Effect of Chaos Parameters on Data Transmission via CSK under Gaussian Noise

Safaa T. M. Jawad, Zahir M. Hussain

Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq.

Abstract

In this work we present a study on the performance of chaos-shift keying (CSK) under Gaussian noise for two chaos generators with different values of chaos parameters, different initial conditions, and different values for the spreading factor (SF). The chaos generators used are the logistic map and the tent map. It is shown that a change in value of chaos parameter has more impact on BER performance than a change in initial value. Also, it is shown that logistic map is much more sensitive to a change of initial condition than tent map, making it a better candidate for secure transmission. Increasing SF will significantly improve BER performance.

Keywords: Chaos, chaos shift key, Gaussian noise.

INTRODUCTION

Recently, many researchers have been looking at methods to utilize the properties of chaos in communication systems and have actually accomplished quite remarkable results. This field of communication is called chaotic communication [1].

The chaotic signals are characterized by their wideband, impulse-like autocorrelation and low cross-correlation properties, they are considered to be useful spread-spectrum signals for carrying digital information.

The concept of chaos synchronization was first proposed theoretically by Pecora and Carroll in 1990 [1] by the fact that power spectra of chaotic systems similar to white noise; thus making them an ideal choice for carrying and hiding signals over a communication channel. This discovery is important in the field of secure communications.

Chaos-based communication systems have been shown to possess certain advantages over traditional spread-spectrum systems. The chaotic systems unlike pseudo random signals that used in conventional SS systems, which are limited in number of generated
sequences and are periodic, can theoretically produce infinite numbers of signals which are non-periodic. This merit and the wideband nature of chaotic signals make them of particular interest in secure communications [2].

Chaotic signal characterized by sensitive to initial conditions and the random-like behavior of chaotic signals in addition to their broadband spectrum, it was believed that information could be hidden efficiently in chaos. So it is impossible to predict in the long term. This merit implies that two signals from the same chaotic systems with slightly change in initial conditions diverge with increasing time and will become uncorrelated signals each other, as illustrated in the Figure 1. We can use this property to support many users per channel and places a heavy burden on unauthorized users attempting to eavesdrop.

In chaos-based communication systems, detection schemes can be broadly classified into coherent and non-coherent types. Coherent systems need to reproduce the chaotic carrier for demodulation at the receiver, whereas non-coherent systems are done solely based on received signal [3].

The basic idea of chaos communication schemes is to mix the message with a chaotic carrier in the transmitter and to send the mixed signal to the receiver, the message can be recovered by compared the transmitted mixed signal to the regenerated message-free chaotic carrier.

Accordingly, a large number of chaotic secure communication schemes have been proposed in the last decades. The leading schemes are chaotic masking where message is added directly to the chaotic carrier, chaotic modulation where the message is injected into the chaotic system to modulate the chaotic carrier, chaotic switching or CSK where a binary message is transmitted by switching between two chaotic attractors; chaotic direct sequence spread spectrum (CDSS) where a binary message is multiplied by the chaotic carrier and encrypted into a CDSS signal [4].

So, in this paper we focus on Chaos Shift Keying (CSK) which is one method of chaotic digital modulation in discrete-time. An efficient chaos generator that can be used to generate chaos shift keying (CSK) sequences is logistic map 1 (LCG1, or simply LG1) [5], where different sequences can be generated using the same generator but with different initial conditions. We used a chaotic logistic map for the generation of chaotic sequences; also used the tent map, which is another commonly used discrete chaotic map [5, 6]. The chaotic sequence generated by the tent map has been widely applied in the field of chaotic spectrum communication, encryption system chaotic optimum algorithm and so on [7]. The difference equations for generators of chaos are given as:

\[ g_{n+1} = 1 - a g_n^2 \quad \ldots \quad (1) \]

\[ f(x) = \begin{cases} 
-\frac{x_n}{a}, & x \in [0, a) \\
\frac{1-x_n}{1-a}, & x \in [a, 1]
\end{cases} \quad \ldots \quad (2) \]

The initial value \( g_0 = 0 \) for LCG1 system lies in the interval \((1, -1)\) in Equation (1).
In equation (2), the system parameter $a \in (0, 1)$ and $x_n \in (0, 1)$. When $a$ varies over $(0, 1)$, the above system becomes a non-linear dynamic system that provides chaotic behavior. The correlative properties of these maps are shown in Figures 2 and 3.

**Figure 1:** Chaotic signals are sensitive to initial conditions, the generating system is tent.

![Tent map](image)

**Figure 2:** Correlation functions of chaotic signals against Time-delay vector, the generating system is LCG1 map (a) auto-correlation (b) cross-correlation

![Auto-correlation](image) (a)

![Cross-correlation](image) (b)
Chaos shift keying

Chaotic switching which is also named chaos shift keying modulation was first proposed in [8]. In recent years, Chaos Shift Keying (CSK) has proved to offer a potential advantage over Conventional methods because its simplicity and high level of unpredictability. The simplest chaos shift keying modulation technique is to transmit one-bit information using two of chaotic generated sequences (g1 and g2) [9].

For CSK g1 and g2 (the chaotic sequences) can be produced in three different methods. First method uses two different chaotic generators. Second method uses one chaotic generator with different initial conditions. And the last method uses the same generator of chaos with identical initial condition to generate a pair of sequences multiplied by two different constants [10].

