Optical digital chaos cryptography

Álvaro Arenas-Pingarrón, Ana P. González-Marcos, José M. Rivas-Moscoso and José A. Martín-Pereda
E.T.S. Ingenieros de Telecomunicación, Universidad Politécnica de Madrid,
Ciudad Universitaria, 28040 Madrid, Spain.

ABSTRACT

In this work we present a new way to mask the data in a one-user communication system when direct sequence – code division multiple access (DS-CDMA) techniques are used. The code is generated by a digital chaotic generator, originally proposed by us and previously reported for a chaos cryptographic system. It is demonstrated that if the user's data signal is encoded with a bipolar phase-shift keying (BPSK) technique, usual in DS-CDMA, it can be easily recovered from a time-frequency domain representation. To avoid this situation, a new system is presented in which a previous dispersive stage is applied to the data signal. A time-frequency domain analysis is performed, and the devices required at the transmitter and receiver end, both user-independent, are presented for the optical domain.

Keywords: digital chaos, optical chaos, chaotic DS-CDMA, chaos cryptography, chaotic codes.

1. INTRODUCTION

Many investigations on spread-spectrum (SS) communications for wireless personal and computer networks have addressed code-division multiple access (CDMA) systems using a direct-sequence (DS) approach, where all users transmit on the same band at the same time, and are only distinguished by means of a code signature. These systems feature four merit factors, namely multipath robustness, potentially high system capacity in terms of number of users, soft degradation of performance and easiness of resource allocation. The code signature is determined by the direct sequence applied, there being different techniques whereby a sequence can be obtained. In section 2 the code generator used will be explained. It. basically consists of a digital chaos generator that produces a chaos sequence.

Chaotic signals have been applied to secure communications for some time, and several schemes have been proposed with different types of chaos generators. These communications systems require an identical chaos generator at the emitter and at the receiver with synchronization between both chaotic generators. The most usual configurations are based on the work of Pecora and Carroll (1), who first demonstrated a technique to synchronize two analog chaos generators.

In section 3 the purpose of this paper will be presented. A time-frequency analysis will show that, with only one user transmitting at a given time, the data information can be easily retrieved from a time-frequency distribution even for signals encoded with an unknown chaotic code. Conversely, when more users are transmitted, the system configuration is that of a CDMA system, and communication can only be established if the code applied to a certain user is previously known by both the emitter and the target receiver..

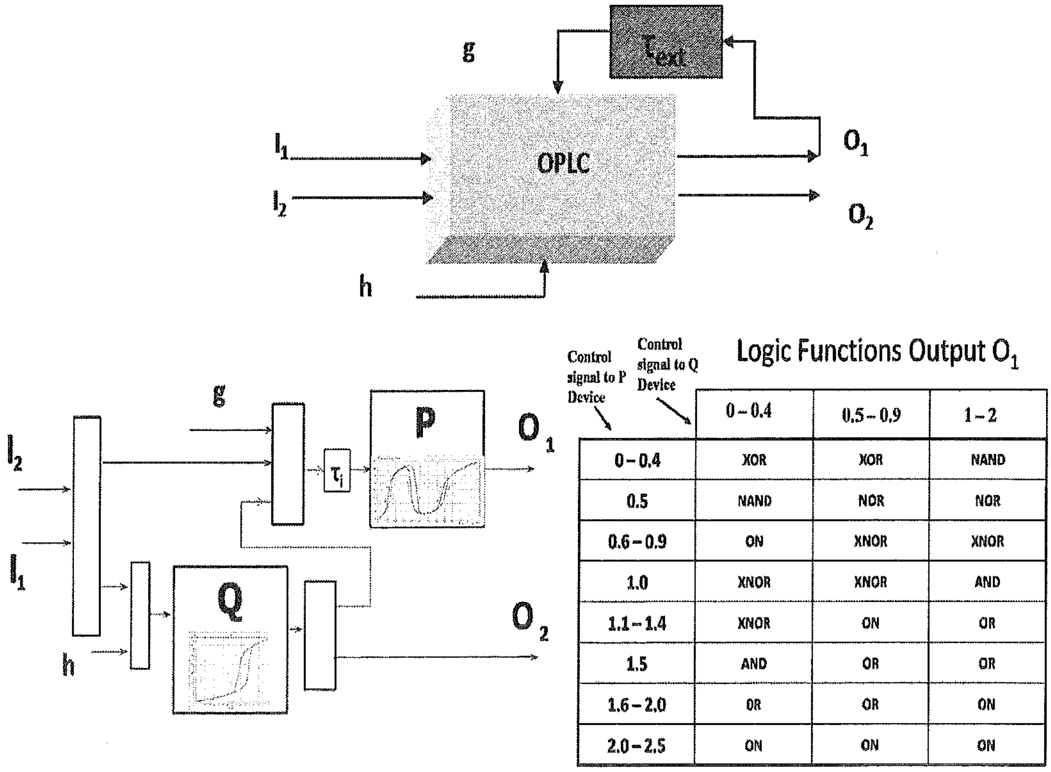
Even though ideas can be transferred between transmission frequency bands, specific approaches have to be considered when optical signals are involved. All our work has been conceived in the optical domain and CDMA has been studied from the point of view of optical networking and computing (2). In section 4 we describe a new way to encode the information signal in two steps. In the first step, we add the phase information to the initial signal with a linear photonic device. This signal is later modulated, in the second step, with a chaotic signal. The chaotic signal is obtained from a photonic generator based on an Optically Programmable Logic Cell (OPLC), previously reported by us for application in optical computing (3). Unlike other optical chaos generators, where the generated chaotic signal is analog and needs to be sampled, this cell can provide a digital signal without any additional operation. The time series generated by the OPLC has been characterized as chaotic through several techniques and has also been applied in areas like finance (4). The involved signals are analyzed by means of time-frequency distributions (5), which show that it is not possible to obtain the data in a first approach.

