An algebraic state estimation approach for the recovery of chaotically encrypted messages

Hebertt Sira-Ramirez, Michel Fliess

An algebraic state estimation approach for the recovery of chaotically encrypted messages

Hebertt Sira-Ramírez*

CINVESTAV-IPN.

Av. IPN No. 2508.

Departamento de Ing. Eléctrica. Sección de Mecatrónica.

Col. San Pedro Zacatenco. A.P. 14740,

07300 México, D.F., México.

hsira@cinvestav.mx

Michel Fliess

Équipe ALIEN, INRIA Futurs

& LIX (CNRS, UMR 7161), École polytechnique

91128 Palaiseau, France

Michel.Fliess@polytechnique.fr

* This research was supported by the Centro de Investagación y Estudios Avanzados del IPN (Cinvestav-IPN), México City, México. and by Conacyt under Research Grant 42231-Y. Phone: + 52(55)50613794

February 22, 2005

Abstract

In this article, we use a variant of a recently introduced algebraic state estimation method obtained from a fast output signal time derivatives computation process. The fast time derivatives calculations are entirely based on the consequences of using the "algebraic approach" in linear systems description (basically; module theory and non-commutative algebra). Here, we demonstrate, through computer simulations, the effectiveness of the proposed algebraic approach in the accurate and fast (i.e. non asymptotic) estimation of the chaotic states in some of the most popular chaotic systems. The proposed state estimation method can then be used in a coding-decoding process of a secret message transmission using the message-modulated chaotic system states and the reliable transmission of the chaotic system observable output. Simulation examples, using Chen's chaotic system and the Rossler system, demonstrate the important features of the proposed fast state estimation method in the accurate extraction of a chaotically encrypted messages. In our simulation results, the proposed approach is shown to be quite robust with respect to (computer generated) transmission noise perturbations. We also propose a way to evade computational singularities associated with the local lack of observability of certain chaotic system outputs and still carry out the encrypting and decoding of secret messages in a reliable manner.

I. Introduction

The field of chaotic systems has undergone considerable development with a fairly good understanding of the phenomenon and its many implications in applied mathematics, physics, engineering and other scientific research areas. The many interesting developments are due to mathematicians, physicists, computer scientists, control engineers and biologists. The state of the art has been summarized in several special issues of known journals which have been devoted to the problem of chaos, in general, and to chaotic systems synchronization and control in particular (See for instance: Special Issues [1993, 1997a, 1997b, 1998, 2000, 2001]). The reader may look into the enormous collection of references about chaotic systems, and related fields, gathered by Professor G. Chen [1997]. A number of books already exist on the subject (see, for instance, [Holden, 1986], [Mira, 1987], [Afraimovitch *et al.*, 1994], [Ott *et al.*, 1994], [Fradkov & Pogromsky, 1998], [Chen, 1999], and many others). The interest in the topic of synchronization and chaotic system state estimation arises from the possibilities of encoding, or masking, messages using as an analog "carrier" a signal representing a state, or an output, of a given chaotic system. The effectively random nature of the carrier signal additively, or multiplicatively, modulated by the masked message signal, makes it "difficult" to attempt the decoding of the message from an intercepted transmission (see [Cuomo *et al.*, 1993]). The problem is then one of effectively recovering the hidden, or encrypted message at the receiving end by means of an estimator system, or an

algorithm, which uses one or several of the transmitted signals.

The chaotic system synchronization problem is, therefore, intimately related to the design of a nonlinear *state observer* for the chaotic encoding system (see [Nijmeijer & Mareels, 1997]). In fact, a possible decoding process is based on the remote generation of the state estimates of the coding system, from a transmitted chaotic output signal, and a suitable comparison of such generated state estimates with the transmitted signals containing the message modulated states. However, in contradistinction to observer design, important limitations and freedoms must be taken into account in the decoding system design problem. Traditionally, asymptotic tracking of the actual transmitter's state is demanded by exciting the designed receiving system with a message-free output. The receiving end system should asymptotically track (synchronize) the states of the transmitting system. This approach however entitles the need to robustly sustain the "unmodelled" addition of a masked signal input after synchronization has taken place (See [Pecora & Carroll, 1991]). This insensitivity, or robustness, property is questionable and difficult to achieve in practise. Several research articles deal with some of these important robustness issues. For a passivity based adaptive approach to synchronization the reader is referred to the interesting articles by Fradkov and Markov [1997] and that by Pogromsky [1998]. On the other hand, a purely state estimation based approach entitles the transmission of the chaotic system output for the purpose of remotely generating the unperturbed states of the transmitting system via a properly designed asymptotic observer. The secret messages are then coded in the chaotic states and these are transmitted for comparison with the unperturbed estimated states. The message signal recovery is then immediate. The Hamiltonian structure of a collection of well known examples of chaotic continuous-time systems is exploited in Sira-Ramírez and Cruz-Herández [2001], to obtain asymptotic state observers requiring the message-free output signal. One important feature is that this observer design merely requires linear-based output injection techniques. A similar approach for signal encryption strategies, dealing with the exact state estimation of discrete time nonlinear chaotic systems, was presented in Sira-Ramírez *et al.* [2002].

In this article, we take an *algebraic viewpoint* for the state estimation problem associated with the chaotic encryption-decoding problem. The article emphasizes the use of the "algebraic derivative method" for the efficient and fast computation of accurate approximations to the successive time derivatives of the transmitted observable output signal received at the decoding end. The

observability of the system output allows one to establish a map constituted by a *differential function* of the output (i.e. a function of the output and a finite number of its time derivatives) from which the state can be immediately computed in a static manner (see [Diop & Fliess, 1991]).

Instead of attempting the construction of an asymptotic nonlinear observer for the transmitter or coding system, a set of model independent formulae is developed for the required approximate computation of the time derivatives of an observable transmitted output signal. From these locally valid output time derivatives, the related transmitter system state vector can be easily computed using the static differential parametrization of the states in terms of the observable chaotic output. The time derivatives of the output signal are computed on the basis of a sufficiently accurate truncated Taylor series approximation in combination with the "algebraic derivative method", recently introduced by the authors in Fliess and Sira-Ramírez [2004] for state estimation of linear controlled systems. The key issue here is to initially view the transmitted chaotic system output as a time signal, with no other systems oriented view of its possible functional dependance upon the system state. As a result, a non-asymptotic, fast, state estimation scheme is obtained. The result of our algebraic estimation approach is a set of accurate piecewise continuous approximations to the actual chaotic system state vector components. The calculation method also provides an on-line updating mechanism that allows for the automatic resetting of the involved computations when the validity of the adopted truncated Taylor series approximation ceases to be valid. Incidentally, our formulae for the on line generation of the output signal time derivatives consist, solely, of terms involving integrations and time convolutions of the original observable output signal. The problem of efficiently calculating time derivatives of a given output signal is not entirely new, and some rather interesting approaches have been also proposed in the past (see Diop *et al* [1994], Pelestan and Grizzle [1999] and Diop *et al.* [2000]).

Section 2 summarizes, in a tutorial fashion, the core of the state estimation process to be proposed by revisiting the problem of efficiently computing time derivatives of signals using the algebraic approach. In that section, we provide several state estimation examples dealing with the well known Lorenz system, Chen's system, Chua's chaotic circuit, Rossler's system and the hysteretic chaotic system. Due to a local observability property found in the first two examples, the output time derivative based state estimation leads to a singularity problem in the reconstruction of one of the state variables. This singularity would invalidate the use of that particular state as

a coding signal. Section 3 explains the coding-decoding process based on the algebraic approach to state estimation and provides some simulation examples of a secret message signal extraction which includes dealing with computer generated additive transmission noise. In section 3, the singularity problem encountered for the Lorenz and the Chen's systems is circumvented by using as a coding signal a nonlinear function of the chaotic observable output and the involved singular state. A simulation example is also furnished depicting the proposed singularity free coding-decoding scheme.

