ANTICIPATING SYNCHRONIZATION BETWEEN SAMPLED-DATA MASTER AND DISCRETE-TIME SLAVE CHAOTIC SYSTEMS

Ramazan Yeniçeri and **Müştak E. Yalçın**
Department of Electronics and Communication Engineering
Istanbul Technicak University
Maslak TR-34469 Istanbul, Turkey
{yenicerir, mustak.yalcin}@itu.edu.tr

Abstract

The anticipating synchronization between time-delay systems is studied with a sampled-data master and discrete-time slave systems in this paper. The rough discrete-time approximation of the original sampled-data system exhibits significant performance when locking to the master system and generating the anticipated signal. System models, coupling schemes, error bound, block diagram of the implemented system are presented with the phase portraits and signal plots in time. The proposed anticipation method by simple discrete-time slave systems enables to use hundreds of slave systems which promises to anticipate the chaotic signal hundreds of τ beforehand using a single digital chip.

Key words

Anticipating, synchronization, chaos, delay.

1 Introduction

The synchronization between chaotic systems need proper coupling scheme, in order to result in a common behavior of coupled systems. Generating the same chaotic signal due to the synchronization has been studied for many systems. The challenge here is the diverging motion of chaotic systems because of their high sensitivity to the initial conditions. Synchronization in time-delay chaotic systems has been introduced by [Voss, 2000]. The coupling scheme has provided the state values in the future to be anticipated beforehand.

The chaos based true random number generators (TRNG), such as the one proposed by [Pareschi et al., 2006], appear as the alternative to the generators based on physical noise [Petrie and Connelly, 2000]. In order to guarantee the security of a random number generator, the signal generated by it should be indistinguishable from a true random sequence. NIST's current statistical test suite SP 800-22rev1a is approved as the trustworthy tool to check the sequence randomness today. Even the sequences generated by a time-delay chaotic system successfully pass the NIST's test suite, they have a fundamental weakness coming from the anticipating synchronization phenomenon. In a proper scheme, locked slave systems generates the signal that passes the randomness tests beforehand. An example system proposed in [Yeniceri and Yalcin, 2013] has been attacked using anticipating synchronization in [Yeniceri et al., 2015]. The aim in this paper is to exhibit the phenomenon using digital slave systems which are simpler that the original analog one.

Paper is organized as follows. Model of the chaotic system and the coupling scheme for the anticipating synchronization have been given in Section 2. It is followed by the 3-rd Section with the implementation details and the results experienced by the implementation. At the end, Section 4 concludes the paper.

2 System Model and Coupling Scheme for Anticipating Synchronization

The following equations have t and t_k arguments which have a relation given by

$$t_k \leq t < t_k + T_s, \tag{1}$$

where T_s is the sampling period of the system. k subscript represents the sampling index. System (2) is the time-delay sampled-data chaotic oscillator which has been proposed in 2014 [Yalcin et al., 2014].

$$\begin{aligned} \dot{x}(t) &= -x(t) + f\big(x(t_k - \tau)\big) \\ f(x) &= 2\left(u(x-1) + u(-x-1)\right) - 1 \end{aligned} \tag{2}$$

Although very low sampling rate annihilates the chaotic motion according to the numerically calculated Lyapunov exponent spectrum and bifurcation diagram, T_s has a practically enough wide range that resides in

the chaotic regime. A coupling scheme which is proposed in [Yeniceri et al., 2015] results in anticipating synchronization of coupled sample-data system. For $p+1$ systems, the coupling scheme is given in Eq. 3.

$$\begin{aligned} \dot{x_0}(t) &= -x_0(t) + f\big(x_0(t_k-\tau)\big) \\ \dot{x_1}(t) &= -x_1(t) + f\big(x_0(t_k)\big) \\ &\vdots \\ \dot{x_p}(t) &= -x_p(t) + f\big(x_{p-1}(t_k)\big) \end{aligned} \tag{3}$$

To demonstrate the existence of synchronization between $x_0(t+\tau)$ and $x_1(t)$, an error variable is defined at first by

$$e(t) = x_0(t+\tau) - x_1(t). \tag{4}$$

If $x_0(t+\tau)$ is written using the first row in Eq. 3, and the second row is subtracted from it, the error system appears as in Eq. 5.

