Digital Communication System With High Security and High Noise Immunity: Security Analysis and Simulation

Ahmed S. Alshammari, Mohamed I Sobhy and Peter Lee
The School of Engineering and Digital Arts
The University of Kent
Canterbury, CT2 7NT
(aa798, M.I.Sobhy, P.Lee)@kent.ac.uk

Abstract. In this paper, our approach is to provide a cryptosystem that can be compared to a One-Time Pad. A new cryptosystem approach based on Lorenz chaotic systems is presented for secure data transmission. The system uses a stream cipher, in which the encryption key varies continuously. Furthermore one or more of the parameters of the Lorenz generator is controlled by an auxiliary chaotic generator for increased security. The CDMA system for four users has been tested using MATLAB-SIMULINK. The system has achieved a good performance in presence of noise compared to other communication systems.

1 Introduction

Code Division Multiple Access (CDMA) technology allows many users to simultaneously use the same communication system and share the same frequency. In a CDMA scheme, each user is assigned a particular spreading sequence to map the information signal. Thus, the spreading information signal using a particular sequence increases the bandwidth of the information signal by a factor of N, which is known as the spreading factor or processing gain [1].

In this paper, we report the design a CDMA system based on a Lorenz stream cipher to enhance system security. The proposed cryptosystem for the CDMA system is compared to a one-time pad. One-time pad encryption is an unbreakable encryption method [1-3]. The encryption method of the one-time pad involves one truly random bit (Letter pad) corresponding to one bit of the plaintext by using the bitwise Exclusive OR gate (XOR) to produce one bit [1]. Any stream cipher can be unbreakable (one-time pad) if the following requirements are met [1]. The key and plaintext must be equal length, the key must satisfy a randomness test and the key must only be used once. We want to compare our cryptosystem with existing symmetric key cryptography systems, such as 3DES, AES and One-Time Pad in terms of the size of the key space of cryptography system must be long enough to be protected from attacks. The larger the size of the key space, the longer the time needed for computation steps to perform a brute force attack, thus, the higher the security. The key is the information needed to recover the plaintext. Table 1 shows the comparison between Lorenz stream cipher and other cryptosystems.

The rest of this paper is organized as follows. In Sec. 2, an encryption system, In Sec. 3, transmitter system. In Sec. 4. Receiver system. In Sec. 5 communication system. Finally the conclusions are given in Sec. 6.

Table 1. Comparison between chaotic system, 3DES, AES and One-Time Pad (OTP)

Factors	3DES	AES	OTP	Lorenz stream cipher
Key Length	168 bits	128,192 or 256 bits	Same as Length of the Plaintext (LP)	576 bits
Cipher Types	Symmetric block Cipher	Symmetric block Cipher	Symmetric stream Cipher	Symmetric stream Cipher
Block Size	64 bits	128,192 ,or 256	-	32 bits
Key Space	2^{168}	$2^{128,}2^{192}$ or 2^{256}	2^{LP}	2^{576}
Security	Not Secure	Considered Secure	Considered Secure	Considered Secure

2 An Encryption System

The encryption technique utilises the output of the Main Lorenz Generator to encrypt the data stream. Both the Main Lorenz Generator and the Auxiliary Lorenz Generator are based on the equations shown below, in which x, y and z are state variables and A, B and C are parameters.

$$\begin{aligned} \dot{x} &= \mathrm{A}\,(y - x) \\ \dot{y} &= \mathrm{B}\,x - y - x\,z \\ \dot{z} &= x\,y - \mathrm{C}\,z \end{aligned} \tag{1}$$

The output of the Auxiliary Lorenz Generator (A[n]) must remain within the range ($7 \leq x[n] \leq 11$). Therefore, the signal response of the Main Lorenz Generator changes continually in a chaotic manner. Fig. 1 shows the SIMULINK Lorenz model where A, B and C are system parameters. The scaling factors S1, S2 and S3 are used to control the output signals frequency band and they are also part of the key in the encryption system.

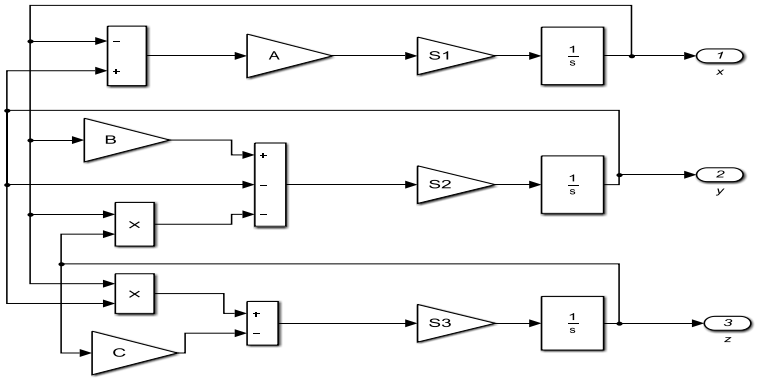

Fig. 1. Lorenz chaotic generator.

