KYBERNETIKA — VOLUME 33 (1997), NUMBER 1, PAGES 41 – 50

SECURE COMMUNICATIONS BASED ON DISCRETE TIME CHAOTIC SYSTEMS

F. Argenti, A. De Angeli, E. Del Re, R. Genesio, P. Pagni and A. Tesi

In this work the problem of designing a secure communication system is addressed. Discrete time chaotic signals are used to mask information samples. *Dead-beat synchronizing* systems permit exact synchronization in finite time. This property can be used in secure communication schemes. An alternative approach uses a combination of chaotic signals to modulate the information to be masked. The sensitivity of the schemes to the key variation is analyzed and some communication issues are also discussed.

1. INTRODUCTION

Synchronizing chaotic systems [10] have been applied as cypher generator in the context of secure communications [3, 4, 6, 8, 14]. In *chaotic masking* a low power information signal is added to a chaotic signal without preventing locking of the authorized receiver to occur. If the information is binary, then *chaotic switching* permits to encode data by means of two different attractors. In *chaotic modulation* the information is modulated on a chaotic carrier through an invertible nonlinear transformation. For more details, see [9] and references therein.

Up to now, apart from a few examples [1, 5, 12, 13], most of research has dealt with *analog systems*. As a drawback, such systems present a *weak robustness* with respect to circuit component variability as well as to channel noise: these disturbances can affect the synchronization process. In this work discrete time secure communication schemes are described. A discrete-time nonlinear map is used as a chaotic generator. The output signal is used to *modulate* the information signal. Two schemes are presented: in the first the self-synchronizing property of such systems [2] is exploited, while in the second the map is used as a pseudo-random generator. The sensitivity of the secure recovery of the information signal with respect to the variation of the keys is also analyzed.

2. DISCRETE TIME CHAOS SYNCHRONIZATION

This section describes the synchronizing discrete-time systems that will be proposed for secure communication applications; for further details see [2, 11].

We will consider the Hénon map, a second order well-known map, represented by the following equations

$$\begin{aligned} x_1(k+1) &= 1 - \alpha x_1^2(k) + x_2(k) \\ x_2(k+1) &= \beta x_1(k). \end{aligned} \tag{1}$$

This map presents a chaotic behaviour in a large neighborhood of the parameter values $\alpha = 1.4$ and $\beta = 0.3$. Let $y(k)$ be the output of the chaotic system:

$$y(k) = 1 - \alpha x_1^2(k). \tag{2}$$

The receiver can reconstruct the state of the chaotic system using the equations

$$\begin{aligned} \hat{x}_1(k+1) &= y(k) + \hat{x}_2(k) \\ \hat{x}_2(k+1) &= \beta \hat{x}_1(k). \end{aligned} \tag{3}$$

From (1) – (3), it can be seen that the synchronization error, $\Delta x_i(k) = \hat{x}_i(k) - x_i(k)$, tends asymptotically to zero for $|\beta| < 1$. Moreover, if the output of the chaotic system is chosen as

$$y(k) = x_1(k) \tag{4}$$

then the synchronization error at the receiver side will satisfy

$$\begin{aligned} \Delta x_1(k+1) &= \Delta x_2(k) \\ \Delta x_2(k+1) &= 0. \end{aligned} \tag{5}$$

Therefore, the sinchronization errors will reach exactly zero in two steps independently of their initial values, that is the system is *dead-beat synchronizing*. More detailed considerations are developed in [2].

3. SECURE COMMUNICATION SCHEMES

One of the main appealing features of a dead-beat synchronizing system is that the same chaotic signal can be generated, in a deterministic way, by both the transmitter and the receiver. This chaotic signal can be used for masking an information signal in a secure communication system.

Let $y(k)$ be a chaotic signal produced at the transmitter side and let $s(k)$ be the information signal to be sent: $y(k)$ is used to mask $s(k)$ so that an unauthorized receiver can not detect $s(k)$. A way to achieve this purpose is to choose a coding function $c(s, y)$, continuous and invertible, so that $c(s, y)$ is transmitted instead of s. At the receiver side, the masking signal $y(k)$ must be exactly known only by the authorized user: this is possible if he or she knows the keys α and β as well as either the initial state of the Hénon map or two initial samples of y. We will assume in the following that the keys of the secure communication are α and β.