$$\dot{e(t)} = -e(t) \tag{5}$$

Asymptotically converging $e(t)$ to 0 proves the anticipating synchronization between the first two coupled systems S_0 and S_1, who are generating $x_0(t)$ and $x_1(t)$ signals. In this paper, S_0 is called the master system, and other, S_i is called i-th slave system. When the slave system locks to the master, $x_1(t) = x_0(t+\tau)$. The general expression, $x_i(t) = x_{i-1}(t+\tau)$, becomes valid . Theoretically, S_p anticipates S_0 $p\tau$ seconds beforehand ($p \in \mathbb{N}$). In [Yeniceri et al., 2015], one master and three slave systems have been implemented and anticipated signals have been demonstrated. In this paper, the slave systems are the ones discretized using forward Euler method and implemented as digital circuits.

The delayed signal is expressed by a linear time invariant delay operator, $x(t_k-\tau) = \mathrm{T}_\tau[x(t_k)]$. Then changing the order of the nonlinearity $f(\cdot)$ and the time operator $\mathrm{T}_\tau[\cdot]$ yields $f(x(t_k-\tau)) = \mathrm{T}_\tau[f(x(t_k))]$. This provides the binary output of the nonlinearity to be delayed, instead of the analog state variable itself. The required delay line for System (2) samples the binary signal from the nonlinearity and hold it along the sampling period. The previous samples in the delay line moves one step all together towards output at each sampling moment. This structure is simply constructed using fundamental memory element for the digital circuits, delay-type (D-type) flipflop, and called *shift register* in digital electronic field. Fig. 1 depicts the D-type flipflop chain as a delay line.

In this paper, p is selected as 3. Integration step of discrete systems h is selected as T_s, which is 0.125 in the model. Delay (τ) is 10. The discrete-time slave systems with the sampled-data master system is given

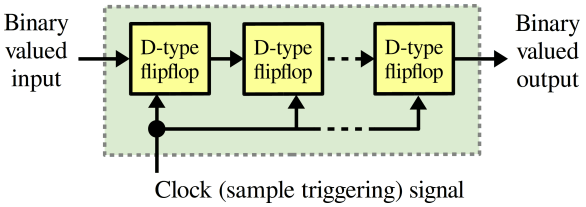


Figure 1. A shift register, which is a D-type flipflop chain, is employed as a delay line for the sampled-data system.

in Eq. 6 with the coupling scheme.

$$\begin{aligned} \dot{x_0}(t) &= -x_0(t) + \mathrm{T}_\tau\Big[f\big(x_0(t_k)\big)\Big] \\ x_1(t_k+T_s) &= (1-T_s)x_1(t_k) + T_s f(x_0(t_k)) \\ x_2(t_k+T_s) &= (1-T_s)x_2(t_k) + T_s f(x_1(t_k)) \\ x_3(t_k+T_s) &= (1-T_s)x_3(t_k) + T_s f(x_2(t_k)) \end{aligned} \tag{6}$$

If the feedback in the System (2) is broken and f is considered as an input, the solution of sampled-data system becomes

$$x(t_k+T_s) = e^{-T_s}x(t_k) + (1-e^{-T_s})f(t_k). \tag{7}$$

Using $\alpha = e^{-T_s}$, the general solution is given by

$$x(nT_s) = \alpha^n x(0) + \sum_{r=0}^{n-1} \alpha^{n-1-r}(1-\alpha)f(t_r). \tag{8}$$

Similarly, the forward Euler integration provides the solution of the discretized system by

$$x_{\mathrm{D}}(nT_s) = \beta^n x_{\mathrm{D}}(0) + \sum_{r=0}^{n-1} \beta^{n-1-r}(1-\beta)f(t_r), \tag{9}$$

where $\beta = (1-h)^{T_s/h}$. As $\alpha < 1$ and $\beta < 1$, the zero-input solution of both systems asymptotically converges to 0. If the error is defined as $e(nT_s) = x_{\mathrm{D}}(nT_s) - x(nT_s)$, and the input applied $f(t_r)$ is ± 2 to both systems, $0 < e(nT_s) \leq e_{\max} = 0.097082$, when $h = T_s = 1/8$. Input signal is defined ± 2 in order to simulate the nonlinear function in Eq. 2. Selecting $h = T_s = 1/8$ gives a very rough digital approximation.

