International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 5, October 2019, pp. 3550~3557
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i5.pp3550-3557

Efficient error correcting scheme for chaos shift keying signals

Hikmat N. Abdullah[1], Thamir R. Saeed[2], Asaad H. Sahar[3]
[1]College of Information Engineering, Al-Nahrain University, Iraq
[2,3]Department of Electrical Engineering, University of Technology, Iraq

Article Info

Article history:

Received Jul 31, 2018
Revised Mar 19, 2019
Accepted Apr 9, 2019

Keywords:

Channel coding
Chaotic shift keying
Error correction algorithm
Normalized correlation
Suboptimal detection

ABSTRACT

An effective error-correction scheme based on normalized correlation for a non coherent chaos communication system with no redundancy bits is proposed in this paper. A modified logistic map is used in the proposed scheme for generating two sequences, one for every data bit value, in a manner that the initial value of the next chaotic sequence is set by the second value of the present chaotic sequence of the similar symbol. This arrangement, thus, has the creation of successive chaotic sequences with identical chaotic dynamics for error correction purpose. The detection symbol is performed prior to correction, on the basis of the suboptimal receiver which anchors on the computation of the shortest distance existing between the received sequence and the modified logistic map's chaotic trajectory. The results of the simulation reveal noticeable Eb/No improvement by the proposed scheme over the prior to the error- correcting scheme with the improvement increasing whenever there is increase in the number of sequence N. Prior to the error-correcting scheme when N=8, a gain of 1.3 dB is accomplished in E_b/N_o at 10^{-3} bit error probability. On the basis of normalized correlation, the most efficient point in our proposed error correction scheme is the absence of any redundant bits needed with minimum delay procedure, in contrast to earlier method that was based on suboptimal method detection and correction. Such performance would render the scheme good candidate for applications requiring high rates of data transmission.

Corresponding Author:

Asaad H. Sahar,
Department of Electrical Engineering,
The University of Technology,
25 Sina'ah street, Baghdad 10120, Iraq.
Email: asaad.ha87@gmail.com

1. INTRODUCTION

For a couple of years now, chaos has attracted a great deal of attention from various scholars like engineers, mathematicians, and physicians [1-3]. The study trend has been transmitting from searching for the proofs of the existence of chaos into solicitations and thorough hypothetical research in past years [4]. Chaos arrangements got from a particular category of various equations are not sporadic and subtle to first circumstances, and it is hard to forecast their impending characters from previous annotations [5]. Because it is turning out that this chaotic system can be easily executed, most scholars in the systems and circuit of the nonlinear field have majorly been focused on creation execution concerning chaos. Chaos systems communications are among the attention-grabbing issues in engineering field [6-8]. Most scholars have concentrated on the designing of non-coherent recognitions that do not require the usage of primary signals (unmodulated carriers) at a receiver for demodulation. In normal system communication, classified under coherent recognition, primary signals require to be generated so that as they arrive at the receiver, they are demodulated. Therefore, the normal systems of communication are challenging when the non-coherent detection is applied. On the contrary, the detection applying chaos non-coherently could demodulate the data with the absence of primary signals because chaos and chaotic sequences possess distinct characteristics.

Thus, the non-coherent recognition is taken as a unique recognition approach by means of chaos. The optimal receiver [9] as well as DCSK (Differential chaos shift keying) [10] are famous for its systems of classic non-coherency.

However, the optimal receiver suffers from complicated calculations and difficult signal detection when the length of chaotic sequence N becomes long. Arai et al. [11] proposed an approach of recognizing symbols by the computing figures of the minimal length from signals received to chaotic map i.e., suboptimal receiver. In place of valuating the PDF, the suboptimal receiver estimates the PDFs through determining the nearest length from the chaotic map to signals that were received. Apart from the application of chaos in modulation systems, chaos pointed out that, a number of scholars who have advanced their application in channel coding [12]. Majorly, the representational dynamic connected with the chaotic maps are devised as a criterion of error correcting. The non-redundant or redundant system based on chaotic channel coding.

