Security analysis of communication system based on the synchronization of different order chaotic systems

Gonzalo Alvarez [a],[*], Luis Hernández [a], Jaime Muñóz [a],
Fausto Montoya [a] and Shujun Li [b]

[a]*Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas,
Serrano 144, 28006–Madrid, Spain*

[b]*Department of Electronic and Information Engineering, Hong Kong Polytechnic
University, Hung Hom, Kowloon, Hong Kong SAR, China*

Abstract

This letter analyzes the security weakness of a recently proposed communication
method based on chaotic modulation and masking using synchronization of two
chaotic systems with different orders. It is shown that its application to secure
communication is unsafe, because it can be broken in two different ways, by high-
pass filtering and by reduced order system synchronization, without knowing neither
the system parameter values nor the system key.

Key words: Secure communication, Cryptanalysis, Synchronization, Different
order chaotic systems
   PACS: 05.45.Ac, 47.20.Ky.

1   Introduction

In recent years, a considerable effort has been devoted to extend the chaotic
communication applications to the field of secure communications. It has been
noticed that there exists an interesting relationship between chaos and cryp-
tography: many properties of chaotic systems have their corresponding coun-
terparts in traditional cryptosystems, such as:

---

[*] Corresponding author: Email: gonzalo@iec.csic.es

- Ergodicity and Confusion: The output has the same distribution for any input.
- Sensitivity to initial conditions/control parameter and Diffusion with a small change in the plaintext/secret key: A small deviation in the input can cause a large change at the output.
- Mixing property and Diffusion with a small change in one plain-block of the whole plaintext: A small deviation in the local area can cause a large change in the whole space.
- Deterministic dynamics and Deterministic pseudo-randomness: A deterministic process can cause a random-like (pseudo-random) behavior.
- Structure complexity and Algorithm (attack) complexity: A simple process has a very high complexity.

As a result of investigating the above relationships, a rich variety of chaos-based cryptosystems for end-to-end communications have been proposed [1–6], some of them fundamentally flawed by a lack of robustness and security [7–13].

Most analog chaos-based cryptosystems are secure communication schemes designed for noisy channels, based on the technique of chaos synchronization, first shown by Pecora and Carrol [14].

Reduced order synchronization is a new interesting topic which has recently drawn attention from several researchers [15–17]. In [16] it is shown that second order driven oscillators can be synchronized with canonical projection of a higher order chaotic system by means of non-linear feedback.

In a recent paper Bowong proposed a scheme based on reduced order synchronization and feedback with application to secure communications [18]. The transmitter is a four-order chaotic oscillator, modulated by the plaintext and whose output is added to the plaintext as a masking signal. The receiver consists of a Duffing second-order system, that is enslaved to the transmitter by means of non-linear feedback of the error.

Bowong presented two examples based on the plaintext modulation of a chaotic oscillator and subsequent additive masking of the plaintext with the oscillator signal. The following equation system defines the transmitter operation:

$$\begin{aligned}
\dot{x}_{1m} &= x_{2m}, \\
\dot{x}_{2m} &= -cx_{2m} - d^2(x_{1m} - x_{3m} - x_{1m}x_{3m}) + u(t), \\
\dot{x}_{3m} &= x_{4m}, \\
\dot{x}_{4m} &= -ax_{4m} - x_{3m} - b^2x_{3m}^3 - f(x_{1m} + x_{1m}^2/2) + e(t), \\
y_T &= x_{1m} + u(t),
\end{aligned} \tag{1}$$

with parameter values:

$$a = 0.03, b = 1, c = 0.3, d = 0.985, f = 0.1, \tag{2}$$

where the function $e(t)$ was specified as $e(t) = 0.7\cos(t)$ and being the term $u(t)$ the plaintext message. The signal $y_T = x_{1m} + u(t)$ constitutes the transmitted ciphertext to the receiver end. Actually, the above Eq. (1) is written as it should be, in spite of the erroneous formulation given in (14) of [18, §4].

