Performance Enhancement of Chaotic Error Correction Coding Using Consecutive Sequences

Asaad H. Sahar[1], Hikmat N. Abdullah[2], and Thamir R. Saed[3]

[1] *University of Baghdad, Baghdad, Iraq,*
[2] *Al-Nahrain University, Baghdad, Iraq,*
[3] *University of Technology, Baghdad, Iraq*

https://doi.org/10.26636/jtit.2023.169423

Abstract — The use of chaotic dynamics for error correction is the subject of extensive research, as the approach allows to avoid the use of redundant data. This work proposes a new technique for non-coherent chaos communications for modifying error-correction depending on chaotic dynamics. In the proposed system, there are two consecutive sequences created from a comparable chaotic map, with the second series being created as the latest value of the initial one. Generation of a sequential chaotic sequence with a comparable chaotic dynamic delivers additional information to the receiver, allowing it to appropriately recover information and, hence, facilitate the receiver's bit-error performance. For error correction and for detecting the symbol that is transmitted, a suboptimal technique based on the nearest distance between chaotic map trajectories over the n-dimensional sequence received is utilized. Simulation results show that the proposed error correction approach improves E_b/N_0 as the dimension of the trajectory map increases, indicating that the method improves overall error correction performance. With the dimension of 4, a gain of 0.8 dB in E_b/N_0 is achieved compared with an approach without any error-correcting schemes, at the bit-error probability of 10^{-3}.

Keywords — chaos communication, DCSK modulation, error correction, suboptimal receiver.

1. Introduction

Chaos-based techniques have been receiving increased attention in recent years in various fields and analyses [1]–[3]. Chaotic series derived from a specific class of difference equations are sensitive to initial conditions, non-periodic, and are difficult to predict based on obsolete data. Furthermore, it was established that simple 1D maps might produce chaotic series. Therefore, many researchers specializing in nonlinear circuits and systems focus on developing chaos applications, since chaotic system execution has become very simple [3]–[5].

In the field of engineering, chaos communication systems are a common topic. Several researchers are focusing on the development of non-coherent detection approaches which do not necessitate the application of basis signals serving as unmodulated carriers for demodulation at the receiver [6]–[8]. In standard communication systems, basis signals ought to be replicated for demodulation at the receiver. Therefore, it is not easy to implement detection of non-coherent signals in such systems. On the other hand, non-coherent detection relying on chaos could demodulate information without any basis signals, because chaotic sequences and chaos are characterized by highly unique features [5], [8]–[12]. Therefore, the non-coherent detection approach is recognized as a distinctive detection method relying on chaos techniques.

The optimum receiver type and differential chaos shift keying (DCSK) modulation [1] are non-coherent systems designed for use in [13]. In a situation where the length of a chaotic series N becomes long, the computation overhead becomes quite complex, rendering signal detection very challenging. To cope with this, Arai *et al*. [14] recommended a technique for identifying symbols based on the computation of the minimum distance between the chaotic map and the received signals, thus creating a suboptimal receiver. Rather than computing PDF, the sub-optimal receiver estimates PDFs by calculating the minimal distance between the chaotic map and the received signals. A number of researchers apply their channel coding approaches without using chaos in modulation schemes [15]. The symbolic dynamics related to chaotic maps are predominantly applied as error correction criteria. It is possible for the chaos-based channel coding methods to either be non-redundant or redundant. The best results in terms of the transmission rate are offered by non-redundant schemes, whereas their redundant counterparts are characterized by better BER performance. In our recent research, we recommended an error-correction scheme that is effective according to normalized correlation for chaos that constitutes non-coherent communication system without redundancy bits [16]. In this paper, a suboptimal receiver capable of error correcting coding is proposed. The said receiver is non-redundant and incorporates a mutual chaos technique based on non-coherent modulation. The designed system applies two consecutive chaotic series determined by a tent map, with the initial value of the second series being the end value of the first sequence. Such a characteristic provides additional information to the receiver, enabling it to retrieve data properly. The system presented below offers decent delay, since the maximum delay for rectifying one bit is determined by the following and the preceding series only.

