Chaotic Modeling and Simulation (CMSIM) 1: 223-230, 2013

Robustness and Bit Error Rate Performance of Qi Hyper Chaos Based Encryption

Guoyuan Qi[1], Dennis Luke Owuor[1] and André E. Botha[2]

[1] Department of Electrical Engineering
Tshwane University of Technology, Pretoria, South Africa
E-mail: qig@tut.ac.za, dennisluke11@yahoo.com
[2] Department of Physics
University of South Africa, Pretoria, South Africa
E-mail: bothaae@unisa.ac.za

Abstract. Recently, in the field of telecommunication, chaotic encryption has drawn much attention because of its ease in design and implementation over conventional encryption methods. In this paper, chaos shift keying (CSK) models are designed based on Qi hyper-chaos. The efficiency and effectiveness of the developed models are evaluated using the bit error rate. By using power spectrum analysis and low pass filtering techniques, the robustness of CSK based on Qi hyper-chaos over CSK based on the Lorenz chaotic system is verified. The results show that the robustness and bit error rate performance of encryption based on Qi hyper-chaos is much better than that based on Lorenz chaos.
Keywords: Chaos, Encryption, Hyper-chaos, BER, CSK.

1. Introduction

Telecommunication as a field has tremendously grown in the last decade. Associated with this growth, is the requirement for efficient and effective secure communication methods [1]. One method of making data secure is through encryption and decryption. Over the past few years, methods of chaotic encryption have developed enormously, and several chaotic systems, such as the Lorenz, Chen and Rössler systems, have been proposed [2-5]. These systems have been employed for encryption and decryption of message signal, image and video during communication. In this context there are a number of different chaotic encryption methods that have been employed for encryption and decryption, for example, chaos synchronization, chaos shift keying and chaotic masking.

Traditional encryption schemes based on integer number theory have been studies for a long time and are considered to be reliable. In contrast, the security of chaotic communication schemes often relies on a mixture of analytic methods and intuition. Encryption and cryptanalysis using chaotic dynamics is a

Received: 30 March 2012 / Accepted: 23 September 2012

ISSN 2241-0503

relatively new field that has only been intensively researched on for less than a decade.

This paper aims to demonstrate the robustness and bit error rate performance of digital message signal encryption based on Qi hyper-chaos systems compared to message signal encryption based on Lorenz chaotic system.

2. Comparison between the Qi hyper-chaotic system and the Lorenz chaotic system

Many proposed chaos-based secure encryption have been totally or partially broken by different attacks [6, 7]. This section provides a detailed comparison between Qi hyper-chaos and the Lorenz chaotic system in terms of their randomness and disorder.
The nonlinear dynamic model representing Qi hyper-chaos is given by [8, 9]:

$$\begin{aligned} \dot{x}_1 &= a(x_2 - x_1) + x_2 x_3 \\ \dot{x}_2 &= b(x_1 + x_2) - x_1 x_3 \\ \dot{x}_3 &= -cx_2 - ex_4 + x_1 x_2 \\ \dot{x}_4 &= -dx_4 + fx_3 + x_1 x_2 \end{aligned} \tag{1}$$

Here $x_i \ (i = 1, 2, 3, 4)$ are the state variables and a, b, c, d, e, f are positive constant parameters. The well-known Lorenz system is given in Ref. [10].
The basic comparisons of the dynamic property between Qi hyper-chaos and Lorenz chaotic system are summarized in the next paragraph [8].

The attractor of Qi hyper-chaotic system exhibits a very irregular and disordered form unlike the butterfly shape produced by the Lorenz chaotic system. The Stochastic distribution of Qi hyper chaos is very similar to that of Gaussian white noise but that of Lorenz has three peaks at its trajectory is unlike Gaussian white noise. Qi hyper-chaotic signal is much more sensitive to initial condition than the Lorenz chaos and other hyper-chaos. With these rich advantages of Qi hyper chaos over Lorenz chaotic system, as demonstrated in [8], there is a need to explore the effects implementing the system for encryption of messages.

3. Qi-Hyper-Chaos-Shift Keying Encryption

3.1 Method 1: Non-Coherent Decryption Based on Bit-Energy Estimation

In this encryption scheme two hyper-chaotic signals are used to encrypt the message signal at the sending end and decryption is done at the receiving end based on energy bit estimation [11, 12].

Two chaos generators produce signals $c_1(t)$ and $c_2(t)$, respectively. During the bit duration, i.e. $[((l-1)T_b),\ lT_b]$, if a binary "+1" is about to be sent, $c_1(t)$ is transmitted, and if "−1" is about to be sent, $c_2(t)$ is transmitted.

The encrypted signal $r(t)$ is then sent through a channel of communication. Thus

$$r(t) = s(t) + \xi(t) \tag{2}$$

where $\xi(t)$ is the noise signal added to the sent signal during communication.

