DIGITAL CHAOTIC CODEC FOR DS-CDMA COMMUNICATION SYSTEMS

Safwan El Assad and Calin Vladeanu
Ecole Polytechnique de l’Université de Nantes, Rue Christian Pauc, B.P. 50609, Nantes Cedex 3, France
1Université Polytechnique de Bucarest, Spaiul Independentei 313, Sector 6, 77531 Bucarest, Roumanie
safwan.ellasad@polytech.univ-nantes.fr

(Received 12 September 2005  -  Accepted 27 March 2006)

ABSTRACT

The potentialities of chaos to secure transmitted messages in digital communications has been proved. This by use Direct Sequence Code Division Multiple Access (DS-CDMA) system using chaotic spreading sequences. Two synchronization methods for Chua’s digital chaotic generator, are presented: the master-slave synchronization and the impulsive synchronization. In the first method, the driving signal is continuously transmitted from the driving to the driven system. In the second method, impulses from the driving system are transmitted to the driven one, by means of a time division scheme. A more robust digital chaotic codec is then developed to increase the complexity of the chaotic digital signal. The later is based on the general structure Penaud’s codec and Frey’s modified codec, associated with the technique of dead-beat chaos synchronisation developed by Angeli. Contrary to the others, the proposed codec is suitable to pass-band modulation. Comparison between these methods is achieved. The principle of the secure communication systems and the general chaotic QAM modem are presented.

Keywords: chaos, communication systems, synchronization, safely

INTRODUCTION

Chaos is a phenomenon that can appear in nonlinear dynamic systems. The idea of using chaotic signals to transmit secure information (by spreading the bandwidth of the transmitted signal) appeared at the beginning of the 90’s after it had been proved by Pecorra and Carroll (Pecorra 1990; 1993) that the chaotic systems can be synchronized. Specifically, it has been shown that, if a chaotic system can be decomposed into subsystems with stable Lyapunov exponents, then it will asymptotically track a replica of itself. At that time, it was a very big achievement to be able to describe the phenomenon of synchronization and to demonstrate the synchronizing behaviour in practice.

The main advantages of such usage are the increased security of the transmission and ease of generation of a great number of distinct sequences. As a consequence, the number of users in the system can be increased. Chaotic signals are very difficult to predict, reconstruct and synchronize, because of their sensitivity to the initial conditions. These
features make the chaotic signal more difficult to intercept as well as to decode the transmitted information. To recover the chaotic spreading signal in the receiver, synchronization between the chaotic sequences in the transmitter and receiver is needed. Therefore, synchronization is the most important requirement for designing chaotic spread spectrum communication systems.

Kocarev et al. (1992) and Kennedy & Kolumban (2000) derive the transmission of digital signals by means of chaotic synchronization numerically as well as experimentally, via Chua’s circuit. The tracking process was robust to allow locking to occur, but without the presence of any perturbations (Yang & Chua, 1997a; 1997b). Furthermore the complexity degree of the generated chaotic signal is very poor.

An alternative approach to generate chaos for secure communications has been demonstrated by Frey (1993). The codec uses a nonlinear filter with finite precision (8 bits) in conjunction with its inverse filter. The nonlinear function used is the left-circulate function suited to hardware implementation. The non-autonomous digital codec produce a quasi-chaotic (QC) signal (since chaotic signal requires infinite precision).

A general structure for a DSP implementation of self-synchronised chaotic encoder/decoder pair with nonlinear function was proposed by Penaud et al. (2000). Different equations can be used with this structure. The encoder is a nonlinear recursive filter with finite precision. All structures above are designed for base band modulation.

In this paper an improved codec structure is proposed (El Assad et al., 2003; El Assad & Tarhini, 2005). It increases the complexity of the generated chaotic signal (compared with the one generated by Chua’s circuit) and it is suitable for pass-band modulation. This architecture is based on the Penaud’s general structure and Frey’s modified codec. It uses the technique of dead-beat chaos synchronisation developed by De Angelis (1995).

