On the Recovering of Encoded Messages by Hyperchaotic Map Synchronization

Miguel S. Suárez C., Carlos Aguilar I., J. Humberto Sossa A. and Ricardo Barrón F.

Centro de Investigación en Computación
Instituto Politécnico Nacional
Av. Juan de Dios Bátiz s/n Esq. con Manuel Othón de Mendizabal Col. San Pedro Zacatenco,
A.P. 75476 07700 México, D.F.,
MÉXICO
caguilar@cic.ipn.mx

ABSTRACT

In this work we propose to use hyperchaotic map synchronization to encode and decode information. The information to be encoded is fed or injected into to the transmitter as an external perturbation. The transmitted signal is used for synchronization and as the encoded information carrier. Once the receiver is synchronized with the transmitter, the former decodes the information by reconstructing the external perturbation. The results obtained were used to build a software to establish secure on-line communication over Internet.

Key-words:

Information Encoding, Information Decoding, Cryptography, Hyperchaotic, Map Synchronization

I. Introduction

In this work we introduce an alternative option to enforce the secrecy of exchanged information through the Internet. For this, we make use of nonlinear exact state reconstructors (see [1]) of hyperchaotic maps (see [6]) chaotic system synchronization (see [6] and [7]) as a tool to recover encoded messages in a discrete-time chaotic signal. Chaotic system synchronization provides with the possibilities of encoding information using one or more state variables of a chaotic system as a carrier in the side of the sender, and decodes it on the side of the receiver. This idea to our knowledge has not been used to solve this problem. The main idea is at least to confuse an intruder exploiting the chaotic nature of the state variables used as carriers and hide the information moved from one point to another (see [2]).

The scheme here presented is based on the synchronization of an encoding system (chaotic system), which we will call the sender, and a decoding system (exact state reconstructor), which we will call the receiver. For synchronization we must understand that under a signal transmission, the receiver is able to reconstruct (maybe asymptotically) that of the sender. The system synchronization problem has been extensibility studied in general in (see [22], [4] and [5]), and particularly its application to chaotic systems synchronization has been found in (see [14] and [15]). Previous works have described the use of synchronization of chaotic systems in the transmission of encoded information, using some state variables for synchronization and other state variables of the same system for encoding that information. Our work differs, because we use the same state variable for synchronization and encoding, which is less expensive in terms of communication channels and computation effort. The methodology we use in order to carry out the synchronization process consists on applying the delay embedding method introduced in nonlinear time series based on the Takens' Theorem (see [8], [9], [10], [11] and [12]).

Finally, it is worth mentioning that our proposal does not pretend to substitute the modern cryptographic and steganographic techniques. We strongly believe that our proposal is an alternative that could be more efficient in some situations, taking into account that the computational effort required is much less that the one needed for instance in cryptography. Ours, as we will see, is much faster. On the other hand, in spite of the fact that the security level of our mechanism is based on the chaotic nature of the system that we use, we can not at the moment say it provides a higher degree of security.

The remaining of this work is organized as follows. Section II covers a brief description of chaotic volume-preservative-maps. Section III is devoted to prove that the chaotic maps presented in previous sections are constructible with respect to a suitable output. In Section IV an encoding mechanism is introduced. Section V describes an actual application that we built to communicate over Internet using encoded messages by means of the results presented in this work. Section VI describes the results of an experimental test. Finally, Section VII is devoted to some conclusions and suggestions for ongoing research.

[1]This research was supported by the Centro de Investigación en Computación of the IPN (CIC-IPN) and by the Coordinación General de Posgrado e Investigación of the IPN, under Research Grant 20020247.

