Радиофизика и радиоастрономия, 1997, т. 2, №4, стр. 473-479

Chaotic Masking without Synchronization

V. B. Ryabov, P. V. Usik, D. M. Vavriv

Institute of Radio Astronomy of NAS of Ukraine,
4 Krasnoznamennaya St., 310002 Kharkov, Ukraine

The paper is received by editor December, 23, 1997

A method of secure communication based on the inversion of a chaotic dynamical system is analyzed. The approach does not require chaotic synchronization of two or several oscillators to be used. The influence of noise in the communication channel and parameter mismatch on the quality of decoded signal is discussed. Autonomous Rössler oscillator and non autonomous pendulum equation are used as examples.

Considerable progress has been recently made in achieving the goal of secure communication by means of chaotic synchronization. The ability of two or more nonlinear oscillators moving chaotically to synchronize has been used to create encoding-decoding units. As for practical implementation of this idea, several ways for constructing the encoding-decoding circuits have been proposed. Two basic groups of methods which draw considerable interest can be mentioned.

The first one has been developed in [1-3]. The scheme includes a transmitter with a nonlinear oscillator capable to operate in a chaotic regime. The transmitted signal is a sum of one of the components of the chaotic oscillator and information signal. It is used for synchronizing the receiver oscillator, supposed to be identical to the one used in the transmitter. The decoded signal is simply the difference between the transmitted signal and the corresponding synchronized component in the receiver. There are several obvious disadvantages of such a setting.

1. The quality of masking is not perfect, for the information is just added to the masking signal, and it can be at least partially recovered by using a signal processing technique based on Takens embedding theorem [4] and/or chaotic filtering [5].

2. The amplitudes of the transmitted and received signal should be kept identical.

3. Synchronization requires a certain time to be achieved, and the information signal destroys the synchronized state in the receiver oscillator.

4. The exact recovery of information is impossible. The smaller is the intensity of the information signal, the better is the quality of the recovered information.

The principal difference of the second group of methods [6,7] is that the information signal is used to drive chaotic oscillators in both the receiver and transmitter. Here, the transmitted signal is a function (generally nonlinear) of chaotic components of the transmitter oscillator and the information signal. This allows to eliminate such shortcoming of previously considered scheme as the demand for the amplitude of the information signal to be small for providing a high quality of synchronization regime and, therefore, the intensity of the information signal may be of the same order of magnitude as that of the masking one. Moreover, the information can be recovered exactly by inverting the nonlinear function used for composing the transmitted signal in the transmitter. But still, this method is not perfect, since several problems persist.

1. This approach also requires stable synchronized regime to be achieved between receiver and transmitter, that may be deteriorated due to communication channel noise or filtering, control parameters mismatch, etc.

2. The amplitudes of the transmitted and received signal are supposed to be made identical.

3. When the amplitude of information signal is high, the chaotic attractor in the receiver or transmitter oscillator may be broken. This situation may occur intermittently and result in a poor quality of masking.

Some of the above mentioned drawbacks may be weakened or partially avoided by introducing other concepts, such as e. g. cascading synchronization [8], generalized synchronization [3], phase synchronization [9], autosynchronization [7], using special kind of filters [10], etc.

In the present communication we would like to discuss an alternative method of using deterministic chaos for the purpose of encoding and decoding information which does not use the phenomenon of synchronization at all. The method is based on the fundamental property of chaotic oscillations that any trajectory representing chaotic motion in the phase space lies on an integral manifold defined by the particular form of governing differential equations. For example, for a non autonomous system

$$\frac{d^2x}{dt^2} + f\left(x, \frac{dx}{dt}\right) = F(t) \qquad (1)$$

the existence of such manifold is manifested in the fact that given the particular shape of a nonlinear function $f\left(x, \frac{dx}{dt}\right)$ and a chaotic solution $x_{ch}(t)$,

one can easily solve the inverse problem of reconstructing the exciting signal (external force) from the chaotic response of the system. Indeed, the relation

$$F(t) \equiv \frac{d^2 x_{ch}(t)}{dt^2} + f\left(x_{ch}(t), \frac{dx_{ch}(t)}{dt} \right) \qquad (2)$$

holds all the time, independently from initial conditions.

