DEVELOPMENT OF A DIGITAL SIGNAL PROCESSOR (DSP) BASED CHAOTIC COMMUNICATION SYSTEM WITH EMPHASIS ON MILITARY APPLICATIONS

Noah F. Reddell
Thad B. Welch

U.S. Naval Academy
Electrical Engineering Department
Annapolis, MD

Erik M. Bollt

U.S. Naval Academy
Mathematics Department
Annapolis, MD

ABSTRACT

We explore the advantages of designing a communication system based on chaos by using digital signal processing techniques. Existing work developing chaotic communication schemes has been done on a theoretical basis or in component based electrical circuits that are not as flexible, particularly for research.

Our work takes a unique technological approach towards exploring the benefits of chaos. We use discrete methods to implement chaotic dynamical systems. Most of our current results are from MATLAB simulations, but we are working towards implementing chaos on digital signal processors (DSPs). These high-speed processors can produce a chaotic carrier through software algorithms rather than in an electrical circuit. The use of discrete methods allows for schemes that out perform earlier systems.

We demonstrate a new dual receiver synchronizing response system that exploits the ability to store samples over an entire bit period and then perform an intelligent comparison. Our results show better bit error probability in comparison to previously published methods. We introduce a method for improving the bit error performance of our scheme by systematically searching for better parameter sets.

1. INTRODUCTION

Chaotic systems are aperiodic, deterministic, and sensitive to slight variations in initial condition. The latter property presents the problem that the behavior of the system cannot be predicted for a significant period of time into the future. The state of a system for the next instant is completely attainable, but in the long run it cannot be calculated with any degree of accuracy.

These systems then produce random-like behavior due to their unpredictability and relatively broad bandwidth. We have looked at both the frequency domain and time domain properties of chaotic systems and find that using them for a message carrier could offer several advantages over traditional modulation schemes such as amplitude modulation and frequency modulation. Our goal is to design a system that can avoid detection by third parties.

Initially, it seems strange to attempt communication using a chaotic carrier since the state of a chaotic system cannot be accurately predicted. However, a number of chaotic communication schemes have been proven possible using the property of synchronization [1], [2].

Some chaotic systems can be synchronized with an identical system by allowing for an influence between the two. Both systems will remain chaotic, but one locks to the other. Once synchronization has been achieved, information can be sent. A transmitter's output is modified in some way by a message. Since the receiver follows what the transmitter's state should be, it can detect the modification caused by a message and thus extract the information from the chaotic signal. Meanwhile, the transmission will hopefully continue to look like noise to an outside observer.

2. SYNCHRONIZED CHAOS

We consider the famous Lorenz System:

$$\begin{aligned} \dot{x} &= \sigma(y-x), \\ \dot{y} &= rx-y-xz, \\ \dot{z} &= xy-bz. \end{aligned} \tag{1}$$

The parameters σ, r, and b have been removed from their original context in Lorenz's convection process but they are still significant for our purposes. The state variables above must be scaled to match the dynamic range of the Digital-to-Analog and Analog-to-Digital

The authors would like to thank the USNA Trident Scholar Program and AFCEA for funding. Also, E.M.B. is funded by the NSF DMS-0071314.

converters (CODECs) on our DSPs. Additionally, the system evolves at a rate that is impractical for the sampling rate of the CODECs. For these reasons, we will use a magnitude and time scaling change of variables. Scaling magnitude by $\frac{1}{A}$ allows the x term to be sent to the Digital-to-Analog converter without saturation. A time scale of T_S allows efficient use of available CODEC bandwidth. These terms will need to be adjusted based on the particular parameters chosen and the time scaling will be tied to the step size of the differential equation solver.

The uniform scaling is given by the substitution:

$$u = \frac{x}{A}, v = \frac{y}{A}, w = \frac{z}{A}. \tag{2}$$

Thus, the scaled drive system (transmitter) is:

$$\begin{aligned} \dot{u} &= T_S\sigma(v-u), \\ \dot{v} &= T_S(ru - v - Auw), \\ \dot{w} &= T_S(Auv - bw). \end{aligned} \tag{3}$$

2.1. Drive - Response Coupling based on Parameter Set Match or Mismatch

In our discrete scheme, we further an idea investigated by Cuomo, et al. [3]. They sent a binary message by adjusting the b parameter of the drive system. This adjustment slightly upsets the synchronization between the drive and response systems. The presence or absence of error at the response system could then be used to determine the message bit.