J. Díaz de León, G. González, J. Figueroa (Eds.): Avances en Ciencias de la Computación, pp. 324-330, 2003.

II. Background on Chaotic Maps

Let us consider a class of nonlinear iterative map, defined as:

$$X(k+1)=F(X(k)) \quad (1)$$

where $X(k)\in\Re^n$ given by $X(k)=[x_1(k),x_2(k)...,x_n(k)]^T$ and $F(\cdot)$ is a nonlinear iterative map given by $F(X(k))=[x_2(k),x_3(k),...,M(X(k))]^T$. with

$$M(X(k))=\left\{\sum_{i=1}^{i=n}a_i x_i(k)+j\right\}\bmod 2j-j.$$

$\{a_1,...a_n\}$ is a set of fixed constants and $k=\{1,2,...,N\}$. Function $\{f+j\}\bmod 2j-j$, means that we take f and add the integer j, divided by $2j$, we keep the remainder, and subtract two for each j. In some cases $M(X(k))$ can also be replaced by the continuous function:

$$M(X(k))=\sin\left(\sum_{i=1}^{i=n}a_i x_i(k)\right),$$

because as in the case of the *modulus* function, for any point x_i of the *sin* function that goes beyond some bounded region, the function moves it back into that region.

Notice that the characteristic polynomial of the linearized system is given by

$$p(s)=a_1+a_2 s+...+a_n s^n.$$

This kind of systems exhibits a chaotic behavior in the cases where the Jacobian of the map in (1) around the equilibrium point zero has one or more eigenvalues outside the unitary circle (see [3], [16] and [17]). It is desirable that the Jacobian of this map has two or more roots outside the unitary circle. If this is the case, their behavior is hyperchaotic. Another very important characteristic of this kind of systems, is that the values of their state variables are always confined to a *n*-dimensional hypercube, no matter what the initial conditions are. If the initial conditions are outside of the hypercube, eventually for some *n-th* iteration the state vector will be inside the hypercube.
It is important to say that hyperchaotic maps have desirable properties that help to accomplish most of the needs that arise in any private and secure communication systems. These maps do not present defined patterns or attractors; they can be synchronized in a few steps and they can be easily implemented in circuitry. In fact the mechanism that is described in the next section only needs *n-1* steps to synchronize for a *n*-dimensional system.

Let us now consider the slight modified version of the system given by (1) as follows:

$$\begin{aligned}X(k+1)&=F(X(k))+Bw(k)\\ y(k)&=h(X(k))=x_1(k)\end{aligned} \quad (2)$$

where $B\in\Re^n$ is a constant vector defined by $B=[0\ \ 0\ \ ...\ \ \lambda]^T$ with $0<|\lambda|<<1$; $y(k)$ and $w(k)\in R$, are the output and the external perturbation, respectively, and $F(\cdot)$ is the nonlinear map previously defined.

Based on the class of systems described in (2) we propose a simple mechanism to encode/decode information under the following assumptions:

A.1) At each *k*-iteration, we dispose of the output values $\{y(k-n),...,y(k-1),y(k)\}$, for all $k>n$.

A.2) The external perturbation satisfies the following: $w_k=0$, for, $k\le n$ and $w_k\neq 0$ for $k>n$.

A.3) The set of parameters $\{a_1,...a_n\}$ are selected such that the characteristic polynomial has one or more roots outside the unitary circle. The initial conditions must be selected in such way that the system does not present periodical behavior.

III. Dead-Beat Synchronization

Let us consider the nonlinear iterative chaotic map given by (1). Then, this class of systems has two important properties:

i) The observability map Ψ defined by $\Psi=[h(k),h\circ F(x),...,h\circ F^{n-1}(x)]=X(k)$ satisfies that the Jacobian $\partial\Psi/\partial X$ equals the identity matrix, therefore the system (1) is called strongly locally observable around $x=0$.

ii) It has unique equilibrium point which is given by $x_1(k)=x_2(k)=...=x_n(k)=x_e$. Indeed from (1) we have two possibilities:

$$x_e=\left\{\left(\sum_{i=1}^{i=n}a_i\right)x_e+j\right\}\bmod 2j-j$$

or

$$x_e=\sin\left(\left(\sum_{i=1}^{i=n}a_i\right)x_e\right)$$

which evidently has unique solution $x_e=0$.

Hence, according to Proposition 2.1 described in [4] (see Appendix), system (1) is constructible with respect to the output $y(k)$ (for more details refer to [13] and [21]). Then,

a map $\Psi : \Re^n \rightarrow \Re^n$ exists, such that state $X(k)$ can be exactly reconstructed from time $k=0$, on terms of the output $y(k)$ and a finite string of previously obtained output, in the form:

$$X(k)=\varphi\big(y((k),y(k-1),...,y(k-n-1)\big),\ k\geq 0.$$

Notice that the above relation is according to the well known Takens' Reconstruction Theorem (see: [5] and [6]).