Optics and Photonics for Counterterrorism and Crime Fighting III,
edited by Colin Lewis, Proc. of SPIE Vol. 6741, 67410L, (2007)
0277-786X/07/$18 · doi: 10.1117/12.737789

2. CODE GENERATOR

Many authors have shown that chaotic spreading sequences can be used as an inexpensive alternative to linear feedback shift register (LFSR) sequences such as maximal-length sequences (m-sequences) or Gold sequences. Unlike m-sequences, the numbers and lengths of chaotic sequences are not restricted. Simulation-based comparisons between Gold sequences and the chaotic sequences generated from chaotic time series obtained from coupled map lattices and the two-dimensional complex valued chaotic Ikeda map have been reported for a synchronous DS/SS system (6). Analytical results for the applicability of chaotic sequences in the chaotic time series based communication systems are available in the literature and their noise-like characteristics have been explained. The performance of chaotic sequences in multiple access communication is well known to be similar to that of pseudo-noise (PN) sequences, but the former sequences outperform the latter in low probability of intercept (LPI) (7).

The system proposed here uses a digital chaos generator already reported by us in (8). The basic idea of the digital chaotic-code generator is shown in Fig. 1. A dynamical system with an external feedback is responsible for generating chaos. However, to obtain a chaotic behavior, the external delay must be chosen in terms of the internal delay (9). The OPLC is a general-purpose logic cell that allows obtaining all the Boolean Logic functions. Because it works in the optical domain it makes it easy to implement an external binary signal and an internal multilevel process. I_1, I_2 are digital data signals and the h input is a CW signal with 3 different values. These three parameters can be used as a secret key. Although the internal design has other parameters that could be used for generating the key, they will not be mentioned here as this is not the objective of the paper. Finally, output signals O_1 and O_2 are digital. The chaotic data is mainly obtained at output O_1 and it can be generated for as long as it is needed.



Control signal to P Device

Control signal to Q Device

Logic Functions Output O_1

	0 – 0.4	0.5 – 0.9	1 – 2
0 – 0.4	XOR	XOR	NAND
0.5	NAND	NOR	NOR
0.6 – 0.9	ON	XNOR	XNOR
1.0	XNOR	XNOR	AND
1.1 – 1.4	XNOR	ON	OR
1.5	AND	OR	OR
1.6 – 2.0	OR	OR	ON
2.0 – 2.5	ON	ON	ON

Fig. 1.- OPLC with feedback for chaos generation at output O1. OPLC internal block diagram and logic table for output O_1.

The internal multilevel process in the OPLC is due to the addition of the input signals. Two devices are dedicated to process the signal. Device Q is based on a bistable device already demonstrated with semiconductor laser amplifiers (SLA), and device P is made of two SLAs biased to work as bistable devices (10). As shown in Fig.1 the input signal to device Q equals the sum of the data signal plus the so-called control signal of device Q: $I_1 + I_2 + h$; in the case of device P a fourth signal (the device-Q output, O_2) is added, with the input signal to device P being given by $I_1 + I_2 + g + O_2$. The feedback signal O_1 is applied to the control input g of device P.

3. CHAOS COMMUNICATION SYSTEM

The possibility of transmitting information between more than one receiver-transmitter pair, in analogy to what happens in standard CDMA systems, where decoding is performed by using correlation techniques instead of synchronization, has been already considered. Communication systems can be asynchronous and synchronous. Asynchronous systems are particularly suitable for links between mobile transmitters and a fixed base in a cellular system. This is one of the reasons to study in this paper the CDMA conditions with a digital chaos code. Nevertheless, a chaos communication system also provides a high level of security, be it a chaos shift keying (CSK) system or a simple system where the data is encrypted with a chaos signal as shown in Fig. 2. All this considered, at least two points must be taken into account: how to synchronize the chaotic generator and how to mask the data signal.

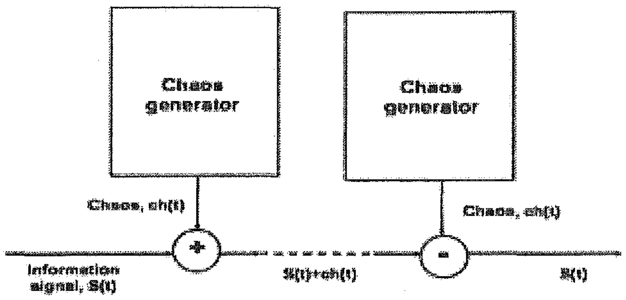


Fig. 2.- Basic configuration of a chaos communication system.

a. Synchronization

For a DS-SS system, the need to synchronize the chaotic signal has been studied since Pecora and Carroll's work. The problem is that there must be identical chaos generators in both emitter and receiver. As Kerckhoffs' principle states, a public knowledge of a system is not a problem from the point of view of security, as only the key must be secret. In Fig. 3 the external secret key is the data signal I, and GI2 can be easily fixed for each transmitter-receiver pair if required; the signal data I can assume different values of frequency and digital data, and GI2 changes the phase by applying a delay.