The paper is presented as follows: the first section gives an overview of secure communication scheme and QAM(16, 256,...) chaotic modem structure. The second section introduces a digitally implemented Chua’s chaotic generator and the synchronization methods. The proposed codec is presented in the third section. The last section summarizes the obtained simulation results before conclusion and underlines the perspectives of using chaos in communication systems.

**PRINCIPLE OF THE SECURE COMMUNICATION SCHEME AND CHAOTIC QAM MODEM STRUCTURE**

**Principle of the secure communication scheme**

In the following (see Figure 1), a general simple secure communication scheme is presented.

Suppose that the chaotic synchronizing process is achieved in K-steps. In this process, $c(n)$ is the chaotic output of the transmitter and $b(n)$ is the information to be sent. The coding function $s(b,c)$ is chosen to be continuous and invertible. Moreover, we split the information in strings of $M$ samples each, with $M >> K$. 
Thereafter, the communication process is performed as follows:

Step A1 (commutators in position A):

- Generation and transmission of the following chaotic sequence:
  \[ \{c(0), c(1), \ldots, c(K - 1)\} \]
- Synchronization: \( \hat{c} = c \)

Step B1 (commutators in position B):

- Generation and transmission of the following coding sequence:
  \[ \{s[b(0), c(K)], s[b(1), c(K + 1)], \ldots, s[b(M - 1), c(K + M - 1)]\} \]
- Decoding: \( \hat{b} = s^{-1}\{s(b, c), \hat{c}\} \)

Step A2 (commutators in position A):

- Generation and transmission of the following chaotic sequence:
  \[ \{c(K + M), c(K + M + 1), \ldots, c(2K + M - 1)\} \]
- Synchronization: \( \hat{c} = c \)

Step B2 (commutators in position B):

- Generation and transmission of the following coding sequence:
  \[ \{s[b(M), c(2K - M)], s[b(M + 1), c(2K + M + 1)], \ldots, s[b(2M - 1), c(2K + 2M - 1)]\} \]
- Decoding: \( \hat{b} = s^{-1}\{s(b, c), \hat{c}\} \)
Chaotic QAM modem structure

The chaotic QAM modulator/demodulator scheme is illustrated in Figure 2.

Figure 2a. Chaotic QAM modem transmitter.

Figure 2b. Chaotic QAM modem receiver.
QAM is a modulation method in which two 90 degrees phase shifted sinusoidal carriers are used to transmit data over a given physical channel. In order to transmit $k$ bits on a symbol interval $T$, each group of $k$ bits is mapped into one of the $M = 2^k$ states of the modulated carrier. On each symbol interval and for each group of $k$ bits (nibble), two values, $a$ and $a'$ are obtained at the output of the QAM mapper. These values modulate the in-phase and in-quadrature carriers. The transmitted signal $s(t)$ is given by:

$$s(t) = A \sum_n a_n x(t - nT) \cos(2\pi f_c t + \phi_c) - A \sum_n a'_n x(t - nT) \sin(2\pi f_c t + \phi_c)$$  \hspace{1cm} (1)$$

$x(t)$ is a pulse waveform having the duration $T$ and unitary amplitude. $\phi_c$ is the phase of the carrier which has the frequency $f_c$.

**PRESENTATION OF THE MAIN GENERATION-SYNCHRONIZATION METHODS**

**Chua’s chaotic generator**

Chua’s circuit has served as the main prototype circuit for studying the chaos. Chua’s circuit is a simple electrical circuit built with linear elements and a nonlinear element (Chua’s diode). The circuit is shown in Figure 3.