II. Signal time derivation through the "algebraic derivative method".

Consider an arbitrary smooth signal, $y(t)$, defined on the non-negative real axis. Suppose it is desired to obtain, on the basis of the continuously measured value of $y(t)$, time signals which closely approximate, during a finite time interval of the real line, a certain number of successive *time derivatives* of the signal $y(t)$.

Below, we propose a method for obtaining close, local, approximations to the time derivatives of $y(t)$ over intervals of time whose length may be arbitrarily fixed to be "small" at the outset, or it may be automatically determined on the basis of the value of an integral squared error criterion. Such a criterion assesses the accuracy of the computed time derivatives of the signal in terms of the reconstruction error of the transmitted signal itself. The proposed calculations, which yield fast (i.e., non asymptotic) estimations of the derivatives of the given signal, are accurately valid over these fixed, or otherwise automatically generated, time intervals and they require to be *reset* when the error criterion reaches a pre-specified threshold value.

For any arbitrary $t_{initial} \geq 0$, the value of the signal at time $t > t_{initial}$ is approximated by the classical truncated Taylor series expansion,

$$\widetilde{y}(t)\mathbf{1}(t - t_{initial}) = \sum_{j=1}^{K} \frac{1}{(j-1)!} y^{(j-1)}(t_{initial})(t - t_{initial})^{(j-1)}, \quad t \geq t_{initial} \tag{1}$$

where $y^{(k)}(t_{initial})$ represents the k-th time derivative of $y(t)$ evaluated at time $t_{initial}$ and K is a strictly positive integer whose magnitude is directly related to the approximating properties of $\tilde{y}(t)$. The function $\mathbf{1}(t - t_{initial})$ is the Dirac unit step, at time $t_{initial}$.

Note that the truncated Taylor series may be represented by the response of an *homogeneous linear time invariant system* with a set of initial conditions represented by the initial value of the

signal $y(t)$ at time $t_{initial}$ and those of the (unknown) first $K-1$ derivatives of such signal at the same instant $t = t_{initial}$.

$$\begin{aligned} \widetilde{y}^{(K)}(t)\mathbf{1}(t - t_{initial}) &= 0, \quad t \geq t_{initial} \\ \widetilde{y}^{(j)}(t_{initial}) &= y^{(j)}(t_{initial}), \quad j = 0, \ldots, K-1 \end{aligned}$$

In operational calculus notation, the approximating system is represented by

$$s^K \widetilde{y}(s) e^{-s\, t_{initial}} - \sum_{j=1}^{K} s^{K-j} y^{(j-1)}(t_{initial}) e^{-s\, t_{initial}} = 0 \tag{2}$$

Clearly, after simplifying out the common factor $e^{-s\, t_{initial}}$ it follows that:

$$\frac{d^K}{ds^K}\left(s^K \widetilde{y}(s)\right) = 0 \tag{3}$$

is independent of all the unknown initial conditions. The crucial observation of the "algebraic derivative" method for computing time derivatives of arbitrary smooth signals is that the set of expressions:

$$s^{-j}\frac{d^K}{ds^K}\left(s^K \widetilde{y}(s)\right) = 0, \;\; j = K-1, K-2, \ldots, 1, \tag{4}$$

yield a triangular system of linear equations from which the time derivatives of the approximating signal $\widetilde{y}$ can be computed, solely in terms of *time convolutions of* $y(t)$. The idea is then to adopt these obtained signals as local approximations to the actual time derivatives of the original signal $y(t)$. Naturally, one reverts to the time domain the calculations made in the frequency domain in order to obtain explicit formulae for approximating the different time derivatives of $y(t)$.

Clearly, the higher the value of K, the closer the approximating features of the obtained formulae to the first few time derivatives of $y(t)$. As a rule of thumb, we may set K to be *twice* the value of the required highest order derivative of $y(t)$.

Example 1: Consider, for instance, the system: $\widetilde{y}^{(4)}(t) = 0$, which is proposed for obtaining a (local) polynomial approximation to the first two derivatives $\dot{y}$ and $\ddot{y}$, of a given sufficiently smooth signal $y(t)$ where, for simplicity, we let $t_{initial} = 0$. We then have that: $\frac{d^4}{ds^4}\left(s^4 \widetilde{y}(s)\right) = 0$. We obtain, after letting $\widetilde{y}$ to be substituted by the actual measured signal y,

$$\frac{d^4}{ds^4}\left(s^4 \widetilde{y}(s)\right) = 24y(s) + 96s\frac{dy(s)}{ds} + 72s^2\frac{d^2y(s)}{ds} + 16s^3\frac{d^3y(s)}{ds^3} + s^4\frac{d^4y(s)}{ds^4} = 0$$

The expressions for $s^{-3}\frac{d^4}{ds^4}\left(s^4\widetilde{y}(s)\right)=0$ and $s^{-2}\frac{d^4}{ds^4}\left(s^4\widetilde{y}(s)\right)=0$, yield

$$\begin{aligned} s^{-3}\frac{d^4}{ds^4}\left(s^4\widetilde{y}(s)\right) &= \left(\frac{24}{s^3}\right)y(s)+\left(\frac{96}{s^2}\right)\frac{dy(s)}{ds}+\left(\frac{72}{s}\right)\frac{d^2y(s)}{ds^2}+16\frac{d^3y(s)}{ds^3}+s\left(\frac{d^4y(s)}{ds^4}\right)=0 \\ s^{-2}\frac{d^4}{ds^4}\left(s^4\widetilde{y}(s)\right) &= \left(\frac{24}{s^2}\right)y(s)+\left(\frac{96}{s}\right)\frac{dy(s)}{ds}+72\frac{d^2y(s)}{ds^2}+16s\frac{d^3y(s)}{ds^3}+s^2\frac{d^4y(s)}{ds^4}=0 \end{aligned}$$

Writing these equalities in the time domain we obtain:

$$\begin{aligned} 24(\int^{(3)} y)-96(\int^{(2)} ty)+72(\int t^2y)-16t^3y+\frac{d}{dt}\left(t^4y(t)\right)=0 \\ 24(\int^{(2)} y)-96(\int ty)+72t^2y(t)-16\frac{d}{dt}\left(t^3y(t)\right)+\frac{d^2}{dt^2}\left(t^4y(t)\right)=0 \end{aligned}$$

Here we have used, for simplicity, the following notation:

$$(\int^{(j)} t^k y)=\int_0^t\int_0^{\sigma_1}\cdots\int_0^{\sigma_{j-1}}\sigma_j^k y(\sigma_j)d\sigma_j\ldots d\sigma_1 \tag{5}$$

The above expressions yield, after some algebraic manipulations, the approximations (or estimates) to the first and second order time derivative of $y(t)$. We obtain

$$\begin{aligned} \left(\frac{dy}{dt}\right)_e &= \frac{1}{t^4}\left[12t^3y-72(\int t^2y)+96(\int^{(2)} ty)-24(\int^{(3)} y)\right] \\ \left(\frac{d^2y}{dt^2}\right)_e &= \frac{1}{t^4}\left[8t^3\left(\dot{y}(t)\right)_e-36t^2y(t)+96(\int ty)-24(\int^{(2)} y)\right] \end{aligned}$$

where, evidently, the second order time derivative expression requires the outcome of the evaluation of the first time derivative expression according to the announced triangular system structure of the equations. Note that, at time $t=0$, the above formulae yield an *indetermination* of the form $0/0$. In fact, due to the finite precision of the numerical processors, the computation will not be accurately defined over a small interval of time of the form: $[0,\epsilon)$. Thus, the formulae for $(dy/dt)_e$ and $(d^2y/dt^2)_e$ are valid for $t\geq\epsilon$. During the interval of time $[0,\epsilon)$, we may replace the value of $(\dot{y})_e$ and $(\ddot{y})_e$ by arbitrary constant values or by appropriate polynomial spline approximations.

It is clear that for any $t\geq\epsilon>0$ the expressions found yield suitable approximations for the first and second order time derivatives of $y(t)$ during an open time interval of the form $[\epsilon,t)$. We now examine the issue of how and when to update, or re-initialize, the computations.