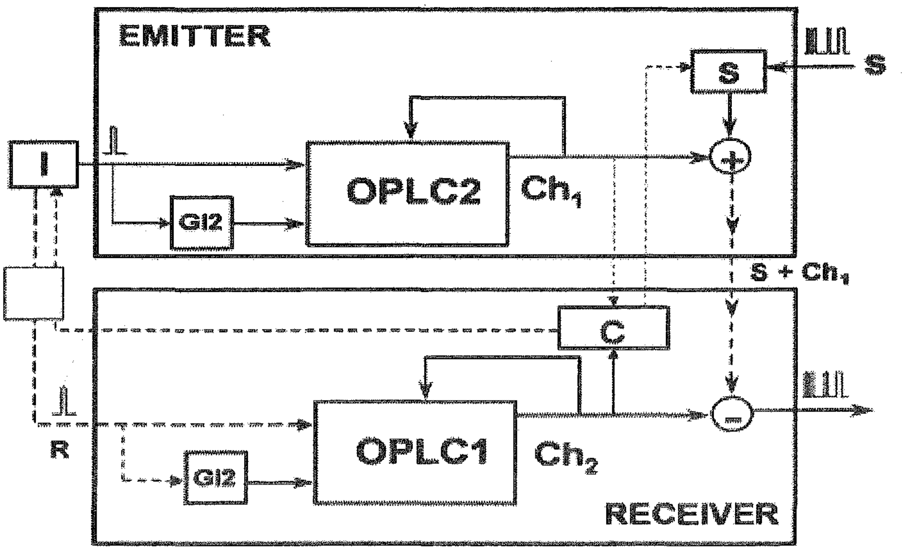


Fig. 3.- Schematic diagram of a proposal for the synchronization of the chaos communication system. More details can be found in (11).

b. Mask.

In a previous work about digital synchronization in optical networks (11), we used an already well-known and patented technique to mask the data: the XNOR function. The use of digital signals simplifies the modulation technique. In the optical domain the XNOR function is realized with the OPLC as can be seen in the logic table of Fig. 1. In this case, logic "0" and "1" are represented by transmission or not of an optical signal, which corresponds to OOK (On–Off keying). However, when masking is performed with a simple XNOR function implemented with a P-device, we have observed that a time-frequency analysis is sufficient to retrieve the data. A more complex analysis with the OPLC in the optical domain still needs to be done.

In this work we present a new method to mask the data from a single user by applying DS-CDMA techniques. In DS-CDMA, bits are subdivided into many short chips following a pattern that represents a user's code. These codes can be unipolar (chips can only assume values '0' and '1'), when amplitude chip modulation is used, or bipolar, through phase modulation, whereby '+1' and '−1' transmission chips are generated. Phase modulation is usually performed by electro-optic modulators, fibre gratings or time delays in combination with phase shifters. Compared to bipolar codes, the cross correlation function of unipolar codes is high and the number of codes in the family is very low. The superiority of bipolar codes justifies our choice of phase modulation in our encoding/decoding system.

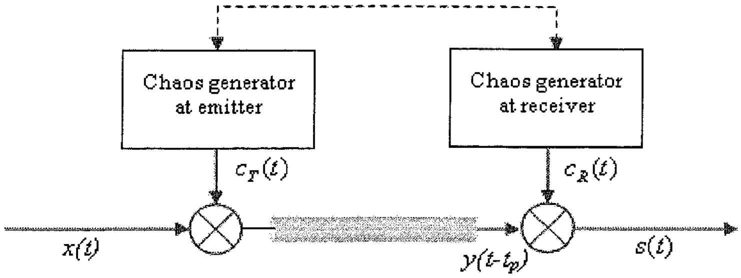


Fig. 4.- Schematic diagram of the encoding/decoding system based on direct binary chaos modulation.

The transmitter comprises a chaos signal generator and a mixer, which multiplies the information and chaos signals. The impulse response of the transmission channel is $h(t)$, which can be approached by a Dirac Delta $\delta(t\text{-}t_p)$ if the dispersion and attenuation "suffered" on the channel are compensated in the receivers. The propagation delay is t_p and the signal to be transmitted on the channel is $y(t)$. The receiver and transmitter are symmetric, being $C_R(t)$ the chaotic signal in the receiver and $s(t)$ the final received data signal, which can be considered an approximation of the input data signal due to the possible lack of synchronization between codes.

Let us assume a channel with compensation of dispersion and attenuation. If we only consider the propagation delay, the system can be represented (see Fig. 4) as follows. At the transmitter,

$$y(t) = x(t) \cdot C_T(t),$$

where $x(t)$ is the information signal and $y(t)$ is the transmitted signal, being $C_T(t)$ the chaotic signal generated at the transmitter.

At the receiver, the recovered signal can be written as

$$s(t) = (y(t) *h(t)) \cdot C_R(t) = y(t\text{-}t_p) \cdot C_R(t) \approx x(t\text{-}t_p) \cdot C_T(t\text{-}t_p) \cdot C_R(t),$$

where $C_R(t)$ is the chaotic code generated at the receiver, and * represents a convolution. If the codes at both ends of the channel coincide and emitter and receiver are perfectly synchronized, we can write, after considering the propagation delay,

$$s(t) = x(t\text{-}t_p) \cdot C_T(t\text{-}t_p) \cdot C_R(t)= x(t\text{-}t_p) \cdot C_T(t\text{-}t_p) \cdot C_T(t\text{-}t_p)= x(t\text{-}t_p)\cdot const.$$

The output signal is then equal, or proportional, to the data input at the transmitter. In this respect, we must assess whether the product of the codes must be a constant, so that the output is proportional to the input, or unity, so that the output equals the input. In either case, the necessary condition is that the codes product must be a constant.

