter A_2, as depicted in Fig. 4. The acceptable threshold for the value of the error is established in the context of the application. If the communication partners are interested in the absolute values of the secret message, an error of up to $50mV = 10\%$ from its amplitude can be tolerable.

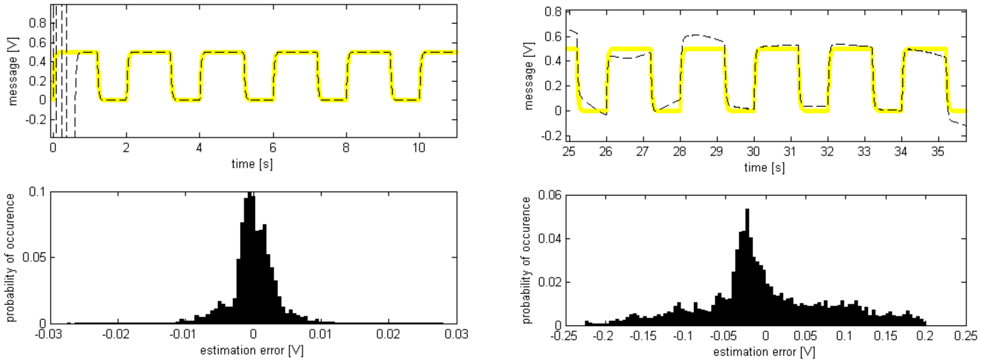

Fig. 4. Reconstruction of the secret message for parameters $(K, L) = (10^{10}, 2 \cdot 10^3)$ when the observer is initialized from random standard normal distributions. The parameter of the receiver is $A_2 = A = 3.48$ (left) and $A_2 = 3.4$ (right).

The proposed scheme can be improved with additional operations, for example taking into account the minimum sampling distance for a chaotic attractor to obtain statistical independent data [8].

B. The second state of the hyperjerk transmitted over the communication channel

If the transmitter chooses the output of (2) to be $z_1 = y = x_2$, the receiver has to solve (7). Having the algebraic solution, he is able to reconstruct the original dynamics, knowing only the output and its successive derivatives.

$$\begin{cases} z_1 = x_2 \\ z_2 = x_3 \\ z_3 = x_4 \\ z_4 = -(x_1 + x_2^2 + A_2 x_3 + x_4) \\ z_5 = -(x_2 + m + 2x_2 x_3 + A_2 x_4 + z_4) \end{cases} \rightarrow \begin{cases} \hat{x}_2 = \hat{z}_1 \\ \hat{x}_3 = \hat{z}_2 \\ \hat{x}_4 = \hat{z}_3 \\ \hat{x}_1 = -(\hat{z}_1^2 + A_2 \hat{z}_2 + \hat{z}_3 + \hat{z}_4) \\ \hat{m} = -(\hat{z}_1 + 2\hat{z}_1 \hat{z}_2 + A_2 \hat{z}_3 + \hat{z}_4 + \hat{z}_5) \end{cases} \quad (7)$$

Again, an observer as the one in (5) can be used to estimate the new coordinates $\{\hat{z}_1, \hat{z}_2, \hat{z}_3, \hat{z}_4\}$. The difference with respect to (5) is represented by the dynamics in (8). The derivative of the message m was not considered due to the appropriate tuning of the afferent observer to overcome the unknown perturbation.

$$\dot{\hat{z}}_5 = -(\hat{z}_2 + 2\hat{z}_2^2 + 2\hat{z}_1\hat{z}_3 + A_2\hat{z}_4 + \hat{z}_5) - 1.1 \cdot L \cdot sign[K \cdot (\hat{z}_5 - v_4)] \qquad (8)$$

The message was, this time, added to the evolution of the first state of the transmitter (2), $\dot{x}_1 = x_2 + m.$ Thus, it appears last in the derivatives of the output $y = x_2$, being the furthest in space from it.