The receiver was constructed as follows:

$$
\begin{aligned}
\dot{x}_{1s} &= x_{2s}, \\
\dot{x}_{2s} &= -\lambda x_{2s} - \omega_0^2 x_{1s} - \gamma x_{1s}^3 + K_1 \cos(\omega_1 t + \theta_1) + K_2 \cos(\omega_2 t + \theta_2) + \upsilon, \\
y_s &= x_{1s},
\end{aligned}
$$

with parameter values:

$$
\lambda = 1, \omega_0 = 10, \gamma = 100, K_1 = K_2 = 1, \omega_1 = 2, \omega_2 = 4, \theta_1 = \theta_2 = 0, \quad (3)
$$

and where υ is the feedback control law which forces the error $e = x_{1s} - x_{1m}$ to converge exponentially to zero as $t \to \infty$.

The retrieved plaintext $\hat{u}(t)$ is calculated as the difference between the ciphertext and the output of the reduced order system $\hat{u}(t) = y_T - y_s = u(t) - e$. It was shown that the transmitter-receiver system was capable of accurately retrieving the plaintext after an initial synchronization period of 10 seconds. Afterwards it was claimed that the system can be used for secure communications and some examples are provided.

In this letter it is shown that the proposed cryptosystem is insecure and two different procedures to break it are also presented: by high-pass filtering and by means of a simple reduced order intruder receiver.

2 Missing security analysis and system key specification

In [18], the author asserted that the scheme is applicable to secure communication. However, no analysis of security was included to support this claim. Furthermore, there is no mention of the secret key, when it is well known that a secure communication system cannot exist without a key. In [18] it is not considered whether there should be a key in the proposed system, what it should consist of, what the available key space would be (how many different keys exist in the system), what precision to use, and how it would be managed. None of these elements should be neglected when describing a secure communication system [19].

Moreover, being the transmitter and the receiver implemented with different kind of systems, it is not explained how the encryption keys, if any, may be related to the corresponding decryption keys. Usually, in many chaotic

cryptosystems the system parameters play the role of key, but it is not the case in [18], because the transmitter and the receiver do not make use of the same parameters.

3   Plaintext retrieval by a filtering attack

It was supposed for some time that chaotic masking was an adequate means for secure transmission, because chaotic systems present some properties as sensitive dependence on parameters and initial conditions, ergodicity, mixing, and dense periodic points. These properties make them similar to pseudo-random noise [20], which has been used traditionally as a masking signal for cryptographic purposes. The basic fundamental requirement of the pseudo-random noise used in cryptography is that its spectrum should be infinitely broad, flat and of much higher power density than the signal to be concealed. In other words, the plaintext power spectrum should be effectively buried into the pseudorandom noise power spectrum.

The secure application proposed in [18] does not satisfy this condition. On the contrary, the spectrum of the signal generated by the chaotic oscillator is of narrow band, decaying very fast with increasing frequency, showing a power density much lower than the plaintext at the plaintext frequencies used. Hence it can not cope with a filtering attack intended to separate the masking signal and the plaintext.

To illustrate this fact we consider the the two examples in [18, §4] corresponding to the following plaintexts:

$$u_1(t) = \cos(7t),$$
$$u_2(t) = (1 + \sin(0.2t))\cos(7t),$$

whose waveforms are illustrated in Fig. 1.

The transmitter proposed in [18] was simulated with a four-order Runge-Kutta integration algorithm in MATLAB 6.5, with a step size of 10^{-3}. Fig. 2 illustrates the logarithmic power spectra, as a function of frequency, of the ciphertexts y_{T1} and y_{T2} when the plaintext signals $u_1(t)$ and $u_2(t)$ are encrypted, respectively, with the same parameter values previously described in (2). The power spectra were calculated using a 8192-point Discrete Fourier Transform with a sampling frequency of 32 Hz; previously, the analyzed signal segments were multiplied by a 4-term Blackman-Harris window [21], to avoid aliasing artifacts.