The basic idea of any error correcting method is redundancy bits, which is extra bits added to the data. The redundancy bits used for error detection and correction that may occur on the data transmitted, in the process of transmission or storage. The redundancy bits affect the data rate of the communication system where the transmission rate conversely proportional with the number of redundant bits [13, 14]. The non-redundant approach is the finest when the transmission rate is considered whereas the redundant methods have got advanced performance of BER. However, the previous works use non-redundant correction depend on the suboptimal receiver, but they have a lot of delay process because the correction of each bit depends on all sequence. In our previous work [15], we designed a suboptimal detection with the modified logistic map. In this study, the design of suboptimal receiver to realize a combined chaos based noncoherent modulation and non-redundant error correcting coding is proposed. The designed system uses two successive chaotic sequences based on the logistic map such that the string started from the second value to the end of the first sequence is used as to represent the string started from the first value of the next sequence if it represents the same bit value. This feature gives the receiver additional information not only for correct recovery but also for correct correction. The proposed non-redundant error correction depends on normalized correlation with minimum delay because the maximum delay for correcting one bit depends on previous and next sequences only.

2. THE SYSTEM OVERVIEW WITH PROPOSED ERROR CORRECTING ALGORITHM

The block diagram of the chaotic shift keying system with the suboptimal receiver is shown in Figure 1. The details of each block are described in the next sections.

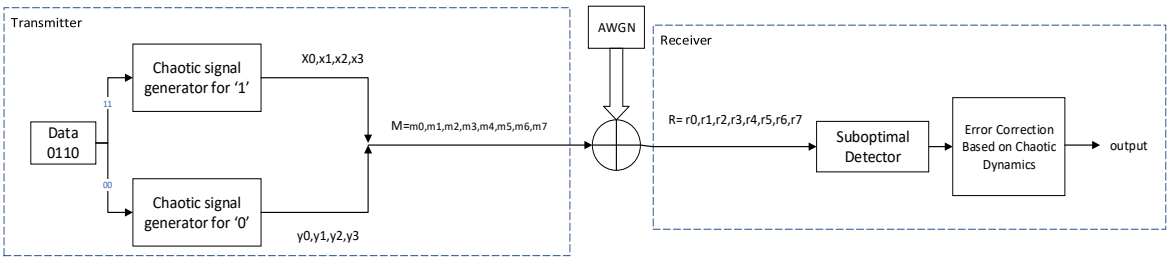


Figure 1. The suboptimal receiver of CSK system with error correcting coding

3. THE TRANSMITTER

In the transmitter side, the message bits are modulated by generating a chaotic sequence from the chaotic map. In this work, we used a modified logistic map [15] which is one of the most straightforward chaotic maps, and it describes by Equation (1).

$$X_{n+1} = -a\left(\frac{X_n^2}{2} - 0.25\right) \qquad (-1 \leq X \leq 1) \tag{1}$$

where a is positive real constant, and it is between $0 < a \leq 4$ represent the control parameter for this map. The encoding architecture of CSK shows in Figure 2. When transmitted K bits through a noisy channel, for each data bit N sequence from identical chaotic map generates, therefore, the amount of data transmitted turn into $K \times N$. For each signal block, the initial value is randomly selected for symbol "1" (x_0) and "0" (y_0) at the beginning. Afterward, the initial value for the next symbol "1" and "0" sequences will be taken from

the second value of the previous sequence. For example, assume $N = 4$ *and* $K = 5$, and the data bits are 01101. The modulated signal vector S which is given as follows:

$$S= (S_0, S_1, S_2, S_3, S_4)$$
$$= (y_0, y_1, y_2, y_3, x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, y_4, y_5, y_6, y_7, x_8, x_9, x_{10}, x_{11})$$
$$= (s_0, s_1, s_2, \ldots\ldots, s_{19}) \quad (2)$$