Our new dual synchronizing response system is as follows. We run two response systems in the receiver DSP. One response system parameter set corresponds to a one-bit and the other corresponds to a zero-bit. Both systems attempt to synchronize with the parameter modulated drive system over the entire bit period. Then, the errors experienced by each response system are compared. The system with less error determines the received bit and both response system states are updated to reflect the better match. By taking advantage of the abilities of DSP hardware, we achieve better performance than a discrete version of the system in [3].

Figure 1 shows the four cases of two drive parameter sets and two response systems. The drive system chooses parameter set A or B based on the message bit. The plots show the drive system and how the response systems (one using set A and one using set B) respond. We desire that a matched set of parameters between the transmitter and receiver causes a quick and tight coupling while a mismatched set leads to large error.

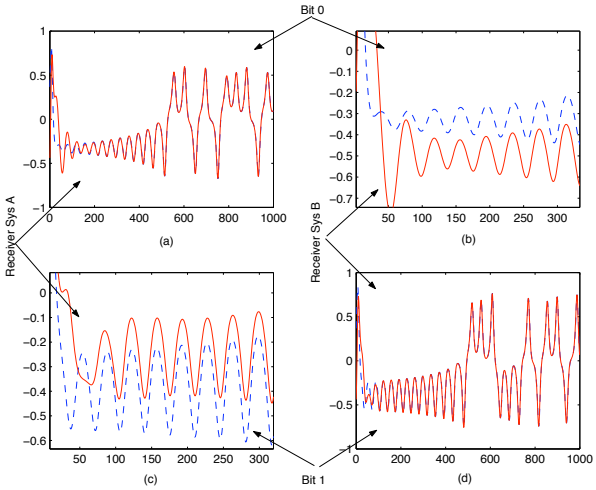

Fig. 1. All possible combinations of bit sent and receiver system, plotted as voltage vs. sample number. (a), transmitter and receiver use parameter set A (b), transmitter uses set A, receiver uses set B, (c), Transmitter uses set B, receiver uses set A (d), transmitter and receiver use parameter set B.

Coupling is achieved by sharing the u term from the drive system with the response system. Notice in eqn. (4) that u takes the place of u_r in the equations for $\dot{v}_r$ and $\dot{w}_r$. The variable u is the influence signal. We maintain the same influence configuration as used by Cuomo, et al. and simplify the analysis by letting σ and r be the same in the response systems as the drive system. The transmitter alters the parameter b based on a message bit. Parameter b_r is the corresponding parameter in the response system. Parameter b_r will either be identical or mismatched to b.

The response system (receiver) is:

$$\begin{aligned} \dot{u}_r &= T_S\sigma(v_r - u_r), \\ \dot{v}_r &= T_S(ru - v_r - Auw_r), \\ \dot{w}_r &= T_S(Auv_r - b_r w_r). \end{aligned} \tag{4}$$

Error terms are used to evaluate coupling:

$$\begin{aligned} e_u &= (u - u_r), \\ e_v &= (v - v_r), \\ e_w &= (w - w_r). \end{aligned} \tag{5}$$

Taking the derivative with respect to time yields

$$\begin{aligned} \dot{e}_u &= (\dot{u} - \dot{u}_r), \\ &= T_S\sigma(v-u) - T_S\sigma(v_r - u_r), \\ &= T_S\sigma(e_v - e_u). \end{aligned}$$

$$\begin{aligned}
\dot{e}_v &= (\dot{v} - \dot{v}_r), \qquad (6)\\
&= T_S(ru - v - Auw - ru + v_r + Auw_r),\\
&= T_S(-e_v - Aue_w).\\
\dot{e}_w &= (\dot{w} - \dot{w}_r),\\
&= T_S(Auv - bw - Auv_r + b_r w_r),\\
&= T_S(Aue_v - bw + b_r w_r).
\end{aligned}$$

2.2. Lyapunov Function Analysis

If we can find a Lyapunov function for the error system above, we can show that it approaches zero over time, and thus the two Lorenz systems synchronize [4]. Lyapunov functions generalize the idea of potential energy. Again we follow Cuomo's lead and use his Lyapunov function as the basis for ours [3].

$$E(e_u, e_v, e_w) = \frac{1}{2}(\frac{1}{\sigma}e_u^2 + e_v^2 + e_w^2). \qquad (7)$$