It can be seen in both examples that the plaintext signal components clearly emerge at 1.114 Hz over the background noise created by the chaotic oscillator,
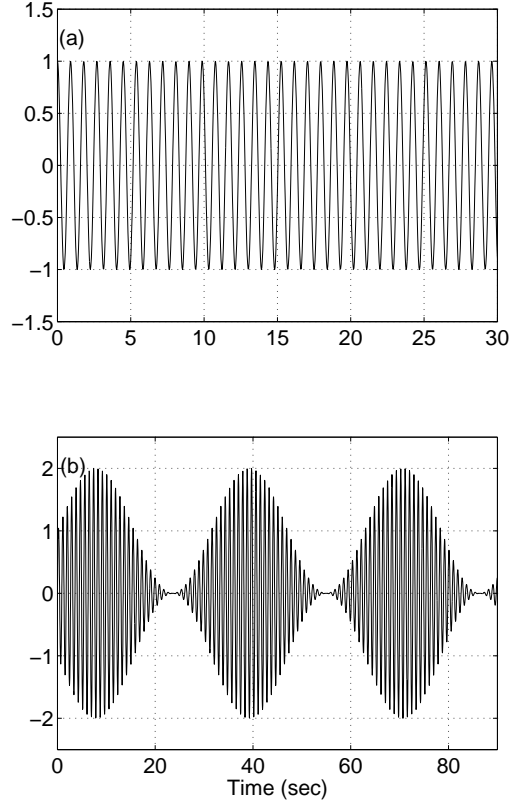
Fig. 1. Plaintext examples described in [18]: (a) $u_1(t) = \cos(7t)$; (b) $u_2(t) = (1 + \sin(0.2t)) \cos(7t)$.

with a power of -3 db, relative to the maximum power of the ciphertext spectrum, while the power density of the ciphertext, at neighboring frequencies, falls below -80 db.

The chaotic receiver of [18] was not used to recover the plaintext. Instead, the ciphertext was high-pass filtered to eliminate the chaotic masking component while retaining the plaintext information. The result is illustrated in Fig. 3. Comparing the result with the plaintext displayed in Fig. 1, it can be appreciated the good estimation of the plaintexts after an initial delay of approximately 29 seconds, due to the filter delay. The filter employed was a 2048 samples finite impulse response digital one, with a cut-off frequency of 1 Hz.

Note that this is the hardest case an attacker can face from the point of view of plaintext frequency, because for higher sound frequencies the spectrum of the background noise created by the chaotic oscillator is even lower.

This plaintext recovering method works equally well for different parameters values of the transmitter, because the maximum power components of its spectrum are concentrated in the frequency range between 0 and 0.3 Hz for all parameter values.
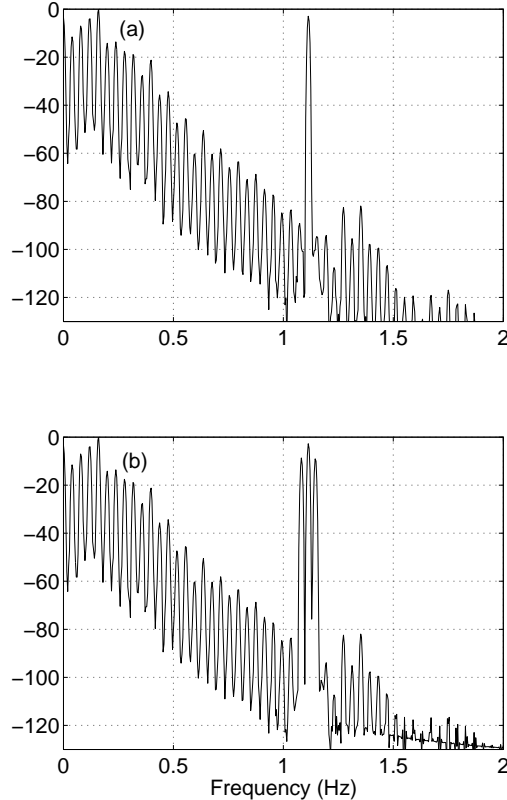
5

Fig. 2. Logarithmic power spectra of the ciphertexts y_{T1} and y_{T2}: (a) corresponding to the plaintext $u_1(t) = \cos(7t)$; (b) corresponding to the plaintext $u_2(t) = (1 + \sin(0.2t))\cos(7t)$.

