IC/95/10

INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS

EXTRACTING MESSAGES MASKED BY CHAOS

Gabriel Pérez

and

Hilda A. Cerdeira

INTERNATIONAL ATOMIC ENERGY AGENCY

UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION

MIRAMARE-TRIESTE

IC/95/10

International Atomic Energy Agency
and
United Nations Educational Scientific and Cultural Organization
INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS

EXTRACTING MESSAGES MASKED BY CHAOS

Gabriel Pérez[1]
Departamento de Física Aplicada,
Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional,
Unidad Mérida, A. P. 73 "Cordemex", 97310 Mérida, Yucatán, México

and

Hilda A. Cerdeira[2]
International Centre for Theoretical Physics, Trieste, Italy.

ABSTRACT

We show how to extract messages that are masked by a chaotic signal in a system of two Lorenz oscillators. This mask removal is done for two different modes of transmission, a digital one where a parameter of the sender is switched between two values, and an analog mode, where a small amplitude message is added to the carrier signal. We achieve this without using a second Lorenz oscillator as receiver, and without doing a full reconstruction of the dynamics. This method is robust with respect to transformations that impede the unmasking using a Lorenz receiver, and is not affected by the broad-band noise that is inherent to the synchronization process. We also discuss the limitations of this way of extraction for messages in high frequency bands.

MIRAMARE –TRIESTE
January 1995

[1]E–mail address: gperez@kin.cieamer.conacyt.mx
[2]E–mail address: cerdeira@ictp.trieste.it

There has been some recent interest in the idea of using enslaving chaotic variables [1] as a way of transmitting information [2, 3, 4, 5, 6, 7]. The principle used here is that if we have two identical nonlinear low-dimensional dynamical systems, where one of the variables from the first system enslaves the second, this chaotic variable can be used as a carrier for a message. The use of these chaotic carriers in a communication channel is intended, among other reasons, for security [8]. The actual transmitted signal is broad-banded and should look at first sight as some type of noise. It is also expected that, since the carrier is able to synchronize only identical dynamical systems, i. e., identical sets of equations [9] with identical —or at least extremely close— parameters, any eavesdropper will be lost in the infinite maze of possible dynamical models and parameter sets and will not be able to extract the message.

Our purpose in this letter is to show that this type of masking can be easily removed, at least in some of the proposed implementations [3, 4], and that this can be achieved without recurring to a nonlinear receiving system. The origin of these weaknesses in the masking is that efficient message reconstruction requires the existence of a low dimensional attractor and a fast relaxation of the dynamics to that attractor, at least in the time scales used in the message. This allows a third party to do a *partial* reconstruction of the dynamics, using some return maps. By analyzing the evolution of the signal on the attracting sets of those maps, the message can be extracted. This process does not use at any moment the full reconstruction of the continuous dynamics of the sender [10], a more time-consuming procedure that requires embedding in a space of larger dimensionality than that of the intended receiver.

To show how this unmasking is done, we will use computer simulations of the sender-receiver circuits used in Ref. [3]. These circuits are built so that their dynamics constitutes a scaled implementation of the Lorenz equations [11]. The equations for the sender are:

$$\frac{dx_1}{d\tau} = \sigma(y_1 - x_1), \tag{1}$$

$$\frac{dy_1}{d\tau} = rx_1 - y_1 - x_1 z_1, \tag{2}$$

$$\frac{dz_1}{d\tau} = x_1 y_1 - b z_1, \tag{3}$$

while for the receiver we have

$$\frac{dx_2}{d\tau} = \sigma(y_2 - x_2), \tag{4}$$

$$\frac{dy_2}{d\tau} = rx_1 - y_2 - x_1 z_2, \tag{5}$$

$$\frac{dz_2}{d\tau} = x_1 y_2 - b z_2. \quad (6)$$

Here $\tau = Kt$, where K is an overall scale factor. The values used here are those from Ref. [3]: $\sigma = 16.0$, $r = 45.6$ and $b = 4.0$. The scale factor has been set to $K = 1/2505$ [12], so that the time scale agrees with the one used in the figures of the cited reference.