In order to understand what is happening at each point in the system, it is convenient to draw on time-frequency representations. In all the diagrams, the signals are represented in base band, that is, by means of their envelope in the temporal domain and their central frequency scaled to zero in the spectral domain. This is so because it is not necessary to make reference to the carrier frequency modulated by the signals. If the carrier frequency should be taken into account, a translation on the spectral axis would have to be done.

Figure 5 shows the signals at the transmitter: signal *x(t)* is formed by three pulses with a Gaussian envelope, being its time-frequency representation in the upper left diagram; the code signal, *$C_T(t)$*, is a binary chaotic sequence of null mean value, which, as can be seen on its time–frequency representation on the upper right-hand side, is uniformly distributed in the time-frequency space; finally, in the bottom graph, the spectrum of the signal to be transmitted, *y(t)*, is spread with respect to that of the data signal *x(t)* due to the modulation.

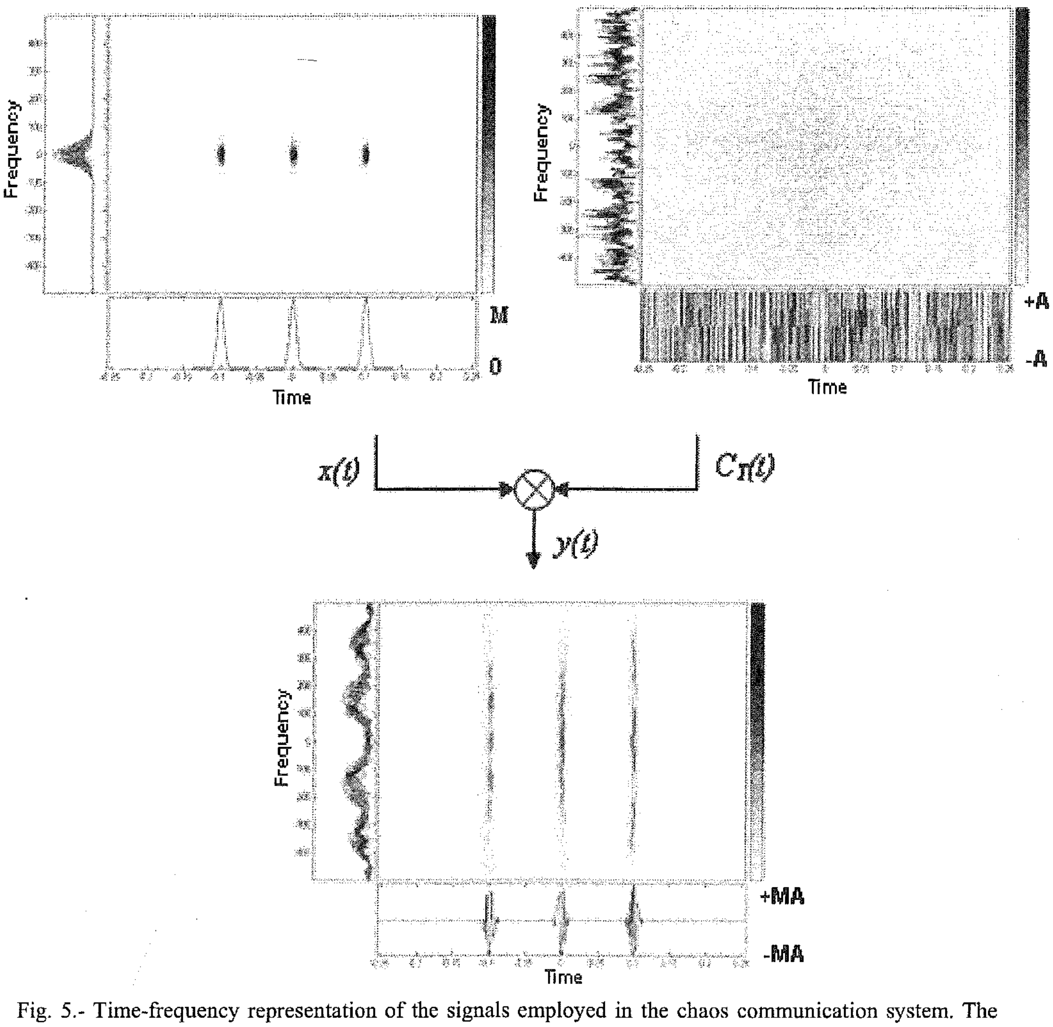


Fig. 5.- Time-frequency representation of the signals employed in the chaos communication system. The modulation format used is BPSK (Binary Phase-Shift keyed). Data signal $x(t)$ (upper left graph), the chaotic signal $C_T(t)$ (upper right), signal to be transmitted $y(t)$ (bottom).

