A new approach in chaos shift keying for secure communication

Lau, Yuu; Hussain, Zahir

Lau, Y., & Hussain, Z. (2005). A new approach in chaos shift keying for secure communication. Proceedings of the Third International Conference on Information Technology and Applications, 630–633. https://doi.org/10.1109/ICITA.2005.30

Published Version: https://doi.org/10.1109/ICITA.2005.30

A New Approach in Chaos Shift Keying for Secure Communication

Yuu-Seng Lau and Zahir M. Hussain
School of Electrical and Computer Engineering, RMIT University
124 La Trobe Street, Melbourne, Victoria 3000, Australia
Emails: s9701549@student.rmit.edu.au, zmhussain@ieee.org

Abstract

A chaotic sequence for chaos shift keying (CSK) that provides auto- and cross-correlation properties (that are similar to those of random white noise) is used for spread spectrum systems. Due to its bifurcation behavior (depending on the initial condition), the number of chaotic sequences that can be generated by a single formula is not restricted and will not repeat itself. These characteristics provide an increase in system capacity and security performance. The paper presents a study of two different commonly used chaotic logistic maps and a modified chaotic logistic map for CSK spread spectrum system. The newly modified logistic map provides similar bits error rate (BER) performance to the best logistic map. Yet, it also provides an additional chaotic parameter for the control of its dynamic property, hence increasing the system security and capacity.

1. Introduction

The principle of spread spectrum (SS) systems is to spread the original information over a broad bandwidth of frequencies. These systems rely on the spreading sequence to provide a white noise like auto- and cross correlation property. Conventionally, a pseudorandom or a pseudo-noise (PN) sequence generator is used for SS systems, but it suffers from the periodicity problem. Because the generation of the pseudorandom sequence, which is a fixed number of states where the state-machine run through each state in a deterministic manner. The periodicity behavior of pseudorandom sequence compromises the overall system security, and reduces the system capacity as well.

Due to intensive research in modelling non-linear dynamical systems using deterministic linear methods, which has made it possible to use chaos theory in this arena. The introduction of these non-linear chaos theories has offered several new applications and performance enhancements to exiting communication systems. A chaotic generator is an unlimited states state-machine, therefore it can produce non-linear and non-repeating sequences. It is very hard to predict chaotic patterns and sequences even when the chaotic function is known to the interceptor. This is because the chaotic function provides a bifurcation behavior, hence a different estimation of the initial condition will lead to a very different chaotic sequence. As a result, This non-linear and non-periodic behavior of the chaotic generator offers potential advantage over conventional pseudo-noise based system in terms of security, synchronization and system capacity of a SS communication. Since synchronization was solved by Pecora and Carroll in 1990 [1], there have been increasing numbers of proposed schemes that utilize chaos theory in SS communication for both analog and digital systems. Such schemes include but are not limited to chaotic masking, chaos modulation, chaos shift keying (CSK), and chaotic CDMA sequence.

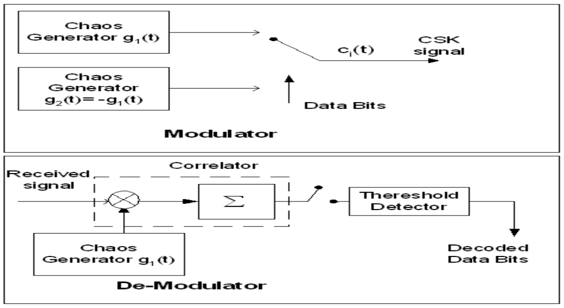

Figure 1. Modulator and demodulator block diagram for chaos shift keying

In this paper, we propose a modified logistic chaotic map for CSK spread spectrum communication and compare it with two different logistic chaotic maps.

2. Chaos Shift Keying (CSK)

The simplest one-bit information chaos shift keying (CSK) modulation scheme for SS systems uses a pair of chaotic sequences (g_1 and g_2) with different bit energies to transmit the binary information For the data bit($\alpha_l = +1$) during the lth bit period, g_1 sequence is radiated from the transmitter , and for the ($\alpha_l = -1$), g_2 sequence is transmitted. The number of chaotic symbol transmitted for one data bit is dependent on the spreading factor (2β). The output of the CSK transmitter is $s_k = \alpha_l g_{v,k}$, v decides which chaos sequence to be send.

The chaotic sequence for CSK g_1 and g_2 can be generated in three different ways. First method: it uses two different chaotic generators. Second method: generating the two sequences using different initial conditions of the same chaotic generator. Third method: the two sequences are generated by the same chaotic generator and same initial condition but multiplied by two different constants. For simplicity, we used the last method to generate two chaotic sequences $g_2 = -g_1$, as shown in Fig. 1. The demodulation can be performed by a correlator at the receiver, as shown in Fig. 1.