The decryption method used is called non-coherent demodulation based on an energy bit estimator. Decryption is done based on some distinguished characteristics of the signal transmitted. The property used in this paper is the bit energy, which is deliberately made different for different symbols in the encryption process.

A Qi hyper-chaos generator is used to produce two chaotic signals; the first chaotic system is assigned different value, i.e. $c_1(t) + M$, where M is the value assigned to separate with $c_2(t)$. At the receiving end the bit energy can be estimated by a square and integration process.

Let energy per bit be $y(lT_b)$. When the energy bit $y(lT_b) > T_h$ then binary "+1" was send, otherwise binary "-1" was send, where $T_h > 0$ is threshold value.

The simulation results of non-coherent demodulation based on bit-energy estimation are shown in Fig. 1, which demonstrates successful performance of encryption and decryption.

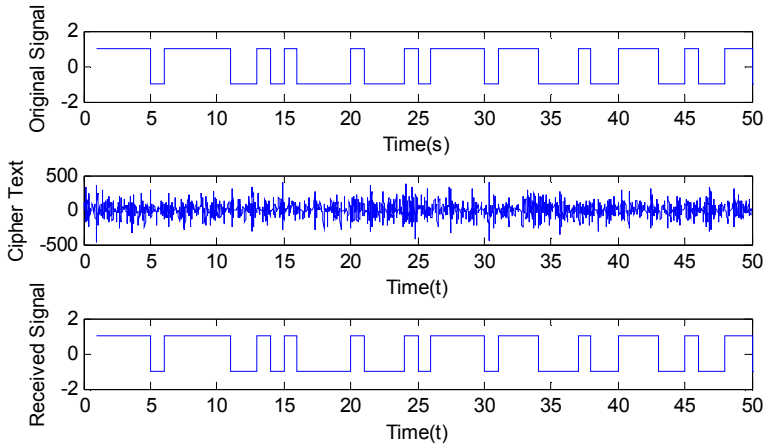

Fig. 1. Qi-Hyper-Chaos-Shift Keying Encryption and decryption

3.2 Method 2: Coherent Demodulation Based on Correlation

The process of correlation is where the "likeness" between two chaotic signals is evaluated. In this method two correlators are employed to evaluate the correlations between the received signal and the two recovered chaotic signals. The outputs of the correlators for the *l*th bit are given by

$$y_1(lT_b) = \int_{(l-1)T_b}^{lT_b} r(t)c_1'(t)\,dt \tag{3}$$

$$y_2(lT_b) = \int_{(l-1)T_b}^{lT_b} r(t)c_2'(t)\,dt \tag{4}$$

where $c_1'(t)$ and $c_2'(t)$ are synchronizations of $c_1(t)$ and $c_2(t)$, respectively. The following equation is used to determine the output to the threshold detector.

$$y_0(lT_b) = y_1(lT_b) - y_2(lT_b) \tag{5}$$

If the output $y_o(lT_b)$ is greater than T_h then +1 was sent, otherwise -1 was sent.

The process of encryption is the same as that of Method 1, but the decryption process takes place with the aid of synchronizations. The decryption proceed by evaluating the correlation of the transmitted signal and the regenerated chaotic carrier as in Eq. (3) and eq. (4), and followed by energy bit calculation then compared in Eq. (5). If the output is greater than the value specified at the threshold then "+1" is decoded otherwise "−1" is decoded.

The simulation results of correlation-type coherent decryption for CSK with two Qi hyper chaos generators are shown in Fig. 2.

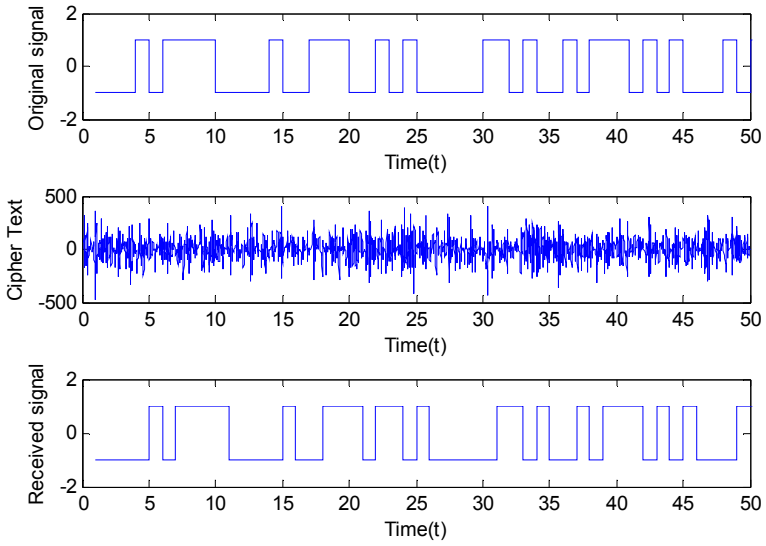

Fig. 2. Comparison between sent and received signal

4. BER Performance of CSK Based on Qi Hyper Chaos Compared to Lorenz Based CSK

Bit Error Rate (BER) is a performance measurement that specifies the number of bit corrupted or destroyed as they are transmitted from its source to its destination [13, 14].
BER measurements compare digital input and output signals to access what fractions of the bit are received incorrectly. It is defined as:

