Chaotic Secure Communication in Rayleigh fading channel

A Elkouny, N. Zakria, M. I. Sobhy

The Electronics Engineering Department, University of Kent at Canterbury

Canterbury, Kent, CT2 7NT, UK

Abstract: This paper presents an encryption algorithm that can be used for text messages, images and recorded voice with high security. The proposed algorithm is then applied to secure communication using a new approach for constructing two chaotically synchronized systems in the presence of a multipath Rayleigh fading channel. The results reveal that synchronization and a signal to chaos ratio of -252dB have been achieved..

1 Introduction

In typical communication systems, based on chaos synchronization schemes, the information to be transmitted is carried from the transmitter to the receiver by a chaotic signal through an analogue channel. The decoding of the information signal in the receiver can be carried out by means of either coherent or non-coherent demodulation schemes. Following these approaches different methods have been developed to mask the contents of a message using chaotic signals [1]. However, it has been shown that most of these methods are not secure because one can extract the encoded message from the transmitted chaotic signal using different unmasking techniques [2]. To overcome the problem of unmasking the information message from the chaotic carrier, different approaches for designing cryptosystems have recently been introduced [3]. In these schemes both conventional cryptographic methods and synchronization of chaotic systems are combined so that the level of security of the transmitted signal is enhanced. Typically these approaches are based on the synchronization of simple chaotic systems. But chaotic synchronization is in general sensitive to additive noise and to channel delay. By the use of binary modulation methods, where the binary data (-1 or +1) is modulated by multiplying it with a chaotic spreading signal, we can to some extent, overcome the channel noise. Following this technique, we must put into consideration that low dimension chaos has a distinct pattern which allows a third party to extract the information easily by constructing a return map [2-3]. This suggests the use of high dimensional chaos and the development of a very tight encryption algorithm in order to enhance the security. In these previous chaos communications systems, the communication channel has not been yet fully addressed. In this paper we consider the problem of combating different channel distortions like time varying fading and multi-path with very high security. In the following section we will illustrate the encryption algorithm then we will address the synchronization problem. Finally, the communication system is detailed with the results that demonstrate the power of the developed system.

2. Lorenz encryption algorithm.

One of the main reasons that previous results have a limitation on the signal to chaos ratios is that the receivers use differentiators to decrypt the signal. Differentiators will always produces large spikes and high error if the signal contains discontinuities, which is always the case for images and text signals. To overcome the above problem the derivative of a state variable is used as the transmitted signal rather than the state variable itself. This has the advantage avoiding differentiation in the receiver. The derivative dx_2/dt is of course readily available in the transmitter before integrating the second equation. The transmitter equations are given by.

$$\begin{aligned} x_1 &= \mathrm{A}_1 \int x_2 - x_1 \,\mathrm{dt} \\ x_2 &= \int \mathrm{A}_2 x_1 - x_2 - \mathrm{S}_1 x_1 x_3 + \mathrm{A} v_{in} \,\mathrm{dt} \qquad (1) \\ x_3 &= \int \mathrm{S}_2 x_1 x_2 - \mathrm{A}_3 x_3 \,\mathrm{dt} \end{aligned}$$

Where the v_{in} is the information signal and S_1, S_2 are scaling factors. This results in the information not being a simple addition to the transmitted signal. The information is also multiplied by a constant A to reduce its value with respect to the chaotic signal. We shall present results where $A = 10^{-13}$ which results in a signal to chaos ratios of about -245dB. The receiver system is given by.

$$x_1 = \mathrm{A}_1 \int x'_2 - x'_1 \, \mathrm{dt}$$
$$v_{out} = \frac{1}{\mathrm{A}} \left(\frac{dx_2}{dt} - A_2 x'_1 + x'_2 + \mathrm{S}_1 x'_1 \, x'_3 \right) \quad (2)$$
$$x'_3 = \int \mathrm{S}_2 x'_1 \, x'_2 - \mathrm{A}_3 x'_3 \, \mathrm{dt}$$

Where v_{out} is the recovered information signal and dx_2/dt is the received signal.

3. Synchronization approach.

Our aim in this section is to achieve synchronization between the transmitter and the receiver in the presence of a time delayed channel and where to insert the encryption keys in the Lorenz chaos generator. These generator keys must be chosen in a way that will not affect the chaotic generator and simultaneously attains the optimum needed security. Integration in its discreet form can be represented as shown in Figure 1 and equation (3).

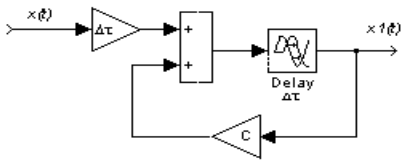


Figure 1. Discreet integrator.

$$x_1(t) = x\ (t - \Delta t)\Delta t + \mathrm{C} x_1(t - \Delta t)$$
$$x(t - \Delta t) = \frac{x_1(t) - \Delta x_1(t - \Delta t)}{\Delta t} \quad (3)$$
$$\text{If } \mathrm{C} \approx 1 \quad \text{then} \quad x(t - \Delta t) = \frac{\Delta x_1}{\Delta t}$$

The main advantage of replacing the integrators of the Lorenz chaotic model with the above-mentioned blocks is that the transmitter will not transmit any signal unless there is an initiator, which is represented by the information signal. Consequently, the receiver is waiting an encrypted signal to initiate it. Lorenz transmitter and receiver subsystems are shown in Figures 2 and 3.