To show synchronization, we want to find that the function $E(e_u, e_v, e_w)$ has a long-term negative slope and so error decreases. Taking the derivative with respect to time:

$$\begin{aligned}
\frac{dE}{dt} &= \frac{\partial E}{\partial e_u}\cdot\frac{\partial e_u}{\partial t} + \frac{\partial E}{\partial e_v}\cdot\frac{\partial e_v}{\partial t} + \frac{\partial E}{\partial e_w}\cdot\frac{\partial e_w}{\partial t}\\
&= \frac{e_u\dot{e}_u}{\sigma} + e_v\dot{e}_v + e_w\dot{e}_w\\
&= T_S(e_u e_v - e_u^2 - e_v^2 - Aue_v e_w \qquad (8)\\
&\quad + Aue_v e_w - e_w(bw - b_r w_r)).
\end{aligned}$$

If $b = b_r$ (Parameter Set Match) then,

$$\begin{aligned}
\frac{dE}{dt} &= T_S(e_u e_v - e_u^2 - e_v^2 - be_w^2)\\
&= T_S(-(e_u - \frac{1}{2}e_v)^2 - \frac{3}{4}e_v^2 - be_w^2). \qquad (9)
\end{aligned}$$

Since E is positive definite and $\dot{E}$ is negative definite with $T_S > 0$, Lyapunov's theorem implies $\mathbf{e}(t)$ approaches 0 as $t \to \infty$. Synchronization will therefore occur. This analysis does not indicate how fast it occurs, but experimentation shows it to be fast enough to achieve a working system.

If $b \neq b_r$ (Parameter Set Mismatch) then,

$$\frac{dE}{dt} = T_S(e_u e_v - e_u^2 - e_v^2 - e_w(bw - b_r w_r)). \qquad (10)$$

The derivative above is inconclusive.

3. IMPROVING BIT ERROR RATE

We are currently developing a systematic analysis to optimize the selection of parameter sets including allowing mismatch in the σ and r parameters as well. For complete freedom in all three parameters for both sets, this is a six dimensional problem and computationally intensive.

We have found that the error performance of the system is essentially based on the difference between the energy of a one-bit and the energy of a zero-bit. Let,

$$E_{\text{diff}} = |E_1 - E_0|. \qquad (11)$$

This energy difference changes for every bit since the system is aperiodic and cannot be calculated in closed form. To improve the systems error performance when subjected to noise, we wish to maximize the average E_{diff} over all transmitted bits.

To illustrate the effects of noise on our scheme, Figure 2 shows a single bit window used in our dual synchronizing receiver scheme. The influence signal from the transmitter is affected by additive white Gaussian noise and the two response systems in the receiver attempt to synchronize to the noisy influence signal. The sum of squares of the error for both receiver systems is used to determine the best match with the influence signal. For this case, SysB represented by the open circles is the better match. This system would then determine the received bit, and the other response system, SysA, would be reset to match the state of SysB before the next bit period.

Because the DSP hardware gives us the ability to compare two response systems against the received signal, we do not have to worry about completely destroying the synchronization by a parameter mismatch which is too large. The parameter matched version will reset the state of both response systems after the bit period. As a result of our system's ability to move forward with the best fit system, we are able to maintain synchronization with an aggressive parameter mismatch.

4. DEVELOPMENT OF THE DISCRETE CARRIER

The differential equations described above are continuous systems and must be modified to run our discrete hardware. This can be done by using numerical techniques to solve the differential equations. We have chosen to use the Runge-Kutta 4-5 algorithm because

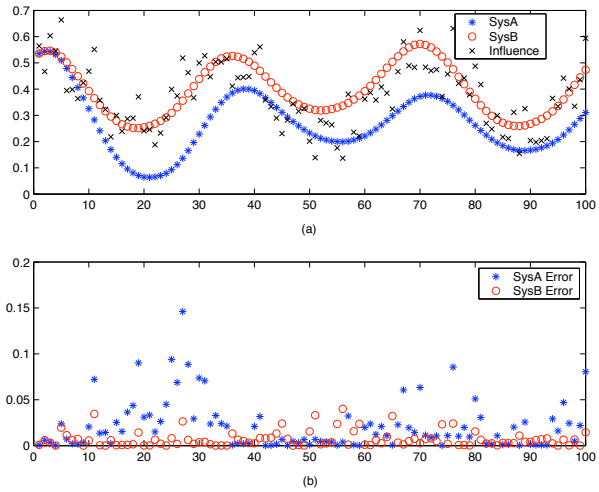

Fig. 2. Receiver evaluation of a particular bit, (a) Noisy influence signal and attempts to synchronize by both response systems (Volts vs. Sample Number), (b) Error^2 between both receivers and the influence signal (Volts^2 vs. Sample Number).

it yields accurate results relative to its processing requirements [5]. The chief issue we have faced when transforming the continuous systems to a discrete environment is that of step size.