If the impulse response of the channel can be modeled by a simple delay t_p, the chaotic signal in the receiver must be treated in such a way that it incorporates this delay related to the chaotic signal at the transmitter. The product of the codes is then given by

$$C_T(t-t_p)\cdot C_R(t)=const. \;\Leftrightarrow\; C_R(t)=C_T(t-t_p).$$

In Fig. 6 we represent the time-frequency distribution for the chaotic and output signals at the receiver, both when there is synchronization between codes (upper graphs), and when the codes are different or the propagation delay has not been regarded (lower graphs). In the first case, the signal obtained is an approach to the data input signal at the transmitter with a delay due to the channel propagation. In all other cases, the signal obtained is again the input signal modulated by the chaos signal.

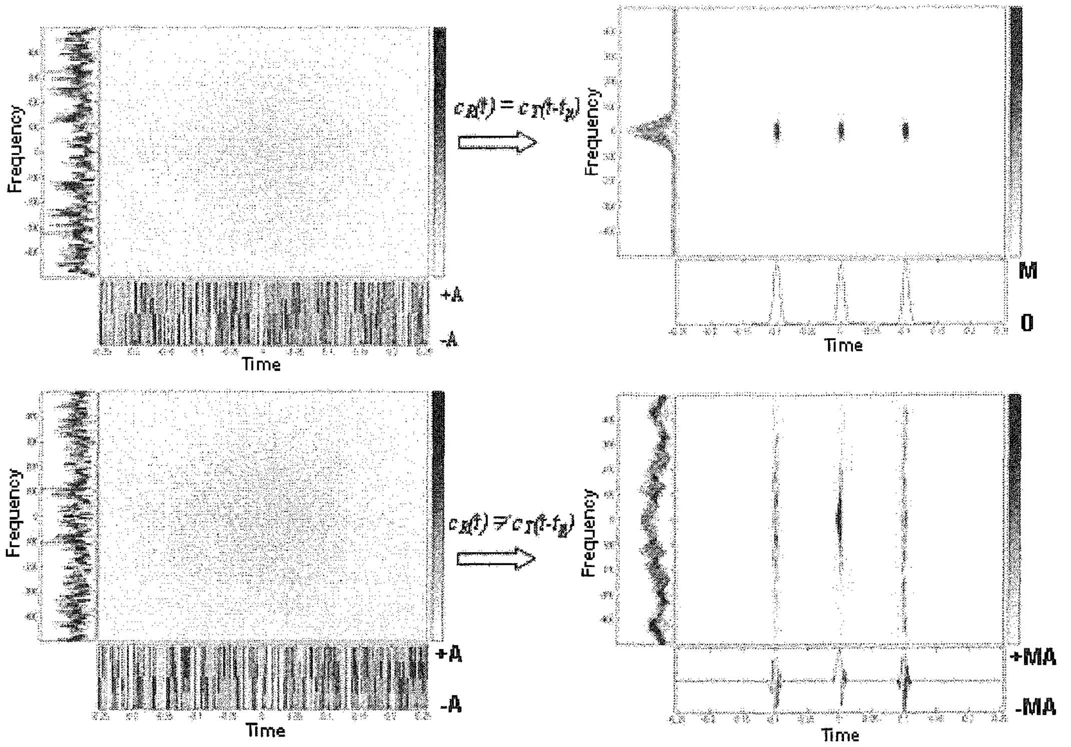


Fig. 6.- Top, received signal when a correct code is used to demodulate: $C_R(t) = C_T(t-t_p)$ (left) and $s(t)\sim x(t-t_p)$ (right). Bottom, incorrectly-decoded received signal: $C_R(t) \neq C_T(t-t_p)$ (left) and $s(t) \neq x(t-t_p)$ (right).

The problem with this type of technique, usually applied in CDMA, is that even when the codes at the transmitter and receiver are delayed with respect to each other or do not match, the data signal can be detected by using an envelope detector. This is due to the fact that the code has a constant amplitude A (except in time-up and time-down) and the only parameter that changes is the phase, which can be 0° or 180°, so the only difference between signal *x(t)* and modulated signal *s(t)* is a constant amplitude value and a phase difference of 0° or 180°. The envelopes of both signals are similar, except during the code pulse's rise-up or fall-down time. This can be seen in the time-frequency representation, on the right-hand side of figure 6, and can be avoided by using a narrow band-pass filter in order to filter the variations between the maximum and minimum values of the code.

The propagation delay depends on the emitter of the information, so that, in a first approach, knowing all the users of a network is sufficient. However, this would make the system less flexible, and therefore it could not be applicable to mobile systems. The solution can be to first synchronize the codes, without the data signal, and then mask the information and send it. This was partially explained in section 3a and has been reported, performed with the OPLC chaos generator, in previous publications (11).

4. NEW DATA MODULATION TECHNIQUE FOR DIGITAL CHAOS COMMUNICATION

The above system configuration is not valid because the mixer only modulates the phase of the signal: the code takes on a positive or negative value but the amplitude does not change. As the information of a signal in the optical domain is in its amplitude value or envelope –amplitude modulation of an optical carrier–, a phase shift (phase modulation) does not mask the information and it can be recovered with an envelope detector that skips the phase.