where y_1, the second value of the sequence for the first symbol "0", has the same value of y_4, the first value for the sequence for the next "0", and similarly for the following values till the end of the corresponding symbol. i.e. $(y_1,y_2,y_3)=(y_4,y_5,y_6)$. From another hand, x_1, the second value of the sequence for the first symbol "1", has the same value of x_4, the first value for the sequence for the next "1", i.e. $(x_1,x_2,x_3)=(x_4,x_5,x_6)$. That always the next sequence is identical to the previous sequence in $(N-1)$ values. This algorithm gives the receiver addition features for detection and correction as will be shown later. When the signal transmitted through noisy channels with a mean of zero and a variance σ^2 the block signal become equal to R = S + noise = R = [r0, r1, r2, …. r19].

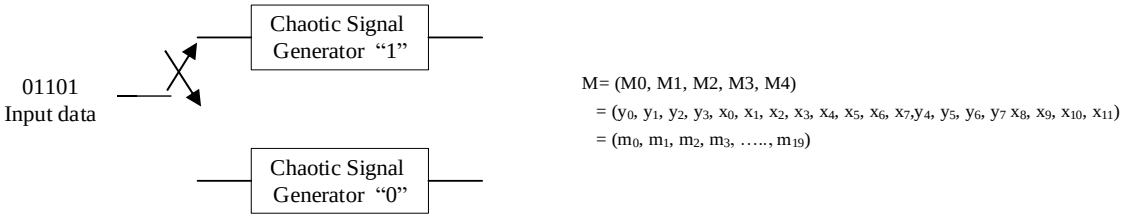


Figure 2. The proposed CSK encoder for error correction

4. NONCOHERENT RECEIVER WITH PROPOSED ERROR CORRECTION

The transmitted signal blocks are recovered by the receiver from the received signal blocks while the information symbols demodulated it. Again, the error correction is performed by the receiver. Because we took the noncoherent receiver into consideration, the chaotic map utilized at the transmitter for the modulation is memorized by the receiver. Nonetheless, the initial value of chaos within the transmitter is never revealed to the receiver. The error-correcting method which we proposed is made up of the suboptimal detector and the error correction on the basis of chaotic dynamics. The proposed detection/error correction method block diagram when $N=K=4$ is illustrated in Figure 3. The noncoherent detection for every received block is, first, performed by the receiver and every symbol demodulated. We had our suboptimal noncoherent detection algorithm, which we introduced in [15], applied in this work. The error-correcting scheme is performed by the receiver after each symbol is demodulated. a description of our suboptimal detector operation will be made available prior to giving an explanation of the proposed error correction operation.

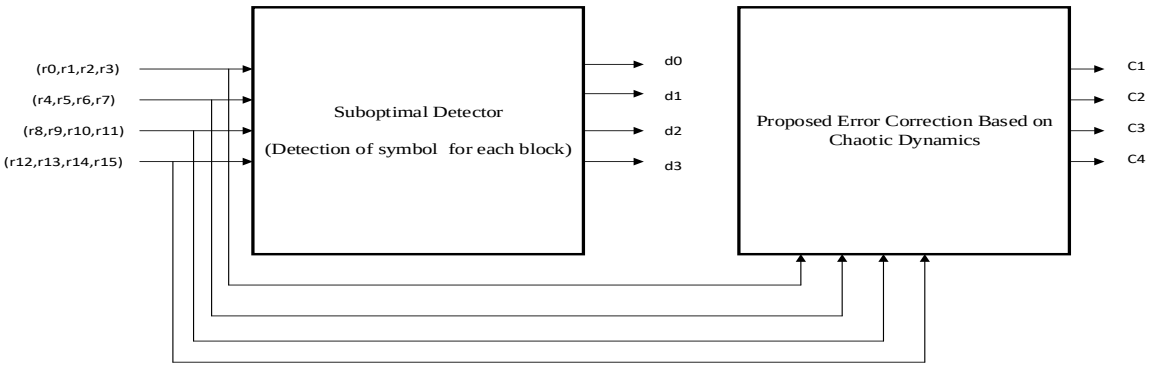


Figure 3. Block diagram of the proposed detection/error correction method when N=K=4