This property can be readily used for the purpose of secure communication (see also [11]). Let $F(t)$ be the sum of a harmonic signal and a small addition $i(t)$ carrying the information

$$F(t) = A\cos(\omega t) + i(t).$$

If $i(t) \equiv 0$, a chaotic oscillation is excited in the system (1). Assume that the perturbation $i(t)$ is sufficiently small for not destroying the chaotic motion in Eq. 1. To decode the chaos+signal mixture, i. e. to separate the $i(t)$ component, it is necessary to design a receiver capable of inverting the Eq. 1 in accordance with Eq. 2. In other words, the received signal has to be twice differentiated and combined with its copy passed through a nonlinear element with the response $f\left(x, \frac{dx}{dt} \right)$ that can be realized with conventional electronic circuits. As a result, the original exciting oscillation $F(t)$ is recovered, which is an additive mixture of the harmonic and information signals.

It should be noted that in such method of encoding, as well as in other conventional schemes, the signal undergoes complicated transformations which can not be expressed in terms of an additive or multiplicative mixture of the signal and the masking chaotic oscillation. An important property of the proposed technique is that the receiver is just a kind of nonlinear filter, performing the operations of differentiation and nonlinear transformation. Due to this last fact, the quality of the signal recovery does not depend on the amplitude of the information signal, and there is no threat of the chaotic oscillation destruction in the receiver. Another advantage of this method is safety of information. Indeed, even if the chaotic attractor at the transmitter end is destroyed by the information signal, i.e. the transmitter generates periodic oscillations mixed with information signal, this results in the absence of masking, but all the information reaches the receiver and is recovered. Close ideas can be also found in [11], where this method was referred to as the synchronization of systems of relative order zero. However, it seems that the term "synchronization" is not applicable for this case at all, since the signal from the transmitter does not synchronize the receiver, and just undergoes a nonlinear transformation in it. So far, this method of secure communication has not attracted much attention due to apparent difficulties of its practical implementation related to a substantial amplification of the communication channel noise when the differentiation of high order is performed in the decoding device. In this paper we discuss several possible solutions to get rid of this problem.

Evidently, there are at least two ways to reduce noise in the output signal. First, it is possible to avoid multiple differentiation in the receiver by increasing the number of chaotic components and/or their derivatives transmitted via the communication channel. The second way consists in applying low-pass filtering for suppressing the noise amplification in the differentiators of the receiver. Our results indicate that the influence of noise can be substantially reduced, and the proposed method is of interest for applications, for it possesses several advantages in comparison to other techniques. We will study the feasibility of both methods by the examples of non autonomous pendulum and autonomous Rössler oscillator, correspondingly.

So, we start with the pendulum equation

$$\frac{d^2 x}{dt^2} + \alpha \frac{dx}{dt} + \omega^2 \sin(x) = A\sin(\Omega t + \varphi_0) + i(t), \qquad (3)$$

where x is generalized phase of the pendulum, ω, its proper frequency, α, the dissipation parameter, A and $\Omega t + \varphi_0$ are the amplitude and phase of the external force, $i(t)$, information signal. This equation is a convenient object for our purpose, for it is a well documented and easily controlled model. In addition, chaotic regimes of the pendulum appear to be stable with respect to comparatively strong perturbations in the form of intense driving signal $i(t)$.

In an ideal situation, the signal $i(t)$ can be restored exactly in the receiver as

$$i(t) = \frac{d^2 x^*(t)}{dt^2} + \alpha \frac{dx^*(t)}{dt} + \omega^2 \sin(x^*(t)) - A\sin(\Omega t + \varphi_0),$$

where $x^*(t)$ is an arbitrary solution of (3) transmitted through the communication channel. However, in any implementation we encounter the problem of extreme sensitivity of the decoding process upon the

mismatch in frequency Ω between the transmitter and receiver systems. As can be easily seen, any small uncertainty in specifying the frequency Ω and the initial phase φ_0 leads to accumulation of the error in the decoded signal with time. So, it appears rather difficult to implement this particular scheme to practice without some modification.