![Figure 3. Chua’s generator and diode characteristic.](image-url)

The differential state equations describing the system are:

$$\begin{align*}
\frac{dv_1}{dt} &= \frac{1}{C_1} [G(v_2 - v_1) - f(v_1)] \\
\frac{dv_2}{dt} &= \frac{1}{C_2} [G(v_1 - v_2) + i_L] \\
\frac{di_L}{dt} &= -\frac{1}{L} v_2
\end{align*}$$  \hspace{1cm} (2)$$
Using the normalized state variables of the circuit, the system (2) becomes (Kennedy & Kolumban, 2000) (suitable for digital implementation):

\[
\begin{align*}
x' &= \alpha[y - x - f(x)] \\
y' &= x - y + z \\
z' &= -\beta y
\end{align*}
\]

(3)

where \( \alpha = \frac{C_2}{C_1} > 0 \) and \( \beta = \frac{C_2}{G^2L} \) are the main parameters of the circuit and \( f(x) \) is the non-linear term, and \( a = \frac{G}{G} < 0, \ b = \frac{G}{G} < 0 \).

\[
f(x) = bx + \frac{1}{2}(a - b)|x + 1| - |x - 1|
\]

(4)

This circuit is the first physical system, whose theoretical behaviour agrees with both computer simulation and experimental results.

The Chua’s circuit is implemented digitally. This design facilitates the synchronization between the generators built in the transmitter and the receiver, and enables the building of exactly identical chaotic circuits. Parameters are chosen to generate a double scroll attractor, as in Figure 11.

Synchronization methods for digital Chua’s chaotic circuit

Now the two main synchronization methods used in Chua’s circuit are presented: the Master-Slave synchronization and the Impulsive synchronization.

**Master-Slave synchronization**

A first approach to synchronize two chaotic systems was made by Pecorra and Caroll. They demonstrated the possibility of synchronizing two chaotic systems, and their method was to decompose the state vector of a dynamic system, in two state sub-vectors: the first describing the master (also called the driving circuit) and the second describing the slave (also called the driven circuit).

The master-slave decomposition method for Chua’s circuit is illustrated in Figure 4.

![Figure 4. Master-Slave decomposition of the Chua’s circuit.](image-url)
The master subsystem in Figure 4 is described by the equation:

\[
\frac{d\hat{v}_2}{dt} = \frac{1}{C_2} \left[ G(r(t) - \hat{v}_2) + i_L \right]
\]

or with the normalized parameters:

\[
\hat{y}' = r - y + z
\]

\[
\hat{z}' = -\beta \hat{y}
\]

(5)

The slave subsystem is described by:

\[
\frac{d\hat{v}_1}{dt} = \frac{1}{C_1} \left[ G(\hat{v}_2 - \hat{v}_1) - f(\hat{v}_1) \right], \text{ i.e. } \hat{x}' = a[\hat{y} - \hat{x} - f(\hat{x})]
\]

(6)

In this case, if the state variable \(r(t)\) from the transmitter is fed into the master subsystem in the receiver, as in Figure 5, it is expected to obtain at its output the approximate value \(\hat{v}_1(t)\) of the state \(v_1(t)\). This hypothesis is exploited in the method of synchronization between two identical chaotic subsystems interconnected by the signal \(\hat{v}_2(t)\) transmitted from the master subsystem. \(\hat{v}_2(t)\) will force the slave subsystem to synchronize all its states with the ones corresponding to the master, in time. The control signal \(r(t)\) (also called the driving signal), will force the receiver to output a signal \(\hat{v}_1(t)\) that will copy the input. So, relating to time, the following relation must be satisfied.

\[
\lim_{t \to \infty} \|\hat{v}_1(t) - v_1(t)\| \to 0
\]

(7)

Figure 5. Block diagram of the simulated system for Master-Slave synchronization.
**Impulsive synchronization**

According to the principle of Figure 1 and Figure 7, in impulsive synchronization, the transmitted signal consists of a sequence of time frames. Each time frame has a length of $T$ seconds and consists of two regions. The first region, which has a length of $Q$ seconds, is the synchronization region consisting of synchronization impulses (samples taken from the state variable of Chua’s circuit). These impulses are used to synchronize the chaotic system in the receiver (the slave) with the one in the transmitter (the master). The modulated message signal is placed within the second region which has the length of $T-Q$ seconds. Usually $T$ is much greater than $Q$. The synchronization between the two chaotic signals generated in the receiver and the transmitter, is achieved by means of the synchronization impulses. These impulses are set as initial conditions for the state variables in the receiver of Figure 6. In this figure, the variables $\{x'_r, y'_r, z'_r\}$ are defined by equations (3) and (4). After receiving the synchronization impulses, the driving and the driven circuits should share the same evolution, and the signals generated will be identical.