C. The third state of the hyperjerk as its output

When the transmitter chooses the output $z_3 = y = x_3$, the coordinate change seen by the receiver is the one in (9). Because of the supplementary difficulty introduced by the singularity of observability manifold, the reconstruction in (10) refers only to the states of the transmitter. For a more detailed frame for the singularity of observability manifolds see [3,4].

$$\begin{cases} z_1 = x_3 \\ z_2 = x_4 \\ z_3 = -(x_1 + x_2^2 + A_2 x_3 + x_4) \\ z_4 = -(x_2 + 2x_2x_3 + A_2x_4 - x_1 - x_2^2 - A_2x_3 - x_4) \end{cases} \qquad (9)$$

The solution in (10) can be obtained if and only if $1 + 2z_1 \neq 0.$

$$\begin{cases} x_3 = z_1 \\ x_4 = z_2 \\ x_2 = -(A_2z_2 + z_3 + z_4)/(1 + 2z_1) \\ x_1 = -[A_2z_1 + z_2 + z_3 + (A_2z_2 + z_3 + z_4)^2/(1 + 2z_1)^2] \end{cases} \qquad (10)$$

Consequently, the singularity observability manifold, when the measured variable is $y = z_1 = x_3$, is given by (11). Each time the measured value is in the vicinity of -0.5, the receiver cannot get the individual values for x_1 and x_2, but only for the sum $x_1 + x_2^2$. The incidence of the singularity of observability for $A = 3.63$ and $(x_1, x_2, x_3, x_4)\big|_{t=0} = (0.85, 0.26, 0.48, 0.18)$ is given in Fig. 5 (left).

$$S_3 = \{(x_1, x_2, x_3, x_4\} \in \Re^4 \mid x_3 = -0.5\} \qquad (11)$$

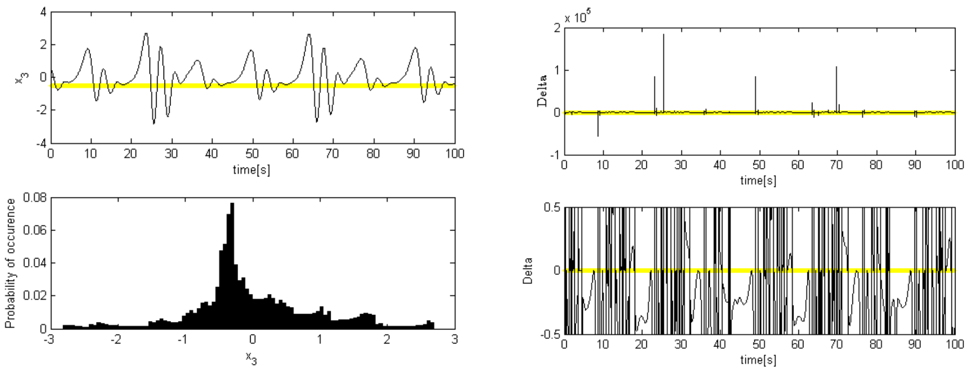

Fig. 5. Transmitter with $A = 3.63$ and $(x_1, x_2, x_3, x_4)|_{t=0} = (0.85, 0.26, 0.48, 0.18)$. ***Left:*** The output x_3 and the singularity of observability (bold line) (top). Distribution of x_3 (bottom). ***Right:*** Discriminant of the quadratic equation in x_2 (13), induced by the measured state x_4.