The following proposition provides the main result which allows us to reconstruct the external perturbation $w(k)$ of (2)

Proposition 1 *Let us consider the system given by (2), under the assumptions A.1 and A.2, then the following estimator recovers the external perturbation* **w**, *delayed n-steps with respect to the output* **y**, *as follows:*

$$\hat{w}(k-n)=y(k)-\left\{\sum_{i=1}^{i=n} a_i y(k-(1+n)+i)+j\right\} \bmod 2j-j \quad (3)$$

Proof:

From (1), we clearly have that:

$$\begin{bmatrix} y(k) \\ y(k+1) \\ \vdots \\ y(k+n-1) \end{bmatrix} = \begin{bmatrix} x_2(k-1) \\ x_3(k-1) \\ \vdots \\ \left(\sum_{i=1}^{i=n} a_i x_i(k-1)+j\right) \bmod 2j-j+w(k-1) \end{bmatrix} \quad (4)$$

From the above vectorial equation, we note that

$$x_i(k-1)=y(k+i-1) \quad (5)$$

Thus, the last component of the vectorial equation (4), can be expressed as:

$$x_n=\left\{\sum_{i=1}^{i=n} a_i y(k+i-2)+j\right\} \bmod 2j-j+w(k+1) \quad (6)$$

From (5) we have that $x_n(k+1-n)=y(k)$. By substituting this result into (6), we have after some algebraic manipulations the external perturbation *w* delayed *n*-steps with respect to the output *y(k)*, as follows:

$$\hat{w}(k-n)=y(k)-\left\{\sum_{i=1}^{i=n} a_i y(k-(1+n)+i+j)\right\} \bmod 2j-j \quad (7)$$

then clearly from (3) and (6), we obtain:

$$\left|\hat{w}(k-n)-k(k-n)\right|=0 \; for \; k>n.$$

Based on Proposition 1, we have designed a practical mechanism to encode/decode information and, from this mechanism we have developed an actual Internet application that allows us to securely communicate across the Internet. The degree of confidence of our mechanism relies on the chaotic or hyperchaotic nature of the carrier signal and the difficulty to exactly reproduce it without the knowledge of the initial conditions and the parameter values used during the encoding process.

Note that in the schema proposed in [4] the transmitter has to send two or more signals to the receiver in order to allow the later to decode the message. At least one signal contains the needed key to reconstruct the remaining states of the transmitter system. The other signals are the encoded messages. On the other hand, the mechanism presented in this paper, only has to send only one signal, which simultaneously is used as a carrier of the message and the key needed to recover that message, which was fed into the transmitter system as an external or exogenous perturbation.

IV. Application to Recovering Encoded Information Embedded into a Chaotic Signal

IV.1 An Encoding Mechanism

Taking into account **Proposition 1**, we describe in this section an encoding mechanism, which uses the chaotic output of the system given by (2), and the message to be encoded as the perturbation $w(k)$. If $w(k)$ is much smaller than $F(X(k))$, then $F(X(k))+w(k)\approx F(X(k))$, thus the difference between $F(X(k))$ and $F(X(k))+w(k)$ is minimal and the chaotic or hyperchaotic nature of $F(X(k))$ is kept in $F(X(k))+w(k)$.

Now, according to **Proposition 1**, we can estimate $w(k)$, that is, we can decode the encoded message.

We present now our main result: a numerical encoding/decoding mechanism. In the sequel, DCED-Mechanism will stand for Discrete Chaotic Encoding-Decoding Mechanism.

DCEC-Mechanism.

1. We send to an authorized recipient the output of the discrete-time chaotic system, i.e., the encoded message $\left(u'_k\right)$. *The authorized recipient is the person who possesses the exact state reconstructor and the needed information to decode the encoded message.*

2.- The recipient reconstructs the chaotic signal, i.e., (y_k), *then she or he performs the following operation:*

$$w_k=\frac{\left(u'_k-y_k\right)}{\lambda},$$

which allows to decode the encoded message.

In the next section we give a description of the application that we developed to communicate across the Internet using the previous results obtained in this work.