There are two methods to effectively utilize the available bandwidth of the CODEC without aliasing. First, the system can be sped up or slowed down by adjusting the RK-45 step size or by adjusting the time scale T_S, which are a related pair. Alternatively, excessive samples can be discarded by decimation, provided the Nyquist condition is met. We have found the step size-T_S pair is the limiting factor. Taking a step that is too big causes the RK-45 algorithm to fail and the discrete system does not emulate its continuous model. Therefore, to efficiently utilize CODEC bandwidth, decimation is the better method provided it can be done without aliasing.

5. SEARCH FOR A BETTER PARAMETER SET

The Lyapunov exponent measures average error growth between two nearby solutions of a system. A positive exponent indicates nearby solutions diverge and are aperiodic. Boundedness and a positive Lyapunov exponent can define a chaotic system. Figure 3 shows the parameter sets that result in a positive Lyapunov exponent for the region shown. Sets with negative exponents can be excluded from the bit energy search since they indicate periodic behavior.

Currently we have not tackled the full six-dimensional problem. Initially we have fixed one parameter set and searched in a three-dimensional space in order to maximize E_{diff}. As long as the set identified to maximize E_{diff} maintains the boundedness of the system, then we expect it to result in the best bit error performance out of all sets in the parameter space.

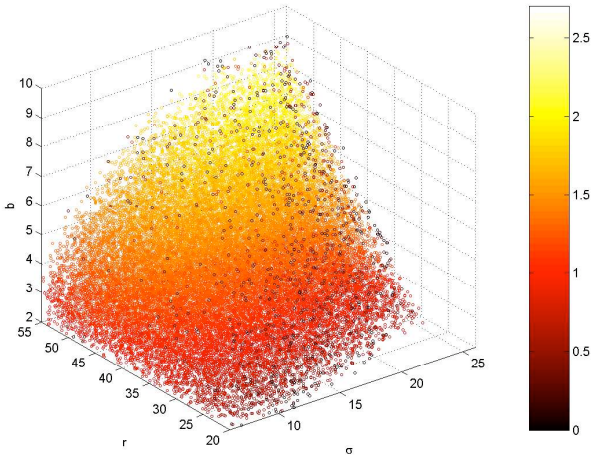

Fig. 3. Lyapunov exponents for one-hundred-thousand parameter sets tested in the displayed range of σ, r, and b. Only positive exponent values are shown as parameter sets with negative Lyapunov exponents cannot be used with our system. Approximately one-third of the sets remain.

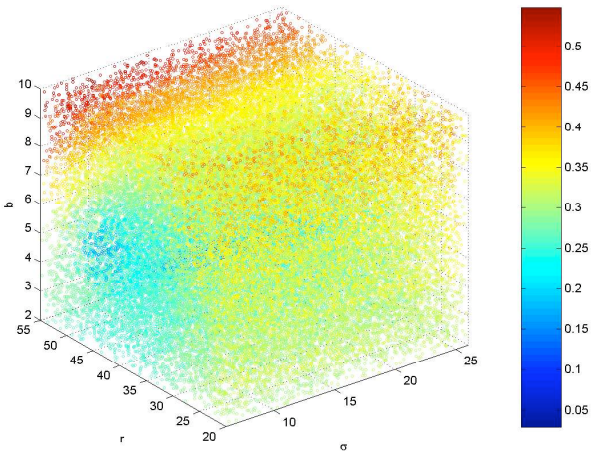

Fig. 4. Bit energies for one-hundred-thousand parameter sets tested in the displayed range of σ, r, and b. One parameter set is fixed at $\sigma = 16.0$, $r = 45.6$, $b = 4.0$ for a zero-bit. The displayed sets are candidates to represent a one-bit.

6. CONCLUSION

The bit error probability performance of our system is shown in Figure 5. By using the dual synchronizing receiver scheme and intelligently picking parameter sets to modulate with, performance has been substantially improved over previous methods.

