Implementation of Digital Chaotic Signal Generator with an Efficient Cross-Correlation in Wireless Communications

Ali Mohammed Noori Hasan, Lwaa Faisal Abdul Ameer

Abstract

This paper describes the digital chaotic signal with ship map design. The robust digital implementation eliminates the variation tolerance and electronics noise problems common in analog chaotic circuits. Generation of good non-repeatable and non-predictable random sequences is of increasing importance in security applications. The use of 1-D chaotic signal to mask useful information and to mask it unrecognizable by the receiver is a field of research in full expansion. The piece-wise 1-D map such as ship map is used for this paper. The main advantages of chaos are the increased security of the transmission and ease of generation of a great number of distinct sequences. As consequence, the number of users in the systems can be increased. Recent investigations show that wireless communication systems are very promising application area of chaotic dynamics. A feature of chaotic signals is super wide bandwidth; the power spectrum extends both to the region of very low frequencies as well as to high frequencies. For the proposed system, the bandwidth is extended from approximately 100 Hz to 50 MHz. The nature of chaotic signal is an aperiodic. Therefore, the resolution of the proposed system is high to provide an aperiodicity of the chaotic signal. In practice the following simulation results on MATLAB software platform show that the effectiveness of the model described which has low-cross-correlation and can meet the actual need. Simulation results show sequence length in $2^{64}$-1-bit with cross-correlation less than 0.0025 for our architecture.

Keywords

Chaotic, wireless communications, cross-correlation, ship map.

1. Introduction

In this paper we present a system that generates chaotic pseudo sequences derived from 1-D discrete map, specially the ship map. Standard chaotic pseudo sequences have limited properties in both low cross-correlation between sequences, and large sequences [1]. Chaos based communications have drawn increased attention over the past 19 years. Chaotic signals are derived from non-linear dynamic systems. They have several properties that make them attractive candidate for communications:

- Wideband spectrum.
- Waveform does not accurately repeats itself.
- Random-like appearance.
- Relatively simple analog and digital hardware implementation [2,3].

In order to be used in all applications, chaotic sequences must seem absolutely random. Therefore, we need a digital chaotic generator with good cryptographic properties, such as: balance on \{0, 1\}; long cycle length; high linear complexity; \delta-like autocorrelation; cross-correlation near to zero [15].

Chaotic systems are dynamical systems which show complex behavior. One of the defining attributes of a chaotic system is the sensitive dependence on its initial conditions [4]. The inherent capability of generating a large space of chaotic pseudo sequences due to sensitive dependence on initial conditions has been the main reason for exploiting chaos in spread spectrum communication systems. Certain one-dimensional chaotic maps exhibit this property and have been shown mathematically to provide a rich set of sequences when their output is recursively feedback into the map [5]. Chaos generators have been proposed as sources of noise-like signals in many applications. In the present work, a chaos source was needed in a wireless communications. Chaotic motion is deterministic and having an exponential dependence on initial conditions. If N is the number of first order autonomous ordinary differential equations needed to describe a dynamical system, then $N \geq 3$ in order for chaotic motion to be possible. For discrete time
invertible maps, $N \geq 2$, but for non-invertible maps, even with $N=1$ chaotic motion is possible. Typically it may occur only for certain values of the parameters or initial conditions of the system [6,7]. Chaotic systems have some major disadvantages as engineering primitives for communication systems. They are non-deterministic which make it hard to control and detect their signals. Chaotic systems are also not designable in that we do not have a principled design methodology for producing desired properties such as conforming to a given spectral envelop. In view of intrinsic randomness and strong sensitivities to initial conditions, the wireless systems evolve into the chaotic state [8].

2. Background Theory

2.1 Dynamical Systems

A dynamical System may be through of as any set of equations giving the time evaluation of the state of a system from knowledge of its previous history. A common setting is a system of $k$ first-order autonomous ordinary differential equations,

\[ \dot{x} = F(x) \quad \text{---(1)} \]

Where $x = (x^{(1)}, x^{(2)}, \ldots, x^{(k)})$ denotes $k$ state components, considered as a vector in $k$-dimensional phase space, $F(x) = (F^{(1)}(x), F^{(2)}(x), \ldots, F^{(k)}(x))$ is a $k$-dimensional vector function of $x$, and $\dot{x}$ denotes the time derivative $d\dot{x}/dt$ [10]. For the discrete time chaotic system, the chaotic sample of the $kth$ iteration is generated from a set of difference equations, i.e.,

\[ x_k = g(x_{k+1}) = g^{(k)}(x_0) \quad \text{---(2)} \]

Where $x$ is the state vector and $g(.)$ denotes the iterative function which is usually called a chaotic map [11].