V An Internet Application: Secure Communication Using an Insecure Communication Channel

The popularity of Internet as an efficient resource to communicate people and to move information from one site to another, brings the necessity of mechanisms to ensure the integrity of the data flowing across that world wide net. It also needs to avoid that non-authorized people have access to it. As we mentioned in the first section, the tools more often used to ensure information secrecy are those that modern cryptography provide, and maybe in a more modest degree those derived from steganographic mechanisms.

In this section we describe an application we built using the results obtained in this work. This system allows to communicate on-line with other people across the Internet as we usually do when we use, for instance, the so-called chat rooms. The whole conversation will be however encoded, and even if somebody can see the bytes that we send or receive, she (or he) won't be able to figure out our conversation.

The system is organized in four modules or subprograms:

a) New Users Registry Module.
b) Start Session Module.
c) Users Logged Control Module.
d) Communication Module.

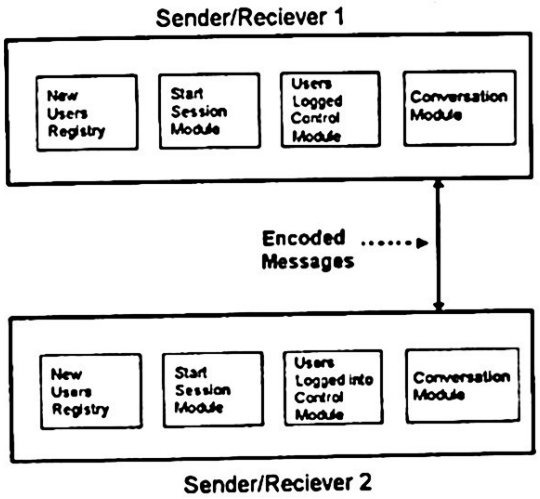

Figure 1 Block Char of the Secure Communication System

Each module was implemented in Java™, version 1.3. Each module has its own graphical interface. The graphical interface was built using the classes provided by the Package Swing, included in the SDK™ 1.3. Data manipulation was done using the MySQL™ data base manager. The modules needed to interact with the data base made use of the JDBC provided by MySQL™, and can be found in *www.mysql.com* . It is worth mentioning that the tools needed to build this system are freely available in the Internet.

New Users Registry Module

This module is composed of two submodules: the graphical interface module and the data base module. The graphical interface module provides a friendly interface that easily allows the user to insert her or his name into the users data base. This is a necessary condition to be able to use the system, and to eventually communicate with the users that are already registered. The database module manages the whole information of each user, such as the user names and their passwords.

Start Session Module

This module allows any already registered user to star a session and to communicate with other registered users. One of the main tasks of this module is to avoid that non-authorized users can loggin onto the system.

Every time a user wants to communicate with another logged user, she (or he) must enter their user name and their password in the provided graphical interface. Once the module has the user name and the corresponding password, it provides access to the users data base to allow or denied access to the system accordingly to the validation process result. Finally, when the user is logged onto the system she (or he) will be able to contact any already logged user through the *Users Logged Control Module*, described below

Users Logged Control Module

This modules provides a list of logged users, by means of a graphical interface. In order to establish a conversation, a user most double-click the username of the person who she (or he) wants to talk with.

This module works as follows. Every user logged onto the system has his own communication channel or thread and is marked as connected into the data base; the module then checks the data base and updates the list of users that are currently using the system. As mentioned before, when a user wants to talk with another connected user, she (or he) has to double-click their user name; then the module gets the IP address from the server data base. Once the module had the IP address, it makes a connection request to this address and if the receiver accepts the connection, a conversation will start.

Conversation Module

This module hides and extracts the messages in each side of the conversation and provides the services needed to move information from one side to the other. The module consists of four submodules: Encoding Submodule, Decoding Submodule, Communication submodule and Graphical Interface Submodule.

The *Encoding and Decoding submodules* as their names suggest, encode and decode the information to be sent and the information received, respectively. Both operation are executed according to the results presented in Section V.

The *Communication Submodule* is needed basically to handle the transmission channel where the encoded information flows. It is also needed to update the list of

logged users. Every logged user has a copy of this submodule. When an user doubles-click the user name of another user a conversation request is made. If the user who receives the conversation request accepts it, then a thread between both users is created. The thread will handle every aspect of the communication among each pair of users. It is important to mention that each thread is an independent process, and it will allow any user to have more than one conversation in a simultaneous fashion.