In this work, two different approaches will be described. In both schemes the information is supposed organized in packets of fixed length, say M, i. e., $[s(lM), s(lM + 1), \ldots, s(lM + M - 1)]$ will be the lth packet.

Scheme A

A.1: Generate a chaotic sequence having N samples, $N \gg M$;

A.2: Split the sequence in blocks of $M+2$ samples;

A.3: Transmit the lth block of the signal, M samples long, masking it with the lth block of the chaotic signal, $M+2$ samples long, i.e., send the following data: $[y(l(M+2)), y(l(M+2)+1), c(s(lM), y(l(M+2)+2)), \ldots, c(s(lM+M-1), y(l(M+2)+M+1))]$.

At the receiver side the first two samples of each block are used to synchronize the map, so that the masking signal y is achieved; then, the samples $[y(l(M+2)+2), \ldots, y(l(M+2)+M+1)]$ are used to decode the information signal s through the inverse function $c^{-1}(c(s,y),y)$.

Scheme A presents a high sensitivity [2] with respect to the choice of the keys of the system: a little difference in the choice of the parameters α and β makes the coded message indecipherable, even if the correct information for synchronization, i.e. the first two samples of each block, is achieved. Some drawbacks of this scheme are now discussed. First, the information for the synchronization of the map must pass through the channel, which in most cases must be modeled as noisy, i.e., it introduces errors in the synchronizing samples: therefore, these samples must be carefully protected with suitable channel codes. Second, the synchronizing samples carry no information, that is the bandwidth needed to transmit the masked signal is greater than that necessary to transmit s. To avoid these problems another scheme is proposed.

Scheme B

B.1: Use a Hénon map with parameters α_0 and β_0 and a given initial state to generate a chaotic sequence $y_0(k)$ having $2L$ samples, where L is the number of signal packets to be transmitted;

B.2: Use the samples $y_0(2l-1, 2l)$, $l = 1, \ldots, L$ to initialize a second Hénon map having parameters α and β. Each time a sequence $y_l(k)$, M samples long, is generated;

B.3: Transmit the lth block of the signal, masking it with the sequence $y_l(k)$, i.e. transmit the following data: $[c(s(lM), y_l(1)), \ldots, c(s(lM+M-1), y_l(M))]$.

In this case, the values α_0 and β_0 are part of the key to be known at the receiver side. In Scheme B, two Hénon maps are used as a pseudo-random generator to modulate the information signal.

An advantage of the schemes here considered is that they are memoryless, that is the effect of an error occurring on a transmitted sample, for example due to the channel noise, does not propagate to neighbouring samples.

An example of secure communication is now described. Consider to use Scheme B. Let the transmitter be described by a Hénon map, say $\mathcal{H}$, with parametric configuration $\alpha = 1.4$ and $\beta = 0.3$. A second Hénon map $\mathcal{H}_0$, with parameters α_0 and

β_0, is used to initialize the state of $\mathcal{H}$. We have assumed $\alpha_0 = 1.4$ and $\beta_0 = 0.3$ again. The coding function $c(s,y) = y/s$ has been chosen. The information has been divided in packets each containing 128 samples. The square wave shown in Figure 1 has been used as information signal; the masked signal, that is the signal actually transmitted, is shown in Figure 2. The authorized receiver reconstructs the signal perfectly. In Figure 3 the signal decoded by an unauthorized receiver is shown: only the parameter β has been changed, with a mismatch with respect to the correct one of 0.0001. Little changes in the other keys lead to similar results. As can be seen, a little difference in the parameters yields a noise-like signal. In the next section the choice of the modulating function and its influence on the overall scheme will be discussed in the details.

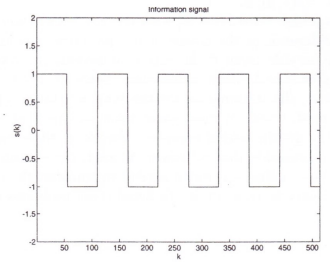

Fig. 1. Square wave information signal.