We propose a solution to this problem consisting in extracting the sum $i(t)+A\sin(\Omega t+\varphi_0)$ rather than $i(t)$ alone, and suppressing the harmonic component by a conventional filtering. This idea is easily put into practice when the frequency Ω is located well above the frequency band of the information signal. In this case the low-pass filtering of the output signal in the receiver accomplishes the goal. Note, that even with such "high frequency" excitation of the pendulum, the spectrum of the induced chaotic signal has intensive components in the low frequency domain, and chaotic masking is effective in the whole frequency band of the information signal.

We have found that the most straightforward and reliable version of the encoding-decoding pendulum-based system is the one utilizing two communication channels, when the first derivative $u_1 \equiv \dfrac{dx^*(t)}{dt}$ and $u_2 \equiv \sin\left(x^*(t)\right)$ are transmitted. This requires only one differentiation to be performed in the receiver that does not produce substantial additional noise. Moreover, in such a scheme the receiver turns out to be linear with respect to the components u_1 and u_2 that gives an advantage of not using an additional device for matching the signal amplitudes at the transmitter and receiver ends. In addition the linearity of the receiver allows in a rather simple manner to compensate the effect of unavoidable filtering introduced by the communication channel [12] that is known to be a severe problem in practice [13].

To examine the feasibility of the proposed scheme, we have experimented with several information signals: sinusoid of constant and modulated amplitude, wide band records of sound, and finally high-dimensional chaotic signals from of the well known Mackey-Glass equation

$$\frac{dx}{dt}=\frac{ax(t-\tau)}{1+\left[x(t-\tau)\right]^{10}}-bx(t)$$

at $a=0.2$, $b=0.1$, $\tau=100$. The results appear qualitatively similar for different types of the signals used, so we present below only those for the Mackey-Glass signals which are known to be the most difficult to recover in conventional methods using synchronization. An example of power spectrum of the signal $\dfrac{dx^*(t)}{dt}$ is shown in Fig. 1, together with the spectrum of $i(t)$. The result of the decoding and subsequent filtration is depicted in Fig. 2 where both the initial signal $i(t)$ and the one recovered in the receiver $\tilde{i}(t)$ are shown, together with their difference. When the control parameters of the receiver match exactly the ones in the transmitter, the signal is recovered practically without distortions, and the effect of noise amplification is negligible.

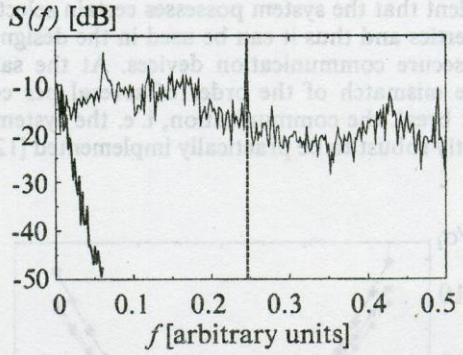

Fig. 1. *Power spectra $S(f)$ of two signals: I) transmitted mixture of chaotic oscillation in the nonautonomous pendulum oscillator (masking) with high dimensional chaotic information signal from Mackey-Glass equation (thin line); II) the signal of Mackey-Glass equation alone (thick line). Dashed line is the excitation frequency*

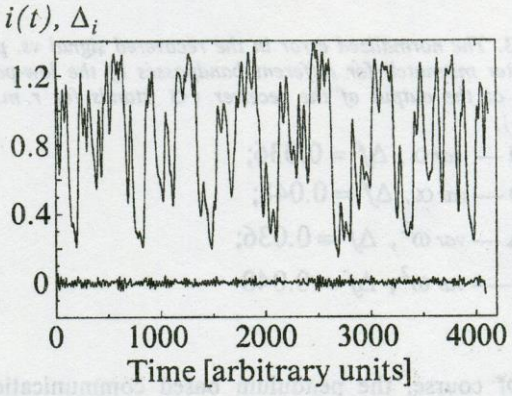

Fig. 2. *Original and recovered signals $i(t)$ at zero noise level and identical parameter values in the transmitter and receiver (two upper lines). The difference Δi between them (lower line)*

As the degree of security for the encoded information is strongly dependent upon the selectivity prop-

erty of receiver with respect to the variation of control parameters, we have also analyzed how the mismatch in the control parameters between encoder and decoder influences the quality of the recovered signal. In Fig. 3 we plot the magnitude of the normalized error

$$error = \sqrt{\frac{D\left(i(t) - \tilde{i}(t)\right)}{D\left(i(t)\right)}},$$

where $D(\bullet)$ stands for dispersion, vs. mismatch in the parameters of dissipation and natural frequency. It is evident that the system possesses certain selectivity properties and thus it can be used in the design of chaotic secure communication devices. At the same time, the mismatch of the order of several per cent does not break the communication, i. e. the system is sufficiently robust to be practically implemented [12].