VI Experimental Test Results

In order to illustrate the effectiveness of the mechanism presented in this work, we encoded ad decoded two messages. The original messages consists of a digitized file of a H. Poncairè photography and a digitized text message which is a fragment that H. Poncairè wrote in the 1903 essay "Science and Method."

The image and text files were chaotically encoded in a byte-by-byte fashion. Figure 2 shows the original image, the encoded image and the recovered image. Similarly, Figure 3 depicts the original text file, the corresponding encoded file and the recovered text.

The experiments were carried out in a personal computer Dell™ Dimension DIM4300 with an Intel™ Pentium™ at 1.6GHz and 128Mb in RAM, running Microsoft™ Windows XP™ Home Edition ver. 2002.

VII Conclusions

We have described in this work a kind of nonlinear maps that have the peculiarity of being chaotic or hyperchaotic according to their eigenvalues. More important, we have explained how to determine which behavior should be expected. We have also shown that it is possible to reconstruct the state vector of this n-dimensional maps if $(n-1)$-delayed values of the output are available. The reconstructor is designed based on the Takens' reconstruction theorem. This reconstruction totally differs from the traditional asymptotic synchronization approach, which is based on nonlinear state observers, and the common generated error is completely avoided. The obtained reconstruction results were applied to a modified version of the hyperchaotic maps originally presented, which include a scaled perturbation signal. After some algebraic manipulation it is clear that the system state vector and the applied perturbation are easily recovered. It is important to mention that the reconstructor only needs one signal to synchronize with the system, which in our case is also the carrier signal.

An application (software) for secure communication over the Internet using the results obtained was developed. This application allows to establish a secure communication channel between different sites. The user can communicate on-line or they can encode any computer file and then send it to a recipient who can decode it. To be able to access the application, any user must be registered in an users database that is located in a public server. The system provides the facility to generate different encode/decode parameters to enforce the secrecy among users.

It is known that one of the major applications of chaotic systems lies in the secure communication area. Due to the properties of the nonlinear maps and their reconstructor described above, they are a suitable option in that area.

Figure 2. Original image, encoded image and recovered image.

"If we knew exactly the laws of nature and
the situation of the universe at the initial
moment, we could predict exactly the situation
of that same universe at a succeeding moment.
but even if it were the case that the natural
laws had no longer any secret for us, we could
still only know the initial situation appproximately.
If that enabled us to predict the succeeding
situation with the same approximation, that is
all we require, and we should say that the phenomenon
had been predicted, that it is governed by laws.
But it is not always so: it may happen that small
differences in the initial conditions produce very
great ones in the final phenomena. A small error in
the former will produce an enormous error in the
latter. Prediction becomes impossible, and we have
the fortuitous phenomenon."
- in a 1903 essay "Science and Method"

"If we knew exactly the laws of nature and
the situation of the universe at the initial
moment, we could predict exactly the situation
of that same universe at a succeeding moment.
but even if it were the case that the natural
laws had no longer any secret for us, we could
still only know the initial situation appproximately.
If that enabled us to predict the succeeding
situation with the same approximation, that is
all we require, and we should say that the phenomenon
had been predicted, that it is governed by laws.
But it is not always so: it may happen that small
differences in the initial conditions produce very
great ones in the final phenomena. A small error in
the former will produce an enormous error in the
latter. Prediction becomes impossible, and we have
the fortuitous phenomenon."
- in a 1903 essay "Science and Method"

Figure 3 Original text, encoded text and recovered text.

Appendix

Proposition 2.1 *Let the nonlinear chaotic system,* $x_{k+1} = f(x_k), y_k = h(x_k)$ *be locally observable, and suppose that corresponding to the constant value,* y_e, *there exists a unique state vector equilibrium value,* x_e. *Then, the system is constructible, i.e. there exists a map* $\varphi : \Re^n \to \Re^n$ *such that the state* x_k *of the system can be exactly reconstructed, from time* $k = 0$, *on, in terms of the output* y_k *and a finite string of previously obtained outputs, in the form:*

$x_k = \varphi(y_k, y_{k-1}, \ldots, y_{k-(n-1)}),\ k \geq 0$ *provided the string of outputs,* $\{y_k\}$ *for* $y - n + 1 < k \leq 0$ *is completely known. Moreover, an initialization of* $\{y_k\}$ *with arbitrarily chosen values,* $y_{-i},\ i = 1,2,\ldots,n-1$, *and the actual* y_0, *still results in an exact reconstruction of* x_k *for all* $k \geq n-1$.