Fig. 2 shows the results from SIMULINK of the Lorenz State Variables, *x, y* and *z*.

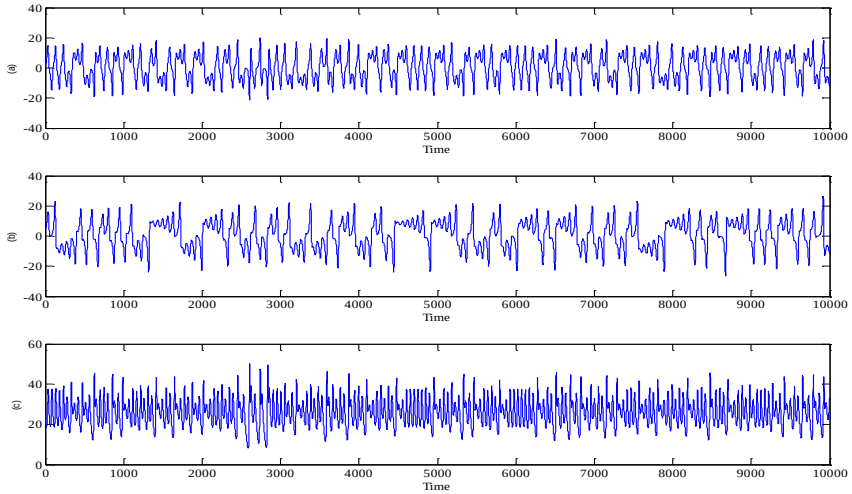

Fig. 2. Lorenz state variables. (a) *x*-state variable, (b) *y*-state variable and (c) *z*-state variable

2.1 Analogue to Digital conversion

Since the Lorenz system generates an analogue signal, an analogue-to-digital convertor (ADC) is necessary in the digital applications. Fig. 3 shows the ADC block diagram. Fig. 4 shows the simulation results of the ADC.

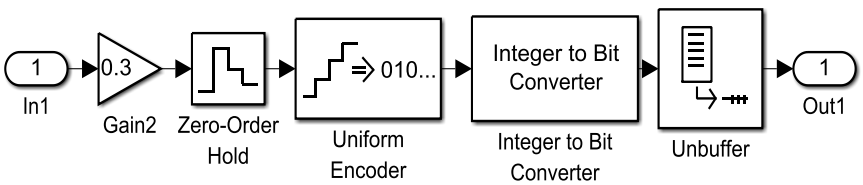

Fig. 3. Analogue-to-digital signal convertor.

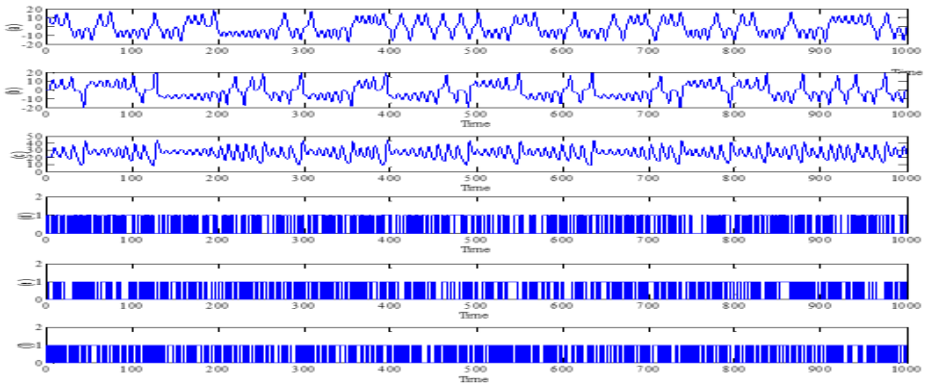

Fig. 4. Analogue chaotic signal converted to digital signal. (a) Analogue signal of *x*-state variable, (b) Analogue signal of *y*-state variable, (c) Analogue signal of *z*-state variable, (d) Digital signal *x*-state variable, (e) Digital signal of *y*-state variable and (f) Digital signal of *z*-state variable.