Thanks to the big separation between the plaintext frequency and the high amplitude components of the masking chaotic signal, our method works equally well with plaintext signals of much lower amplitudes than the plaintexts $u_1(t)$ and $u_2(t)$ of the examples described in [18]. For instance, we present in Fig. 4 the retrieved text corresponding to the plaintext $u_3(t) = 0.0032(1 + \sin(0.2t))\cos(7t)$, that has a power level of -50db with respect to $u_2(t)$; but, as can be seen, the retrieved signal waveform is still perfectly preserved.

4 Plaintext retrieval by reduced order system synchronization

As mentioned in Sec. 1, many secure communication systems based on chaotic modulation and masking have been proposed in the past. In any of them the knowledge of the transmitter parameter values was mandatory to operate the receiver, since they played the role of system key. Some of them were compromised because it was possible to recover the system parameters carrying out an elaborate ciphertext signal analysis.
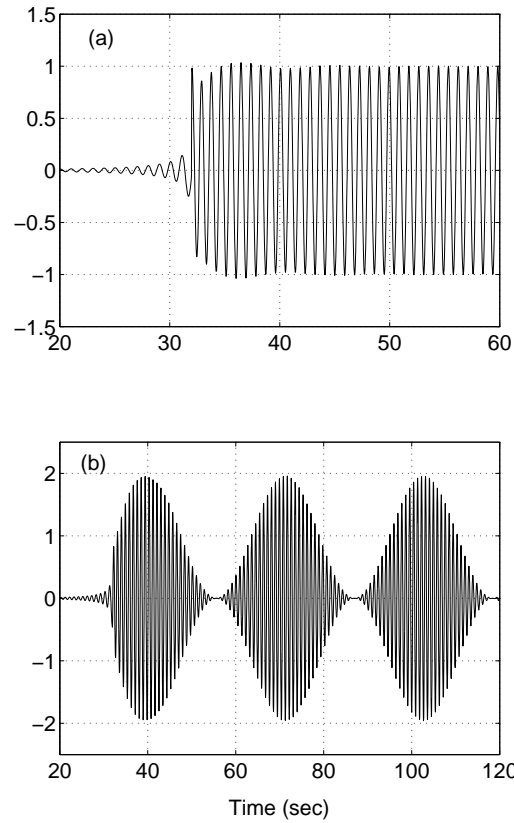
6

Fig. 3. Retrieved texts $\hat{u}_1(t)$ and $\hat{u}_2(t)$, by high pass filtering of the two plaintext examples: (a) $u_1(t) = \cos(7t)$; (b) $u_2(t) = (1 + \sin(0.2\ t))\ \cos(7\ t)$.
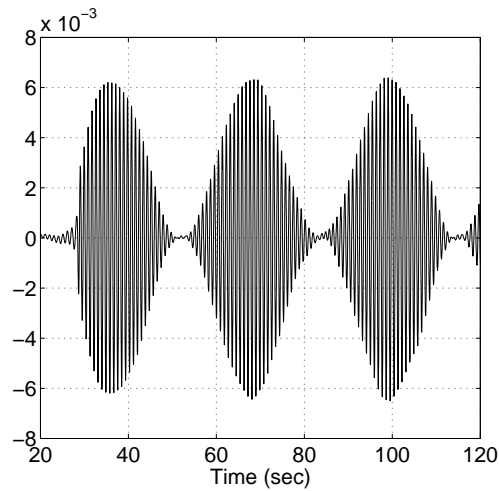

Fig. 4. Retrieved text $\hat{u}_3(t)$ by high-pass filtering of the ciphertext $y_T = x_{1m} + u_3(t)$, corresponding to the low power level plaintext $u_3(t) = 0.0032(1 + \sin(0.2t))\cos(7t)$.

But the chaotic transmitter and the modulation and masking procedure described in [18] was designed in such a way as to enable the plaintext retrieval with a reduced order receiver that did not even required the knowledge of any transmitter parameters. As a true encryption mechanism must necessar-

7

ily make use of a key, this communication system may be only envisaged as an ordinary codification system, rather than a secure one, because the only required knowledge to recover the plaintext message is the receiver structure.