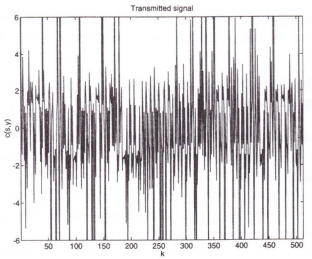

Fig. 2. Transmitted signal.

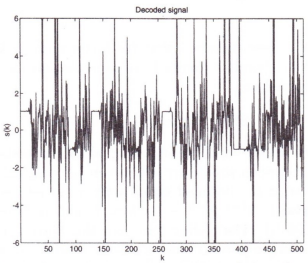

Fig. 3. Decoded signal with $\Delta\beta = 0.0001$ and the other keys unchanged.

4. COMMUNICATION ISSUES

Some communication issues deserve a more detailed discussion and are analyzed in this section. The tests presented here have been performed using Scheme B.

4.1. Choice of the modulating function

In a digital transmission system the information signal is binary encoded. Suppose the input signal is PCM coded with b bit/sample. Depending on the choice of the modulating function $c(s, y)$, the masked signal to be sent through the communication channel may assume real values and, therefore, needs a further quantization. The quantization process introduces an irreversible mapping, so that also the signal reconstructed by the authorized receiver will be affected by an error. The examples of $c(s, y)$ proposed in [2] belongs to this class of masking functions.

We present here some results obtained using also invertible functions $c(s, y)$ operating on discrete values. For example, suppose $c(s, y) = \mathrm{XOR}(s, y)$, where XOR is computed on the binary representations of the operands. This choice implies that the masking signal y is represented with the same number of bits as s: this is accomplished by quantizing y with 2^b levels, between its minimum and maximum values. The authorized receiver, which is able to perfectly reconstruct the masking sequence, performs the same quantization process. In this case the inverse function is $c^{-1}(x, y) = \mathrm{XOR}(x, y)$.

Another example of invertible function is $c(s, y) = \mathrm{XOR}(\mathrm{RR}(s), y)$, where $\mathrm{RR}(a)$ performs the *Right–Rotation* of a, i.e., shifts the bits of a one bit right, with the LSB becoming the MSB (the RR( ) function has been used also in [5]); $c^{-1}(x, y) = \mathrm{LR}(\mathrm{XOR}(x, y))$ performs the inverse operation, where LR( ) is the one bit *Left–Rotation* operator.

To evaluate the effectiveness of the proposed coding functions some tests have been performed using a speech signal sampled at $f_c = 11025$ kHz, 8 bit/sample. The results obtained by masking the signal with different coding functions and transmitting it with 8 bit/sample are reported in Table 1. The SNR_a and SNR_u are the Signal–to–Noise Ratio (SNR) experienced by the authorized and an unauthorized

receiver, respectively. We have supposed that the latter receiver knew all the keys except β, with $\Delta\beta = 0.001$ (similar results have been obtained changing the other keys). The SNR is computed as:

$$\mathrm{SNR} = 10 \log_{10} \frac{\sigma_s^2}{\mathrm{MSE}} \tag{6}$$

where σ_s is the standard deviation of the input signal (in our tests $\sigma_s = 43.10$) and $\mathrm{MSE} = E[(s - s_d)^2]$ is the mean square error between the original and the decoded signal. For a comparison, if the decoded signal were a discrete variable uniformly distributed in the interval $(-2^{b-1}, 2^{b-1} - 1)$, $b = 8$, uncorrelated with the input signal then $\mathrm{SNR} = -5.96$ dB. The coding functions that have been chosen are the multiplication, the division (to prevent from too large output values the amplitudes far from zero less than a given threshold are multiplied instead of divided), the XOR and the XOR–RR. In Table 1 the degradation of the quality measured by SNR_a is due to the quantization of the masked signal.

Table 1. Results with PCM speech signal, 8 bit/sample.

$c(s, x)$	SNR_a (dB)	SNR_u (dB)
$*$	20.94	-3.40
$/$	15.45	-3.37
XOR	∞	-5.59
XOR–RR	∞	-5.80

In Figure 4 the normalized cross-covariance γ_t between the input signal and the masked signal transmitted through the channel is shown, while Figure 5 shows the normalized cross-covariance γ_r between the input signal and the signal decoded by the unauthorized receiver. As can be seen, even if the latter cross-covariance is low for every modulation function used, this does not hold for γ_t. This corresponds also to a certain intelligibility (measured with subjective tests) of the masked signal when the multiplication and division functions are used as $c(s, y)$.