D. The fourth state of the hyperjerk measured at the receiver's end

The output of the transmitter is $z_4 = y = x_4$, such that the coordinate change between the transmitter's state space and the receiver's is:

$$\begin{cases} z_1 = x_4 \\ z_2 = -(x_1 + x_2^2 + A_2 x_3 + z_1) \\ z_3 = -(x_2 + 2x_2 x_3 + A_2 z_1 + z_2) \\ z_4 = -(x_3 + 2x_2 z_1 + 2x_3^2 + A_2 z_2 + z_3) \end{cases} \tag{12}$$

The system (12) can be rewritten as in (13), where the quadratic equation in x_2 must have unique solution, as a cryptographic function has to be injective.

$$\begin{aligned} & z_1 = x_4 \\ & x_1 = -(z_1 + z_2) - (x_2^2 + A_2 x_3) \\ & \left.\begin{aligned} z_3 x_3 &= -x_2 x_3 (1 + 2x_3) - x_3 (A_2 z_1 + z_2) \\ z_4 x_2 &= -x_3 x_2 (1 + 2x_3) - 2z_1 x_2^2 - x_2 (A_2 z_2 + z_3) \end{aligned}\right\} \xrightarrow{(-)} \\ & \rightarrow 2z_1 x_2^2 + x_2 (A_2 z_2 + z_3 + z_4) - x_3 (A_2 z_1 + z_2 + z_3) = 0 \end{aligned} \tag{13}$$

To fulfill this requirement, the discriminant $\Delta = (A_2 z_2 + z_3 + z_4)^2 + 8z_1 x_3 (A_2 z_1 + z_2 + z_3)$ must be null. In this case, the solution of system (12) is the one from (14), where the conditions $\hat{z}_1 \neq 0$ and $A_2 \hat{z}_1 + \hat{z}_2 + \hat{z}_3 \neq 0$ must also be fulfilled. Still, the discriminant Δ is rarely zero, as illustrated in Fig. 4 (right) for $A = 3.63$ and $(x_1, x_2, x_3, x_4)\big|_{t=0} = (0.85, 0.26, 0.48, 0.18),$ where the measured variable is x_4.

$$\begin{cases} \hat{x}_4 = \hat{z}_1 \\ \hat{x}_2 = -0.25 \cdot (A_2\hat{z}_2 + \hat{z}_3 + \hat{z}_4) / \hat{z}_1 \\ \hat{x}_3 = -(A_2\hat{z}_2 + \hat{z}_3 + \hat{z}_4)^2 / [8\hat{z}_1(A_2\hat{z}_1 + \hat{z}_2 + \hat{z}_3)] \\ \hat{x}_1 = -(\hat{z}_1 + \hat{z}_2) - (\hat{x}_2^2 + A_2\hat{x}_3) \end{cases} \tag{14}$$

3. Conclusions

The continuous-time hyperchaotic behavior implies the existence of at least a fourth dimensional state space. Increased randomness and high unpredictability makes them suitable for cryptographic applications. One of the simplest jounce (hyperjerk) system was analyzed to decide upon the possibility to reconstruct all four states, at the receiving end, when a transmitter sends over the communication channel only one of the four state variables it possess. The first and the second states were proved to engender full reconstruction when measured by the receiver. For the third state of the hyperjerk chosen as its output, the receiver cannot always recover all the states of the dynamics used to send information. The incidence of the singularity of observability is given for some values of the parameter and the initial conditions of the transmitter. When the fourth state of the hyperjerk is measured at the receiver’s end, the algebraic system the receiver must solve, in order to get the original states from the estimates of the changed coordinates, can be restrained to a quadratic equation. The discriminant must be null, as a cryptographic function has to be injective. Still, the discriminant Δ is rarely zero, allowing the estimation of only some combinations of the unmeasured states, not their individual values.

A simple secret communication scheme, with the output of the transmitter being is its first state, was proposed. This choice leads to an identity between the original state space and the estimates obtained by a properly tuned higher order sliding-mode observer, thus the message being easily recovered by the receiver. The distributions of the estimation errors were considered for identical initialization of the transmitter and the receiver, and for different starting point for the latter. The receiver was shown to be robust to initial conditions change, but sensitive to parameter mismatch. Future improvements of the proposed scheme were suggested.

Acknowledgement

The work has been funded by the Sectoral Operational Programme Human Resources Development 2007-2013 of the Ministry of European Funds through the Financial Agreement POSDRU/159/1.5/S/132395.