2.2 Randomness test

Initially, the Lorenz Generator bit stream failed to pass the NIST randomness test [5]. Therefore, an additional SIMULINK subsystem was developed to scramble the chaotic bit stream to generate a truly random bit stream. Table 2 shows the NIST randomness test of the three chaotic signals: *x*-state, *y*-state and *z*-state before scrambling.

Table 2 NIST randomness test for *x*, *y* and *z* signals.

Statistical Test	***x*-state**		***y*-state**		***z*-state**	
	Status	**P-value**	**Status**	**P-value**	**Status**	**P-value**
Frequency	Fail	0.000	Fail	0.000	Fail	0.000
Block Frequency	Fail	0.000	Fail	0.000	Fail	0.000
CUSUM-Forward	Fail	0.000	Fail	0.000	Fail	0.000
CUSUM-Reverse	Fail	0.000	Fail	0.000	Fail	0.000
Runs	Fail	0.000	Fail	0.000	Fail	0.000
Long Runs of Ones	Fail	0.000	Fail	0.000	Fail	0.000
Rank	Fail	0.000	Fail	0.000	Fail	0.000
FFT Test	Fail	0.000	Fail	0.000	Fail	0.000
Non-Overlapping	Fail	0.000	Fail	0.000	Fail	0.000
Overlapping	Fail	0.000	Fail	0.000	Fail	0.000
Approximate Entropy	Fail	0.000	Fail	0.000	Fail	0.000
Linear Complexity	Fail	0.000	Fail	0.000	Fail	0.000
Serial	pass	0.350	Fail	0.000	Fail	0.000

2.3 Scrambling scheme of Lorenz chaotic signal

Two chaotic bit streams (*x*-state and *y*-state) have been used to generate a truly random key. The last 12 bits in row are extracted from *x*-state and last 20 bits are extracted from *y*-state. Then, the 32 bits are assembled with a concatenate block. The 32 bits are then serialized to generate a bit stream, which is used as a key stream for data encryption. Fig. 5 shows the SIMULINK model of the scrambling method. Table 3 indicates that the key stream now passes the NIST randomness test.

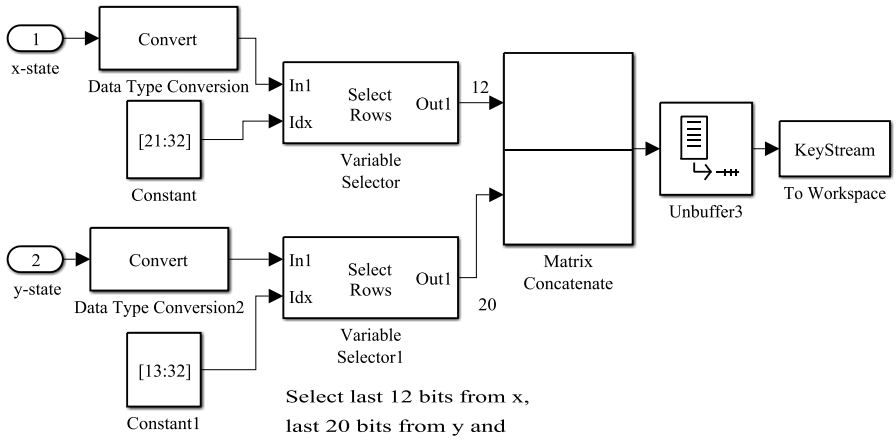

Fig. 5. Scrambling scheme of the Lorenz signals.

Table 3 NIST randomness test

Statistical Test	Status	P-value	Statistical Test	Status	P-value
Frequency	Pass	0.350485	**FFT Test**	Pass	0.534146
Block Frequency	Pass	0.350485	**Non-overlapping**	Pass	0.066882
CUSUM-Forward	Pass	0.739918	**Overlapping**	Pass	0.122325
CUSUM-Reverse	Pass	0.534146	**Approximate Entropy**	Pass	0.911413
Runs	Pass	0.350485	**Linear Complexity**	Pass	0.739918
Long Runs of Ones	Pass	0.911413	**Serial**	Pass	0.739918
Rank	Pass	0.739918			

2.4 High system parameter sensitivity

The system parameters of the first Lorenz generator is A=9.7, B=26.2 and C=2.44. The system parameters of the second Lorenz generator has the same parameters except for one which is (A parameter). This parameter has been changed from 9.7 to $9.7+10^{-15}$. Thus, we can generate infinite spreading codes for infinite number of users.