Among many other interesting properties, chaotic systems possess the sensitivity to initial condition property, i.e., state trajectories corresponding to nearly initial state diverge exponentially of a chaotic system is thus fundamentally difficult, this sensitivity is actually advantageous in the estimation of past state [12]. The dynamical chaos has a number of features that make it attractive for use in communication systems as carrier or modulated oscillations. Among these features, there are generation of complicated oscillations in simple structure devices; many different chaotic modes can be controlled by small variations of the system parameters; variety of methods for putting information in the chaotic signals; self synchronization of transmitter and receiver; confidentiality of communications [13]. Symbolic dynamics is a part of the general theory of dynamical system [14]. In this paper the dynamical systems are generated by the ship map in the spaces of sequences $w = \{w_k\}$.

In the practical problems, for the given time series high dimension space is usually needed to display more information contained in the signal. This is called “phase space reconstruction”. Initial objective of phase space reconstruction was to restore chaotic attractor in the high dimension phase space. As one of the most important characteristics chaotic attractor is specific motional orbits that implies the rule of chaotic system [9].

2.2 Iterative Chaotic Function

A piece-wise linear function is a function which consist of a finite number of contiguous linear segments [1]. The proposed map for this paper which is a complex dynamics is the ship map, it is a piece-wise linear 1-D map. The dynamics of the Markov piece-wise linear chaotic map As follows [15]:

\[ x(n) = \begin{cases} 
\frac{x(n-1) + 2p}{2p}, & \text{if } 0 \leq x(n-1) < p \\
\frac{x(n-1) - 2p}{2p}, & \text{if } p \leq x(n-1) < 0.5 \\
F[1 - x(n-1)], & \text{if } 0.5 \leq x(n-1) < 1 
\end{cases} \quad \text{---(3)} \]

\[ x(n) = \begin{cases} 
\frac{x(n-1) + 2p}{2p}, & \text{if } 0 \leq x(n-1) < p \\
\frac{x(n-1) - 2p}{2p}, & \text{if } p \leq x(n-1) < 0.5 \\
F[1 - x(n-1)], & \text{if } 0.5 \leq x(n-1) < 1 
\end{cases} \quad \text{---(3)} \]
Implementation of Digital Chaotic Signal Generator with an Efficient Cross-Correlation in Wireless Communications
Ali Mohammed Noori Hasan, Lwaa Faisal Abdul Ameer