5. THE SUBOPTIMAL DETECTOR

The detection of symbols is accomplished through the computation of the shortest distance existing between the received signal and the chaotic map. The use of a nonlinear map in this work is for determining the closest map to the received point R. The computation of this distance that exists between the point R and the two maps is performed by obtaining the nonlinear map tangent equation and undertaking computation for the minimum distance from received point R= (ri, ri+1) where i = 1, 2, 3, 4…, N–1 to the point of the tangent. The received point and the distance to the modified logistic map function tangent are illustrated in Figure 4.

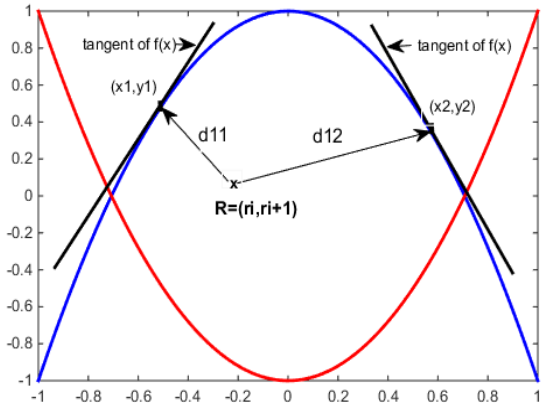


Figure 4. The calculation of minimum distance using the tangent of the nonlinear map

The shortest distance, based on Figure 4, from the received point to the symbol's two functions. Equation (3) is used in computing for "1"

$$d_1 = \sqrt{(x - r_1)^2 + (f(x) - r_2)^2} \quad (3)$$

where the nonlinear map function symbolized by f(x) is given by

$$f(x) = -a\left(\frac{x^2}{2} - 0.25\right) \quad (4)$$

where a=4. Removal of the equation's square root (3) gives

$$d_1^2 = (x - r_1)^2 + (f(x) - r_2)^2 \quad (5)$$

Obtaining the distance yield

$$\frac{\partial (d_1)^2}{\partial x} = 16x^3 + (8r_2 - 6)x - 2r_1 \quad (6)$$

Finding the equation's roots (6) calls for it to be equated to zero

$$16x^3 + (8r_2 - 6)x - 2r_1 = 0 \quad (7)$$

Now, trying to substitute x= (x1, x2, x3) in equation (1) as a method of finding (y1, y2, y3) and then finding the minimum distance for "1". Similar steps are used in finding the minimum distance for "0". The cumulative distance for "1" ($\sum d_1$) and "0" ($\sum d_0$) is computed by the suboptimal receiver for all the bits sequence. The detector makes the decision on which bit is "0" or "1" based on the shortest distance computed, if $\sum d_0 > \sum d_1$, the decoding of the signal is performed as "1", and if not it, is decoded as "0".

6. THE PROPOSED ERROR-CORRECTING METHOD

After the demodulation of each symbol, the receiver performs the error-correcting method. The basic idea of the scheme is that each detected bit is partially correlated (N-1 chaotic samples out of N chaotic