$$\mathrm{BER} = \frac{N_e}{N_t} \tag{6}$$

Where N_e is the number of error bits received over time t, and N_t is the total number of bits transmitted. Signal to Noise Ratio (SNR) is defined as the ratio of a signal power to noise power and it is normally expressed in decibel (dB). The mathematical expression of SNR is:

$$\mathrm{SNR} = 10\log_{10}\left(\frac{\mathrm{SignalPower}}{\mathrm{NoisePower}}\right)\mathrm{dB} \tag{7}$$

Relationship between the system's SNR and BER is that the higher the SNR, The lower would be the corresponding BER

$$\mathrm{BER} = \left(1/\mathrm{SNR}\right)^k \tag{8}$$

where k is a specific subcarrier index.
In this paper simulation of BER is done using Bertool tool in Matlab\Simulink.

Fig. 3 shows the comparison of the BER performance between chaos based CSK using energy bit estimation method for decryption (Simulation 0) and Qi hyper chaos CSK based using correlation method for decryption (Simulation 1).

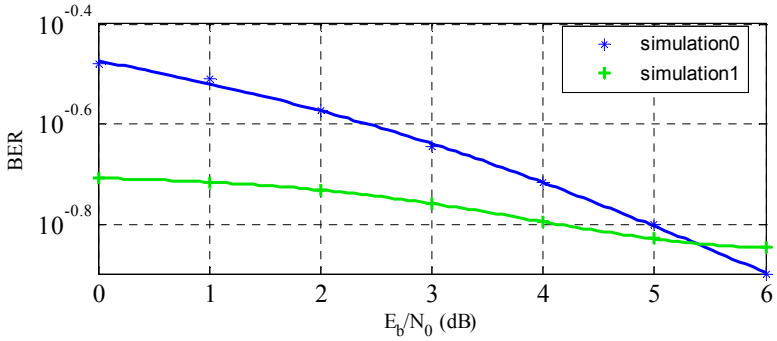

Fig 3: Comparing the BER performance between Qi hyper-chaos based CSK using energy bit estimation method for decryption and using correlation method for decryption.

The BER performance of the latter is seen to be much lower than the former; hence, the correlation method for decryption is more efficient compared the energy bit estimation method for decryption.

Qi hyper-chaos CSK based on correlation method has better performance because with the aid of synchronization the low frequency noise and high frequency noise can be easily eliminated.

5. Power Spectrum and Low Pass Filter Methods of Attacking Chaos Based Secure Communication

Security during communication is fundamental since it is one of the components that add up to effective and efficient communication. There are varieties of methods that have been proposed to attack chaos-based secure communication schemes. In different cases in literature [14] they have indicated successfully breaking of chaos encryption without knowing the secrete key or the parameters used during encryption. This kind of attack is only possible if the received message $m(t)$ is a periodic signal or if $m(t)$ consists of periodic frames within a given duration. The attack can be accomplished using two methods power spectrum analysis and low pass filter technique and return map analysis.

Power spectrum and low pass filter technique are very powerful schemes that can be used to break chaotic communication without knowing the parameters or the initial components used during encryption.These two methods are implemented in this paper to determine how robust CSK based on Qi hyper is.The message signal encrypted by Lorenz chaotic system hereby successfully extracted by the filter and decision circuit as shown Fig. 4

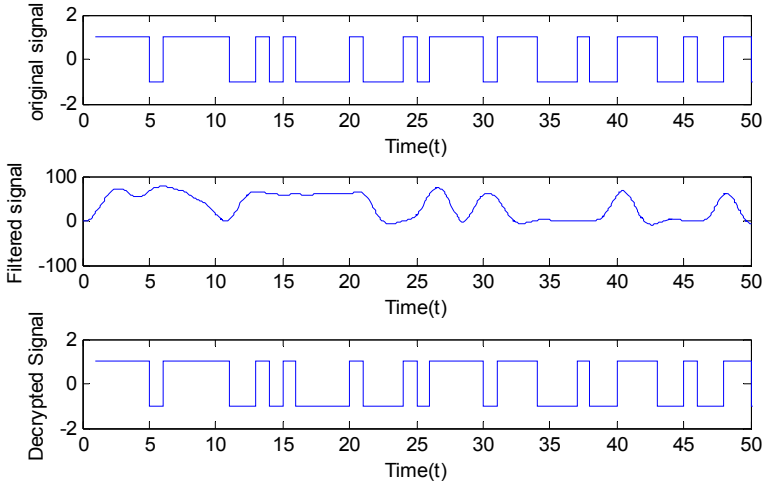

Fig. 4. Attacking Lorenz Chaos through power spectrum and low pass filter

The attempt to attack message signal encrypted based on Qi hyper-chaotic system was unsuccessfully as shown Fig. 5