Moreover, it is possible to implement a whole family of alternative receivers to the one proposed in [18]. Hence, a determined eavesdropper, still ignoring the precise structure of the transmitter nor its design parameters, may implement an alternative intruder receiver of its own design, also based on reduced order synchronization and feedback, capable of retrieving the ciphertext just as well as the authorized one.

To demonstrate this threat we have developed an extremely simple intruder receiver of order two, with linear feedback, constructed as follows:

$$\dot{x}_{1s} = x_{2s},$$
$$\dot{x}_{2s} = 100 \; \hat{u}(t) - x_{2s},$$

being $\hat{u}(t) = y_T - x_{1s}$ the retrieved plaintext. The initial conditions were arbitrarily chosen as

$$x_{1m}(0) = x_{2m}(0) = x_{3m}(0) = x_{4m}(0) = 0, x_{1s}(0) = 0.1, x_{2s}(0) = 1.$$

This simple receiver may decrypt the ciphertext as well as the receiver proposed in [18]. Fig. 5 illustrates the perfect synchronism between the transmitter variable x_{1m} and our intruder receiver variable x_{1s}, attained after a transient of 4 seconds, when no plaintext signal is present. The efficiency as intruder decoder is illustrated in Fig. 6, where the retrieved $\hat{u}_1(t)$ and $\hat{u}_2(t)$ texts corresponding to the plaintexts $u_1(t) = \cos(7t)$ and $u_2(t) = (1+\sin(0.2\;t))\;\cos(7\;t)$ are shown, comparing with the plaintexts illustrated in Fig. 1 it can be appreciated the perfect decoding after a short initial transient.

5 Conclusion

In summary, the chaotic masking cryptosystem proposed in [18] is rather weak, since it can be broken in two different ways, without knowing the system parameters nor it detailed structure: by high pass filtering and by an intruder receiver based on reduced order synchronization and feedback. There is no mention about what the key is, nor what the key space is, a fundamental aspect in every secure communication system. The total lack of security discourages the application of this synchronization scheme to secure applications.
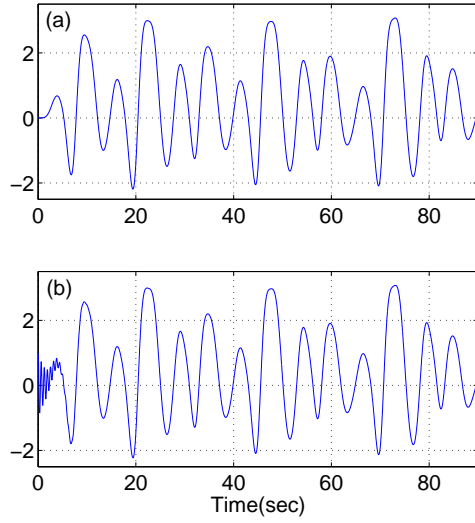
Fig. 5. Synchronism between transmitter and intruder receiver, when no plaintext signal is present: (a) transmitter variable x_{1m} v. time; (b) receiver variable x_{1s} v. time.
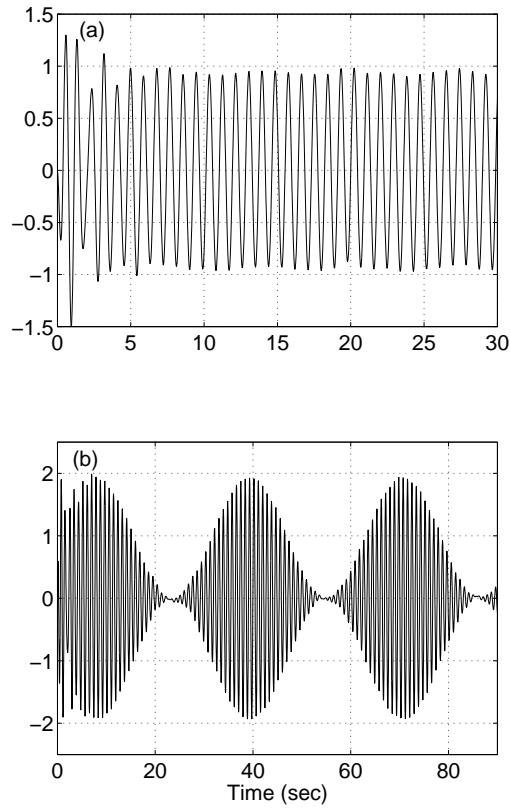