Table (1) 5-stage chaotic ship map sequence generation

<table>
<thead>
<tr>
<th>No.</th>
<th>x_n</th>
<th>X_{n+1}</th>
<th>No.</th>
<th>x_n</th>
<th>X_{n+1}</th>
<th>No.</th>
<th>x_n</th>
<th>X_{n+1}</th>
<th>No.</th>
<th>x_n</th>
<th>X_{n+1}</th>
<th>No.</th>
<th>x_n</th>
<th>X_{n+1}</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.9375</td>
<td>0.4063</td>
<td>16</td>
<td>0.25</td>
<td>0.5313</td>
<td>32</td>
<td>0.9063</td>
<td>0.3438</td>
<td>48</td>
<td>0.0313</td>
<td>0.375</td>
<td>1</td>
<td>0.4063</td>
<td>0.8438</td>
</tr>
<tr>
<td>1</td>
<td>0.4063</td>
<td>0.8438</td>
<td>17</td>
<td>0.5313</td>
<td>0.875</td>
<td>33</td>
<td>0.3438</td>
<td>0.6875</td>
<td>49</td>
<td>0.375</td>
<td>0.7813</td>
<td>2</td>
<td>0.8438</td>
<td>0.1875</td>
</tr>
<tr>
<td>2</td>
<td>0.8438</td>
<td>0.1875</td>
<td>18</td>
<td>0.875</td>
<td>0.2813</td>
<td>34</td>
<td>0.6875</td>
<td>0.5625</td>
<td>50</td>
<td>0.7813</td>
<td>0.0625</td>
<td>3</td>
<td>0.0625</td>
<td>0.0463</td>
</tr>
<tr>
<td>3</td>
<td>0.0625</td>
<td>0.0463</td>
<td>19</td>
<td>0.2813</td>
<td>0.5625</td>
<td>35</td>
<td>0.5625</td>
<td>0.8125</td>
<td>51</td>
<td>0.0625</td>
<td>0.3438</td>
<td>4</td>
<td>0.3438</td>
<td>0.1563</td>
</tr>
<tr>
<td>4</td>
<td>0.3438</td>
<td>0.1563</td>
<td>20</td>
<td>0.5625</td>
<td>0.8438</td>
<td>36</td>
<td>0.8125</td>
<td>0.125</td>
<td>52</td>
<td>0.3438</td>
<td>0.7188</td>
<td>5</td>
<td>0.1563</td>
<td>0.0</td>
</tr>
<tr>
<td>5</td>
<td>0.1563</td>
<td>0.0</td>
<td>21</td>
<td>0.8438</td>
<td>0.2188</td>
<td>37</td>
<td>0.125</td>
<td>0.1875</td>
<td>53</td>
<td>0.7188</td>
<td>0.5313</td>
<td>6</td>
<td>0.2188</td>
<td>0.0938</td>
</tr>
<tr>
<td>6</td>
<td>0.2188</td>
<td>0.0938</td>
<td>22</td>
<td>0.5625</td>
<td>0.8125</td>
<td>38</td>
<td>0.8125</td>
<td>0.0313</td>
<td>54</td>
<td>0.5313</td>
<td>0.9063</td>
<td>7</td>
<td>0.0313</td>
<td>0.4063</td>
</tr>
<tr>
<td>7</td>
<td>0.0313</td>
<td>0.4063</td>
<td>23</td>
<td>0.4063</td>
<td>0.875</td>
<td>39</td>
<td>0.875</td>
<td>0.25</td>
<td>55</td>
<td>0.9063</td>
<td>0.3125</td>
<td>8</td>
<td>0.4063</td>
<td>0.7813</td>
</tr>
<tr>
<td>8</td>
<td>0.4063</td>
<td>0.7813</td>
<td>24</td>
<td>0.875</td>
<td>0.1563</td>
<td>40</td>
<td>0.1563</td>
<td>0.0</td>
<td>56</td>
<td>0.3125</td>
<td>0.6563</td>
<td>9</td>
<td>0.1563</td>
<td>0.75</td>
</tr>
<tr>
<td>9</td>
<td>0.1563</td>
<td>0.75</td>
<td>25</td>
<td>0.8125</td>
<td>0.125</td>
<td>41</td>
<td>0.8125</td>
<td>0.75</td>
<td>57</td>
<td>0.6563</td>
<td>0.6563</td>
<td>10</td>
<td>0.125</td>
<td>0.0</td>
</tr>
<tr>
<td>10</td>
<td>0.125</td>
<td>0.0</td>
<td>26</td>
<td>0.8125</td>
<td>0.125</td>
<td>42</td>
<td>0.8125</td>
<td>0.75</td>
<td>58</td>
<td>0.6563</td>
<td>0.625</td>
<td>11</td>
<td>0.125</td>
<td>0.0</td>
</tr>
<tr>
<td>11</td>
<td>0.125</td>
<td>0.0</td>
<td>27</td>
<td>0.8125</td>
<td>0.125</td>
<td>43</td>
<td>0.8125</td>
<td>0.75</td>
<td>59</td>
<td>0.625</td>
<td>0.7188</td>
<td>12</td>
<td>0.8125</td>
<td>0.0</td>
</tr>
<tr>
<td>12</td>
<td>0.8125</td>
<td>0.0</td>
<td>28</td>
<td>0.8125</td>
<td>0.125</td>
<td>44</td>
<td>0.8125</td>
<td>0.75</td>
<td>60</td>
<td>0.7188</td>
<td>0.5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>0.8125</td>
<td>0.5</td>
<td>29</td>
<td>0.8125</td>
<td>0.125</td>
<td>45</td>
<td>0.8125</td>
<td>0.75</td>
<td>61</td>
<td>0.5</td>
<td>0.9375</td>
<td>14</td>
<td>0.8125</td>
<td>0.0</td>
</tr>
<tr>
<td>14</td>
<td>0.8125</td>
<td>0.0</td>
<td>30</td>
<td>0.8125</td>
<td>0.125</td>
<td>46</td>
<td>0.8125</td>
<td>0.75</td>
<td>62</td>
<td>0.5</td>
<td>0.9375</td>
<td>15</td>
<td>0.8125</td>
<td>0.0</td>
</tr>
</tbody>
</table>