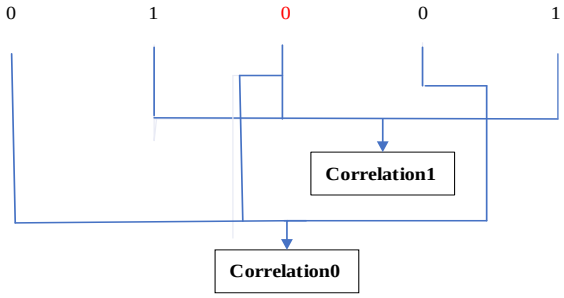
samples that represent each bit) two times. One time with its proceeded and next zeros and other time with its proceeded and next ones. According to the correlation results, the correction is done depending on which result is maximum. If the correlation result of ones is greater than zeros it is corrected to be one, otherwise, it is corrected to be zero. For ease of explanation, consider the following example. Let *N=4*, *k=5*, data = [01101], and an error occurs at R_2, then the flow of the proposed error correction method will be as shown in Figure 5. After the detection, the receiver arranges the received samples according to the decoded symbols and if an error occurs when the receiver detects symbol it uses the feature of each successive sequences is identical with *(N -1)* and use normalized correlation shown in equation (8).

$$\text{normalized correlation} = \frac{\sum_{n=1}^{N} r(n)\hat{r}(n-1)}{\sqrt{\sum_{n=1}^{N} r^2(n) \sum_{n=0}^{N-1} \hat{r}^2(n)}} \quad (8)$$

In Figure 5, an error occurs at the third bit. The receiver computes the normalized correlation for (0) between the third sequence and previous (0) and in addition to normalized correlation for the next (0) and the same steps used for (1) (by using previous (1) and next (1)). If the correlation for 1 is greater than 0, it means that the third bit is 1 instead of 0. The receiver uses the algorithm of correction for each bit on the symbol.

Received signals = [R_0, R_1, R_2, R_3, R_4]

Received signals = [(r_{00},r_{01},r_{02},r_{03}), (r_{10},r_{11},r_{12},r_{13}), (r_{20},r_{21},r_{22},r_{23}), (r_{30},r_{31},r_{32},r_{33}), (r_{40},r_{41},r_{42},r_{43})]



Received signal for 1= [(r_{10},r_{11},r_{12},r_{13}), (r_{20},r_{21},r_{22},r_{23}), (r_{40},r_{41},r_{42},r_{43})]
1 0 1

Normalized correlation1 = norm corr. [(r_{10},r_{11},r_{12},r_{13}),(r_{20},r_{21},r_{22},r_{23})] + norm corr.[r_{20},r_{21},r_{22},r_{23}),(r_{40},r_{41},r_{42},r_{43})]

Received signal for 0 = [(r_{00},r_{01},r_{02},r_{03}), (r_{20},r_{21},r_{22},r_{23}), (r_{30},r_{31},r_{32},r_{33})]
0 0 0

Normalized correlation0 = norm corr. [(r_{00},r_{01},r_{02},r_{03}),(r_{20},r_{21},r_{22},r_{23})] + norm corr.[r_{20},r_{21},r_{22},r_{23}), (r_{30},r_{31},r_{32},r_{33})]

As Normalized correlation1> Normalized correlation0

∴ the decoded signal=(01101)

Figure 5. The proposed error correction method

7. SIMULATION RESULTS

The performance of the proposed error-correcting method has been assessed with computer simulations through MATLAB. The simulation parameters are as follows: within the transmitting side, we suppose K =32. The control parameter is set as a =4 for the modified logistic map. The chaotic sequence's length per 1 bit is selected to assume the values N=4, 5, 6, 7 and 8. Figure 6 illustrates the BER versus Eb/N0 with N as the parameter for the suboptimal receiver without error-correction. Figure 6 illustrates that at BER = 10^{-3}, 4.2 dB gain in Eb/N0 is acquired once N = 8 over N = 4. This enhancement is referred to the raise of spreading factor of the chaotic signal. Nevertheless, the penalty for this enhancement is the raise in the intricacy of the suboptimal detection system regarding the amount of mathematical operations carried out.