The discrete-time (digital) system resembles the original sampled-data system in the above error range. Simulations show that digital system's state may incorrectly pass the thresholds in the f function due to the error, and generate faulty f values for finite sampling periods. This reduces the anticipating synchronization performance of the digital systems while p is increasing. However, for $p = 3$ as in this paper, the 3-rd slave signal successfully predicts the master systems state signal. Synchronization performance may be polished by smaller h values in exchange for implementation complexity. The preferred feature in this paper is

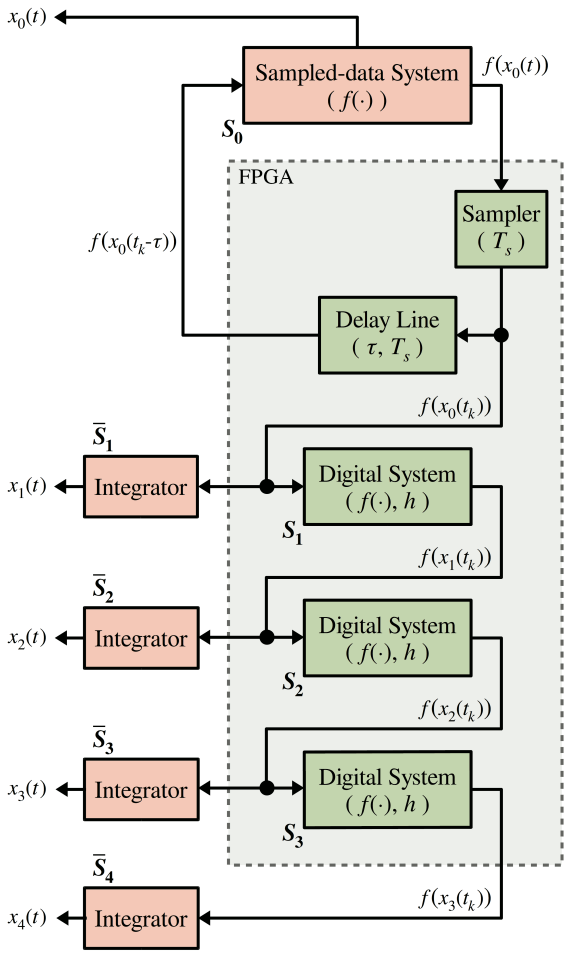


Figure 2. Block diagram of coupled systems for anticipating synchronization. S_1, S_2, and S_3 are digital slave systems whose states are hidden. In order to measure the hidden states, integrators ($\overline{S_1}$, $\overline{S_2}$, and $\overline{S_3}$) are employed. They work like sampled data system, as they continuously integrate the sampled and held binary signal.

the slave system simplicity, thus the system is implemented as explained in the next section with $h = 1/8$.

3 Electronic Implementation and Experimental Results

The System (6) is implemented by a mixed signal circuit whose block diagram is drawn in Fig. 2. The red blocks are analog (continuos time, continuous amplitude signal) circuits. The green blocks in the Field Programmable Gate Array (FPGA) region are digital (discrete-time, quantized amplitude signal) circuits. FPGA is a configurable digital device, that you can build the designed digital circuit using its functional blocks and programmable interconnections. One should note that, the discrete-time systems hold their signal value between the sampling moments. Therefore, the digital Delay Line acts the sample and hold role for the analog S_0 system, which is integrating the Delay Line output signal in continuous time. The time constant of analog S_0 system, which is used as the time normalization factor, is 10μs. The real delay is 100μs that means $\tau = 10$ in the implementation. T_s equals to 1250ns (equal to $1/8$ before time normalization), so the flipflop count on the delay line is 80. Digital S_1, S_2, and S_3 circuits iterate at the beginning of each T_s period, and generate the signals from $f(x_1(t_k))$ to $f(x_3(t_k))$. Their states ($x_1(t_k)$ to $x_3(t_k)$) are not observable in the proposed implementation. In order to observe these states, they are re-generated outside the digital device (FPGA) using the drive signals ($f(x_0(t_k))$ to $f(x_2(t_k))$) by analog integrators. The analog integrators are simple serial RC circuits. The voltage signal over the capacitors of these RC couples represent the internal (non-observable) x_1, x_2, and x_3 states.