In the second set of equations, the use of x_1 instead of x_2 in Eqs. (5) and (6) has the effect of enslaving the second oscillator to the first. This means that if we start the two oscillators from different initial conditions, but using in both the same set of parameters, the variables in the receiver will soon approach the values of those of the sender. The equation for x_2 in the receiver serves as a check of this enslavement, since the process makes x_2 approach x_1.

The actual transmission of data is implemented in one of two ways. The first one, digital, changes the parameter b in the equations of the sender between its reference value $b = 4.0$ and a shifted one of $b = 4.4$. The corresponding parameter in the receiver is kept fixed at the reference value, giving as a result that the oscillators synchronize when the parameters are equal and are frustrated when they are different. This frustration is manifested in the squared difference $(x_2 - x_1)^2$, which presents persistent fluctuations when the two b's are different. Examples of how this process works are given in Refs. [3, 5].

The second option for transmission of messages is to add a small amplitude analog message $m(t)$ to the variable $x_1(t)$ we get from the sender, producing a modified drive $s(t) = x_1(t) + m(t)$. This new drive is fed to the receiver. A synchronization of sorts is achieved, but it is far from perfect, since the incoming signal is not exactly a variable of the Lorenz system. However, the frustration in the synchronization process can still be used as a way of recovering the message, using for this purpose the difference $s(t) - x_2(t)$. This process, however, is nontrivial. The difference between drive and response does not exactly reproduce the added message $m(t)$, and the correlation between the two is strongly dependent on the frequencies involved. This happens because, as can be easily seen in any numerical simulation, the error in the synchronization process decays in its own time scale, and not monotonously. Given initially unsynchronized oscillators, for the parameters we are using here, the difference $x_2 - x_1$ decays in a time scale of roughly 10^{-4} sec., and presents oscillations with a broad spectrum of frequencies, with a peak around $f_0 \approx 3$ KHz.

This synchronization delay affects the quality of the recovered message. For frequencies comparable with those predominant in the synchronization noise, the reconstructed message gets a large admixture of noise and does not reproduce the message well. For

smaller frequencies one finds that the reconstructed message contains a broad spectrum of frequencies above the transmitted one, and that the output approximatedly reproduces the input message only if we perform a low pass filtering.

For very high frequencies, well above f_0, a different phenomenon occurs. The period of the message is much smaller than the decay time of the synchronization process, and the message and the synchronization– frustration mechanism decouple. This makes the recovered message practically identical to the original one. However, this decoupling happens at such high frequencies that a careful eavesdropper may be able to notice some peaks in an otherwise broad spectrum, this being so because the power spectrum of the Lorenz oscillator is quite low at high frequencies.

Our approach to this problem comes from the discovery by Lorenz [11] that by following just one of the variables in the set of Eqs. (1)–(3), one can produce a return map where the dynamics is attracted to an almost 1-D set. Following this lead, we constructed the following return map from the $x(t)$ variable in the Lorenz oscillator: Starting from some arbitrary point in time, define t_n as the time when $x(t)$ reaches its nth (local) maximum, and X_n as the value of x at that moment. Similarly, define another return map by setting u_m as the time when $x(t)$ reaches its mth local minimum, and Y_m as the value of x at that moment. Using these discrete values we can construct the return maps X_{n+1} vs. X_n, and Y_{m+1} vs. Y_m. These two maps have attractors that look almost 1-D. Under the transformation $Y \to -Y$ the attractor for the Y map is identical to that of the X map. This is due to the fact that the underlying dynamics is invariant under the transformation $x \to -x$, $y \to -y$, $z \to z$, and therefore the maxima of $x(t)$ and the minima of $-x(t)$ give the same return map.