A. Calculations resettings

The validity of the formulae found for the estimates of $\dot{y}$ and $\ddot{y}$ in the open time interval $[\epsilon,t)$ becomes questionable as t grows, due to the approximate nature of the adopted truncated Taylor

series expansion. The calculations need to be reset, or updated, at some finite time t_r. It is not difficult to see that for any resetting time, t_r, we also have the following approximation formulae valid:

$$\begin{aligned}\left(\frac{dy}{dt}\right)_e &= \frac{1}{(t-t_r)^4}\left[12(t-t_r)^3 y(t) - 72(\int_{t_r}(t-t_r)^2 y) + 96(\int_{t_r}^{(2)}(t-t_r)y) - 24(\int_{t_r}^{(3)} y)\right] \\ \left(\frac{d^2y}{dt^2}\right)_e &= \frac{1}{(t-t_r)^4}\left[8(t-t_r)^3\left(\dot{y}(t)\right)_e - 36(t-t_r)^2 y(t) + 96(\int_{t_r}(t-t_r)y) - 24(\int_{t_r}^{(2)} y)\right]\end{aligned}$$

where we have now used the notation:

$$(\int_{t_r}^{(j)}(t-t_r)^k y) = \int_{t_r}^{t}\int_{t_r}^{\sigma_1}\cdots\int_{t_r}^{\sigma_{j-1}}(\sigma_j - t_r)^k y(\sigma_j)d\sigma_j\ldots d\sigma_1 \tag{6}$$

As before, the above formulae for the estimates of $\dot{y}$ and $\ddot{y}$ are valid after a small time interval, of duration ϵ, has elapsed from the instant $t = t_r$, i.e. during the interval $[t_r + \epsilon, t)$. A new resetting is to be carried out when the validity of the approximation becomes questionable. We remark that during the time interval, $[t_r, t_r + \epsilon]$, we may adopt as temporary values for the time derivative estimates $(\dot{y}(t))_e$ and $(\ddot{y}(t))_e$, either constant values of the form $\dot{y}(t_r^-)$ and $\ddot{y}(t_r^-)$ i.e. the last computed values of the time derivatives of the interval $[t_{r-1} + \epsilon, t_r]$, or, alternatively, polynomial splines whose parameters are determined on the basis of the last values of the previously computed time derivatives at time t_r. For instance, we may opt for straight line approximations for the first time derivative and a constant approximation for the second time derivative:

$$\begin{aligned}\dot{y}(t) &= \dot{y}(t_r^-) + (t-t_r)\ddot{y}(t_r^-), \quad \forall t \in [t_r, t_r+\epsilon] \\ \ddot{y}(t) &= \ddot{y}(t_r^-) \ \ \forall t \in [t_r, t_r+\epsilon]\end{aligned}$$

If a larger number of computed time derivatives are available at time t_r, higher order polynomial spline approximations are possible during the small intervals $[t_r, t_r + \epsilon]$. We remark that the time interval of validity of the formulae, which is of the form $[t_r + \epsilon, t_{r+1})$, can also be determined to be fixed at the outset. Of course, this usually entitles choosing a rather small value, say, for the quantity, $t_{r+1} - t_r$, and, perhaps, of some additional off-line trial and error runs. This procedure is, of course, highly dependent upon the encoding system and requires judgment, rather than an objective criterion evaluation.

In the context of this example, but with the aim of proposing a general calculation updating procedure, we now provide an objective criterion for determining a reasonable time instant for the

resettings of the derivative calculations, given that the actual values of such derivatives are not known beforehand.

Note that, at any time t, we may easily generate an estimate, or a reconstruction, of the actual signal $y(t)$ on the basis of the computed time derivatives, up to that moment. Any deviation of this estimated value from the actual (measured) value of the original signal $y(t)$ obeys to the fact that the computed value of the time derivatives of the original signal are drifting from their actual values. Hence, we propose to operate a calculation resetting when the value of the absolute integral squared error surpasses a small constant threshold value $\delta > 0$. i.e. when

$$\int_{t_r}^{t} |e(\sigma)|^2 d\sigma \geq \delta$$

with $e(t)$ defined as $e(t) = y(t) - \widehat{y}(t)$ and $\widehat{y}(t)$ being a generated estimate of $y(t)$ itself, computed on the basis of known data as follows:

$$\widehat{y}(t) = y(t_r) + \left(\dot{y}(t_r)\right)_e (t - t_r) + \frac{1}{2} \left(\ddot{y}(t_r)\right)_e (t - t_r)^2 \tag{7}$$

with $(\dot{y}(t_r))_e$ and $(\ddot{y}(t_r))_e$ being the computed first and second time derivatives of y at time t_r.

In general, however, in cases where more than two time derivatives of a signal are to be computed, one may propose a more general integral square error criterion by involving higher order time derivative estimates.

B. Observability of nonlinear systems

Consider a smooth nonlinear system, characterized by a state vector $x \in R^n$, of the form,

$$\begin{aligned} \dot{x} &= f(x), \\ y &= h(x) \end{aligned} \tag{8}$$

where y is the output of the system and $h(\cdot)$ is a smooth scalar map taking values on the real line. The output $y = h(x)$ of the system is said to be *locally observable* if the following map is locally full rank n,

$$\begin{bmatrix} y \\ \dot{y} \\ \vdots \\ y^{(n-1)} \end{bmatrix} = \begin{bmatrix} h(x) \\ L_f h(x) \\ \vdots \\ L_f^{n-1} h(x) \end{bmatrix} \tag{9}$$

where $L_f^k h(x)$ stands, in local coordinates, for $\frac{\partial L_f^{k-1} h(x)}{\partial x} f(x)$ with $L_f^0 h(x) = h(x)$.

A well known result establishes that if the above map is locally full rank n, then the state vector, x, of the system can be locally expressed as a smooth *differential function* of y i.e. a smooth function of y and a finite number (in fact $n-1$) of its time derivatives (see [Diop & Fliess, 1991] and also [Fliess, 1987]). We also address this type of function as a *differential parametrization* of the state x in terms of the observable output y. We have then that x can be uniquely expressed as

$$x = \Phi(y, \dot{y}, \ddot{y}, \cdots, y^{(n-1)})$$

for some smooth function Φ.

C. State estimation for a Lorenz system

Consider the model of the popular *Lorenz system*, (see [Lorenz, 1963]):

$$\begin{aligned} \dot{x}_1 &= \sigma(x_2 - x_1) \\ \dot{x}_2 &= r x_1 - x_2 - x_1 x_3 \\ \dot{x}_3 &= x_1 x_2 - b x_3 \end{aligned} \tag{10}$$

where $y = x_1$ is the measured output variable. The parameters σ, r and b are assumed to be known parameters. The system is observable from the output y in all of R^3 except on the line $y = x_1 = 0$.

A local differential parametrization of the system states in terms of the measured output y is given by

$$\begin{aligned} x_1 &= y \\ x_2 &= \frac{1}{\sigma}\dot{y} + y \\ x_3 &= -\frac{1}{y}\left[\frac{1}{\sigma}\ddot{y} + \left(\sigma - \frac{1}{\sigma}\right)\dot{y} - (r+1)y\right] \end{aligned} \tag{11}$$