Fig. 3 have four phase portraits which are generated by the given implementation. The original attractor in [Yalcin et al., 2014] that exist on the $x(t-\tau)$-$x(t)$ state space has the shape like the letter 'V'. The same attractor is observed on $x_0(t)$-$x_1(t)$ plane (Fig. 3(a)), on $x_1(t)$-$x_2(t)$ plane (Fig. 3(b))on $x_2(t)$-$x_3(t)$ plane (Fig. 3(c)), and on $x_3(t)$-$x_4(t)$ plane (Fig. 3(d)). Recorded signals over time using an analog oscilloscope have been plotted in Fig. 4. From top the bottom, each signal is anticipated by the below one 100μs before. The time shift between the signals equals to the delay line length (100μs).

4 Conclusion

Three digital systems has been coupled to a time-delay sampled-data chaotic system. Anticipating synchronization has been achieved by the proposed slave systems. Chaotic attractors are created by synchronized systems and demonstrated. The simplicity of the digital slave system provides an opportunity to fit more than 100 slave systems into a single FPGA chip.

References

Pareschi, F., Setti, G., and Rovatti, R. (2006). A fast chaos-based true random number generator for cryptographic applications. In *Solid-State Circuits Conference, 2006. ESSCIRC 2006. Proceedings of the 32nd European*, pages 130–133.

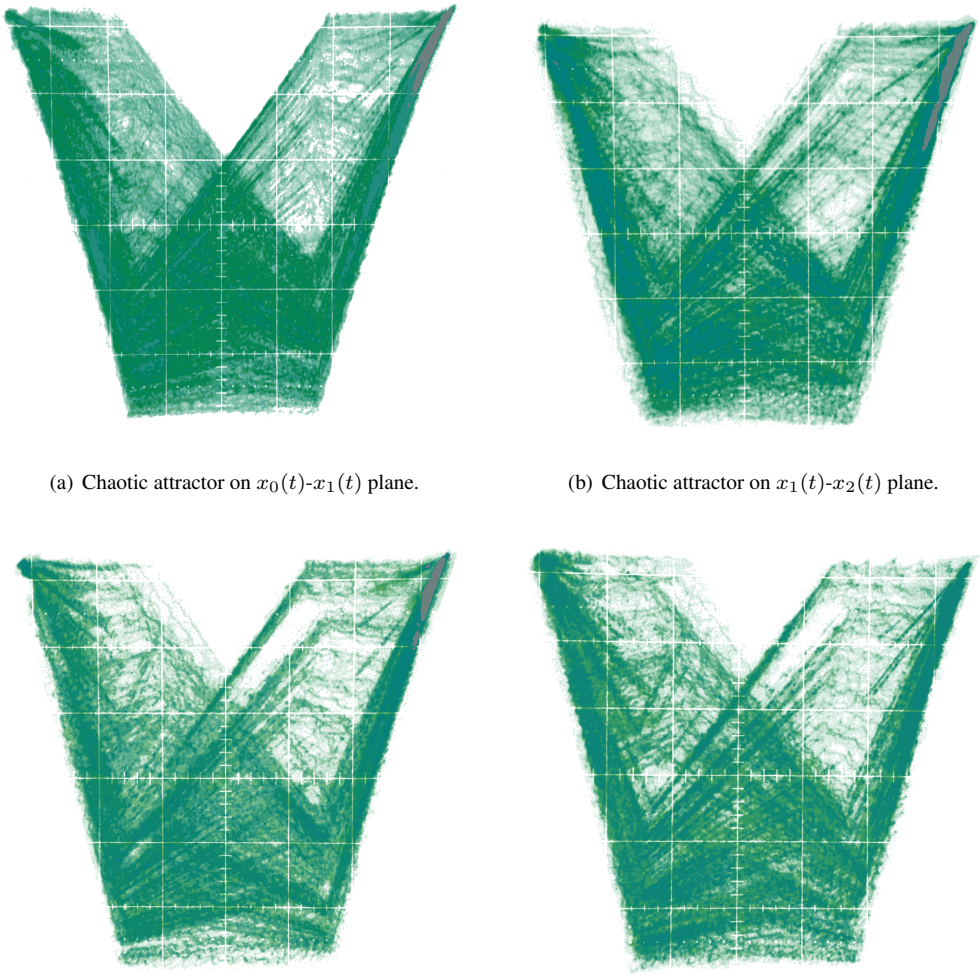
Petrie, C. S. and Connelly, J. A. (2000). A noise-based ic random number generator for applications in cryptography. *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on*, 47(5):615–621.