We will not use directly these two return maps; after some experimentation we have found that we get better results using the linear combinations $A_n = (X_n + Y_n)/2$, $B_n = X_n - Y_n$, $C_n = (X_{n+1} + Y_n)/2$, and $D_n = Y_n - X_{n+1}$. These are simply the average value of a consecutive maximum-minimum pair, and the distance between them. The return maps A_n vs. B_n and C_n vs. D_n have very simple attractors. Each is given by 3 smooth almost 1-D unconnected segments, and they have the same inversion symmetry as for the X and Y maps, so that the A vs. B section is identical to the $-C$ vs. $-D$ section. These are shown in Fig.1 .

The key to extracting messages from the chaotic mask, in this digital mode, is to recognize that a small change in the parameters of the sender not only frustrates the synchronization but also affects the attractor obtained in the return map (here we will

just superimpose the A vs. B and the $-C$ vs. $-D$ return maps). Since the change in parameters is small, the only effect is a shift in the position of the segments of the attractor, while its general form is conserved. Therefore, the attractor obtained when there is a message shows splitting, with two close parallel branches appearing where only one segment was found for the unperturbed Lorenz oscillator (see Fig.2).

Once we have realized that the switching between the two parameters means also switching between the two parallel branches of the attractor, it is a simple task to go back to the return map and start classifying the points accordingly to which branch of the attractor they fall in. We use only the points that are clearly separated, and assign a 0 or 1 value to each branch of a split segment. Then, we read in the time sequences the values t_n and a_n and plot the assigned value vs. time. The result will probably be meaningless, since we have done the assignment of 0's and 1's in an arbitrary way. We need to try different assignments and compare the results. The correct one will be that that shows always long sequencies of only 0's or only 1's. This is so because the bits of the original message have to be long enough (in time) as to overcome the synchronization lag, and that gives $x_1(t)$ in the sender enough time to run through several maxima and minima. Here we have three split segments, which means that we need to try four possible assignments of zeros and ones. (The assignment for the first segment is arbitrary). In Fig.3 we show the messages extracted using the correct assignment and a typical wrong one.

It is clear from these results that this simple algorithm permits the reconstruction of the message, except for the small ambiguity of deciding which bits are identified as 1's and which as 0's. As a bonus, out scheme is robust with respect to transformations that affect the mask removal using a Lorenz oscillator, something that we should expect from the amplification of the signal needed for long distance transmissions. In particular, the simple affine modification $x_1'(t) = ax_1(t) + b$, with a and b constants, is ignored by our scheme, except for an unimportant breaking of the symmetry between the A vs. B and C vs. D maps. On the other hand, it can completely spoil the synchronization-frustration process needed for transmission between Lorenz systems.

For the analog mode, the separation of a signal into a small-amplitude message and a carrier is not much more difficult than the extraction of digital messages done before, at least for low frequencies. We use the same principle, i. e., the fact that perturbations of any kind on the carrier signal affect the (quasi) 1-D attractors of the return map. For the analog mode of transmission the effect of adding the message $s(t)$ to the carrier $x_1(t)$ is to

smear the attractor, making its 3 segments into 3 diffuse stripes. If we superimpose the original "silent" attractor —which should become apparent in an actual transmission as a denser line that forms during any silences the message happens to have— to these stripes, we find that the broadening is almost symmetric, with equal spreads at both sides.

What we do in order to recover the message from the return maps is to measure the distance between the present position of the points in the attractor, and the place they should have appeared in the absence of a message, i. e., in the silent attractor, taking into account to which side of it the point has moved. This distance can be reasonable approximated by the closest distance to the silent attractor. In our case, stripes 1 and 3 of the attractor are almost vertical, and stripe 2 is approximatedly horizontal. Therefore, is enough to take the x-distance to the silent attractor for stripes 1 and 3, and the y-distance for stripe 2. Once this is done, we need to assign an amplitude factor (including sign) to segments 2 and 3 (segment 1 is assigned +1.0 by default), and do some trial and error adjustments — mostly for the signs — on these two amplitudes in order to get a meaningful output.