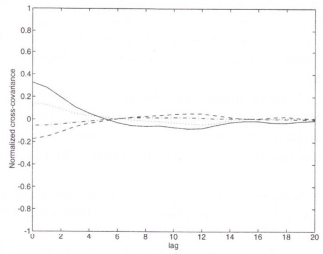

Fig. 4. Normalized cross-covariance between the PCM 8 bit/sample speech input and the masked signal, varying with $c(s, y)$: multiplication (solid), division (dots), XOR (dashes), XOR–RR (dashes and dots).

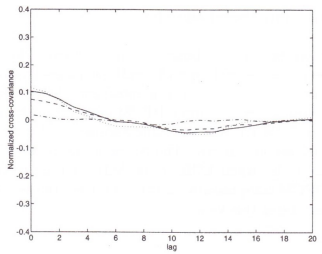

Fig. 5. Normalized cross-covariance between the PCM 8 bit/sample speech input and the signal decoded by an unauthorized receiver ($\Delta\beta = 0.001$), varying with $c(s, y)$: multiplication (solid), division (dots), XOR (dashes), XOR–RR (dashes and dots).

The sensitivity to the key variation is shown in Figure 6, where the SNR experienced by an unauthorized receiver versus the variations of the parameters α and β from the correct keys is shown (the keys α_0 and β_0 are supposed known). The modulating function is the XOR–RR. The SNRs obtained suggest a complete unintelligibility even when the keys variation is kept small: this has been confirmed by some subjective tests. Similar results are found when α and β are assumed known and α_0 and β_0 are changed.

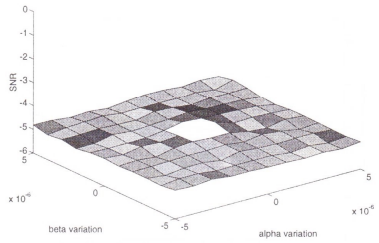

Fig. 6. SNR experienced by an unauthorized receiver versus $\Delta\alpha$ and $\Delta\beta$ (PCM, 8 bit/sample, XOR–RR have been used).

4.2. Application to compressed signals

The PCM is the simplest example of binary coding system. However, more efficient methods of representing a signal (speech, audio or images) have been designed and standardized [7]. To test the secure communication scheme when applied to a compressed signal, the simple zero-th order DPCM scheme has been used. Table 2 refers to a 4 bit/sample DPCM scheme: the same parameters defined in the previous subsection for the PCM case are shown. The degradation of the SNR experienced by the authorized receiver also when XOR or the XOR–RR are used as modulating function is due to the DPCM compression: as it can be seen, the use of multiplication or division further deteriorates this value.

Table 2. Results with zero-th order DPCM compressed signal, 4 bit/sample.

$c(s, x)$	SNR_a (dB)	SNR_u (dB)
$*$	9.38	-4.94
/	7.59	-5.33
XOR	13.84	-4.90
XOR–RR	13.84	-5.12

Figure 7 and Figure 8 show the normalized cross-covariance between the input signal and either the masked signal or the signal decoded by the non-authorized receiver, respectively. As in the PCM case, subjective tests of intelligibility are in favour of the XOR and the XOR–RR functions. The sensitivity to the key variation is shown in Figure 9. The results are similar to those obtained for the PCM case.

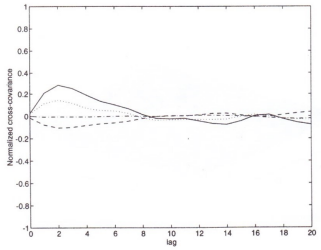

Fig. 7. Normalized cross-covariance between the speech input and the uncompressed (zero-th order DPCM, 4 bit/sample) masked signal varying with $c(s, y)$: multiplication (solid), division (dots), XOR (dashes), XOR-RR (dashes and dots).