Voss, H. U. (2000). Anticipating chaotic synchronization. *Phys. Rev. E*, 61(5):5115–5119.

Yalcin, M., Yeniceri, R., and Ozoguz, S. (2014). A chaotic time-delay sampled-data system and its implementation. *International Journal of Bifurcation and Chaos*, 24(3):1450039.

Yeniceri, R., Kilinc, S., and Yalcin, M. E. (2015). Attack on a chaos-based random number generator using anticipating synchronization. *International Journal of Bifurcation and Chaos*, 25(02):1550021.

Yeniceri, R. and Yalcin, M. E. (2013). True random bit generation with time-delay sampled-data feedback system. *Electronics Letters*, 49(8):543–545.



(a) Chaotic attractor on $x_0(t)$-$x_1(t)$ plane.

(b) Chaotic attractor on $x_1(t)$-$x_2(t)$ plane.

(c) Chaotic attractor on $x_2(t)$-$x_3(t)$ plane.

(d) Chaotic attractor on $x_3(t)$-$x_4(t)$ plane.

Figure 3. The chaotic attractors observed by an analog oscilloscope. Phase planes used for observation have been noted below subfigures.

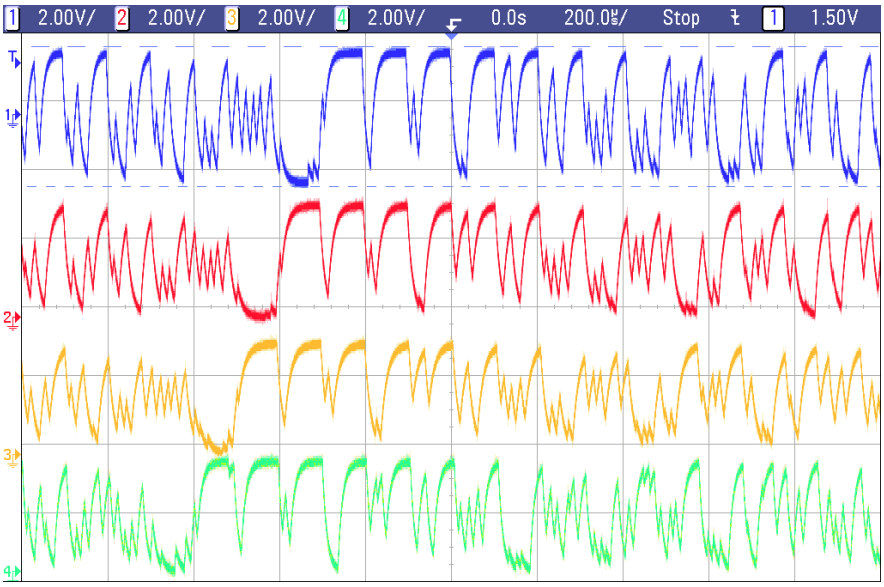


Figure 4. From top to bottom, $x_0(t)$ (blue), $x_1(t)$ (red), $x_2(t)$ (yellow), $x_3(t)$ (green) in a 2ms-long record. Each have 100μs left-shift in reference to the one up signal.