The results of this procedure are quite satisfactory for frequencies below a cut-off $f_c \approx 3000$ Hz, which is the value where the power spectrum for the synchronization noise peaks. For these low frequencies, the carrier has several maxima and minima for each period of the message, allowing for a good reconstruction, with some redundance to spare, and little noise. (See Fig.4). The quality of the recovered message deteriorates as we go trough f_c, and for frequencies larger than this cut-off the results are very poor. Very often, the output misses completely the oscillations in the message. For frequencies well above the cut-off the return map does not work, since it samples the signal at a rate too low compared to the message's period.

In conclusion, we have shown that it is possible for a diligent eavesdropper to uncover messages transmitted using a Lorenz-Lorenz chaotic pair. The digital mode of transmission is easily and efficiently unmasked, even allowing for signals that have been corrupted, say by an imperfect amplification process. Given the sharp separation of the two branches of the attractor, this scheme will work even under small noise conditions.

For the masking of analog messages the mask removal will work for frequencies up to a cut-off given roughly by the peak frequency of the noisy synchronization spectrum. For frequencies close to this cut-off both extraction schemes give poor results, while for frequencies much higher than the cutoff our approach to mask removal does not work.

Since the main limiting element in our unmasking algorithm is the existence of a cut-off

frequency, it seems that all that is needed to defeat the eavesdropper is to transmit only in the high frequency bands. In this case, however, sender and receiver will be working in a sector where the power spectrum of the Lorenz oscillator is quite low, and it may not be enough to mask the signal.

What we have done here for Lorentz oscillators should also work for transmissions done using other synchronized chaotic systems. In general, dynamics where just one variable is enough to enslave a set of differential equations will have only one positive Lyapunov exponent. Other exponents being negative enough as to insure fast synchronization, the attractors in 2-d return maps will be (quasi) 1-D sets, and will necessarily show the effects of any perturbation over the carrier. These effects may occasionally not be clean enough to allow unmasking, but there is always a chance that a good choice of return maps will spoil security for chaotic transmissions.

References

[1] L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. **64**, 821 (1990); Phys. Rev. A **44**, 2374 (1991); T. L. Carroll and L. M. Pecora, IEEE Trans. Circuits Sys. **38**, 453 (1991).

[2] A. V. Oppenheim, G. W. Wornell, S. H. Isabelle and K. Cuomo, *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing ICASSP 92*, pg. 117 (IEEE, New York, 1992); K. Cuomo and A. V. Oppenheim, *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing ICASSP 93*, (IEEE, New York, 1993);

[3] K. Cuomo and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993);

[4] K. Murali and M. Lakshmanan, Phys. Rev. E **48**, R1624 (1993); Int. Jour. Bifurcations and Chaos **3**, (1993).

[5] U. Parlitz *et. al*, Int. Jour. Bifurcations and Chaos **2**, 973 (1992).

[6] S. Hayes, C. Grebogi and E. Ott, Phys. Rev. Lett. **70**, 3031 (1993).

[7] K. S. Halle *et. al*, Int. Jour. Bifurcations and Chaos **3**, 469 (1993).

[8] Comments on the use of these systems for secure communications have appeared in many sources. See for instance: I. Amato, Science **261**, 429 (1993), J. C. G Lesurf, Nature **365** 604 (1993).

[9] It was found recently that the slave system does not have to be identical to the master. The evolution equations for the slave may contain extra terms, as long as they go to zero when synchronization is achieved. See M. Ding and E. Ott, Phys. Rev. E **49**, R945 (1994).

[10] N. H. Packard, J. P. Crutchfield, J. D. Farmer and R. S. Packard and Shaw, Phys. Rev. Lett **45**, 712 (1980); F. Takens, in *Dynamical Systems and Turbulence*, edited by D. A. Rand and L. S. Young, pg. 366 (Springer, Heildelberg, 1981); P. Grassberger *et. al.*, Chaos **3**, 127 (1993).

[11] E. Lorenz, J. Atmos. Sci. **20**, 130 (1963).

[12] K. Cuomo, personal communication.

FIGURE CAPTIONS

Fig.1. Attractors of the return maps obtained from the maxima and minima of $x(t)$ in the Lorenz oscillator. Here we have superimposed the attractors for the maps A_n vs. B_n and $-C_n$ vs. $-D_n$, whose definitions are given in the text. The 3 segments of the attractor are labeled for later convenience.