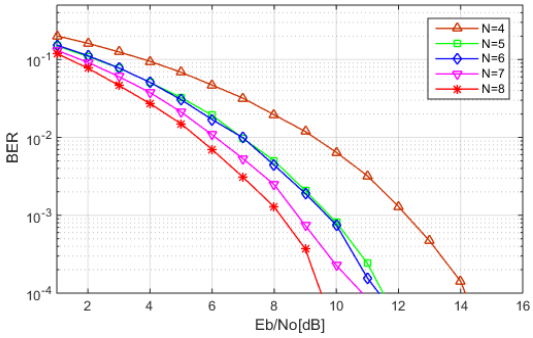


Figure 6. BER performance for a suboptimal receiver for different value of N

Figure 7 illustrates the BER performance versus Eb/N0 for the proposed technique as contrasted with the suboptimal receiver prior to the error-correcting when N = 4, 6, and 8 respectively. It may be observed from this figure that the enhancement within BER is enlarged as N increased. For example, at BER = 10^{-3}, the attained gains within Eb/N0 for N = 4, 6, and 8 are 0.6, 1, and 1.3 dB respectively. Even though the gain values of the coding scheme are not high, its performance is deemed extremely good given that it generates error correction without the necessity for redundant bits.

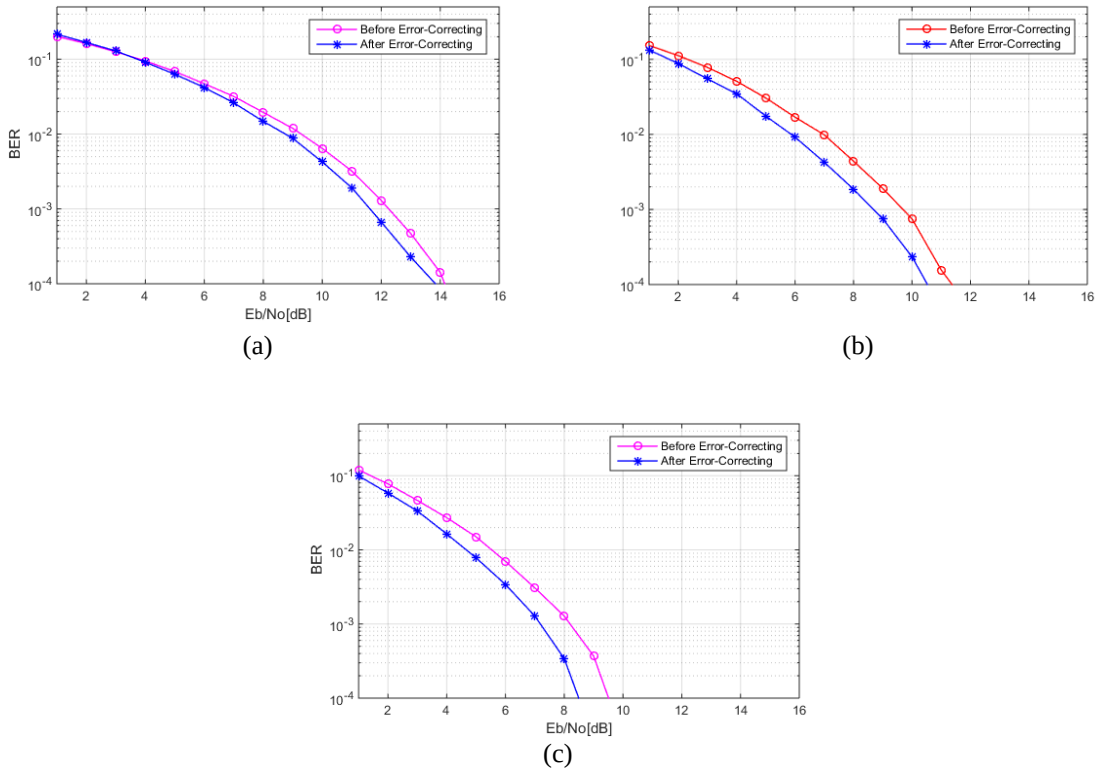


Figure 7. BER performance before and after error correction (a) N=4, (b) N=6, (c) N=8

Figure 8 shows the BER performance of the proposed system as compared with the system work in [12] that uses linear chaotic tent map when N=4 for both cases. From this figure, it may be observed that the proposed method has better performance in noisy channel. At BER = 10^{-3}, 2.45 dB gain in E_b/N_0 is obtained using the proposed method over the previous method. The improvement introduced by the proposed method is referred to the nature of the trajectory of chaotic map and the spreading factor of signal. The use of chaotic map with values alternating between positive and negative values acts to reduce BER in noisy channel.