The performance of the CSK system in an AWGN environment can be derived following the method used in [2]. For a correlator type receiver, the correlator output for the lth bit y_l is given by $y_l = \sum_{k=kk}^{2\beta l} r_k g_k, kk = 2\beta(l-1)+1$ $r_k = s_k + \eta_k$ is the received signal in an AGWN environment. η_k is an additive Gaussian white noise.

$$y_l = \alpha_l \sum_{k=2\beta(l-1)+1}^{2\beta l} g_k^2 + \sum_{k=2\beta(l-1)+1}^{2\beta l} \eta_k g_k \qquad (1)$$

The first term is the required signal and second term is noise. If we consider a sum of a large number of random variables in the system, we can assume the system to follow a normal distribution (Central Limit Theorem). The probability of error is

$$\begin{aligned} \text{BER}_{CSK} &= \text{Prob}(\alpha_l = 1) \times \text{Prob}(y_l \leq 0 \mid \alpha_l = 1) \\ &+ \text{Prob}(\alpha_l = -1) \times \text{Prob}(y_l > 1 \mid \alpha_l = -1) \\ &= \frac{1}{4}[\text{erfc}(\frac{\text{E}[y_l \mid (\alpha_l = +1)]}{\sqrt{2\text{var}[y_l \mid (\alpha_l = +1)]}}) \\ &\quad + \text{erfc}(\frac{-\text{E}[y_l \mid (\alpha_l = -1)]}{\sqrt{2\text{var}[y_l \mid (\alpha_l = -1)]}})] \qquad (2) \end{aligned}$$

From [2], the variance of $y_l \mid (\alpha_l = +1)$ equals the variance of $y_l \mid (\alpha_l = -1)$ and the $\text{E}[y_l \mid (\alpha_l = +1)] = -\text{E}[y_l \mid (\alpha_l = -1)]$. Hence, equation (2) can be simplified to

$$\begin{aligned} \text{BER}_{CSK} &= \frac{1}{4}[\text{erfc}(\frac{\text{E}[y_l \mid (\alpha_l = +1)]}{\sqrt{2\text{var}[y_l \mid (\alpha_l = +1)]}}) \\ &\quad + \text{erfc}(\frac{\text{E}[y_l \mid (\alpha_l = +1)]}{\sqrt{2\text{var}[y_l \mid (\alpha_l = +1)]}})] \\ &= \frac{1}{2}[\text{erfc}(\frac{\text{E}[y_l \mid (\alpha_l = +1)]}{\sqrt{2\text{var}[y_l \mid (\alpha_l = +1)]}})] \qquad (3) \end{aligned}$$

where erfc(.) is the complementary error function defined as $\text{erfc}(\psi) \equiv \frac{2}{\sqrt{\pi}} \int_{\psi}^{\infty} e^{-\lambda^2} d\lambda$.

For AWGN environment, we know that the mean $\text{E}[\eta_k] = 0$. As a result, the mean of $y_l \mid (\alpha_l = +1)$ is

$$\begin{aligned} \text{E}[y_l \mid (\alpha_l = +1)] &= \sum_{k=2\beta(l-1)+1}^{2\beta l} \text{E}[g_k^2] \\ &+ \sum_{k=2\beta(l-1)+1}^{2\beta l} \text{E}[\eta_k]\text{E}[g_k] \\ &= 2\beta P_s \qquad (4) \end{aligned}$$

The average power of the chaotic signal is $P_s = \text{E}[g_k^2]$. The variance of $y_l \mid (\alpha_l = +1)$ is

$$\begin{aligned} \text{var}[y_l \mid \alpha_l = +1] &= 2\text{cov}[\sum_{k=2\beta(l-1)+1}^{2\beta l} g_k^2, \sum_{k=2\beta(l-1)+1}^{2\beta l} \eta_k g_k] \\ &+ \text{var}[\sum_{k=2\beta(l-1)+1}^{2\beta l} \eta_k g_k] \\ &+ \text{var}[\sum_{k=2\beta(l-1)+1}^{2\beta l} g_k^2] \qquad (5) \end{aligned}$$

From [2] we know that

$$\begin{aligned} 2\text{cov}[\sum_{k=2\beta(l-1)+1}^{2\beta l} g_k^2, \sum_{k=2\beta(l-1)+1}^{2\beta l} \eta_k g_k] &= 0 \\ \text{var}[\sum_{k=2\beta(l-1)+1}^{2\beta l} \eta_k g_k] &= \beta N_o P_s \\ \text{var}[\sum_{k=2\beta(l-1)+1}^{2\beta l} g_k^2] &= 2\beta\Lambda \end{aligned}$$

where $\Lambda = \text{var}[g_k^2]$. Hence

$$\text{var}[y_l \mid \alpha_l = +1] = 2\beta\Lambda + \beta N_o P_s. \qquad (6)$$