2.5 The key space of the proposed cryptosystem

At the transmitter system, there are two Lorenz generators, and each generator has three constants, three initial conditions and three frequency multipliers. Thus, the total number of the parameter is 18. The word length represented by 32-bits.The key space of the system is $2^{(18*32)} = 2^{576}$. The key space of a secure cryptosystem as is suggested by previous research [6] should be greater than 2^{100}. Thus, the cryptosystem key space of 2^{576} is huge and enough to resist any brute force attack.

3 Transmitter system

In this application, the spread sequence is a chaotic digital signal generated using Lorenz chaotic systems [4]. The simulation results of the information signal spread using 32-bit length is shown in Fig. 6.

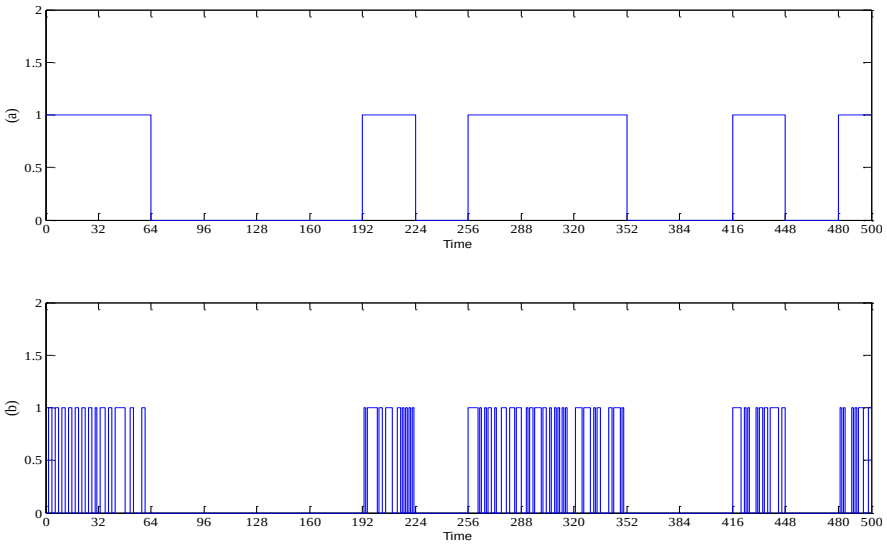

Fig. 6. Simulation results of user data spreading. (a) Information signal, and (b) Spreading the information signal using 32-bits length.

The encrypted unipolar stream consisting of ones and zeros is encoded to a bipolar stream of ± 1, so 0 is encoded to -1 and 1 stays, the same. The aim from encoding is to overcome the channel noise and to reduce the bit error probability at the receiver. Another reason to use bipolar encoding is that there is no security for a one user system. The user data transmitted through the channel can be easily recognised. However, if we have multiple-users, then it is not case.

All four user data are combined using an adder block. Fig. 7 shows the user data encryption process. Fig. 8 shows the all four user data are combined.

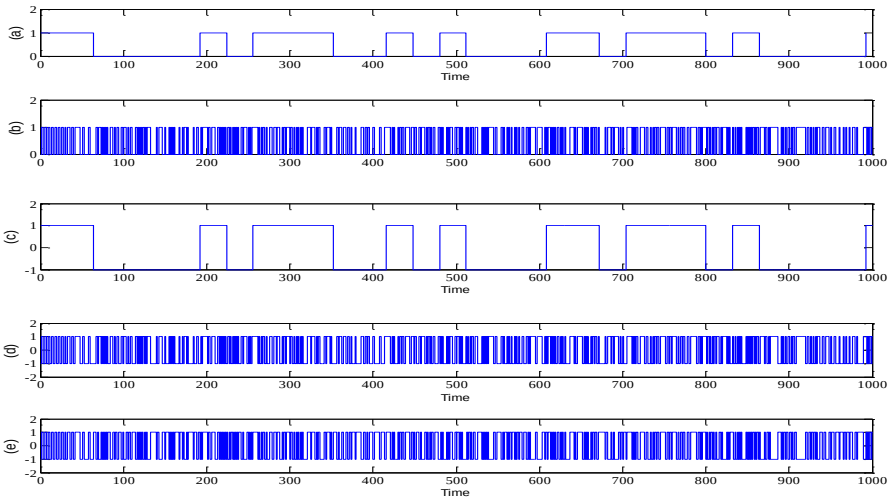

Fig. 7. SIMULINK results of the user data encryption process. (a) Information signal, (b) Lorenz binary stream, (c) Information signal is encoded to bipolar, (d) Lorenz binary stream is encoded to bipolar and (e) Encrypted information signal.