For the generation of the time derivatives of the measured output $y(t) = x_1(t)$ we may propose a 7th order truncated Taylor series expansion, around the re-initialization time t_r, of the form

$$y(t) = \sum_{i=1}^{7} \frac{y^{(i-1)}(t_r)}{(i-1)!}(t - t_r)^{(i-1)}$$

which leads, modulo a fixed time translation, to the identity

$$\frac{d^7}{ds^7}\left[s^7 y(s)\right] = 0$$

Based on this, we use the specific formulae:

$$\begin{aligned}
n_1(t) &= 42(t-t_r)^6 y(t) - 882(\int_{t_r}(t-t_r)^5 y) + 7350(\int_{t_r}^{(2)}(t-t_r)^4 y) - 29400(\int_{t_r}^{(3)}(t-t_r)^3 y) \\
&\quad +52920(\int_{t_r}^{(4)}(t-t_r)^2 y) - 35280(\int_{t_r}^{(5)}(t-t_r) y) + 5040(\int_{t_r}^{(6)} y) \\
d(t) &= (t-t_r)^7 \\
(\dot{y}(t))_e &= \begin{cases} (\dot{y}(t_r^-))_e + (t-t_r)(\ddot{y}(t_r^-))_e & \text{for } t \in [t_r, t_r+\epsilon) \\ \dfrac{n_1(t)}{d(t)} & \text{for } t \geq t_r+\epsilon \end{cases}
\end{aligned}$$

$$\begin{aligned}
n_2(t) &= 630(t-t_r)^5 y(t) + 35(t-t_r)^6 (\dot{y}(t))_e + 7350(\int_{t_r}(t-t_r)^4 y) - 29400(\int_{t_r}^{(2)}(t-t_r)^3 y) \\
&\quad +52920(\int_{t_r}^{(3)}(t-t_r)^2 y) - 35280(\int_{t_r}^{(4)}(t-t_r) y) + 5040(\int_{t_r}^{(5)} y) \\
d(t) &= (t-t_r)^7 \\
(\ddot{y}(t))_e &= \begin{cases} \ddot{y}(t_r^-) & \text{for } t \in [t_r, t_r+\epsilon) \\ \dfrac{n_2(t)}{d(t)} & \text{for } t \geq t_r+\epsilon \end{cases}
\end{aligned}$$

where the notation used is the same defined in equation (6)[1]. Note that, instead of constant values, we may also use spline polynomial approximations, for the estimates of the time derivatives of the signal $y(t)$, during the small intervals $[t_r, t_r+\epsilon)$, occurring right after the instants t_r at which the resettings of the calculations is carried out.

The differential parametrization (11) allows one to propose the following state estimates for the unmeasured states x_2 and x_3,

$$\begin{aligned}
x_{2e} &= \frac{1}{\sigma}(\dot{y})_e + y \\
x_{3e} &= -\frac{1}{y}\left[\frac{1}{\sigma}(\ddot{y})_e + \left(\sigma - \frac{1}{\sigma}\right)(\dot{y})_e - (r+1)y\right]
\end{aligned} \tag{12}$$

[1]Naturally at time $t=0$, for the initial calculation convergence interval: $[0, \epsilon)$, the unavailability of previously calculated time derivatives forces one to chose arbitrary constant values, preferably zero, of the estimated derivatives during this small time interval.

Note, however, that as clarified before, the estimate of the state variable x_3 undergoes a singularity every time the signal, $y = x_1$, goes through the value of 0. We will propose a singularity-free coding decoding process which allows us to also use x_3 as part of a chaotic coding signal.

C.1 Simulations

For the computer simulations we have taken the following parameter values:

$$\sigma = 10, \quad r = 28, \quad b = \frac{8}{3}$$

Figure 1 shows the computer simulation of the Lorenz system actual state trajectories along with the estimated values of the states x_2 and x_3. The computation of the first and second time derivatives of the measured output allows, of course, to estimate the state variable x_2 and x_3 using the static state estimation formula (12). The calculation intervals were chosen to be fixed of value 0.15 [sec], while the small interval of time, right after the calculation resettings, was set to be defined by $\epsilon = 0.01$ [s]. Note that the calculation resetting interval was taken to be rather "large". Nevertheless, the accuracy of the estimations and the performance of the algorithm are quite remarkable.

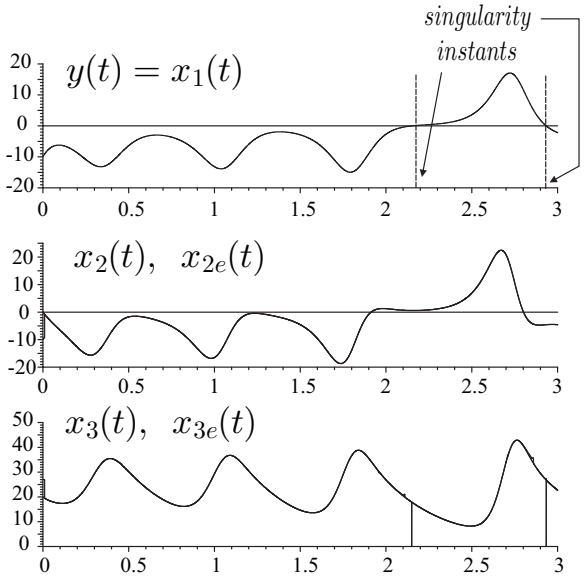

Fig. 1. State estimates of a Lorenz system

From the figure, it is evident that when $y(t) = x_1(t)$ goes through zero, a singularity centers around this time instant for the estimation of x_3 (modulo the effects of the finite step integration

algorithm). Naturally, this fact makes the state x_3 a questionable candidate for coding message signals that need to be secretly transmitted.

In order to give an idea of the speed of the, fast, non-asymptotic convergence as well as the accuracy of the state calculations around the resetting times, we show, in Figure 2, an inset of the previous simulations around the initial time, $t = 0$. The calculation intervals of 0.15 seconds and the calculation accuracy holding time of 0.01 seconds are clearly depicted in this figure.

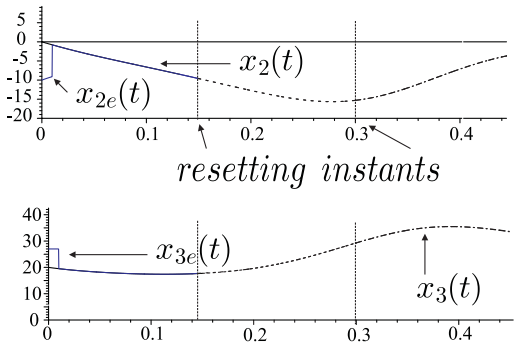

Fig. 2. An inset for the Lorenz state estimation

D. State estimation for Chen's system

Consider now *Chen's system* (see [Chen, 1993]):

$$\begin{aligned} \dot{x}_1 &= a(x_2 - x_1) \\ \dot{x}_2 &= (c - a)x_1 + cx_2 - x_1x_3 \\ \dot{x}_3 &= x_1x_2 - bx_3 \end{aligned} \tag{13}$$

where $y = x_1$ is the output variable. The parameters a, b and c are assumed to be known. The system is observable from the output y except at the line $y = x_1 = 0$.

A local differential parametrization of the system states, in terms of the measured output y, is given by

$$\begin{aligned} x_1 &= y \\ x_2 &= \frac{1}{a}\dot{y} + y \\ x_3 &= -\frac{1}{y}\left[\frac{1}{a}\ddot{y} + \left(1 - \frac{c}{a}\right)\dot{y} + (a - 2c)y\right] \end{aligned} \tag{14}$$

For the generation of the time derivatives of the output $y(t) = x_1(t)$, we again propose the same 7th order truncated Taylor series expansion, around the re-initialization time t_r, used in the previous example. Therefore, we used the same derivative calculation formulae presented in the Lorenz system example.

D.1 Simulations

For the computer simulations, we have taken the following parameter values:

$$a = 35, \quad b = 3, \quad c = 28$$

Figure 3 shows the computer simulation of Chen's system actual state trajectories and the estimated trajectories of the states x_2 and x_3. This time, the calculation interval was chosen to be defined by $t_r = 0.1$ [sec], while the small interval of time, after the calculation resetting, was set to be defined by $\epsilon = 0.01$ [s].