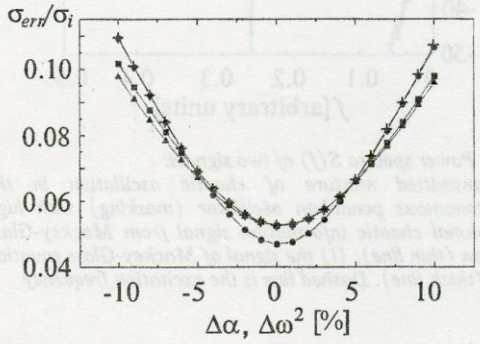

Fig. 3. *The normalized error in the recovered signal vs. parameter mismatch for different bandpasses of the low-pass filter at the output of the receiver (σ stands for r. m. s. value):*

— ■ — $var\,\alpha$, $\Delta f = 0.036$;

— ● — $var\,\alpha$, $\Delta f = 0.048$;

— ▲ — $var\,\omega^2$, $\Delta f = 0.036$;

—+— $var\,\omega^2$, $\Delta f = 0.048$

Of course, the pendulum based communication scheme is not free from drawbacks. One of them consists in the necessity to transmit two components of the masked signal that requires the corresponding broadening of the communication channel bandwidth or using two channels instead of a single one. Another shortcoming is a small number of control parameters defining the state of the receiver (dissipation α and natural frequency ω) that lowers the degree of security of the proposed system.

The just considered technique is feasible not only for non autonomous systems of the type (1), but also for autonomous ones. We demonstrate this fact by the example of Rössler oscillator

$$\begin{aligned} \frac{dx}{dt} &= -(y+z), \\ \frac{dy}{dt} &= x + ay, \\ \frac{dz}{dt} &= b + z(x-c) + i(t), \end{aligned} \qquad (4)$$

where a, b, c are control parameters, $i(t)$, the information signal. Using Eq. 4 for constructing the transmitter, one can decode the information $i(t)$ in the receiver by inverting Eqs. 4 with respect to $i(t)$ via the formula [14]

$$i(t) = -\frac{d^3y}{dt^3} + a\frac{d^2y}{dt^2} - \frac{dy}{dt} - \left(a\frac{dy}{dt} - y - \frac{d^2y}{dt^2}\right)\left(\frac{dy}{dt} - ay - c\right) - b. \qquad (5)$$

So, after transmitting a single component $y(t)$ the information can be recovered by performing the transformations (5) in the receiver. In principle, the scheme can be realized with a single transmission channel. If there is no noise in the communication channel and the control parameters of the receiver and transmitter match exactly, then a perfect recovery of the information is readily obtained.

However, the situation turns out to be very sensitive to the appearance of noise in the communication channel. The main source of huge errors in the decoded signal is triple differentiation in the receiver which makes the output noise intensity several orders of magnitude higher than that at the input. Say, if the input signal to noise ratio (SNR) is about 1 %, then the intensity of noise after the decoding procedure may reach the values of 10^5 % at moderately small values of time differentiation constant used in the procedure of numeric differentiation. A way of improving the resulting SNR is to perform low-pass filtering of the additive noise component in the receiver. The filtering has to be applied after each differentiation that occurs in the receiver circuits. At each stage of differentiation-filtration, the bandpass of the filter should be carefully tuned to minimize the error value. This method allows to reach reasonable level of SNR (~ 10÷12 %) at the output of the de-

coder at moderate noise level (~ 5 %) of the input of the receiver (Fig. 4).