![Figure 6. Digital scheme of Chua’s receiver generator for impulsive synchronization.](image_url)

![Figure 7. Illustration of the concept of a time-frame and its components.](image_url)
PROPOSED DIGITAL CHAOTIC CODEC

In Figure 8, a more general structure of Penaud’s auto-synchronizing codec is presented. The decoder uses the dead-bit synchronization technique (De Angeli, 1995). Moreover this structure will be used in pass-band modulation instead of base-band modulation.

As shown in this figure, the general coder is realised by associating a non linear function $F_{NL}(x)$ with a delayed feedback loop. It is defined by the following equation:

$$
e_u[n] = F_{NL}\left( k_u(n) + \sum_{i=1}^{m} [G_i \times e_u(n-D_i) + s(n)] \right) \quad (8)$$

where

$$F_{NL}(x) = \begin{cases} 
  x & \text{if } x < 2^{N-1} \\
  x \mod(2^N) & \text{otherwise}
\end{cases} \quad (9)$$

The index $u$ in equation (8) means an unsigned number. Also, all additions are modulo $2^N$, where $N$ is the binary equivalent word length. These operators are assumed to be generally nonlinear operations. The general decoder, which presents the dead-bit synchronization feature, is an open loop version of the coder.

Figure 8a. General structure of the used auto-synchronizing coder.
Figure 8b. General structure of the used auto-synchronizing decoder.

The proposed digital chaotic codec, is based on Frey’s modified codec and uses a particular case (interesting for software and hardware implementation) of the system given by equation (8).

The generated chaotic signal of the system verify the quasi-chaotic (QC) properties, listed bellow, by experimental way:
- The zero input response has a broad noiselike spectrum for almost all choices of initial condition. Under the same conditions, the autocorrelation function of the response is similar to an uncorrelated noise sequence.
- The response of the filter to arbitrary inputs has a broadband noise-like spectrum for almost all choices of initial conditions. Under the same conditions, the autocorrelation function of the response is similar to an uncorrelated noise sequence.
- The response of the filter to almost all arbitrary inputs is uncorrelated to the input for almost all choices of initial conditions.
- The responses of the filter to the same input sequences are uncorrelated to one another for almost all choices of different initial conditions.
- For almost all choices of input to two identical filters having different but arbitrarily close initial states, the states of the two filters will diverge.

**Coder structure**

The coder uses the following particular case of the system driven by equation (8):

\[ m = 2, \ G_1 = 1, \ G_2 = 2, \ D_1 = 1, \ D_2 = 2, \] and a nonlinear left-circulate function, as see in Figure 9.

All operations inside the loop work in the unsigned number representation modulo \(2^N\). The delivered chaotic signal \(e_u(n)\) is composed by \(2^N\) quantized levels \(Q_n\) including...
the interval between $[0, 2^N - 1]$, represented with $N$ bits and having the duration of $T_{ch}$ seconds for each chip.

$$e_u(n) = \text{mod}[k_u(n) + \text{mod}[e_u(n-1) + \text{circ}[e_u(n-2)]]]$$

(10)

where

$$\text{circ}[e_u(n-2)] = \text{mod}[2e_u(n-2) + s_u(n)]$$

(11)

and

$$s_u[n] = \begin{cases} 0 & \text{if } e_u(n-2) < 2^{N-1} \\ 1 & \text{otherwise} \end{cases}$$

(12)