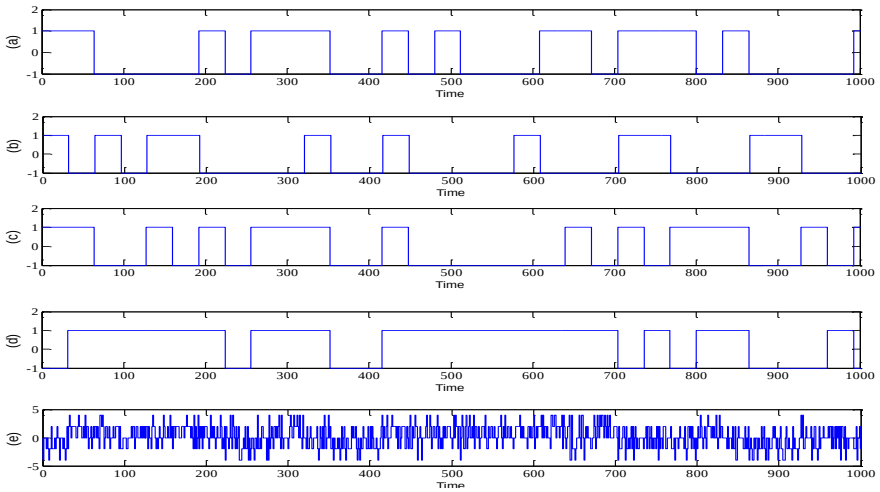

Fig. 8. SIMULINK results for combined four user data. (a) User data 1, (b) User data 2, (c) User data 3, (d) User data 4, and (e) All four user data are combined.

3.1 Auto –correlation based on Lorenz Generator

We used auto-correlation function to test the Lorenz binary stream for *x*-state. Four different code sizes have been used, 32, 64, 128 and 256-bits. In Fig. 9, the plot of auto-correlation for 32-bits shows the maximum value is 32 and similarly to the 64, 128 and 256-bits.

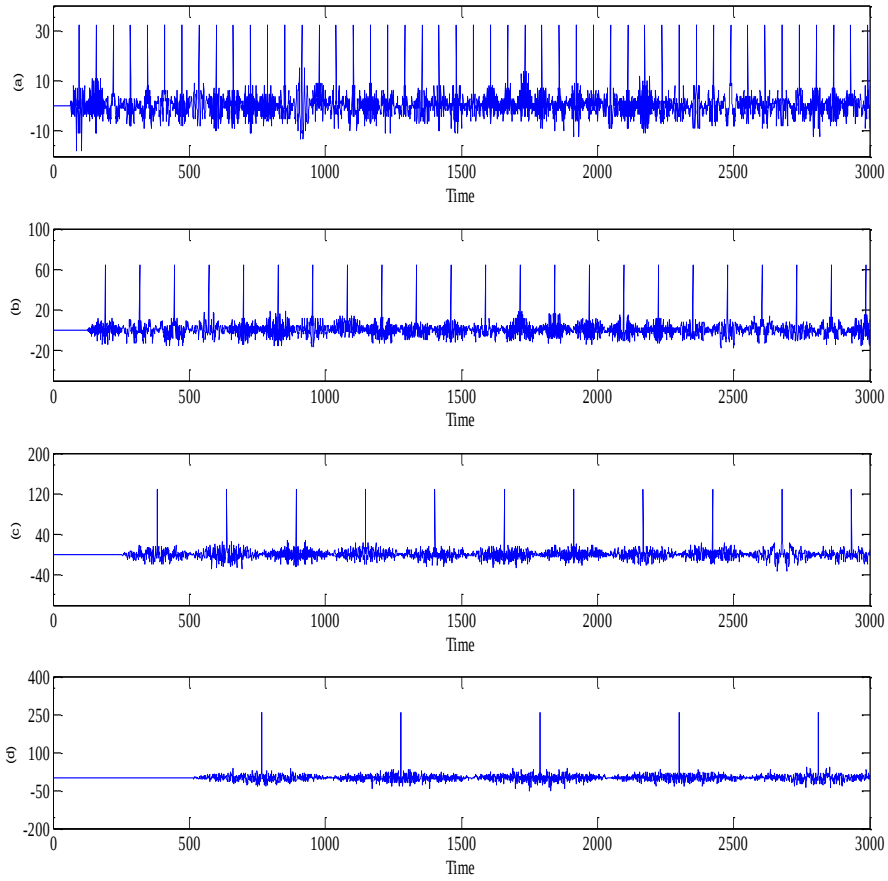

Fig. 9. The plot of the auto-correlation function. (a) Auto-correlation function of 32-bits long, (b) Auto-correlation function of 64-bits long, (c) Auto-correlation function of 128-bits long and (d) Auto-correlation function of 256 bit-long.