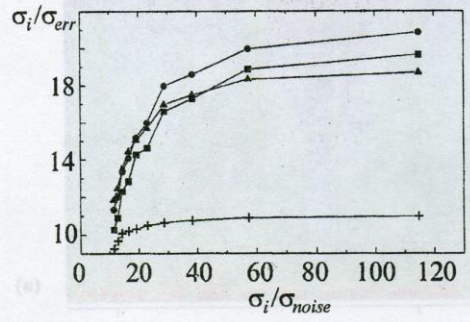

Fig. 4. *The normalized error in the recovered signal vs. normalized noise intensity in the communication channel for different bandpasses of the low-pass filter at the output of the receiver.*

Δf *of filter:*

—■— 0.06;

—●— 0.048;

—▲— 0.036;

—+— 0.024

There is also another important consideration concerning SNR which should be taken into account. Note that there are three characteristic amplitudes in any encoding-decoding scheme: the amplitude y_{ch} of chaotic signal of the Rössler oscillator mixed with the information signal (transmitted signal), the intensity of the information signal itself $i(t)$, and the noise level $n(t)$ in the communication channel. Let's denote the corresponding r. m. s. values as σ_{ch}, σ_i, and σ_n, and keep in mind that in a typical situation the inequality $\sigma_{ch} > \sigma_i > \sigma_n$ holds. The SNR at the input of the receiver is defined by σ_{ch}/σ_n, whereas the corresponding value at the output has σ_i in the nominator, and the r. m. s. of the output error, σ_{er}, in the denominator. So, apart from the problem of error growth in the receiver, there is an additional cause of lower SNR value in the decoded signal, which is defined by the ratio σ_{ch}/σ_n. Therefore, in order to reach the maximal possible SNR, it is necessary to increase the value of σ_i as much as possible. (Note, that the value of σ_{ch} is only slightly dependent upon σ_i, and the phase portrait of the corresponding attractor shown in Fig. 5 remains almost unchanged with σ_i). This, however, may result in a poor quality of masking the information, especially in conventional methods of encoding based on synchronization of chaotic oscillators and additive masking of information. Our approach, is not so sensitive to the amplitude of information signal and provides a good quality of masking even at rather high levels of information signal. For example, in Fig. 6 we present the dynamic spectra of a musical record (a) and its encoded versions by a conventional method of [7] (b) and our method (c). The color represents the amplitude of windowed Fourier components. The transition from small to large amplitudes corresponds to blue-yellow-red sequence. One can easily recognize the patterns present in Fig. 6a on the dynamic spectrum of Fig. 6b, whereas they are evidently absent in Fig. 6c. We would like to note that such kind of presentation and judgment of the quality of masking turns out to be well consistent with auditory perception of a human. The absence of patterns on a dynamic spectrum manifests itself as a pure noise when listening to the masked record.

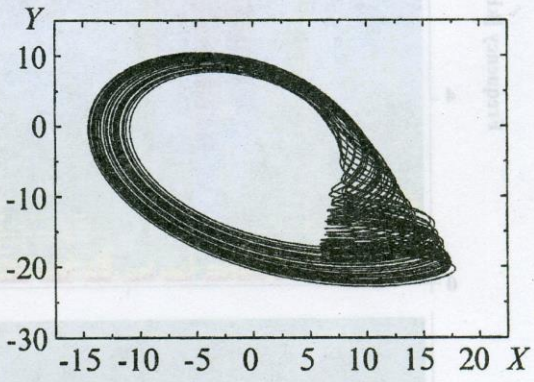

Fig. 5. *Phase portrait of the Rössler oscillator influenced by the information signal. The intensity of the information signal is about 1/3 of the masked one. The overall appearance of the attractor and its size in the phase space almost does not depend upon the amplitude of information signal*

To conclude, we have performed a feasibility analysis of encoder-decoder scheme based on the notion of an inverse system and chaotic masking. It has been demonstrated that this concept, which does not require synchronization of transmitter and receiver oscillators, can be effectively implemented by using either non autonomous or autonomous chaotic oscillators as encoders of information. The advantage of the proposed approach consists in the possibility to avoid several serious drawbacks typical of traditional chaotic masking schemes based on the phenomenon