References

[1] Sira H., Aguilar C., Suárez M., Exact State Reconstructors in the Recovery of Messages Encrypted by the States of Nonlinear Discrete-time Chaotic Systems, *International Journal of Bifurcation and Chaos*, Vol. 12, num. 1, 2002.

[2] Cuomo, G., Oppenheim, A. V., Strogatz, S. H. Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications, IEEE Trans. Circuits Syst-II: Analog and Digital Signal Processing, 40, 626-633, 1997.

[3] Carrol, T. L., Pecora, L. M., Synchronization Hyperchaotic Volume-Preserving Maps and Circuits, *IEEE Trans. on Circuits ans Systems-I: Fundamental Theory and Applications*, Vol. 45, num. 6, 1997

[4] Special Issue, Chaos synchronization and control: theory and applications, IEEE Trans. Circuit Syst.-I: Fundamental Theory and Applications, vol. 40, 1993.

[5] Special Issue, Chaos synchronization and control: theory and applications, IEEE Trans. Circuit Syst.-I: Fundamental Theory and Applications, vol. 44, 1993

[6] Parlitz, U., Junge, L., Kocarev, L., Chaos Synchronization, *Lecture Notes in Control and Information Sciences 244*, New Directions in Nonlinear Observer Design, H. Nijmeier and T.I. Fossen (Eds.), Springer Verlag, pp. 511-525, 1999.

[7] Parlitz, U., Junge, L., Synchronization of chaotic systems, *Proceedings of the European Control Conference ECC'99*, Paper F1056-5, 31.Aug.-3.Sept. 1999, Karsruhe, Germany, 1999.

[8] : Packard, N. H., Crutchfield, J. P., Farmer, J. D., Shaw, R. S., Geometry From a Time Series, Phys. Rev. Lett. 45, pp. 712-716, 1980.

[9] Sauer T., Yorke J. & Casdagli M., Embedology, *J.Stat. Phys. 65*, pp 579-616, 1991.

[10] Takens F., Detecting strange attractors in turbulence, in Dynamical Systems and Turbulence, eds. *Rand, D.A. & Young*, L.-S. (Springer-Verlag, Berlin), pp. 366-381, 1981.

[11] : Parlitz U., Zöller R., Holzfuss J and Lauterborn W., Reconstructing Physical Variables and Parameters From Dynamical Systems, International Journal of Bifurcation and Chaos, vol. 4, pp.1715-1719, 1994.

[12] Itoh Makoto, Wah Wu Chai, Chua Leon O., Communication Systems Via Chaotic Signals From a Reconstruction Viewpoint, International Journal of Bifurcation and Chaos, vol. 7, pp.275-286, 1997.

[13] Isidori, A., *NonLinear Control Systems*, 2nd. ed. Berlin, (Springer-Verlag, Germany), 1989.

[14] : Pecora L.M. and Carroll T.L., Synchronization in chaotic systems, Phys. Rev. Lett.,vol 64, pp. 821-824, 1990.

[15] : Huijberts Henri, Nijmeijer H, and Willems Rob, System Identification in Communication with Chaotic Systems, IEEE Transactions on Circuits and Systems -I: Fundamental Theory and Applications, vol. 47, pp. 800-808.2000.

[16] Lichtenberg, A. J. and Lieberman, M. A., *Regular and Stochastic Motion*, New York, Springer-Verlag, 1983.

[17] Pecora, L. M. and Carroll, T. L., Johnson, G., Mar, D.[1997]. Volume-Preserving and Volume Expanding, Syncrhonized Chaotic Systems, *Physical Review E*, vol. 56, 1997.

[18] Kotta, Ü., *Lecture Notes in Control and Information Sciences* 205, Springer-Verlag, London, 1995

[19] Special1997 : Special Issue Systems and Control Letters, 31, 1997.