One of the restriction aspects to the chaotic coding scheme is the raise of computational complexity regarding the amount of multiplications required. Our proposed error correcting technique enhances the delay parameter as contrasted with technique in [12] which as well employs suboptimal technique. Figure 9 illustrates the computational complexity of proposed technique by means of normalized correlation about the amount of multiplications as contrasted with the suboptimal technique. It may be viewed in this figure that a considerable reduction in computations is attained using the proposed technique and this reduction rises as N increases. This lessening is referred to calculating the correlations linked to the earlier and next bits only rather than all bits stream of as in the conventional technique. At N=8, the number of reduction acquired is 68%.

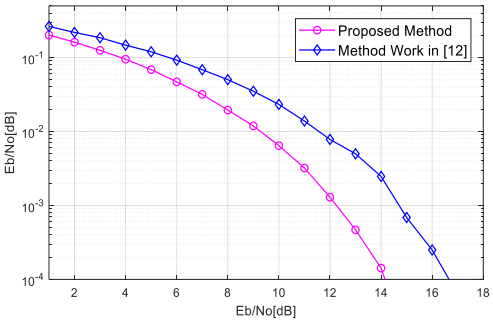


Figure 8. BER performance for proposed method and method in [12] when N=4

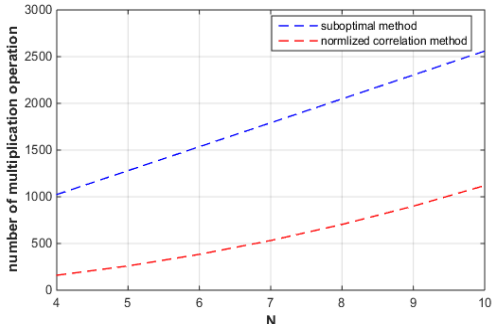


Figure 9. Computational complexity of chaotic coding scheme with N as a parameter for error correction method

8. CONCLUSION

Chaotic dynamics may be used as extra information to appropriately recover the conveyed data. The error-correcting system does not need any redundant bit sequence given that the error correction uses the chaotic dynamics inherent in the conveyed signal blocks. The scheme provides enhancement in Eb/N0 over traditional chaotic shift keying scheme and this enhancement is augmented as the amount of the sequence is enlarged. The proposed error correction reduces the delay in operation as contrasted with other techniques since the correction delay relies just on computations linked to the earlier and next bits. The capability of the system to correct errors without redundancy may be deemed as the radical section of the performance enhancement.

ACKNOWLEDGMENTS

The authors would like to thank the head and the staff of communication engineering laboratory of electrical engineering department at the university of technology for their support and endless cooperation throughout this work.

REFERENCES

[1] G. Kolumba´n, et al., "Differential chaos shift keying: A robust coding for chaos communication," *in Proceedings of NDES'96 international conference*, pp. 87-92, Jan 1996.
[2] S. Fadhel, et al., "Chaos Image Encryption Methods: A Survey Study," *Bulletin of Electrical Engineering and Informatics*, vol. 6, pp. 99-104, Mar 2017.
[3] F. C. M. Lau and C. K. Tse, "Chaos-Based Digital Communication Systems," Springer, 2003.
[4] E. R. Arboleda, et al., "Chaotic Rivest-Shamir-Adlerman Algorithm with Data Encryption Standard Scheduling," *Bulletin of Electrical Engineering and Informatics*, vol. 6, pp. 219-227, Sep 2017.
[5] A. D. Wowor and V. B. Liwandouw, "Domain Examination of Chaos Logistics Function As A Key Generator in Cryptography," *IJECE* , vol. 8, pp. 4577-4583, Dec 2018.
[6] P. Stavroulakis, "Chaos Applications in Telecommunications," Talor & Francis Group, 2006.
[7] A. Sambas, et al., "A New Chaotic System with a Pear-Shaped Equilibrium and Its Circuit Simulation," *IJECE*, vol. 8, pp. 4951-4958, Dec 2018.
[8] H. A. Abdullah and H. N. Abdullah, "A New Chaotic Map for Secure Transmission," *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 16, pp.1135-1142, Jun 2018.