Fig. 6. Retrieved texts $\hat{u}_1(t)$ and $\hat{u}_2(t)$, by our intruder receiver for the two plaintext examples: (a) $u_1(t) = \cos(7t)$; (b) $u_2(t) = (1 + \sin(0.2\,t))\,\cos(7\,t)$.

9

Acknowledgements

References

[1] K. M. Cuomo, A. V. Oppenheim, Chaotic signals and systems for communications, in: Proc. IEEE ICASSP III, 1993, pp. 137–140.

[2] K. M. Cuomo, A. V. Oppenheim, Circuit implementation of synchronized chaos with applications to communications, Phys. Rev. Lett. 71 (1) (1993) 65–68.

[3] C. W. Wu, L. O. Chua, A simple way to synchronize chaotic systems with applications to secure communication systems, Int. J. Bifurcat. Chaos 3 (6) (1993) 1619–1627.

[4] R. Lozi, L. O. Chua, Secure communications via chaotic synchronization. II. Noise reduction by cascading two identical receivers, Int. J. Bifurcat. Chaos 3 (5) (1993) 1319–1325.

[5] S. Li, X. Mou, Y. Cai, Improving security of a chaotic encryption approach, Phys. Lett. A 290 (3-4) (2001) 127–133.

[6] T. Yang, A survey of chaotic secure communication systems, Int. J. Comput. Cognit. 2 (2004) 81–130.

[7] K. M. Short, Steps toward unmasking secure communications, Int. J. Bifurcat. Chaos 4 (4) (1994) 959–977.

[8] C.-S. Zhou, T. l. Chen, Extracting information masked by chaos and contaminated with noise: Some considerations on the security of communication approaches using chaos, Phys. Lett. A 234 (1997) 429–435.

[9] G. Álvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis of a chaotic secure communication system, Phys. Lett. A 306 (4) (2003) 200–205.

[10] G. Álvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis of a discrete chaotic cryptosystem using external key, Phys. Lett. A 319 (2003) 334–339.

[11] S. Li, X. Mou, Y. Cai, Z. Ji, J. Zhang, On the securrity of a chaotic encryption scheme: problems with computerized chaos in finite computing precision, Comput. Phys. Commun. 153 (2003) 52–58.

[12] S. Li, X. Mou, B. L. Yang, Z. Ji, J. Zhang, Problems with a probabilistic encryption scheme based on chaotic systems, Int. J. Bifurcat. Chaos 13 (10) (2003) 3063–3077.

[13] G. Álvarez, F. Montoya, M. Romera, G. Pastor, Breaking parameter modulated chaotic secure communication system, Chaos Soliton. Fract. 21 (4) (2004) 783–787.

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

[15] X. Gong, C. H. Lai, On the synchronization of different chaotic oscillators, Chaos Soliton. Fract. 11 (2000) 1231–1235.

[16] R. Femat, G. Solis-Perales, Synchronization of chaotic systems with different order, Phys. Rev. A 65 (2002) 036226–1–036226–7.

[17] X. Wang, S. S. Ge, Synchronization of two uncertain chaotic systems via adaptive backstepping, Int. J. Bifurcation and Chaos 11 (6) (2001) 1743–1751.

[18] S. Bowong, Stability analysis for the sinchronization of chaotic systems with different order: application to secure communication, Phys. Lett. A 326 (1-2) (2004) 102–113.

[19] G. Alvarez, S. Li, Cryptographic requirements for chaotic secure communications, arXiv:nlin.CD/0311039, 2003.

[20] R. L. Devaney, A first course in chaotic dynamical systems, Addison-Wesley, Reading, MA., 1992.

[21] F. J. Harris, On the use of windows for harmonic analysis with the discrete Fourier transform, IEEE Proc. 66 (1) (1978) 51–83.