The carry bit function $s_u[n]$ plays the role of a noise source that is correlated in a nonlinear way to the response $e_u(n)$. The input signal $k_u(n)$ plays in our application the role of an additional key, which does not allow an unauthorized eavesdropper to recover the generated signal. Finally, after considering all things, we can write:

$$e_u(n) = \text{mod}[k_u(n) + e_u(n-1) + 2e_u(n-2) + s_u(n)]$$

(13)

The system states are given by:

$$x_1(n) = e_u(n-1) \text{ and } x_2(n) = e_u(n-2)$$

In order to reduce the signal’s mean power, and to make its amplitude independent of the number of levels (in fact on $N$), the generated signal $e_u(n)$ is, first converted on a signed signal $e_s(n)$ (The index means «signed») in the 2’s complement in the $2^N$ representation set: $[C2, 2^N]$, and then normalized by the maximum absolute value of the quantized levels. So the effective transmitted signal is:

$$e'_s(n) = \sum_n q_n \times p_{T_{ch}}(t-nT_{ch})$$

(14)

with

$$-2^{N-1} \leq q_n < \frac{2^{N-1} - 1}{2^{N-1}} \Rightarrow -1 \leq q_n < 1 \text{ and } p_{T_{ch}} = \begin{cases} 1 & \text{if } 0 \leq t < T_{ch} \\ 0 & \text{otherwise} \end{cases}$$

Figure 9. Coder structure.
Decoder structure

The receiver’s chaotic signal generator, which presents the dead-beat synchronization feature, is an open loop version of the transmitter generator. This means that the receiver’s chaotic spreading sequence generator is having almost the same implementation scheme, as in the transmitter, with the difference that a link in the loop is cut, in order to obtain the open-loop version. It seems that the best way to open the loop is to make a cut before and after one of the two delay elements in the scheme presented in Figure 9. The cut comes up with some other necessary modifications in the scheme, like the need to have the output of the transmitter generator, and both the input and the output of the receiver generator, virtually in the same point. This cut is marked with «x» in Figure 9. So, considering all the comments above, the block scheme of the receiver’s chaotic generator is presented in Figure 10. First, the received signal is increased in amplitude by the factor $2^{N-1}$, in order to have in the receiver the same values for the $q_n$ quantized levels, as in the transmitter. The following operations are identical to those performed in the transmitter generator. The output signal $\hat{e}(n)$ is a normalized signed representation signal which, is an estimation of the input signal $e_s(n)$. According to the dead-beat synchronization principle the output signal $\hat{e}(n)$ is synchronized to the transmitted chaotic signal, in a few steps (corresponding to two samples in the sequence). For an error free case, when the additive noise and transmission channel delay are ignored, the synchronized receiver sequence is identical to the transmitted sequence. For a more realistic case, when at least these two impairments must be considered, the deadbeat synchronization scheme is generating a signal with errors, where the error rate depends on the noise level. Any delay in the transmission channel is compensated by the auto synchronizing dead-beat scheme.

![Decoder structure](image)

Figure 10. Decoder structure.
COMPARATIVE SIMULATION RESULTS

Generated chaotic signal

For Chua’s circuit generator, the parameters are chosen to generate a double scroll attractor. The values of these parameters are: $L = 18mH$, $C_2 = 100nF$, $C_1 = 10nF$, $G = 0.58106ms$, $G_b = -0.407ms$, $G_a = -0.755ms$, $E = 1V$, which yields for the normalized parameters: $\alpha = 10$, $\beta = 16.4547$, $a = -1.2994$ and $b = -0.7004$. The initial conditions of the three state variable are: $v_1(0) = -0.204V$, $v_2(0) = 0.045V$, $i_L(0) = 1.561mA$, or for the normalized values: $x(0) = -0.204$, $y(0) = 0.045$, $z(0) = 0.3115$.

Figures 11, 12 and 13 show the double scroll attractor, the first state variable and its autocorrelation function generated by the digital implemented Chua’s circuit, with normalized parameters values. Results obtained in Figures 12 and 13 show that, the generated signal is not enough random.