where the position control parameter $p \in (0,0.5)$ and $x(i) \in (0,1)$. If $p=0.25$, the dynamics of the ship map is obtained in equation (4),

$$
x(n+1) = \begin{cases} 
1-2x(n-1)+0.5, & \text{if } 0 \leq x(n-1) \leq 0.25 \\
2x(n-1), & \text{if } 0.25 \leq x(n-1) \leq 0.5 \\
1-2x(n-1), & \text{if } 0.5 \leq x(n-1) \leq 0.75 \\
2x(n-1) - 0.5, & \text{if } 0.75 \leq x(n-1) \leq 1
\end{cases}
$$

These equations have a phase space which spans in the unit interval. Binary partition (0,1) for generating symbolic dynamics is shown in figure (2).

Figure (1) 5-stage chaotic ship map sequence generation

Figure (2) generating partition of ship map
3. System Implementation

3-1 Illustration: 5-stage ship map implementation

Table (1) illustrates the sequence generation by the chaotic ship map. Assume that the initial state of the register is “11110”. During operation, the system reaches the following states:

Figure (3) generating partition of 5-stage chaotic ship map

Figure (4) chaotic orbits of 5-stage chaotic ship map

In the present work, the implementation of the ship map (length of linear feedback shift register LFSR is 64) is shown in figure (5) was used.

4. System Simulation Results

Table (2) summarized results from software simulations of our system along with conventional m-, Gold, and chaotic "tent map" sequence systems. The first selection shows maximum period length and cross-correlation value for standard value for standard m-sequence with length of 215-1bits. In the second selection is the value for Gold sequence of the same length. In the third row is the value for chaotic "tent map" sequence of the same length. The bottom row shows results for the chaotic "ship map" sequence generated by the new architecture with length of 264-1. The cross-correlation properties for the current work are excellent as well. The correlation performance will improve further as sequence length is increased. This is particularly important in wireless communication systems. Auto- and cross-correlation performance of the proposed system is shown in figure (6). Figures (6-a) and (6-b) indicate that the proposed system provides approximately zero cross correlation and δ-like auto-correlation, these properties are necessary to use a chaotic signal instead of the sinusoidal signal as a carrier in the wireless communication systems and to achieve multiple-access capability. Figures (6-c) and (6-d) indicate the power spectrum extends both to the region of very low frequencies as well as to high frequencies, for the proposed system, the bandwidth is extended from approximately 100 Hz to 50 MHz, this property provide super wide spread spectrum that is necessary to provide resistant to jamming, multipath protection and low probability of interception that enhances the security property.
Table (2) Period length and cross-correlation
Comparison of various Generators with clock frequency 1GHz.

<table>
<thead>
<tr>
<th>Sequence Type</th>
<th>Period length (sec)</th>
<th>Cross-correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>m-sequence $2^{15}$-1=32767-bit with clock (50MHz)</td>
<td>0.0006553 5</td>
<td>0.06638</td>
</tr>
<tr>
<td>Gold-sequence $2^{15}$-1=32767-bit with clock (50MHz)</td>
<td>0.0006553 5</td>
<td>0.00784</td>
</tr>
<tr>
<td>Chaotic-sequence “tent map” $2^{15}$-1=32767-bit with clock (50MHz)</td>
<td>0.01495</td>
<td>0.00394</td>
</tr>
<tr>
<td>Chaotic-sequence “ship map” $2^{64}$-1=18446744073709551615-bit, with clock (1GHz) (current work)</td>
<td>184467440 73.7095</td>
<td>0.0025</td>
</tr>
</tbody>
</table>

5. Discussions and Conclusions

In the paper we propose a system for generation of long chaotic pseudo sequence of the ship map. Generation chaotic analog electronics is not feasible using standard circuit topologies. Component variation caused by imperfect fabrication causes the same divergence of output sequences as dose varying initial conditions. In wireless applications, a low-cross correlation, large sequence, low cost, super wide bandwidth and random-like appearance properties are required. Figure (6) show that the system is provided the required properties in wireless communications where the cross-correlation is less than 0.0025, δ-like.
autocorrelation and the bandwidth is extended from approximately 100 Hz to 50 MHz.

6. References