Fig.2. Segment 2 of the attractor of the return map, split by the use of both $b = 4.$ and $b = 4.4$ in the generation of the signal. The other two segments of the attractor undergo similar splitting.

Fig.3. Unmasking of a digital transmission, using the return map. In (a) we show the results obtained with the correct assignment of 0's and 1's to segments 2 and 3 of the attractor. In (b) we show the results of a typical wrong assignment. The correct unmasking gives results identical to the original message, which was the word "1010011101". Each bit is 4 msec. long.

Fig.4. Unmasking of analog messages using the return map. The dotted lines are the original message $m(t) = 0.1\sin(2\pi ft)$, and the solid line is the reconstructed messages. In (a) we have $f = 750$ Hz., and in (b) $f = 3$ KHz.

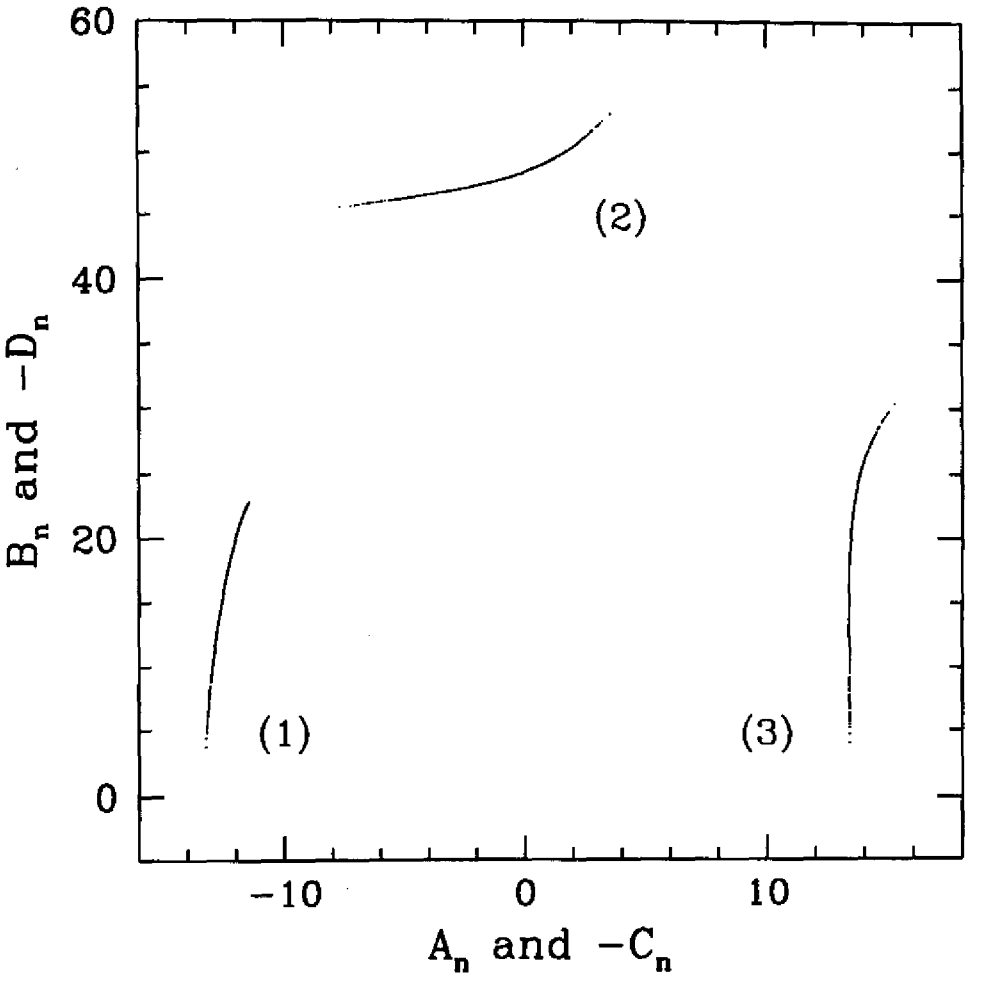

Fig.1

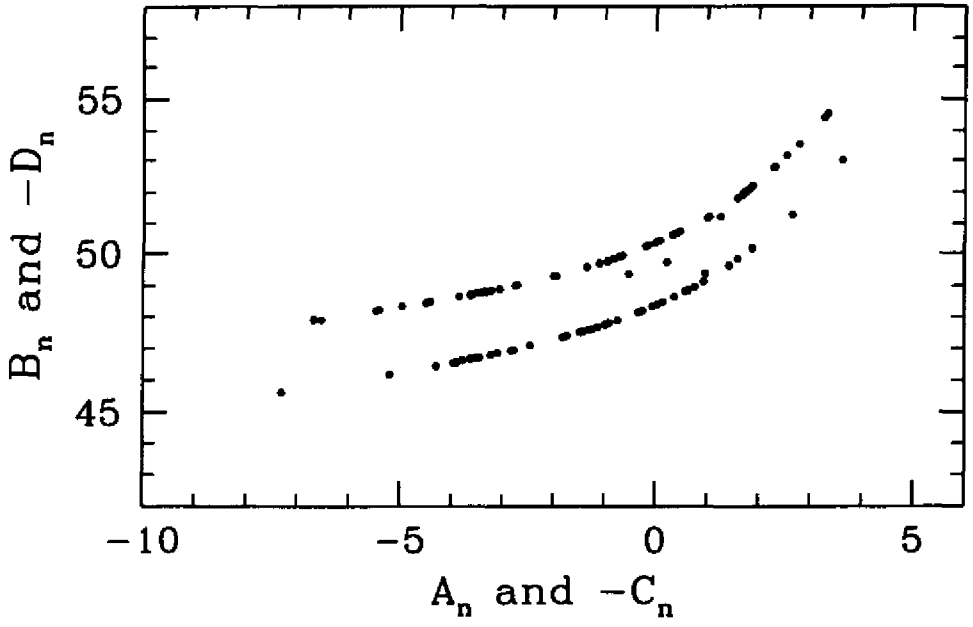
55
50
45
B_n and $-D_n$
−10
−5
0
5
A_n and $-C_n$

Fig.2

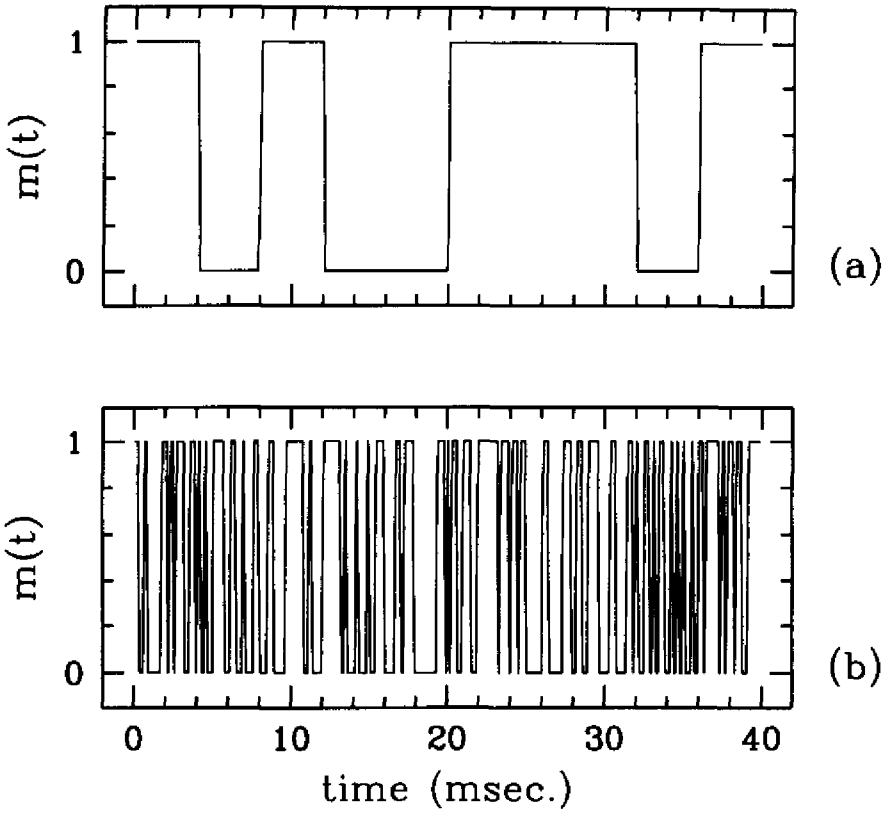
1
0
m(t)
(a)
1
0
m(t)
(b)
0
10
20
30
40
time (msec.)