Comparison between the cross-correlation and auto-correlation of the chaotic signals is given in Table 4.

3.2 Cross-correlation based on Lorenz Generator

In Fig. 10 shows the cross-correlation shows low for 32-bits of *x* and *y, x* and *z*. Thus, using *x* and *y, x* and *z* for user data spreading are recommend to mitigate the multi-user interference and achieved better bit error rate. On the other hand, using *y* and *z* should be avoided due to three spikes in time series.

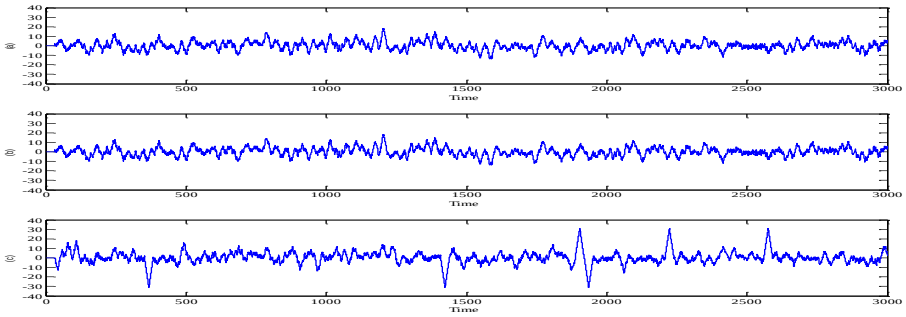

Fig. 10. The plot of the cross-correlation function for 32-bits (a) *x* xcorr *y* (b) *x* xcorr *z* and (c) *y* xcorr *z*.

Table 4 shows the auto-correlation, cross correlation, threshold and difference between auto-correlation and cross-correlation for 32, 64, 128 and 256-bits.

TABLE 4 Auto-correlation and cross-correlation for 32, 64,128 and 256-bits.

Word-length	Auto-correlation	Cross-correlation	Threshold value (τ)	difference between auto-correlation & cross-correlation)
32-bits	32	8	$8 < \tau \leq 32$	24
64-bits	64	20	$20 < \tau \leq 64$	44
128-bits	128	25	$25 < \tau \leq 128$	103
256-bits	256	40	$40 < \tau \leq 256$	216

From these results, the auto-correlation is much larger than cross-correlation and these mean that we can use the chaotic systems for detecting the CDMA signals.

4 Receiver System

4.1 De-spreading based on cross-product and summation

The cross-product block and summation have been used to retrieve the transmitted user data which is shown in Fig 11.

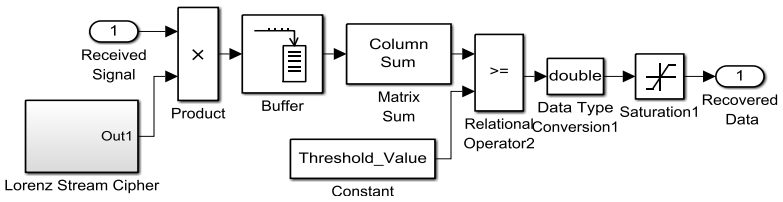

Fig. 11. De-spreading using cross product and summation.

Fig. 12 shows a whole user data extraction process. Fig. 13 shows the four user data transmitted and recovered.