Substituting (4) and (6) into (3), the BER for the CSK can be found as follows

$$\begin{aligned} \text{BER}_{CSK} &= \frac{1}{2}\text{erfc}(\frac{2\beta P_s}{\sqrt{4\beta\Lambda + 2\beta N_o P_s}}) \\ &= \frac{1}{2}\text{erfc}(\frac{1}{\sqrt{\frac{\Lambda}{\beta P_s^2} + \frac{N_o}{E_b}}}) \qquad (7) \end{aligned}$$

where $E_b = 2\beta P_s$. From equation (7), the BER can be improved by reducing the variance of $g_k^2 (= \Lambda)$, increasing the spreading factor (2β), or increasing the signal power P_s (the $\text{E}[g_k^2]$).

3. Chaos Sequence

For simplicity, one dimension chaotic logistic map is studied in this section. To obtain the BER performance for each logistic map, the signal power P_s and the variance Λ are either calculated from their probability density function (pdf) or numerically.

3.1. Logistic Map 1

One of the simplest chaotic logistic maps used for generation chaotic sequences is given by [2, 3]

$$g_{n+1} = 1 - 2g_n^2 \tag{8}$$

which has the invariant probability density function [2, 4]

$$\rho(g) = \begin{cases} \frac{1}{\pi\sqrt{1-g^2}} & \text{, if } \mid g \mid < 1 \\ 0 & \text{, otherwise} \end{cases} \tag{9}$$

Since $\rho(g)$ is an even function, the mean value $\mathrm{E}[g_k]$ is

$$\mathrm{E}[g_k] = \int_{-\infty}^{\infty} g\rho(g)dg = \int_{-1}^{1} g\rho(g)dg = 0 \tag{10}$$

and the auto-covariance of $\{x_k\}$ is equal to zero [2]

$$\mathrm{cov}[g_i, g_k] = E[g_j, g_k] - E[g_j]E[g_k] = E[g_j g_k] = 0. \tag{11}$$

Hence P_s and Λ can be manually calculated

$$P_s = \mathrm{E}[g_k^2] = \int_{-\infty}^{\infty} g^2\rho(g)dg = \int_{-1}^{1} g^2 \frac{1}{\pi\sqrt{1-g^2}}dg = \frac{1}{2} \tag{12}$$

$$\Lambda = \mathrm{var}[g_k^2] = \mathrm{E}[g_k^4] - \mathrm{E}^2[g_k^2] = \int_{-1}^{1} g^4\rho(g)dg - \frac{1}{4} = \frac{1}{8} \tag{13}$$

The BER performances for this logistic map are shown in Figs. 2 - 5.

3.2. Logistic Map 2

Another dynamic system capable of exhibiting chaos used in spreading spectrum is proposed in [5]

$$g_{n+1} = ag_n(1 - g_n) \tag{14}$$

where a is the bifurcation parameter or control, considered to be in the interval $3.57 < a \leq 4$ for the system to be a non-period chaos system.

Table 1. Statistics of M - Logistic Map 2

a	$\mathrm{E}[g_k^2]$ or P_s	Λ
4	$\frac{1}{2}$	$\frac{1}{8}$
3.97	$\frac{9}{20}$	0.111
3.95	0.410	$\frac{1}{10}$
3.90	0.392	0.095

Since logistic map 2 provides a bifurcation parameter, it increases the system security. The attacker needs to know both the initial condition and the bifurcation parameter value a before it can demodulate the transmitted information. The drawback of this system is the output of the above sequence lies in the interval $0 \leq g_n \leq 1$, which will decrease the P_s and lead to a lower BER performance. The probability density function for this system is not provided. Numerical simulation is used to obtain $P_s = \frac{3}{8}$ and $\Lambda = 0.1333$ when $a = 4$. The BER performance for this logistic map is shown in Figs. 2 - 5 for different spreading factors. A modified version of this logistic is proposed in next section which is shown to have a higher value of P_s and a lower value for Λ.

3.3. Modified Logistic Map 2 (M-Logistic)

Modified logistic map 2 is a scaled and shifted version of the logistic map 2.

$$\begin{aligned} g_{n+1} &= ag_n(1 - g_n) \\ j_{n+1} &= 2(g_{n+1} - 0.5) \end{aligned} \tag{15}$$

where j_n is the output chaotic sequence for CSK and a is the bifurcation parameter or control, considered to be in the interval $3.57 < a \leq 4$. Again, the probability density function for this system is not provided. Numerical simulation is used to obtain P_s and Λ for different values of a.

From Table 1, the BER can be calculated using equation (7). The BER performances for this logistic map are shown in Figs. 2- 5.