Figure 3: Correlation functions of chaotic signals against Time-delay vector, the generating system is tent map (a) auto-correlation (b) cross-correlation
For simplicity, we are dependent on the last method, where the $l$th data bit during the $l$th bit period is $(\alpha_l = +1)$ to be sent, sequences $g_1$ that it is transmitted, and if $(\alpha_l = -1)$ to be sent, sequence $g_2$ that it is transmitted.

The spreading factor (SF) is the length of chaos sequence to be sent for each binary bit. The CSK transmitter can be produce: $c_k = \alpha_l g_{v,k}$, $v$ decides which sequence chaos to be transmitted. We used in this work the pair sequences of chaos using the same chaotic generator are related as $g_2 = -g_1$ [11].

We will simulate chaos shift keying using LCG1 and tent generator and show them in secure communications under Gaussian noise with different chaos parameters and initial conditions. We are illustrating in Fig. (4) CSK generated by LCG1 map using equation (1) and tent map using equation (2) in figure (5) that used to generate chaos signal with spreading factor SF=5.

**Figure 4:** CSK system, generating system is LCG1 map with IC=0.70001, $a=2$

**Figure 5:** CSK system, generating system is Tent map with IC=0.70001 and chaos parameter $a=0.65$
Where CSK can be used under two detection schemes: Coherent detection is achieved by reproducing copies of the chaotic basis functions in the receiver; this production of replica of chaotic carriers in coherent systems is usually performed through a synchronization process and detection is achieved by correlating the incoming signal with reproduced carriers. The non-coherent systems introduce more practical forms of systems because they do not require the reproduction of chaotic carriers at the receiver side [3, 12].

To enhance the security performance under Gaussian noise, a large spreading factor can be used. We can simulation the BER performance of CSK system generated using two generators under Gaussian noise and using BER to measure the effect of channel imperfections on the transmitted signal that is obtained and the BER is calculated to determine how effective and efficient the communication is. In telecommunications, the bit error is the number of received bits of data stream over a communication channel that have been altered due to noise, interference, distortion or synchronization errors [13, 14, 15, 16]. We use spreading factor to measure the performance of security versus SNR in noisy environment.

**Performance of CSK in Multimedia**

In this section, the system was simulated with the rice image by deliberately estimating the initial condition and security parameter $a$ - emulating the process that would otherwise be used by an attacker. So, we note from Figures 6 and 7 that non-coherent CSK system is a high error than coherent CSK under Gaussian noise in LCG1.

![Figure 6: BER performance of coherent CSK under AWGN](image)

**Figure 6:** BER performance of coherent CSK under AWGN
Also, we note from the figures that illustrated below, the change in value of chaos parameter 'a' of tent map changes BER significantly and the change in initial condition of chaos (IC) has little effect. In figures (8), (10) and (12) the performance of BER of coherent CSK when the value of chaos parameter is increased, then SNR is increased and a BER is increased but large value of SF is less error as shown. In non-coherent CSK the SNR is high for different values of SF and for different values of chaos parameters with low BER in signal that high SF as illustrated in figures (9), (11) and (13). We note from this simulation that the generator tent map is best from LCG1 map in non-coherent.

Figure 7: BER performance of non-coherent CSK under AWGN

Figure 8: BER performance of coherent CSK under AWGN
Figure 9: BER performance of non-coherent CSK under AWGN

Figure 10: BER performance of coherent CSK under AWGN

Figure 11: BER performance of non-coherent CSK under AWGN
Effect of Chaos Parameters on Data Transmission via CSK under Gaussian Noise

**Figure 12:** BER performance of coherent CSK under AWGN

**Figure 13:** BER performance of non-coherent CSK under AWGN

Figures 14 and 15 illustrate performance CSK on image using LCG1 under AWGN noise with SF=3. It is clear that a small change in initial condition results into a distorted image. In tent map less distortion in image is obtained if one uses an estimate of initial condition as in Figures 16 and 17. We conclude that LCG1 is more secure than tent map in BER performance of coherent CSK and also in the non-coherent CSK because a small change in initial condition results in a totally unclear image and BER is very high.
Figure 14: Multimedia performance of the LCG1 non-coherent CSK system in AWGN environment (SF = 3) with estimated initial condition $x=0.70000000000001$.

Figure 15: Multimedia performance of the LCG1 coherent CSK system in AWGN environment (SF = 3) with exact initial condition $x=0.700001$.

Figure 16: Multimedia performance of the tent map coherent CSK system in AWGN environment (SF = 3) with exact initial condition $x=0.700001$. 
Performance of CSK using Random Data Transmission

In the previous section, we simulated the transmission data as an image. In this section we simulated random data transmission and compare between two generators as illustrated in figures below. BER performance in LCG1 is very high for a small change in initial condition (IC) as illustrated Figures 18, 19.

Figure 18: BER performance of coherent CSK under AWGN
When a small change in initial condition of chaos generator of tent map under AWGN, BER increases as illustrated in the Figures 21, 23 and 25. Also, BER is increased if chaos parameter is changed as shown in Figures 20, 22 and 24.
Effect of Chaos Parameters on Data Transmission via CSK under Gaussian Noise

**Figure 21:** BER performance of non-coherent CSK under AWGN

**Figure 22:** BER performance of coherent CSK under AWGN

**Figure 23:** BER performance of non-coherent CSK under AWGN
CONCLUSION

The performance of chaos-shift keying is extensively studied under various kinds of noise, maps, and different values of spreading factor (SF). Performance has been considered in two directions: bit error rate and security level under Gaussian noise. We conclude that changing the chaos parameter has more significant effect on BER performance than changing the initial condition of chaos generator, we found that LCG1 map is more secure than tent map in multimedia transmission.
REFERENCES