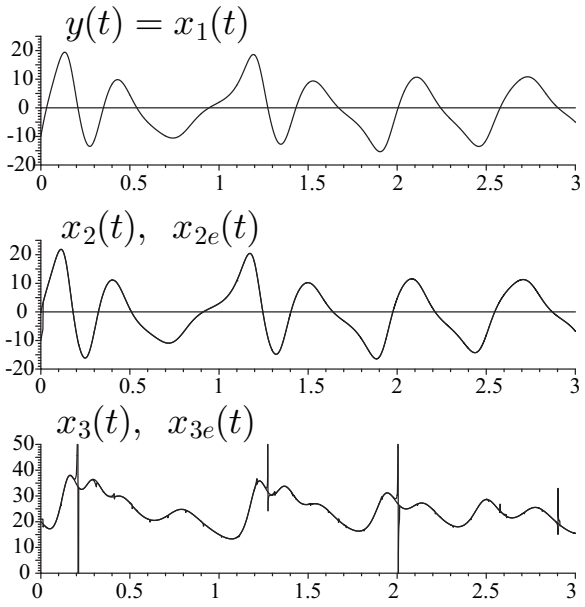

Fig. 3. State estimates of Chen's system

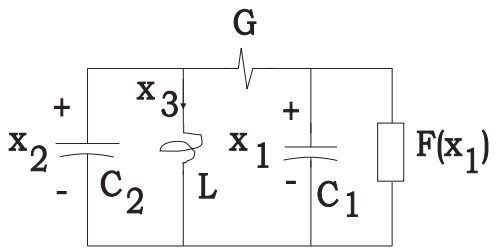

Fig. 4. Chua's circuit

E. State estimation for Chua's circuit

Consider Chua's circuit, (see [Wu & Chua, 1993]) shown in Fig. 4. This circuit is described by the following set of nonlinear differential equations:

$$\begin{aligned} C_1\dot{x}_1 &= G\,(x_2 - x_1) - F(x_1) \\ C_2\dot{x}_2 &= G\,(x_1 - x_2) + x_3 \\ L\dot{x}_3 &= -x_2 \end{aligned} \tag{15}$$

where $F(x_1)$ is a voltage -dependent nonlinear function of the form:

$$F(x_1) = ax_1 + \frac{1}{2}(b-a)\left(|1+x_1| - |1-x_1|\right), \quad a,\ b < 0$$

clearly playing the role of a *negative* resistor.

In order to facilitate the exposition, we adopt a normalized form of the above circuit (See [Huijberts *et al.*, 1998]):

$$\begin{aligned} \dot{z}_1 &= \beta(-z_1 + z_2 - \phi(z_1)) \\ \dot{z}_2 &= z_1 - z_2 + z_3 \\ \dot{z}_3 &= -\gamma z_2 \end{aligned} \tag{16}$$

with,

$$\phi(z_1) = az_1 + \frac{1}{2}(b-a)\left\{|\ 1+z_1\ | - |\ 1-z_1\ |\right\}$$

The system is clearly non differentiable due to the presence of the term $\phi(z_1)$. This makes the output $y = z_1$ not suitable for our state estimation technique since the corresponding differential parametrization of z_3 requires the time derivative of the function $\phi(z_1)$. Nevertheless, the output

$y = x_3$ is *globally observable* and the state of the normalized system enjoys a singularity free (linear) differential parametrization. Indeed

$$\begin{aligned} z_1 &= -\frac{1}{\gamma}\ddot{y} + \frac{1}{\gamma}\dot{y} - y \\ z_2 &= -\frac{1}{\gamma}\dot{y} \\ z_3 &= y \end{aligned} \tag{17}$$

The time derivatives of the measured output $y(t) = z_3(t)$ may be generated exactly in the same form as before.

E.1 Simulations

For the computer simulations we have taken the following parameter values:

$$a = -\frac{5}{7}, \quad b = -\frac{8}{7}, \quad \beta = 15.6, \quad \gamma = 27$$

Figure 5 shows the computer simulation of the normalized Chua's circuit actual state trajectories and the estimated values of the normalized states z_2 and z_3. This time, the calculation interval was chosen to be defined by $t_r = 0.3$ [sec], while the small interval of time, after the calculation resetting, was set to be defined by $\epsilon = 0.02$ [s].

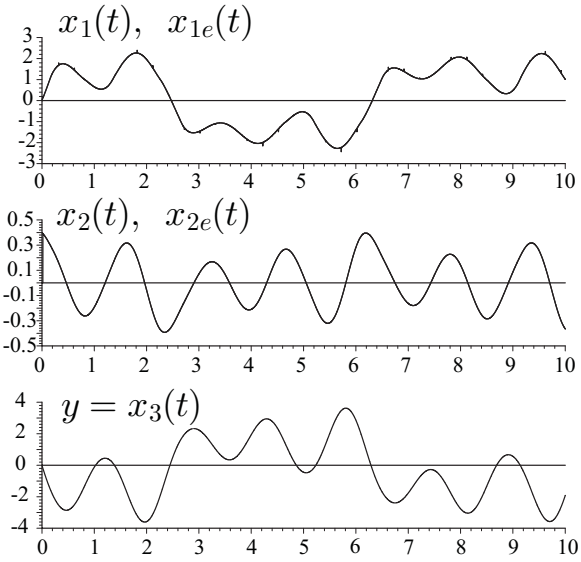

Fig. 5. State estimates of normalized Chua's chaotic circuit

F. State estimation for Rossler's system

Consider now *Rossler's system* described by Pecora and Carroll [1991]:

$$\begin{aligned} \dot{x}_1 &= -(x_2 + x_3) \\ \dot{x}_2 &= x_1 + a x_2 \\ \dot{x}_3 &= b + x_1 x_3 - c x_3 \end{aligned} \tag{18}$$

where $y = x_2$ is the output variable. The parameters a, b and c are known quantities. The system is globally observable from the output $y = x_2$.

A (linear) differential parametrization of the system states, in terms of the measured output y, is given by

$$\begin{aligned} x_1 &= \dot{y} - a y \\ x_2 &= y \\ x_3 &= -\ddot{y} - a\dot{y} - y \end{aligned} \tag{19}$$

As in the previous examples, we used a 7th order Taylor series expansion, around the re-initialization time t_r, for the output signal $y(t) = x_2(t)$. The derivative calculation formulae, presented in the first example, are still the same in this example as those in the Lorenz example.

Note that Rossler's system also exhibits a lack of global observability when the system output is chosen to be $y = x_3$. Indeed, in such a case we have the following differential parametrization of the system states

$$\begin{aligned} x_1 &= \frac{\dot{y} + cy - b}{y} \\ x_2 &= -\frac{(\ddot{y} + c\dot{y})y - (\dot{y} + cy - b)\dot{y}}{y^2} - y \\ x_3 &= y \end{aligned} \tag{20}$$

F.1 Simulations

For the computer simulations we have taken the following parameter values for Rossler's chaotic system:

$$a = b = 0.2, \quad c = 5$$

Figure 6 shows the computer simulation of Rossler's system actual state trajectories and the estimated values of the states x_1 and x_3. This time, the calculation interval was chosen to be of 0.1 [sec], while the small interval of time, after the calculation resetting, was set to be defined by $\epsilon = 0.01$ [s].

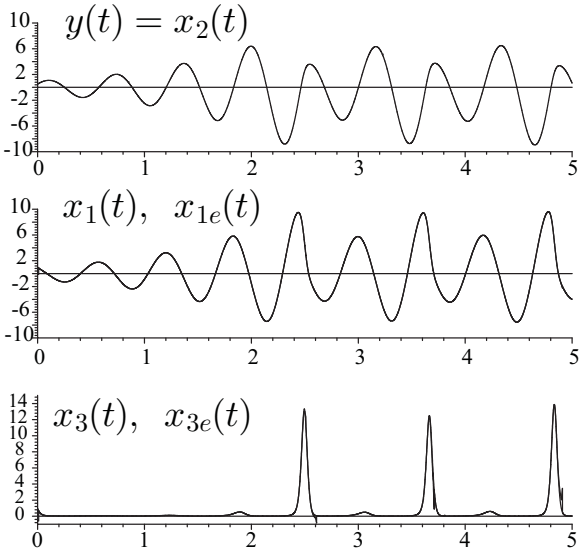

Fig. 6. State estimates for Rossler's system

G. State estimation for the hysteretic circuit

Consider now the following chaotic circuit treated by Carroll and Pecora [1991]:

$$\begin{aligned} \dot{x}_1 &= x_2 + \gamma x_1 + c x_3 \\ \dot{x}_2 &= -\omega x_1 - \delta x_2 \\ \epsilon \dot{x}_3 &= (1 - x_3^2)(s x_1 + x_3) - \beta x_3 \end{aligned} \tag{21}$$

where $y = x_2$ is the output variable. The parameters γ, c, ω, β and ϵ are all perfectly known quantities. The system is globally observable from the output $y = x_2$.