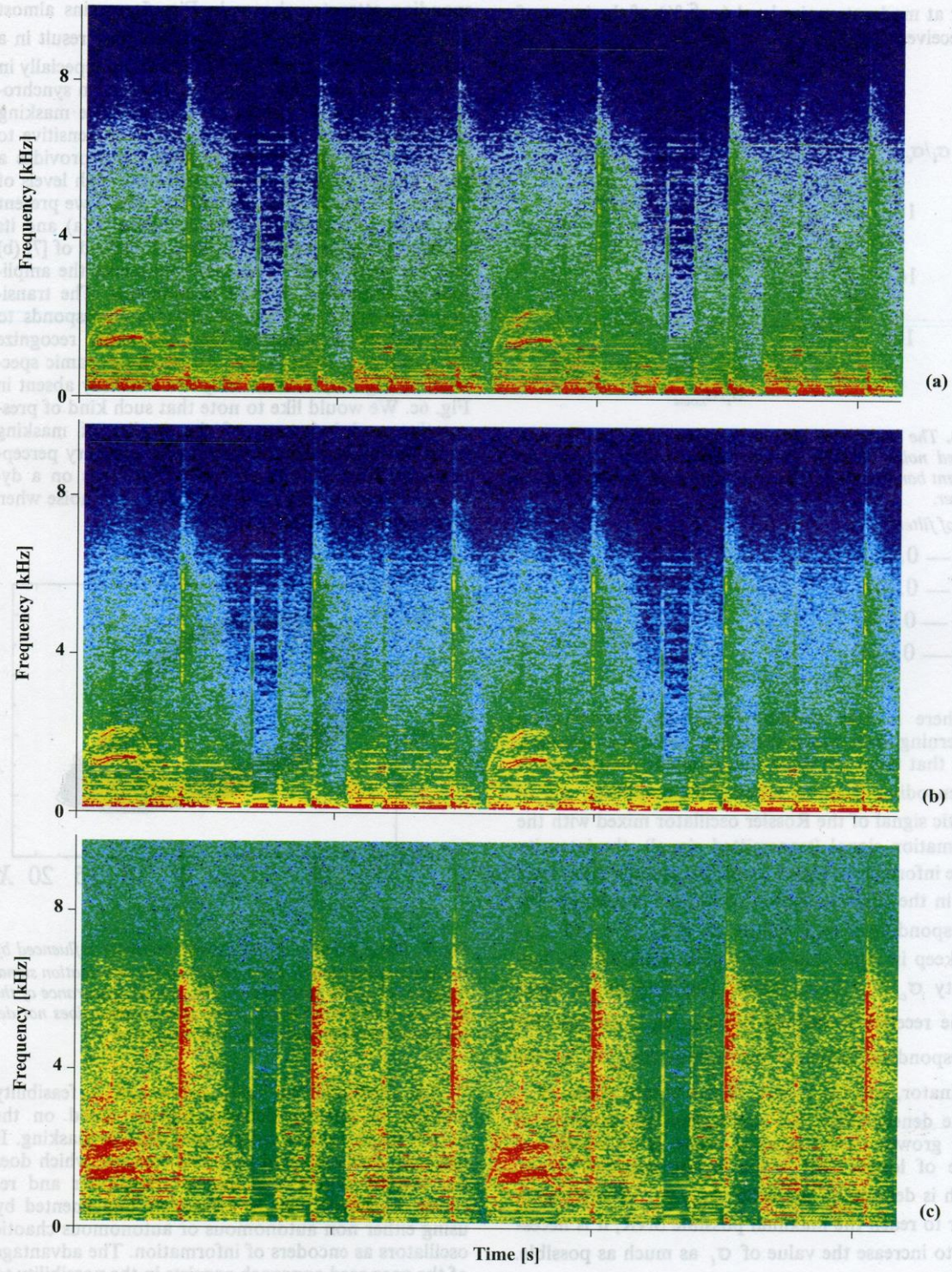

Fig. 6. *Dynamic spectra (windowed Fourier transform) of a musical record: original signal (a), additive mixture of chaotic and information signals, poor quality of masking (b), high quality masking of information (c)*

of synchronization. In particular I) the quality of masking the information is substantially improved; II) the danger for the chaotic regime to be destroyed in the receiver is absent; III) the receiver is not inertial, i. e. there is no synchronization delay in the decoding; IV) the amplitude of the information signal need not be small compared to the chaotic masking oscillation; V) exact recovery of information is possible.