REFERENCES

[1]. *K. E. Chlouverakis and J.C. Sprott*, “Chaotic hyperjerk systems,” Chaos, Solitons & Fractals, **Vol. 28**, Issue 3, pp. 739–746, May 2006. http://dx.doi.org/10.1016/j.chaos.2005.08.019

[2]. *L. Chunbiao, J. C. Sprott, W. Thio, and Z. Huanqiang*, "A New Piecewise Linear Hyperchaotic Circuit," IEEE Transactions on Circuits and Systems II: Express Briefs, **vol.61**, no.12, pp.977-981, Dec. 2014. http://dx.doi.org/10.1109/TCSII.2014.2356912

[3]. *O. Datcu, R. Tauleigne, A. Vlad and J.-P. Barbot*, “Observability-Singularity Manifolds in the Context of Chaos Based Cryptography,” Proc. of the 3rd International Conference on Systems and Control - ICSC'13. Algeria, Oct. 2013. http://dx.doi.org/10.1109/icosc.2013.6750843

[4]. *M. Frunzete, A. Luca, A. Vlad and J.-P. Barbot*, “Observability and Singularity in the Context of Rössler Map,” Scientific Bulletin of the University POLITEHNICA of Bucharest, **vol. 74**, no. 1, Bucharest, pp. 83-92, 2012. PMid:23005843

[5]. *M. Frunzete, J.-P. Barbot, C. Letellier*, “Influence of the singular manifold of non observable states in reconstructing chaotic attractors,” Phys. Rev. E, American Physical Society, 2012, **86** (2).

[6]. *C. Letellier, L. Aguirre, J. Maquet,* “How the choice of the observable may influence the analysis of nonlinear dynamical systems, Communications in Nonlinear Science and Numerical Simulation,” **Vol. 11**, Issue 5, August 2006, pp. 555–576. doi:10.1016/j.cnsns.2005.01.003.

[7]. *A. Levant*, “Higher-Order Sliding Modes,” Differentiation And Output-Feedback Control, Int. J. Control, **Vol. 76**, Nos 9/10, 924–941, 2003. http://dx.doi.org/10.1080/0020717031000099029

[8]. *A. Luca, A. Vlad,* “Generating Identically and Independently Distributed Samples Starting from Chaotic Signals,” Proceeding of International Symposium on Signal, Circuits & Systems – ISSCS 2005, Ia□i, pp. 227-230, July 2005.

[9]. *L. M. Pecora and T. L. Carroll*, “Synchronization in chaotic systems,” Phys. Rev. Lett. **64**, pp. 821 – 825, February 1990.

[10]. *L. Pecora*, “Hyperchaos harnessed,” Phys. World, **vol. 9**, no. 5, pp. 17–18, May 1996.

[11]. *G. Pérez and H. A. Cerdeira*, “Extracting messages masked by chaos,” Phys. Rev. Lett., **vol. 74**, pp. 1970–1973, 1995. http://dx.doi.org/10.1103/PhysRevLett.74.1970, PMid: 10057809

[12]. *O. E. Rössler*, “An equation for hyperchaos,” Phys. Lett. A, **vol. 71**, No. 2/3, pp. 155–157, Apr. 1979. 1979. http://dx.doi.org/10.1016/0375-9601(79)90150-6

[13]. *J. C. Sprott*, “Some Simple Chaotic Flows,” Phys. Rev. E, **Vol. 50**, No. 2, pp. R647-R650, August 1994. http://dx.doi.org/10.1103/PhysRevE.50.R647, PMid:9962166

[14]. *J. C. Sprott and S. J. Linz*, “Algebraically Simple Chaotic Flows,” International Journal of Chaos Theory and Applications **5**, pp. 3-22, 2000.

[15]. *T. Yang*, “A Survey of Chaotic Secure Communication Systems,” International Journal of Computational Cognition, Vol. 2, No. 2, pp. 81–130, June 2004.