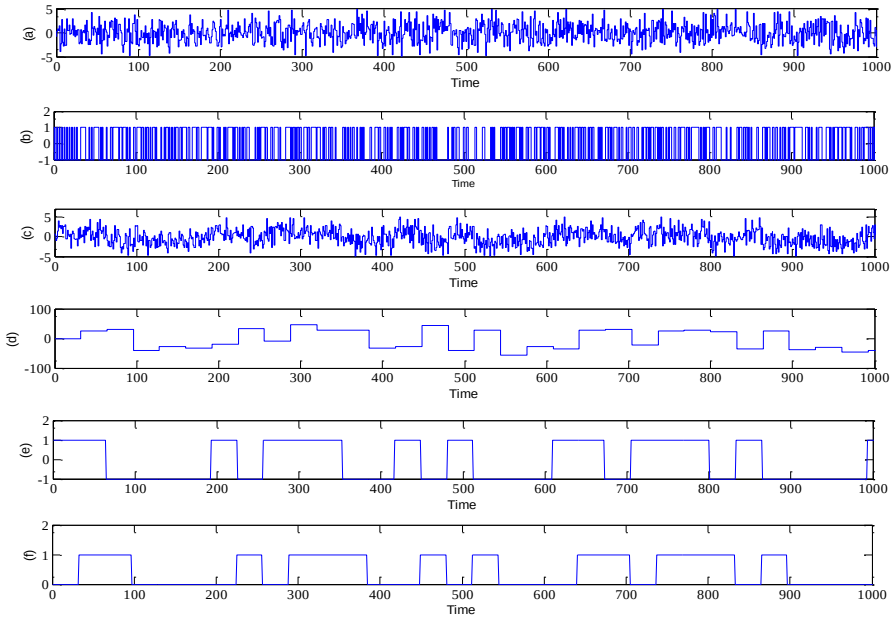

Fig. 12. User data extraction process.(a) Lorenz chaotic signal, (b) Multiplication process, (c) accumulator, (e) User data transmitted and (f) Recovered data.

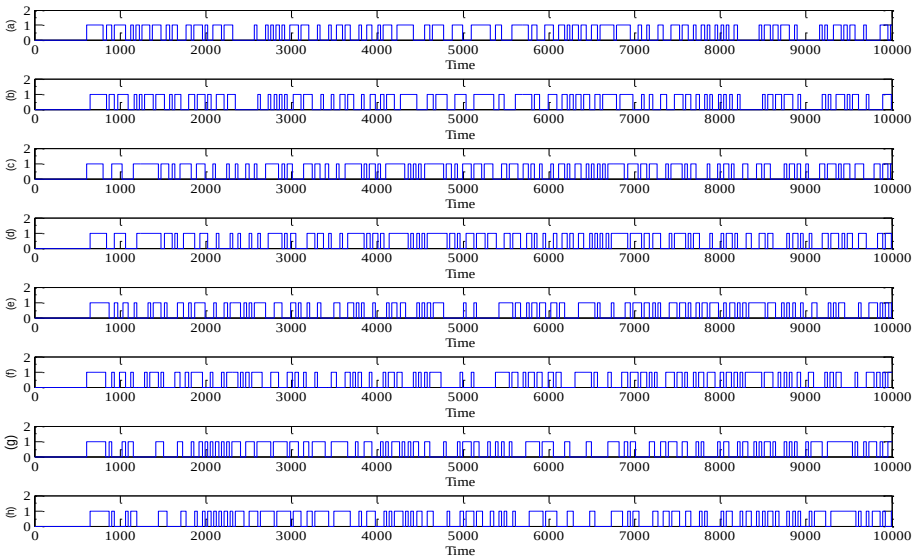

Fig. 13. Four user data transmitted and recovered. (a) User data 1, (b) user data 1 recovered, (c) user data 2, (d) user data 2 recovered, (e) user data 3, (f) user data 4 recovered, (g) user data 4, and (h) user data 4 recovered.

5 Communication System with added noise

The received signal r (t) is given by

$$r\,(t) = s(t) + n(t) + j(t) + c(t) \tag{2}$$

Where s(t) is the desired signal and n(t) is the noise from the channel and j(t) is the jamming signal and c(t) is the cross-talk noise from other users. The SNR is calculated using the equation below, in which P_1 is the signal power and P_2 is the signal with added noise.

$$SNR_{dB} = 10\log_{10}\left(\frac{P_1}{P_2 - P_1}\right) \tag{3}$$

The performance of CDMA system has been analyzed in this research work. The performance results were evaluated in terms of Signal to Noise Ratio (SNR) of the CDMA system for four users. Results have been evaluated numerically and compared to standard accepted BER of 10^{-6}. In this simulation test, the number of bits transmitted was $1e^6$ for each user. The plot of BER versus Signal to Noise Ratio (SNR) is shown in Fig. 14. The system performance has achieved no bit error at the signal to noise ratio of -2.974dB. The system has achieved a good performance based on the results obtained and compared to other communication systems [5].