Intrinsic properties of the proposed scheme require the narrow bandwidth of the information bearing signal compared to the bandwidth of the masking oscillation. This restriction is motivated first by the demand of the robustness of the algorithm to the noise in communication channel, and, second, by the necessity to remove the driving sinusoidal oscillation from the decoded signal.

The proposed method of chaotic encoding-decoding may be also used with autonomous systems, like Rössler oscillator. However, its practical implementation encounters several difficulties originating from the amplification of noise in differentiating circuits of the receiver. Nevertheless, as our calculations show, the output noise can be substantially reduced by using multichannel communication schemes and smoothing filters in the differentiation operators.

So defined procedure turns out to be a sufficiently robust one, in the sense that small uncertainties in specifying the function $f(\bullet)$ in the reconstruction process result in small differences between the reconstructed signal $\tilde{F}(t)$ and the original one $F(t)$. Another important property of the proposed technique is its asymptotic stability, i. e. the absence of error accumulation effect with time. In the decoding procedure the errors are not accumulated with time, as could be expected in any chaotic system with exponential divergence of any nearby trajectories, mainly due to the local character of signal transformation (2) at any time moment. So defined decoding process is in essence just a kind of nonlinear filtration, which preserves one-to-one correspondence between input and output signals.

References

1. V. S. Afraimovich, N. N. Verichev, and M. I. Rabinovich. Radiophys. Quantum Electron. 1986, **29**, p. 795.
2. L. Pecora and T. Caroll. Phys. Rev. Lett. 1990, **64**, p. 821.
3. N. F. Rulkov, M. M. Sushchik, and L. S. Tsimring. Phys. Rev. 1995, E **51**, p. 980.
4. F. Takens. In Proc. Warwick Symp. 1980, edited by D. A. Rand and L.-S. Young. Lecture notes in Mathematics, vol. 898. Springer, Berlin, 1981, p. 366.
5. D. S. Broomhead and G. P. King. Physica. 1986, D **20**, 217.
6. A. R. Volkovskii and N. F. Rulkov. Pis'ma Zh. Tekh. Fiz. 1993, **19**, p. 71 [Tech. Phys. Lett. 1993, **19**, p. 97].
7. U. Parlitz, L. Kocarev, T. Stojanovsky, and H. Preckel. Phys. Rev. 1996, E **53**, p. 4351.
8. T. L. Caroll and L. M. Pecora. Physica. 1993, D **67**, 126.
9. M. G. Rosenblum, A. S. Pikovsky, and J. Kurths. Phys. Rev. Lett. 1996, **76**, p. 1804.
10. N. J. Corron and D. W. Hahs. IEEE Trans. Circuits Syst. 1997, I **44**, p. 373.
11. U. Feldmann, M. Hasler, and W. Schwarz. Int. J. of Circuit Theory and Applications. 1996, **24**, p. 551.
12. V. Dronov. Kharkov State Univ., M. S. Thes. 1997 (unpublished).
13. N. F. Rulkov and L. S. Tsimring. IEEE Trans. Circuits Syst. 1997, I, (to be published).
14. V. S. Anishchenko, A. N. Pavlov, and N. B. Pavlov. Sov. Phys. Tech. Phys. 1997 (to be published).

Хаотическая маскировка без синхронизации

Д. М. Ваврив, В. Б. Рябов, П. В. Усик

Анализируется метод скрытной передачи информации, основанный на инвертировании хаотической динамической системы. Предлагаемый авторами подход не требует использования хаотической синхронизации двух или более осцилляторов. Обсуждается влияние шумов в канале связи и несовпадения параметров на качество декодирования сигнала. Как примеры используются автономный осциллятор Росслера и неавтономное уравнение маятника.

Хаотичне маскування без синхронізації

Д. М. Ваврів, В. Б. Рябов, П. В. Усік

Аналізується метод прихованого передавання інформації, що базується на інвертуванні хаотичної динамічної системи. Запропонований авторами підхід не потребує використання хаотичної синхронізації двох або більше осциляторів. Обговорюється вплив шумів у каналі зв'язку та розходження параметрів на якість декодування сигналу. Автономний осцилятор Рьосслера та неавтономне рівняння маятника використані як приклади.