We have discovered, while trying to ascertain the cause of bit errors for relatively large $\frac{E_b}{N_0}$, that they are largely due to characteristics of the system itself. For basic transmission schemes like BPSK, the energy in a bit is always the same and errors occur when the noise energy is large. This is not true for this chaotic scheme. It turns out that the Lorenz system occasionally goes into regions where the power of u is significantly less than the long-term average. When the bit window corresponds to these regions, the energy in those bits is less. The histograms in Figure 6 indicate the majority of errors occur when the bit energy is small rather than when the noise energy is large.

Using a discrete processing approach to explore the benefits of chaos has produced many promising results and has opened up several paths for further investigation. Discretely generating the chaotic waveforms has both helped to streamline development time and improve upon earlier systems. We continue to work towards a system that works effectively but impedes detection by a third party. We believe that such a system could be useful for camouflaged military wireless communications.

7. REFERENCES

[1] L.M. Pecora and T.L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, pp. 821–824, Feb. 1990.

[2] L.M. Pecora et al., "Fundamentals of synchronization in chaotic systems, concepts, and applications," *Chaos*, vol. 7, pp. 520–533, 1990.

[3] K.M. Cuomo, A.V. Oppenheim, and S.H. Strogatz, "Synchronization of lorenz-based chaotic circuits with applications to communications," *IEEE Trans. on Circuits and Systems*, vol. 40, pp. 626–632, Oct. 1993.

[4] H.K. Khalil, *Nonlinear Systems*, Prentice Hall, New York, second edition, 1996.

[5] S.H. Strogatz, *Nonlinear Dynamics and Chaos*, Addison-Wesley, Reading, MA, 1994.

[6] T.L. Carroll and L.M. Pecora, "Using multiple attractor chaotic systems for communication," *Chaos*, vol. 9, pp. 445–451, June 1999.

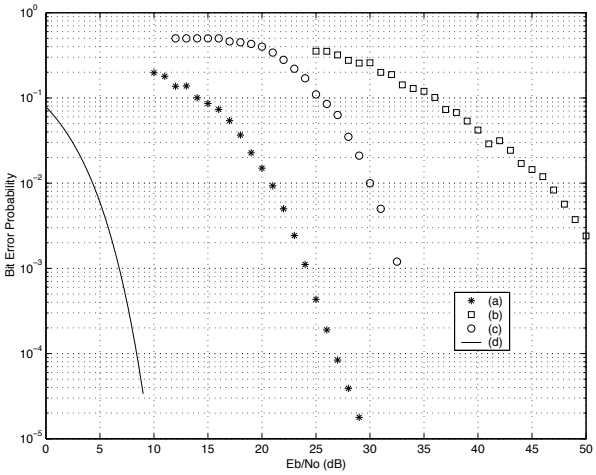

Fig. 5. Bit error probability as a function of the ratio of energy per bit E_b to noise power spectral density N_0 for several communications schemes. (a), the asterisks show the performance of our discrete system using parameter modulation techniques with a good parameter set (b), the open squares show the performance of our discrete system using the more conservative parameter mismatch used in [3] (c), the open circles show the performance of the multiple attractor system in [6] (d), the solid line shows results for baseband BPSK for comparison.

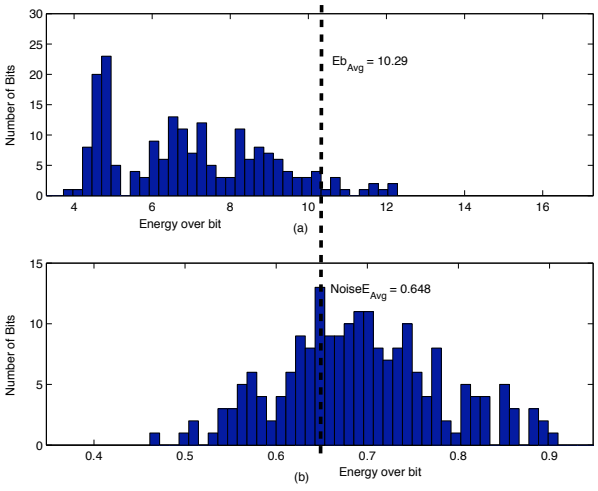

Fig. 6. Histograms of (a), bit energy and (b), noise energy for the dual synchronizing response system over 200 errors bits at $\frac{E_b}{N_0} = 29dB$. The average bit energy and average noise energy for all bits is indicated by the dashed line.