A differential parametrization of the system states, in terms of the measured output y, is given

by

$$\begin{aligned} x_1 &= -\frac{1}{\omega}\left[\dot{y} + \delta y\right] \\ x_2 &= y \\ x_3 &= \frac{1}{c}\left[-\frac{1}{\omega}\left(\ddot{y} + \delta\dot{y}\right) - y + \frac{\gamma}{\omega}\left(\dot{y} + \delta y\right)\right] \end{aligned} \tag{22}$$

G.1 Simulations

For the computer simulations we have taken the following parameter values:

$$\gamma = 0.2,\ c = 2,\ \omega = 10,\ \delta = 0.001,\ s = 1.667,$$

$$\beta = 0.001,\ \epsilon = 0.3$$

Figure 7 shows the computer simulation of the hysteretic circuit actual state trajectories $x_1(t)$, $x_3(t)$ along with the estimated trajectories of those states $x_{1e}(t)$ and $x_{3e}(t)$. This time, the calculation interval was chosen to be of 0.25 [sec], while the small interval of time, after the calculation resetting, was set to be defined by $\epsilon = 0.04$ [s].

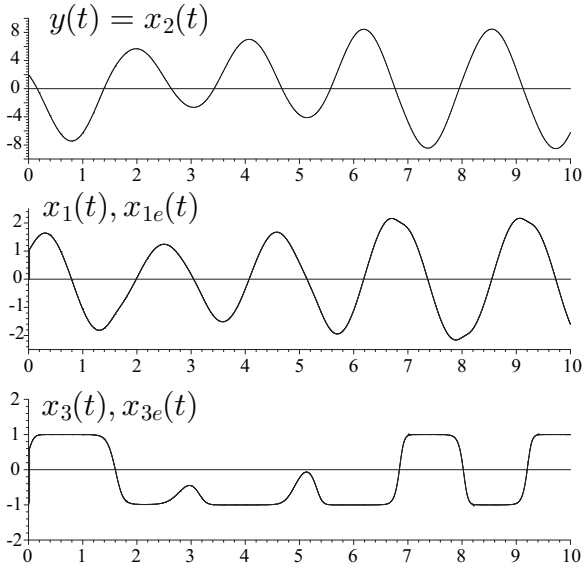

Fig. 7. State estimates for the hysteretic circuit

Note that the hysteretic circuit also exhibits a lack of global observability when the system output is chosen to be $y = x_3$. Indeed, in such a case we have the following differential parametrization

of the system states,

$$\begin{aligned} x_1 &= \frac{1}{s}\left[\frac{\epsilon\dot{y}+\beta y}{1-y^2} - y\right] \\ x_2 &= \frac{1}{s}\left[\frac{(\epsilon\ddot{y}+\beta\dot{y})\,(1-y^2)+2(\epsilon\dot{y}+\beta y)y\dot{y}}{(1-y^2)^2} - \dot{y}\right] \\ &\quad -\frac{\gamma}{s}\left[\frac{\epsilon\dot{y}+\beta y}{1-y^2} - y\right] - cy \\ x_3 &= y \end{aligned} \tag{23}$$

Clearly, there is a lack of observability at the values $y = \pm 1$. In fact, the hysteretic circuit state variable $y = x_3$ exhibits open intervals of time where y is rather close to either 1 or -1 and it actually achieves these extreme singular values at certain instants of time within those time intervals. The rather singular behavior of the state estimates x_1 and x_2, for this case, are shown in Figure 8.

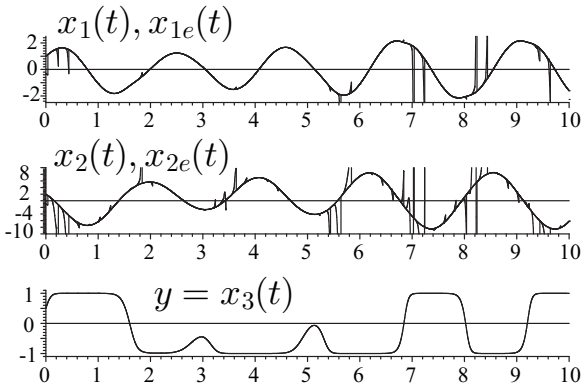

Fig. 8. Singular state estimates for the hysteretic cicuit

III. Coding-decoding process

The previous examples point to the fact that in our algebraic state reconstruction approach, the state variables are accurately reconstructed from the output signal alone. In the particular case of the Lorenz and Chen's system, a hidden signal transmission is possible through at least one of the chaotic states (x_2) of these systems. The subsequent message decoding is performed with the help of the proposed state estimation process at the receiving end as explained below.

Suppose a secret message, $m(t)$, is to be sent over a certain communication channel, possibly of analog nature. For the encoding process, we add the secret message signal, $m(t)$, say, to

the masking state signal, $x_2(t)$, of the chaotic system. The obtained signal $z(t) = x_2(t) + m(t)$ is sent towards the receiving end along with the output signal $y(t)$. At the receiving end, the transmitted output signal $y(t)$ is used in the algebraic state estimation scheme for the accurate reconstruction of the chaotic system state $x_2(t)$. This process results in the estimated signal $x_{2e}(t)$. A reconstruction of the hidden message is immediately obtained by forming the estimated secret message signal: $m_e(t) = z(t) - x_{2e}(t)$. The coding-decoding process is depicted in the Figure 9.

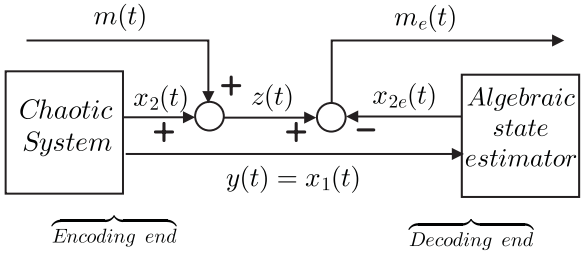

Fig. 9. Coding decoding process

In order to ensure that the addition of the message signal, $m(t)$, to the transmitted state does not become evident, one usually scales down the message amplitude so that its maximum amplitude represents only a fraction of the maximum chaotic masking signal amplitude. As a rule of thumb we use message amplitudes which are, roughly, 5 % of the masking state signal amplitude.

A. A simulation example

Using the previously described coding-decoding process, we used Chen's chaotic system for the secret signal encoding-transmission and subsequent decoding process through the algebraic state estimator already discussed at length in the previous section. Figure 10 depicts the transmitted signals: $y = x_1(t)$ and $z(t) = x_2(t) + m(t)$, as well as the recovered message $m_e(t)$ compared with the actual message signal $m(t)$. The signal used as $m(t)$ was set to be given by

$$m(t) = \cos\left[\sqrt{215t} - 20\sin(202t)\right]\sin(25t), \quad t \in [1, 2] \tag{24}$$

In order to assess the behavior of our coding-decoding scheme with respect to transmission noises, we used a noisy output signal $y(t) = x_1(t) + \xi(t)$ and a noisy coding state transmission $z(t) = x_2(t) + m(t) + 10\xi(t)$, with $\xi(t)$ being a computer generated noisy perturbation process taking values in the interval $[-0.0025, 0.0025]$. This computer generated noise is synthesized on the basis of a rectangular (uniform) probability density function for the corresponding digital

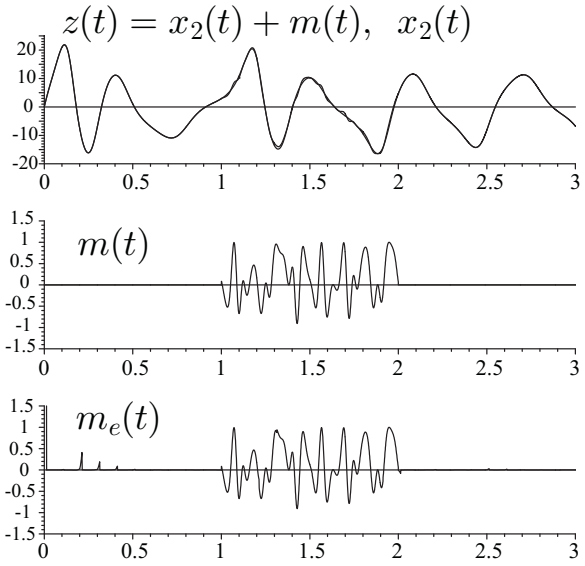

Fig. 10. A simulation example of encrypted message recovery

computer random number generation comprising the piecewise constant values of the perturbation signal. The simulations are depicted in Figure 11. In this instance, we used as the secret signal the signal $m(t)$, given in (24), amplified by a factor of 2.