[9] M. Hasler and T. Schimming, "Chaos communication over noisy channels," *Int. J. Bifurcation and Chaos*, vol. 10, pp. 719-736, Apr 2000.
[10] Z. Liu and J. Zhang, "Design of the differential chaos shift keying communication system based on DSP builder," *Computer Modelling & New Technologies*, vol. 18, pp. 138-143, 2014.
[11] S. Arai and Y. Nishio, "Suboptimal receiver using shortest distance approximation method for chaos shift keying," *Journal of Signal Processing*, vol. 13, pp. 161-169, 2009.
[12] S. Arai, et al., "Error-correcting scheme based on chaotic dynamics and its performance for non-coherent chaos communications," *Journal of Non-linear Theory and its Applications, IEICE*, vol. 1, pp. 196-206, 2010.
[13] W. C. Huffman and V. Pless, "Fundamentals of Error-Correcting Codes," Cambridge University Press, 2003.
[14] V. G. Jadhao and P. D. Gawand, "Performance Analysis of Linear Block Code, Convolution code and Concatenated code to Study Their Comparative Effectiveness," vol. 1, pp. 53-61, Jun 2012.
[15] H. N. Abdullah, et al., "Suboptimal Detection of Modified Logistic Map Based Chaos Shift Keying Modulation," *U.P.B. Sci. Bull., Series C Journal*, vol. 80, 2018.

BIOGRAPHIES OF AUTHORS

Hikmat. N. Abdullah was born in Baghdad, Iraq in 1974. He obtained his B.Sc. in Electrical Engineering in 1995, M.Sc. in Communication Engineering in 1998 at University of Al-Mustansiryah, Iraq and Ph.D. in Communication Engineering in 2004 at University of Technology, Iraq. From 1998 to 2015 he worked as associate professor in the Electrical Engineering Department, at Al-Mustansiryah University, Iraq. Since the beginning of 2015 he works as full professor in college of Information Engineering at Al-Nahrain University, Iraq. From 2011–2013 he got a research award from International Institute of Education (IIE/USA) at Bonn-Rhein-Sieg university of applied sciences, Germany. He is a senior member of IEEE association since 2014. He is interested in subjects of wireless communication systems and chaotic communications.

Thamir Rashed Saeed was Born in Baghdad, Iraq on February 10, 1965. He received the B.Sc. degree from military engineering college in Baghdad in 1987, the M.Sc. degree from military engineering college in Baghdad in 1994 and Ph.D. degree from AL-Rashed college of engineering and Science in Baghdad 2003. From 1994 to 2003, he worked with military engineering college in Baghdad as a member of teaching staff. From 2003 till now, he worked with the University of Technology in Baghdad as a member of teaching staff. Currently, he is Assist. Professor of electrical engineering at university of Technology. His major interests are in digital signal processing, digital circuit design for DSP based on FPGA, Radar, sensors network and Pattern Recognition.

Asaad Hameed Sahar was born in Baghdad, Iraq in 1987. He obtained his B.Sc. in Electronics Engineering in 2010, M.S.c. in Electronics Engineering in 2013 at University of Technology, Iraq. In 2015 he joined Ph.D. study in Electronic and Communication Engineering at University of Technology.