Figs. 2 - 5 show that logistic map 1 and M-logistic map 2 with $a = 4$ provide same BER. However, M-logistic map 2 can enhance the security due to its extra bifurcation parameter a, although it still provides a BER performance close to logistic map 1.

Similar to the initial condition case, the parameter a for logistic map 2 and M-logistic map 2 need to be precise. A slight difference in these parameters will generate totaly different chaotic sequences. Hence, this will provide an extra parameter for security enhancement. This extra bifurcation parameter a not only acts to enhance security but it also can be used as a multi-user and a synchronization parameter.

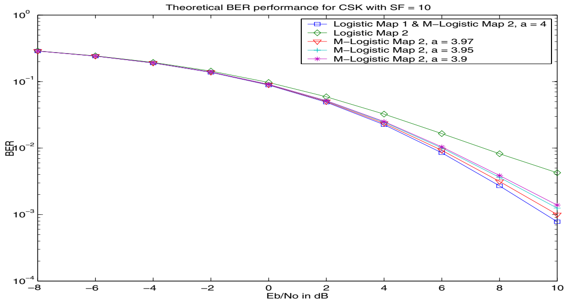

Figure 2. Theoretical BER performance for different CSK logistic maps with SF = 10

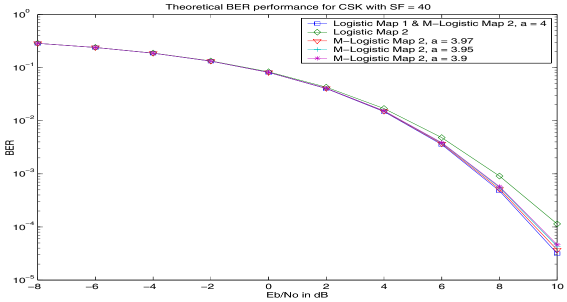

Figure 3. Theoretical BER performance for different CSK logistic maps with SF = 40

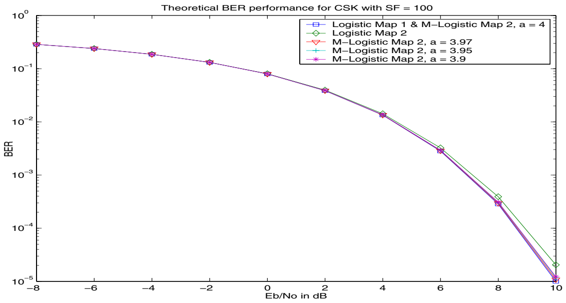

Figure 4. Theoretical BER performance for different CSK logistic maps with SF = 100

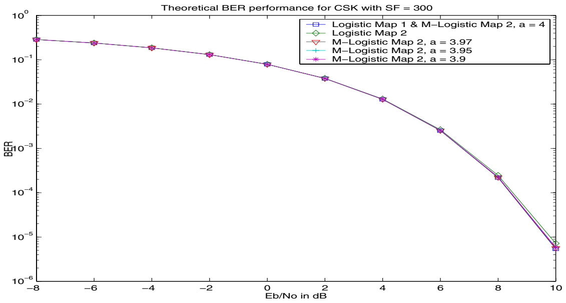

Figure 5. Theoretical BER performance for different CSK logistic maps with SF = 300

In general, an increase in the spreading factor will provide better BER performance. However, when the spreading factor is at a higher value range (larger than 100), the BER performance curves of the three logistic maps approach each other.

4. Conclusion

We proposed a modified logistic chaotic map for chaos-shift-keying (CSK) spread spectrum communication and compared it with two different logistic chaotic maps. It is shown that the proposed scheme provides BER performance close to the optimum performance. In addition, it provides an extra parameter for better security performance. This parameter can also be used for other purposes such as synchronization in a multi-user environments.

References

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

[2] F. C. M. Lau, C. K. Tse, M. Ye, and S. F. Hau, "Coexistence of chaos-based and conventional digital communication systems of equal bit rate", *IEEE Trans. Circuits Syst. I*, vol. 51, No.2, Feb. 2004, pp. 391-408.

[3] S. S. Rao, and S. P. Howard, "Correlation performance of chaotic signals in spread specturm systems", in *Proc. IEEE Digital Signal Processing Workshop*, Sept. 1996, pp. 506-509.

[4] T. Kohda, and A. Tsuneda, "Even- and odd-correlation fucntions of chaotic chebyshev bit sequences for CDMA", in *Proc. IEEE Int. Symp. Spread Specturm Technology and Applications*, 1994, pp. 391-395.

[5] G. Heidari-Bateni, and C. D. McGillem, "A chaotic direct-sequence spread-specturm communication system", *IEEE Trans. Communications*, vol. 42, Issue 234, Feb/Mar/Apr. 1994, pp. 1524 - 1527.