To avoid this situation, the input signal must be changed in such a way that there should be information in its own phase and therefore the phase modulator be rendered useful. The output signal from the phase modulator would then be constant in amplitude, and the phase would be 0° or 180°. With the same configuration, another solution could be to add amplitude values to the code, but then it would be difficult for the following condition to be fulfilled:

$$C_i(t) \cdot C_i(t) = const. \quad \text{and} \quad C_j(t) \cdot C_i(t) \neq const.$$

All in all, the easiest choice is the first, and as such the new system configuration, in the optical domain, is represented in Fig. 7. It shows the circulator and an element that produces linear dispersion in reflection with an impulse response given by

$$h_D(t) = A \cdot \exp(ja\pi \cdot t^2),$$

where a is the instant frequency slope of the system, and the response modulus is constant (12). The time-frequency distribution of the dispersive element is shown in the upper left diagram of Fig. 8. As can be seen, the distribution is a straight line of slope a. The dispersive element can be done with a fiber Bragg grating, where the part of the signal with a wavelength proportional to the instant period of the refractive index is reflected. As the phase of the impulse response is quadratic (the instant frequency is equal to the time derivative of the temporal phase), the output signal from the fiber Bragg grating $x_D(t)$ contains phase information, unlike input signal $x(t)$. Under these conditions, the phase modulation of signal $x_D(t)$ performed in the mixer with the binary code $C_T(t)$ manages to securely mask the data signal. The dispersive element can have the same impulse response for all transmitters in the network.

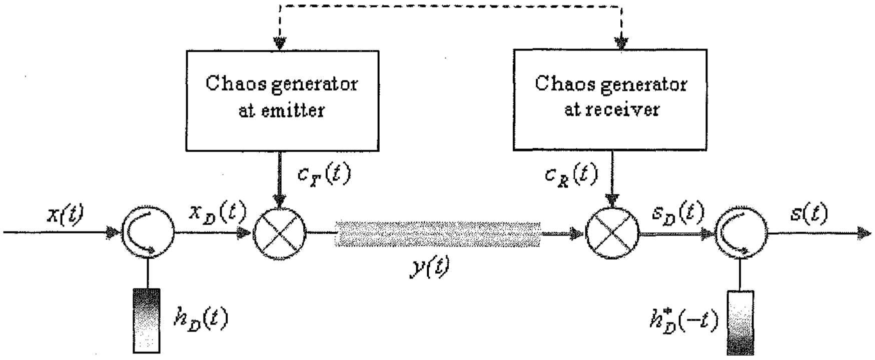


Fig. 7.- Schematic diagram of the encoding/decoding system based on pulse dispersion and direct binary chaos modulation.

a. Optical transmitter

In Fig. 8 the time-frequency distribution of the signals and the impulse response at the transmitter end have been represented. Signal *x(t)* is made up of three pulses with a Gaussian envelope. As in Fig. 5, these pulses do not overlap in the temporal domain, and therefore are orthogonal. The impulse response of the dispersive system $h_D(t)$ is represented in the time-frequency domain by an straight line, whose length is limited by the Bragg grating fiber length, as can be seen in the upper right graph.

The signal reflected in the dispersive device, $x_D(t)$, is plotted in the bottom left graph. It can be observed in the time-frequency plot that the Gaussian pulses are spread with the same slope as the impulse response $h_D(t)$, overlapping in the temporal domain in contrast to signal *x(t)*. In spite of this, their orthogonality is maintained since they do not overlap in the time-frequency space.

The dispersed signal is encoded with the chaotic signal $C_T(t)$, with the same time-frequency distribution as shown in Fig. 5. The product of the chaotic code and the dispersed information signal, *y(t),* is represented in the bottom right graph. It exhibits a spread spectrum and a uniform time-frequency distribution throughout the duration of signal $x_D(t)$.