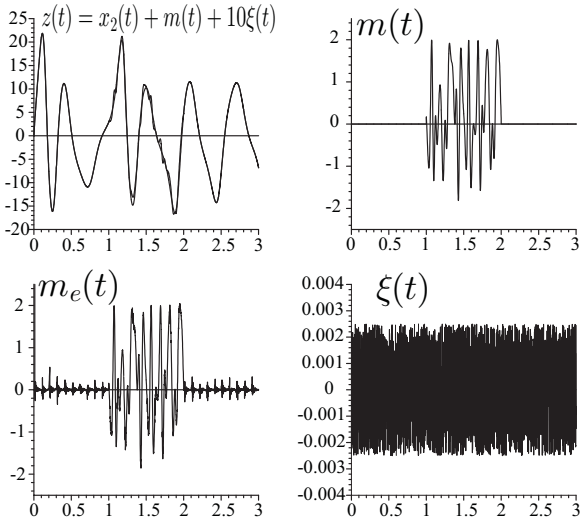

Fig. 11. Encrypted message recovery from a noisy output and a noisy encoding state transmission

B. Simultaneous chaotic encoding-decoding with singularity avoidance

The singularities present in the estimation of the state x_3, in the Lorenz, the Chen's examples make the variable x_3 a useless state for coded signal transmission. Similarly, in the Rossler example and in the hysteretic circuit example, with the output variable taken to be $y = x_3$, both variables x_1 and x_2 would be rather inconvenient for encryption and transmission purposes.

A rather direct way to evade these singularities is suggested by the differential parametrization of the states themselves. For instance, in the Lorenz and Chen's examples, rather than using x_3 for coding purposes, we used the *product signal* $x_3(t)y(t)$, this masking signal could be used to transmit and recover messages without any singularities. Indeed, let $w(t) = x_3(t)y(t)$ and transmit the signal $\zeta(t) = w(t) + n(t)$, where $n(t)$ is a message to be sent towards the receiving end. In Chen's system with $y = x_1$, the estimation of the signal $w(t) = x_3(t)y(t)$, denoted by $\widehat{w}(t)$ is simply obtained from (14) as,

$$\widehat{w}(t) = -\left[\frac{1}{a}\left(\ddot{y}\right)_e + \left(1 - \frac{c}{a}\right)\left(\dot{y}\right)_e + (a - 2c)y\right]$$

The message signal estimate, $n_e(t)$, is immediately recovered from the simple substraction operation:

$$n_e(t) = \zeta(t) - \widehat{w}(t)$$

The fading of $x_3(t)y(t)$ near a zero crossing of $y(t)$ does not affect the encryption, nor the decoding processes. Figure 12 depicts the proposed singularity free encryption process.

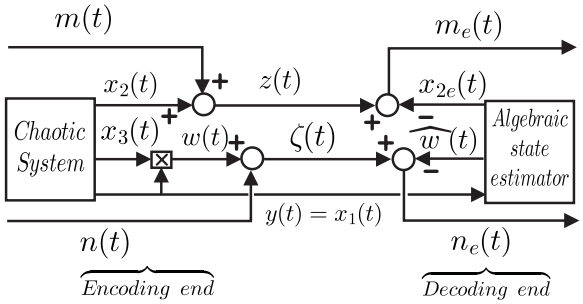

Fig. 12. Simultaneous chaotic encoding decoding with singularity avoidance

Evidently, a similar procedure involving the product signals $x_1(t)y(t)$ and $x_2(t)y^2(t)$ can be proposed for evading the singularities in Rossler's system, when the output is taken to be $y = x_3$ (see (20)). In the hysteretic circuit, when $y = x_3$, one must take the nonlinear signals $x_1(t)(1 - y^2(t))$ and $x_2(t)(1 - y^2(t))^2$ for coding-decoding purposes (see (23)).

B.1 Simulations

Using the previously described coding-decoding process with singularity avoidance, we used Chen's chaotic system for signal encoding-transmission of two secret messages $m(t)$ and $n(t)$. The subsequent decoding process for the coding chaotic signal $w(t) = x_3(t)y(t)$ was carried out through the algebraic state estimator as already discussed above. Figure (13) depicts the singularity free signal $w(t) = x_3(t)y(t)$, along with the transmitted signal $\zeta(t) = x_3(t)y(t) + n(t)$. The figure also shows the recovered message $n_e(t)$ and the actual message $n(t)$. In order to keep the amplitude of the message, roughly speaking, at a 5 % of the value of the carrier signal amplitude. The signal to be transmitted was amplified by a factor of 40, evidently, this scaling has no bearing whatsoever over the recovery of the actual signal once its multiple value is safely received at the decoding end and the scaling factor is known. In order to send the message signal: $\sin\left[\sqrt{512t} + 5\sin(10t)\right]\sin(15t)$, we used in this instance the signal:

$$n(t) = 40\sin\left[\sqrt{512t} + 5\sin(10t)\right]\sin(15t), \quad t \in [0.5, 1.5]$$

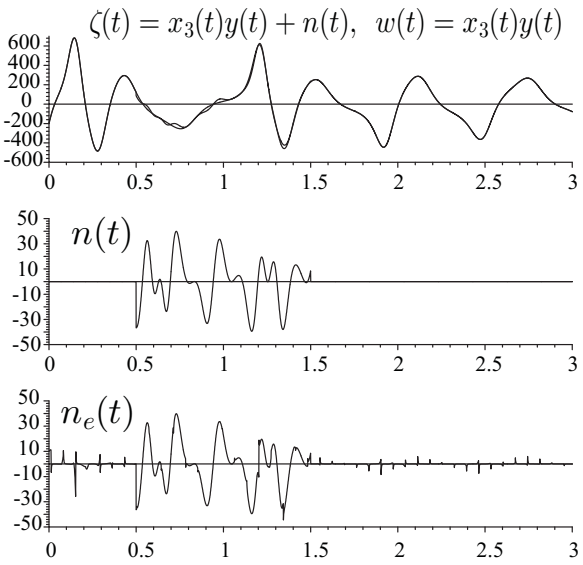

Fig. 13. Chaotic encoding-decoding with singularity avoidance

IV. Conclusions

In this article, we have introduced, in the context of well known chaotic system examples, a fast non-model based successive time derivative calculations of a measured observable output signal.

This procedure is readily used as a tool for the state estimation process, to be carried out at the receiving end, in a chaotic system state-based modulation, and transmission, of encrypted secret message signals. At the receiving end, the state variables of the unperturbed transmitting chaotic system are accurately, locally, calculated from formulae using the transmitted observable output alone and some time convolutions. The process entitles the on-line local computation of a sufficient number of its time derivatives and the use of a static map, guaranteed by the local observability of the output variable, relating these output time derivatives to the system states (in fact, in the examples here presented, only two time derivatives of such outputs are required). The generation, at the receiving end, of the required coding system state estimates, or reconstructions, is carried out using the (static) model based differential parametrization of the encrypting system states in terms of the measured output variable.