This system, represented in Figure 9, was started for many initials conditions $(x_1(0), x_2(0))$, with or without the input signal $k_u(n)$. The obtained results show that, generated signals verify the QC-properties. This verification is based on the observation of the time and frequency representations of signals, and also their autocorrelation and cross-correlation functions. We present below some simulation results for the following parameters and initial conditions:

$N = 16$; $T_{ch} = 5ns$; $k_u(n) = 0$; $x_1(0) = 20000$; $x_2(0) = 400$

and $x_1(0) = 20002$; $x_2(0) = 402$

Figure 14 represent the time domain variation of the encoded signal, which is a more random signal compared with the one of Figure 12. In fact, the results shown in Figures 15 and 16, precisely the DFT and the autocorrelation function of the encoded signal are clearly noise-like. The cross-correlation function between pairs of encoded signals corresponding to different cycles was also computed for a variety of cases. Figure 17 shows the cross-correlation function (in dashed line) of encoded signal due to different states compared with one of their autocorrelation functions. In spite of the fact of close initial conditions, we remark a very week correlation between two delivered signals by the same generator.

Figure 11. Double-scroll attractor.
Figure 12. Time domain variation of $x$.

Figure 13. Autocorrelation function of $x$.

Figure 14. Time domain variation of the multilevel chaotic signal.
Figure 15. DFT spectrum of the multilevel chaotic signal.

Figure 16. Autocorrelation function of the multilevel chaotic signal.

Figure 17. Comparison: cross-correlation — due to the different states and autocorrelation functions.
Synchronization

Simulations are performed for the synchronization between the two chaotic systems. The chaotic signal generated in the transmitter is fed onto the X input of an oscilloscope, and the signal generated in the receiver is fed into the Y axis of the same oscilloscope. When the two signals are identical, they are synchronized, and a 45-degree line will appear on the screen of the oscilloscope. To be synchronized, both chaotic circuits start from the same initial conditions. Also, for the circuit components, the same values of the parameters are set in both the transmitter and the receiver.

When noise is not added in the communication channel, identical synchronization between the chaotic signals in the receiver and transmitter is achieved for the three synchronization methods: master-slave decomposition, impulsive synchronization and dead beat synchronization. That means a very thin 45-degree line appears on the screen of the oscilloscope. In case of a very small white Gaussian noise added to the transmitted driving signal, the identical synchronization between the transmitter and the receiver is lost for all synchronization methods. This situation is illustrated in Figures 18 and 19, under a SNR=15 dB condition. We observe that, the impulsive synchronization method is more effective than the master-slave decomposition in what noise performance is concerned, and also with reference to the communication channel resources used by the signal.

Figure 18. De-synchronization of $x$ signal for the master-slave method and SNR=15 dB.

Figure 19. De-synchronization of $x$ signal for the impulsive method and SNR=15 dB.
CONCLUSION

The results presented in this paper show that there is a great potential of using chaotic signals in a digital radio communication system. In order to be able to use this potential, the chaotic sequences generated in the receiver and transmitter must be perfectly synchronized. When noise is added, the results show that the implemented methods are not very efficient because the synchronization of the chaotic signals is lost. The proposed coder/decoder is more effective compared with the one of Chua's circuit. Indeed, the generated chaotic signal is more random and verify the QC properties. Also the ease of the digital software and hardware implementation of the mentioned coder/decoder.

Future work will focus on finding robust discrete-time synchronization methods and on integrating them in a real and practical digital communication system. Also, an attempt will be done to convert the multilevel chaotic signal into a binary one. This binary chaotic signal will be further used as a PN sequence for data spreading, as in a CDMA system.

ACKNOWLEDGEMENT

This work is made within the framework of the research project RNRT "ACSCOM" “Apport du Chaos dans la Sécurité des Systèmes Communicants Optiques et Mobiles”

REFERENCES