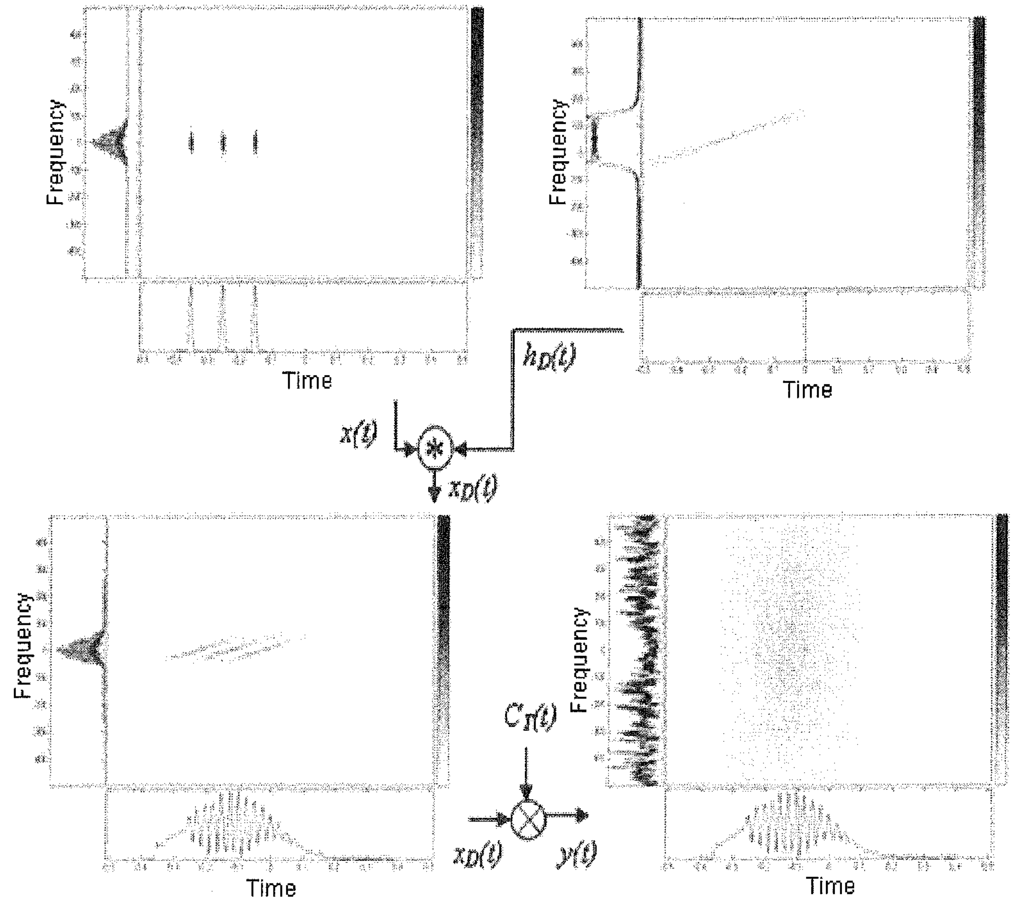


Fig. 8.- Time-frequency representation of the signals involved at the data pulse dispersion and direct binary chaos modulation encoding system: information signal *x(t)* (upper left), impulse response of dispersive medium based on fiber Bragg grating $h_D(t)$ (upper right), dispersed information signal $x_D(t)$ (bottom left) and transmitted signal *y(t)* (bottom right) after modulation with chaotic signal $C_T(t)$ in Fig. 5.

b. Optical receiver

At the receiver, all the signals involved are represented in Fig. 9. In order to compensate the linear dispersion generated at the emitter, another Bragg grating is used in the receiver. The impulse response must now be $h_D^*(-t)$, so that the dispersion slope is the opposite to the one applied at the transmitter, $h_D(t)$, that is,

$$h_D^*(-t) = A \cdot \exp(-ja\pi \cdot t^2).$$

If the dispersions have infinite time duration, we can write

$$h_D(t) * h_D^*(-t) = \delta(t) \cdot const.$$

On the upper side of Fig. 9 we show the time-frequency distribution of $h_D^*(-t)$.

If the code signal applied to $y(t)$ coincides in shape and is correctly syncronized with the channel delay, the bottom left-hand side of Fig. 9 shows that, after dispersion cancellation with $h_D^*(-t)$, the input signal $x(t)$ can be detected.

On the other hand, if $C_R(t) \neq C_T(t-t_p)$, the dispersion compensation in the Bragg reflector produces an output as shown on the bottom right-hand side of Fig. 9, which has a great temporal and spectral dispersion and does not match the input signal $x(t)$.

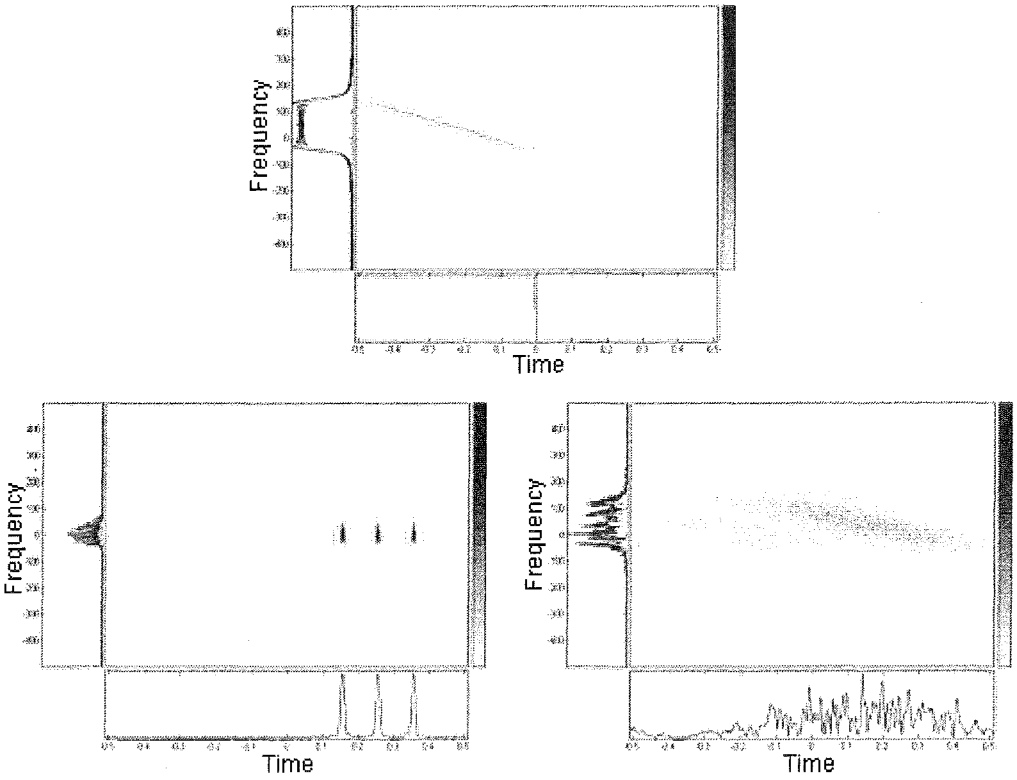


Fig. 9.- Time-frequency distribution of impulse response of dispersion compensation device $h_D^*(-t)$ (top), recovered signal $\boldsymbol{s(t) = x(t)}$ with $C_R(t) = C_T(t-t_p)$ (bottom left), and time-spread detected signal $\boldsymbol{s(t) \neq x(t)}$ (bottom right) with $C_R(t) \neq C_T(t-t_p)$.