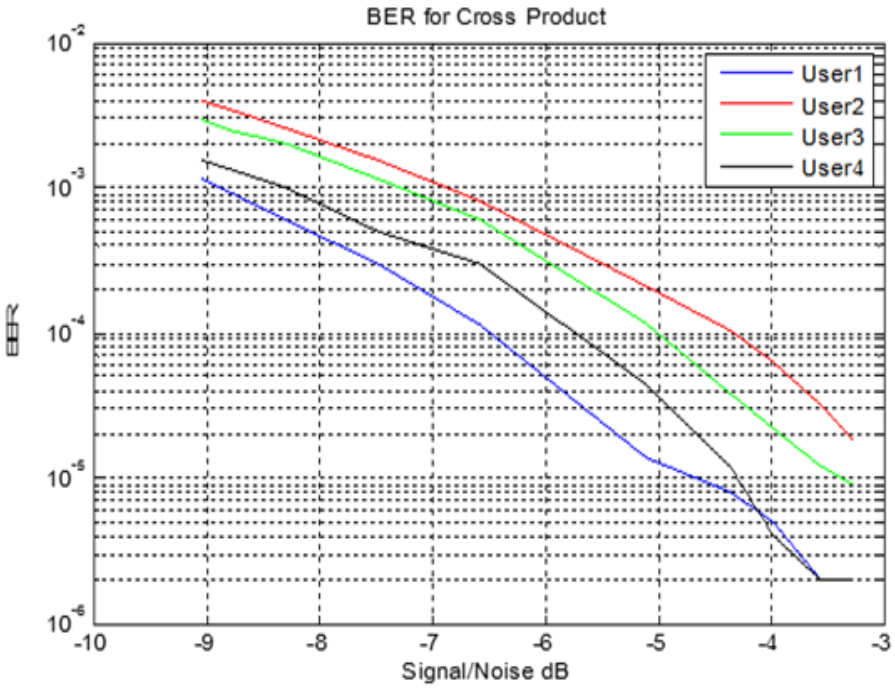

Fig. 14. Upper noise bound vs. S/N (dB).

6 Digital hardware implementation

In this paper we presented the criteria for designing a digital communication system with high security and high immunity from noise, jamming and cross-talk. The system has been implemented using Field Programmable Gate Arrays (FPGA) and the design objectives have been realized. Details of the digital implementation will be reported in a future publication.

In the digital implantation additional blocks for clock and data recovery were designed and implemented as well as routines for synchronizing the chaotic generators.

7 Conclusion

In this paper, a complete CDMA system based on Lorenz stream cipher has been described. The data encryption is based on two Lorenz generators (main and auxiliary). The auxiliary Lorenz generator serves to continuously vary one or more parameter(s) of the main Lorenz generator; in the case of the system described in this chapter, only the A parameter is varied. The data encryption uses a symmetric cipher which a key length of 576-bits. This is a key space of the system is 2^{576}. The scrambling scheme was developed and Lorenz stream cipher binary stream passed the NIST randomness test successfully. In addition, the system output signal has a high sensitivity to small changes in any parameter. Moreover, the auto-correlation and cross correlation for 32-bits have good results. The maximum auto-correlation and cross-correlation functions for (32, 64, 128 and 256-bits) have shown good results. The performance results were evaluated in terms of Signal to Noise Ratio (SNR) of the CDMA system for four users. Results have been evaluated and compared to standard accepted BER of 10^{-6}. The system performance were shown a good results. At -2.974 signal to noise ratio, the system achieved no bit error with $1e^6$ bits transmitted for four users. The system has achieved a good performance based on the results obtained and compared to other communication systems.

References

1. G. Kaddoum, Wireless chaos-based communication systems: A comprehensive survey. IEEE Access, (2016) vol. 4, 2621-2648
2. M. Electronics, One Time Pad Encryption, http://www.cryptomuseum.com/manuf/mils/files/mils_otp_proof.pdf.
3. B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley. New York (1996)
4. N. J. Croft, M. S. Olivier, Using an approximated one-time pad to secure short messaging service (SMS), the Southern African Telecommunication Networks and Applications Conference. South Africa,(2005) 26-31
5. NIST Special Publication 800-22, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (2000)

6. S.-L. Chen, S.-M. Chang, T.T. Hwang, W.-W. Lin, Digital secure communication using robust hyper-chaotic systems, Int. J. Bifurc. Chaos, (2008) vol. 18, no. 11, 3325–3339
7. M. Suneel, Electronic circuit realization of the logistic map, Sadhana (2006) vol. 31, 69-78
8. B. Jovic, C. P. Unsworth, Chaos-based multi-user time division multiplexing communication system, IET Communications, (2007)vol. 1, 549-55