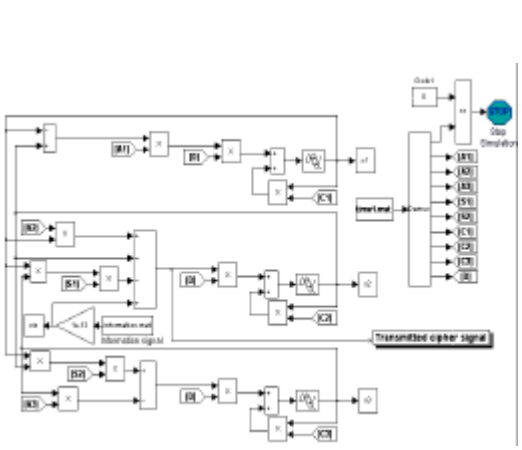


Figure 2. Lorenz transmitter subsystem.

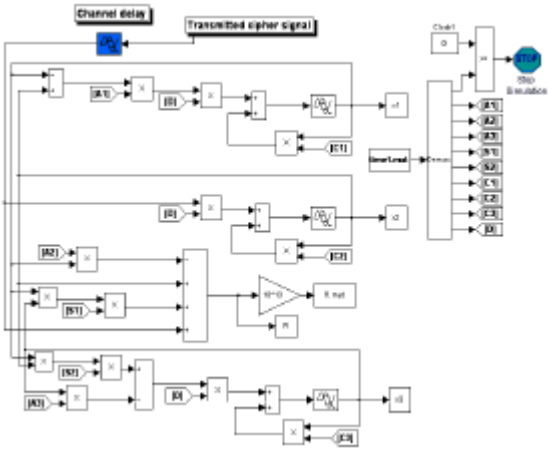


Figure 3. Lorenz receiver subsystem.

4. CDMA communication system

The most important properties of Spread spectrum communication are its multiple access capability, multipath interference rejection and narrow band interference rejection [4]. In CDMA the modulated information-bearing signal (the data signal) is directly modulated by a digital signal. The receiver correlates the received signal with a synchronously generated replica of the code signal to recover the original information-bearing signal. This implies that the receiver must know the code signal used to modulate the data. The data signal can be either an analogue signal or a digital one. In our case it will be a digital signal. The code signal, which is a noise-like sequence, consists of a number of code bits that can be either '+1' or '-1'. The most important demand for the development of suitable codes is to have a low cross-correlation between the codes assigned for different users and to have local autocorrelation in order to well synchronize and lock the locally generated code signal to the received signal. To obtain the desired spreading of the signal the bit rate of the code signal must be much higher than that of the information signal. Several families of binary PNcodes exist as m-sequences, Gold codes and Kasami sequences [4-5]. In the transmitter part of our developed communication system, the encrypted signal is binary coded then transformed into bipolar (+1, -1). After that, the data signal is multiplied by the Kasami sequences as shown in Figure 5.

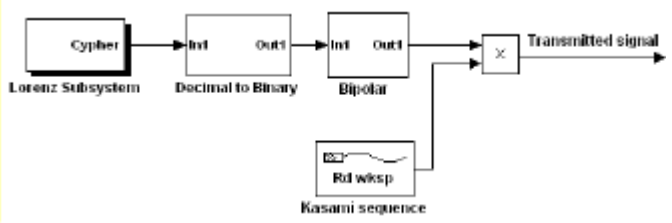


Figure 5. Transmitter part.

For the receiver part, we have developed two models depending on the value of the Doppler frequency. If the Doppler frequency is less than or equal to 1 Hz then we can use the simpler receiver shown in Figure 6.

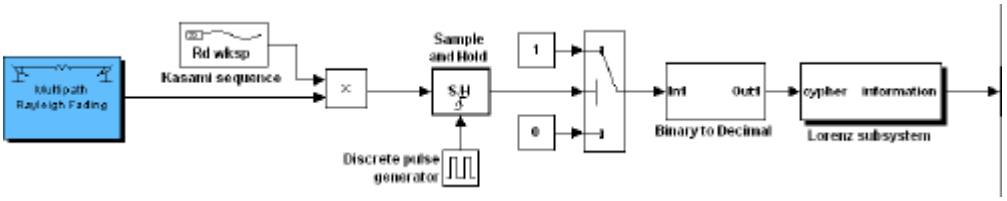


Figure 6. Simpler version of the receiver.

While for higher Doppler frequency, we have constructed a more complicated one shown in Figure 7. Using Rayleigh channel with Doppler frequency 5 Hz and two delay vectors equal to 0.01 and 0.02 the experiment results are shown in Figure 8.