As a result, when the code signal applied by the receiver is not correct, it is impossible to recover the information from the masked signal, unlike what happened with the first system configuration presented in this paper, usually employed in CDMA.

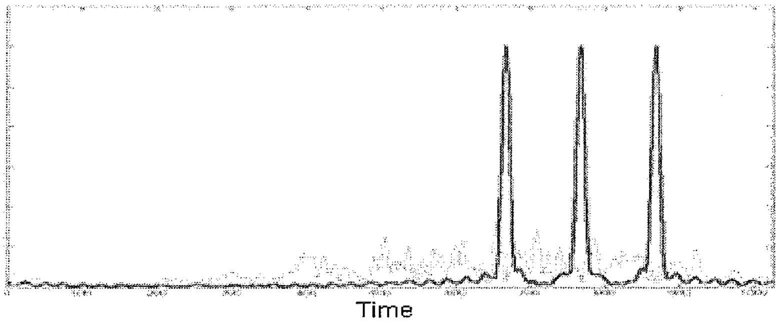


Fig. 10.- Comparison between the modulus of the decoded signals' time profile obtained with the proposed encoding/decoding system based on dispersion and modulation: Gaussian pulses recovered with $C_R(t) = C_T(t-t_p)$ and time-spread signal obtained with $C_R(t) \neq C_T(t-t_p)$.

5. CONCLUSIONS

In this paper we have proposed a novel method for masking the information signal from an emitter in an optical communication system with an OPLC-based digital chaos generator preceded by a linear dispersive element. We have observed that BPSK modulation of the data signal with a chaotic sequence from the OPLC does not provide an appropriate level of security: the information can indeed be retrieved with an envelope detector in the receiver, regardless of the correct synchronization of the emitter and receiver chaos generators or the receiver's knowledge of the code used by the emitter. By dispersing the input signal with a dispersive device, such as a fiber Bragg grating, prior to encoding, we have proved that the data is imprinted with phase information that causes pulse overlapping in the time domain and gives rise, after encoding, to spectrum spreading and a uniform time-frequency distribution that ensures secure masking of the signal. We have presented modeling results that confirm the impossibility of recovering the information from the masked signal without the correct chaotic code in the receiver and code synchronization.

ACKNOWLEDGMENTS

This work was partly supported by the Ministerio de Educación y Ciencia, Spain, through grant TEC2006-13874-C02-02 and a Juan de la Cierva contract.

REFERENCES

1. *Synchronization in Chaotic Systems,* Louis M. Pecora and Thomas L. Carroll, Physical Review Letters **64**, 821-824, 1990.
2. *Coherent Optical CDMA (OCDMA) Systems Used for High-Capacity Optical Fiber Networks-System Description, OTDMA Comparison, and OCDMA/WDMA Networking*, Wei Huang, Mohamed H. M. Nizam, Ivan Andonovic and Moshe Tur. June 2000, Journal of Lightwave Technology, Vol. 18 Issue 6 Pp. 765-778.
3. *Method to analyze the influence of hysteresis in optical arithmetic unit.* González-Marcos, Ana y Martín-Pereda, José A. s.l. : Society of Photo-Optical Instrumentation Engineers, November de 2001, Optical Engineering, Vols. 40-11, pp. 2371-2385.
4. Libro de Resúmenes. Nolineal 2007 Ciudad Real, 6–9 de Junio de 2007 Universidad de Castilla-La Mancha
5. S. Quian y D. Chen. *Joint Time-Frequency Analysis,* Englewood Cliffs, NJ: Prentice Hall, 1996.
6. *Performance enhancement of DS/CDMA system using chaotic complex spreading sequence,* Kurian, A.P.; Puthusserypady, S.; Su Myat Htut. May 2005, Wireless Communications, IEEE Transactions on, Volume: 4, Issue: 3, pp. 984- 989

7. *Chaotic sequences for spread spectrum: an alternative to PN-sequences* G. Heidari-Bateni in IEEE Int. Conf. Sel. Topics Wireless Communications Vancouver, BC, Canada, 1992, pp. 437-440.

8. *Digital chaotic output from an optically processing element.* González-Marcos, Ana y Martín-Pereda, José A. s.l. : Society of Photo-Optical Instrumentation Engineers, February de 1996, Optical Engineering, Vol. 35, pp. 525-533.

9. *Analysis of irregular behaviour on an optical computing logic cell.* González-Marcos, A. and Martín-Pereda, J. A. s.l. : Elsevier Science Ltd., 2000, Optics & Lasser Technology, Vol. 32, pp. 457-466.

10. *Modeling Reflective Bistability in Vertical-Cavity Semiconductor Optical Amplifiers.* Hurtado, A., Gonzalez-Marcos, A. and Martin-Pereda, J. A. , March 2005, IEEE Journal of Quantum Electronics, Vol. 41, pp. 376-383.

11. Gonzalez-Marcos, A. y Martin-Pereda, J. A. Digital Chaos Syncronization In Optical Networks. [edited] G. de Marchis y R. Sabella. *Optical Network Design and Modelling II.* s.l. : Kluwer Academic Publishers, 1999, pp. 175-186.

12. J. Azaña y M.A. Muriel, "Real-Time Optical Spectrum Analysis Based on the Time-Space Duality in Chirped Fiber Gratings", *Journal of Quantum Electronics*, May 2000 vol.36, no. 5, pp 517-525.