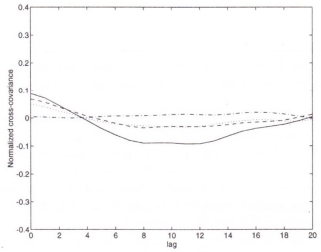

Fig. 8. Normalized cross-covariance between the speech input (transmitted with zero-th order DPCM, 4 bit/sample) and the signal decoded by an unauthorized receiver ($\Delta\beta = 0.001$), varying with $c(s, y)$: multiplication (solid), division (dots), XOR (dashes), XOR–RR (dashes and dots).

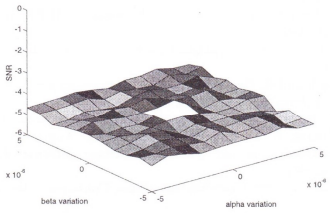

Fig. 9. SNR experienced by an unauthorized receiver versus $\Delta\alpha$ and $\Delta\beta$ (DPCM, 4 bit/sample, XOR-RR have been used).

5. CONCLUSIONS

In this work some schemes for secure communications using the Hénon map are discussed. In the two approaches presented, the first exploits the *self-synchronizing* property of this map, while the second avoids the transmission of synchronizing samples. Some communication issues regarding the quantization of the masked signal as well as the application of the scheme to a DPCM compressed signal have been discussed.

(Received February 14, 1996.)

REFERENCES

[1] H. D. J. Abarbanel and P. S. Lindsay: Secure communications and unstable periodic orbits of strange attractors. IEEE Trans. Circuits and Systems (Part II) *40* (1993), 643–645.

[2] A. De Angeli, R. Genesio and A. Tesi: Dead–beat chaos synchronization in discrete–time systems. IEEE Trans. Circuits and Systems (1995).

[3] K. M. Cuomo and A. V. Oppenheim: Circuit implementation of synchronized chaos with applications to communications. Phys. Rev. Lett. *71* (1993), 65–68.

[4] H. Dedieu, M. P. Kennedy and M. Hasler: Chaos shift keying: modulation and demodulation of a chaotic carrier using self–synchronizing Chua's circuits. IEEE Trans. Circuits and Systems (Part II) *40* (1993), 634–642.

[5] D. R. Frey: Chaotic digital encoding: an approach to secure communication. IEEE Trans. Circuits and Systems (Part II) *40* (1993), 660–666.

[6] K. S. Halle, C. W. Wu, M. Itoh and L. O. Chua: Spread–spectrum communications through modulation of chaos. Internat. J. Bifurcation and Chaos *3* (1993), 469–477.

[7] N. S. Jayant and P. Noll: Digital coding of waveforms. Prentice Hall, 1984.

[8] Lj. Kocarev, K. S. Halle, K. Eckert, L. O. Chua and U. Parlitz: Experimental demonstration of secure communications via chaotic synchronization. Internat. J. Bifurcation and Chaos *2* (1992), 709–713.

[9] M. J. Ogorzalek: Timing chaos. Part I: Synchronization. IEEE Trans. Circuits and Systems (Part I) *40* (1993), 693–699.

[10] L. M. Pecora and T. L. Carroll: Synchronization in chaotic systems. Phys. Rev. Lett. *64* (1990), 821–824.

[11] A. Tesi, A. De Angeli and R. Genesio: On the system decomposition for synchronizing chaos. Internat. J. Bifurcation and Chaos *4* (1994), 6.

[12] M. d. S. Vieira, P. Khoury, A. J. Lichtenberg, M. A. Lieberman, W. Wonchoba, J. Gullicksen, J. Y. Huang, R. Sherman and M. Steinberg: Numerical and experimental studies of self–synchronization and synchronized chaos. Internat. J. Bifurcation and Chaos *2* (1992), 645–657.

[13] M. d. S. Vieira: Proc. of First Experimental Chaos Conference, World Scientific, Singapore 1992.

[14] C. W. Wu and L. O. Chua: A simple way to synchronize chaotic systems with application to secure communication systems. Internat. J. Bifurcation and Chaos *3* (1993), 1619–1627.

F. Argenti, P. Pagni, E. Del Re, Dipartimento di Ingegneria Elettronica, University of Florence, Via di Santa Marta, 3–50139 Florence. Italy.

A. De Angeli, R. Genesio, A. Tesi, Dipartimento di Sistemi e Informatica, University of Florence, Via di Santa Marta, 3–50139 Florence. Italy.