Fig.3

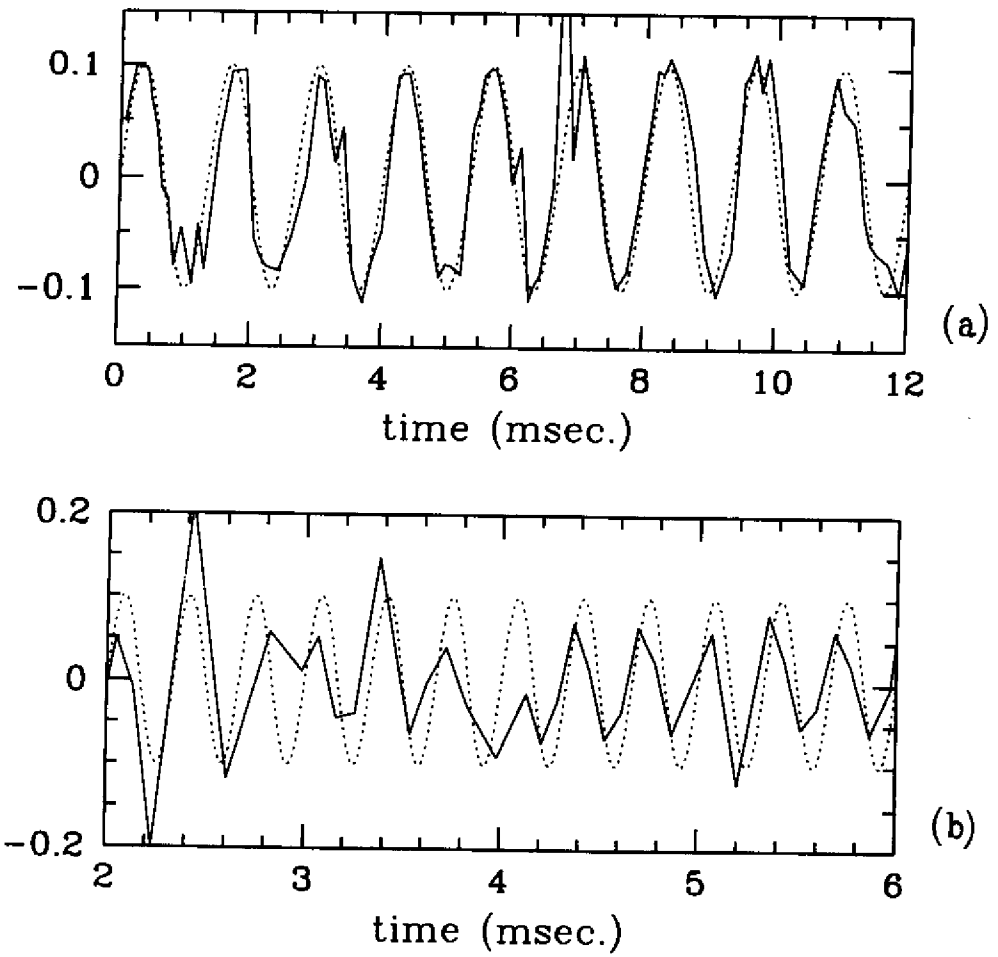

Fig.4