An efficient computational method is proposed for the piecewise continuous on-line computation of the first few time derivatives of the chaotic output signal along with, possibly, an automatic resetting calculation mechanism based on an on-line evaluated integral quadratic error criterion. In practise one can also use a fixed calculation interval of sufficiently small length. The successive time derivative generation method is based on a combination of a truncated (polynomial) approximating Taylor series expansion of the output signal and the use of the *algebraic derivative method* on a time invariant homogeneous linear system of sufficiently high order. The estimation of the unperturbed carrier states, at the receiving end, is then used in the traditional message decoding scheme. The masking and recovery of the transmitted message naturally requires the transmission of the chaotic system output signal and of the chaotic states additively perturbed by the secret message signal. Several simulation examples were presented which depict the effectiveness of the proposed approach. The proposed estimation scheme for one of the chaotic states, in the Lorenz, in Chen's system, in Rossler's system and in the hysteretic circuit examples, suffer from the presence of singularities at each zero crossing of the chosen system output. This is caused by an instantaneous loss of the required output observability (a common phenomenon in nonlinear systems where observability is definitely a local concept). A method which evades such singularities in the calculations and still allows one to use the troublesome state in the encrypting-decoding process is also proposed. Interestingly enough some chaotic systems were shown to have global observability properties with linear differential parameterizations of the states.

The *algebraic derivative method* for time signal derivative calculations was developed by the authors in connection with parameter estimation and fast state estimation in linear control systems. The method, naturally derives from the framework of *module theory* and the implications of *non-commutative algebra* in linear systems theory. We remark that such a method has also been successfully used in fault detection problems of uncertain systems (see [Fliess *et al.*, 2004]), signal compression, and the output feedback control of nonlinear systems (See [Fliess & Sira-Ramírez, 2004]).

Potential areas of application of the proposed output signal derivative calculation scheme in state estimation problems are: sliding mode control, nonlinear systems identification, combined nonlinear state estimation and parameter identification and hyper-chaotic signal encoding-decoding schemes.

V. References

Afraimovitch, V. S., Nekorkin, V. I., Osipov, G.V., and Shalfeev, V. D., [1994] "Stability, Structures and Chaos in Synchronization Networks, " World Scientific Pub. Co., Singapore.

Carroll, T.L. and Pecora, L. [1991] "Synchronizing chaotic circuits" *IEEE Trans. on Circ. Systems*, **38**(4), 453-456.

Chen, G., [1997] "Control and synchronization of chaotic systems (bibliography)," ECE Dept, Univ of Houston, TX. – available from ftp: "ftp.egr.uh.edu/pub/TeX/chaos.tex" (login name "anonymous" password: your email address).

Chen, G., [1999] *Controlling Chaos and Bifurcations in Engineering Systems*, CRC Press, Boca Raton, Florida, USA.

Cuomo, K. M., Oppenheim, A. V. & Strogatz, S. H. [1993] " Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications," *IEEE Trans. Circuits Syst-II: Analog and Digital Signal Processing*, **40**(10), 626-633.

S. Diop, J.W. Grizzle and F. Chaplais, [2000] "On numerical differentiation algorithms for nonlinear estimation", in *Proc. of the 2000 IEEE Conf. on Decision and Control*, Sydney, Australia.

S. Diop and M. Fliess, [1991]"Nonlinear observability, identifiability and persistent trajectories" in *Proc. 36th IEEE Conf. on Decision and Control*, Brighton, England

S. Diop, J.W. Grizzle, P.E. Moraal, and A. Stefanopoulou, [1994] " Interpolation and Numerical

Differentiation for Observer Design", in *1994 American Control Conference*, Baltimore, USA.

M. Fliess, C. Join and H. Sira-Ramírez, [2004] "Robust Residual Generation for Linear Fault Diagnosis: An Algebraic Setting with Examples" *Int. J. of Control*, **77**(14), 1223-1242.

M. Fliess and H. Sira-Ramírez [2003] "An algebraic framework for linear identification" *ESAIM, Control, Optimization and Calculus of Variations*, **9**(1), 151-168.

M. Fliess and H. Sira-Ramírez [2004] "Reconstructeurs d'Etat" *C.R. Academie des Sciences de Paris*, Série I, **338**(1), 91-96.

M. Fliess and H. Sira-Ramírez [2004] " Control via State Estimations of Flat Systems" *IFAC Nolcos Conference*, Stutgart, Germany.

Fliess, M., [1987] "Quelques Remarques sur les Observateurs non Lineaires, " *11* eme *Colloque GRETSI sur le Traitement du Signal et des Images*, Nice, France.

Fradkov, A. L. & Markov, A. Yu. [1997] "Adaptive Synchronization of Chaotic Systems Based on Speed Gradient Method and Passification," *IEEE Trans. Circuit and Syst-I: Fundamental Theory and Applications*, **44**(10), 905-917.

Fradkov, A. L. & Pogromsky, A. Yu. [1998] *Introduction to control of oscillations and chaos*, Series A, **35**, World Scientific Publishing Co.

Huijberts, H. J. C., Nijmeijer, H. & Willems, R. M. A. [1998] "A control perspective on communications using chaotic systems," *Proc. 37th IEEE Conf. on Decision and Control*, Tampa, Florida, USA.

Holden, A. V. [1986] *Chaos*, Princeton University Press, Princeton, N. J., USA.

Lorenz, E. N. [1963] "Deterministic non-periodic flow", *J. of Athmosph. Science*, **20**, 130-141.

Mira, C. [1987] *Chaotic Dynamics*, World Scientific, Singapore.

Nijmeijer, H. & Mareels, M. Y. [1997] "An Observer Looks at Synchronization," *IEEE Trans. on Circ. and Systems-I: Fundamental Theory and Applications*, **44**(10), 882-890.

Ott, E., Sauer, T. & Yorke, J. A. (Eds.) [1994] *Coping with Chaos: Analysis of Chaotic Data and the Exploitation of Chaotic Systems*, New York: Wiley- Interscience.

Pecora, L. M. & Carroll, T. L. [1991] "Driving systems with chaotic signals," *Phys. Rev.*, **A44**(4), 2374-2383.

F. Plestan and J.W. Grizzle, [1999] "Synthesis of nonlinear observers via structural analysis and numerical differentiation". in *Proc. of the 1999 European Control Conference, Karlsruhe,*

Germany.

Pogromsky, A. Yu. [1998] "Passivity-based design of synchronizing systems, " *Int. J. Bifurcation and Chaos*, **8**(2), 295-319.

Special Issue [1993] "Chaos synchronization and control: theory and applications," *IEEE Trans. Circuit Syst.-I: Fundamental Theory and Applications*, **40**(10).

Special Issue [1997a] *Syst. Contr. Lett.* **31**(5).

Special Issue [1997b] "Chaos synchronization and control: theory and applications", *IEEE Trans. Circuit Syst.-I: Fundamental Theory and Applications*, **44**(10).

Special Issue [1999] "Communications, Information Processing and Control Using Chaos" *Int. J. of Circ. Th. and Appl.* **28**.

Special Issue [2000] "Control and Synchronization of Chaos", *Int. J. of Bifurcations and Chaos*, **10**.

Special Issue [2001] "Application of Chaos in Modern Communication Systems" *IEEE. Trans. on Circ. and Syst.-I:Fundamental Theory and Applications* **48**(12).

Sira-Ramírez, H., & Cruz-Hernández, C., [2001] "Synchronization of Chaotic Systems: A Hamiltonian Systems Approach" *Int. J. of Bifurcations and Chaos*, **11**(5), 1381-1395.

Sira-Ramírez, H., Aguilar-Ibáñez, C., and Suárez-Castañon, M., [2002] "Exact State Reconstruction in the Recovery of Messages encrypted by the States of nonlinear discrete-time chaotic systems", *Int. J. of Bifurcation and Chaos*, **12**(1), 169-177.

Wu, C. W. & Chua, L. [1993] "A simple way to synchronize chaotic systems with applications to secure communication systems," *Int. J. Bifurcation and Chaos*, **3**(6), 1619-1627.