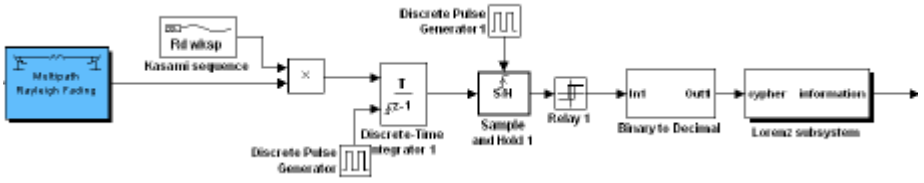


Figure 7. Complex version of the receiver.

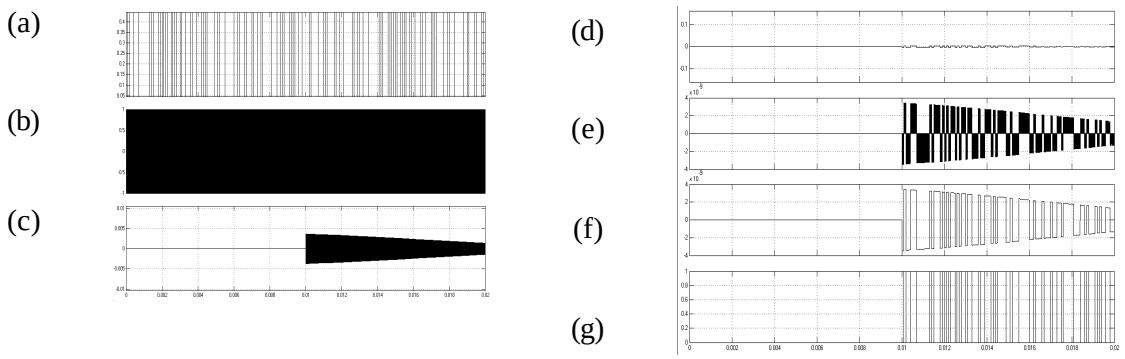
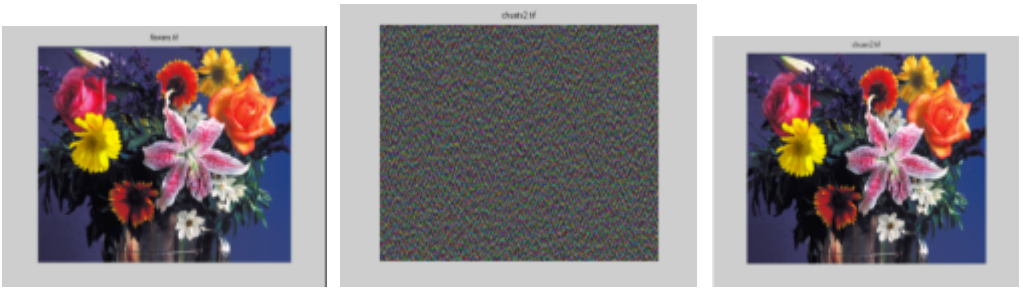


Figure 8. (a) The ciphered binary signal, (b)The spreading signal, (c) Received signal from Rayleigh channel with Doppler frequency = 5 Hz, (d) Received signal after being multiplied by the Kasami code in the receiver part, (e) After discrete time integrator, (f) After sample and hold and finally (g) after the relay .

Three very important features are observed in this system. The first is its ability to transmit very low signal to chaos ratio and to recover the information without any loss. Signal to chaos ratios between -220 dB and -261dB have been achieved depending on the complexity of the information signal. The second is that any error in each of the cipher keys of order 10^{-16} of its original value will not recover the information signal. Figure 9 shows a JPEG image transmitted then recovered at -256 dB signal to chaos ratio. The third important feature that this system can be used as a base for multi-channel communication system.



(a) (b) (c)

Figure 9. The original JPEG image (a), the encrypted (b) and the recovered image (c).

5. Conclusion

In this work, an approach has been developed to resolve the chaotic synchronization in the presence of a multipath Rayleigh fading channel and its application to secure communications. This proposal utilizes modified discrete integration to overcome the synchronization problem. The developed model can be used for text, images and voice signals with extremely high security. Results confirm the proposed scheme's effectiveness.

References.

[1] Chang-song Zhou, Yian-lun Chen, Robust communication via chaotic synchronization based on contraction maps, Phys. Rev. Lett. A, vol. 225, pp. 60-66, 1997.

[2] Tao Yang, Lin-Bao Yang, Chun-Mei Yang, Breaking chaotic secure communication using a spectrogram, Phys. Rev. Lett. A, vol. 247, pp. 105-111, 1998.

[3] Migkai Nan, Chak-nam Wong, Kim-fung Tsang, Xiangquan Shi, Secure digital communication on linearly synchronized chaotic maps, Phys. Rev. Lett. A, vol. 268, pp. 61-68, 2000.

[4] Ramjee Prasad, CDMA for Wireless Personal Communications, Artech House, 1996.

[5] J. Viterbi, CDMA: Principles of Spread Spectrum Communication. Addison-Wesley, 1995.