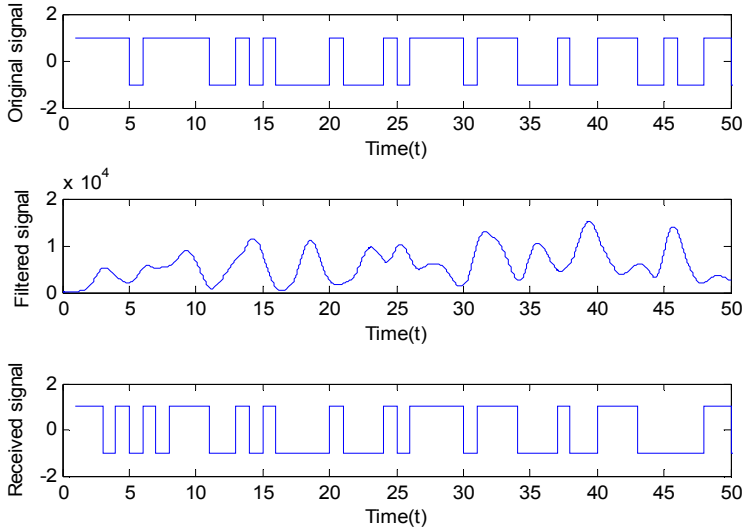

Fig. 5. Attacking Qi hyper-chaos through power spectrum and low pass filter, The simulation results in Fig. 5 indicates that it is not easy to attack digital message signal encryption based on Qi hyper-chaos. The difficulty in attacking message signal based on Qi hyper-chaos can be attributed to the rich properties of Qi hyper-chaos.

6. Conclusion

In this paper message signal based on Qi hyper-chaos has been implemented. The BER performance comparison between Qi hyper-chaos and Lorenz chaos shows that Qi hyper-chaos based CSK has better performance compared to Lorenz based CSK. The rich properties of Qi hyper chaos such us high frequency spectrum, high level of disorder, etc. have made it very cumbersome for low pass-filter and power spectrum analysis method to be successful in attacking and decrypting the encrypted message signal sent.

References

1. C. I. Rincu and A. Serbanescu. Chaos-Based Cryptography. A Possible Solution For Information Security, *Bulletin of the Transilvania University of Brasov*, vol. 2,51, 2009.
2. M. Baptista. Cryptography with chaos, *Physics Letters A*, vol. 240: 50-54, 1998.
3. L. M. Pecora and T. L. Carroll. Synchronization in chaotic systems, *Physical review letters*, vol 64: 821-824, 1990.
4. T. L. Carroll and L. M. Pecora. Synchronizing chaotic circuits, *Circuits and Systems, IEEE Transactions*, vol. 38: 453-456, 1991.
5. J. Lü and G. Chen. A new chaotic attractor coined, *Int. J. Bifurc. Chaos,* vol. 12: 659–661, 2002.
6. G. Álvarez, S. Li. Comput, *Commun*, vol. 27, 2004.

7. G. Hu, Z. Feng, R. Meng, *IEEE Trans. Circuits Syst.* 50-275, 2003.
8. G. Qi, et al. On a new hyperchaotic system, *Physics Letters A,* vol. 372:124-136, 2008.
9. G. Qi, et al. "A new hyperchaotic system and its circuit implementation, *Chaos, Solitons & Fractals,* vol. 40:2544-2549, 2009.
10. E. N. Lorenz. Deterministic nonperiodic flow, *J. Atmospheric Sc.,* vol. 20: 130-141, 1963.
11. C. Tse and F. Lau. Chaos-based digital communication systems, *Operating Principles, Analysis Methods and Performance Evaluation (Springer Verlag, Berlin)* 2004.
12. M. P. Kennedy and G. Kolumbán. *Digital communications using chaos*, *Signal processing*, vol. 80: 1307-1320, 2000.
13. W. M. Tam, et al. An approach to calculating the bit-error rate of a coherent chaos-shift-keying digital communication system under a noisy multiuser environment, Circuits and *Systems: Fundamental Theory and Applications, IEEE Transactions*, vol. 49:210-223, 2002.
14. M. Sushchik, et al. Performance analysis of correlation-based communication schemes utilizing chaos, Circuits *and Systems I: Fundamental Theory and Applications, IEEE Transactions*, vol. 47:1684-1691, 2000.