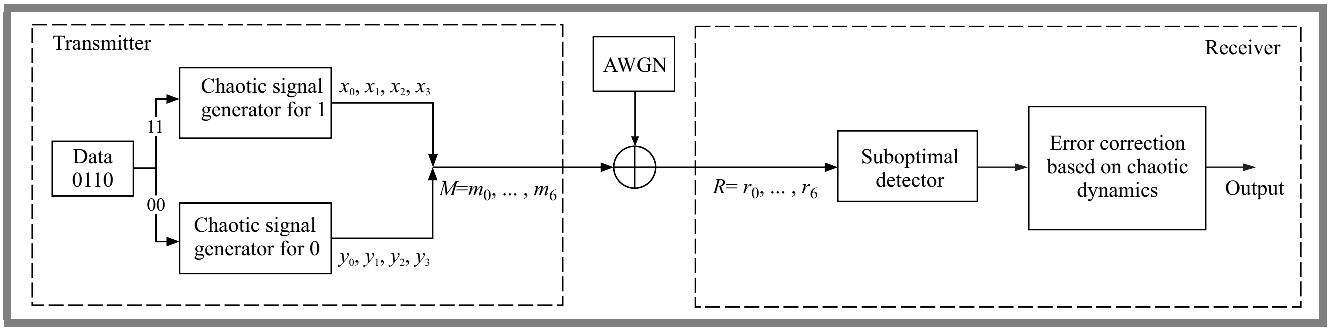

Fig. 1. CSK system with the proposed error correction coding scheme.

2. Structure of the Proposed System

Figure 1 shows a chaotic shift keying (CSK) block diagram with a suboptimal receiver system. The transmitter side applies one from two potential chaotic maps for modulation of input data. This map is chosen based on the input bit value of 1 or 0. During the modulation process, the data are encrypted concurrently through the creation of a statistical correlation between the two sequential chaotic signals that correspond to the two sequential data bits.

This concept of the receiver allows to retrieve more data and to determine the initial value of each series.

On the transmitter side, the input data are encrypted using a series created by the chaotic map in the transmitter. A skew tent map is used in this paper, which is described by:

$$x_{i+1} = \begin{cases} \dfrac{2x_i + 1 - a}{1 + a} & -1 \leqslant x_i \leqslant a \\ \dfrac{-2x_i + 1 + a}{1 - a} & a \leqslant x_i \leqslant 1 \end{cases} . \tag{1}$$

The top position from the skew tent map is $a = 0.05$. When data symbol is 1, the chaotic series defined by Eq. (1), are utilized. For the data symbol of 0, the inverse tent map is used in order to generate the chaotic sequence, as shown in Fig. 2. Next, N chaotic signals are created from the same chaotic map for each data bit. Thus, in the case of K bits having been transmitted, the number of chaotic signals becomes $K \times N$. The initial value of the chaotic sequence is chosen randomly to ensure that the chaotic sequence is unique, with the initial value of y_0 for symbol 0 and x_0 for symbol 1. The current sequence's end value becomes the first value of the following one, with the same symbol value.

For example, if $N = 4$, $K = 5$, and the data bits are 01101, the initial value for the sequence decoding symbol of 1 is x_0, and the initial value for the sequence decoding the symbol of 0 is y_0. Both of these values are chosen randomly at the start, as shown in Fig. 3. The vector of the transmitted signal s is:

$$\begin{aligned} \mathbf{s} &= (s_0, \ldots, s_4) \\ &= (y_0, \ldots, y3, x_0, \ldots, x_7, y_4, \ldots, y_7, x_8, \ldots, x_{11}) \\ &= (s_0, \ldots, s_{19}) \, . \end{aligned} \tag{2}$$

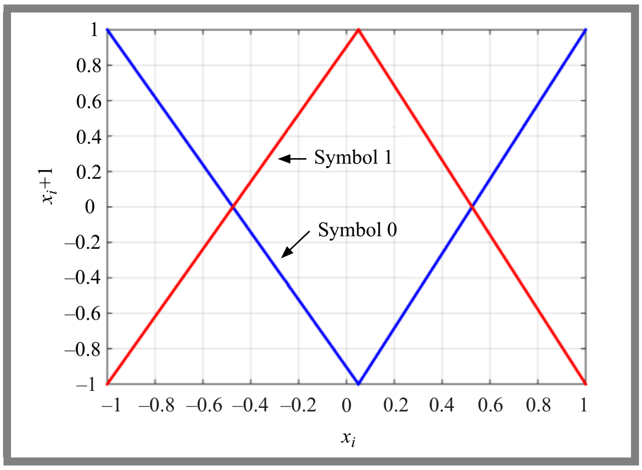

Fig. 2. Tent map trajectory.

The initial value, which is the end value of the second sequence, is utilized to create the third series. The end value of the first sequence, i.e. the initial value, is used to create the fourth series. The chaotic dynamics of subsequent chaotic series formed in this manner follow the same idea. More information regarding such a feature is sent to the receiver, so the noisy signal can be recovered. Since the proposed error correction approach for the transmitted chaotic signal uses chaotic dynamics, no additional redundancy bits are required.

2.1. Noisy Channel

AWGN has a variance of $N_0 = \sigma^2$ and an average value of 0. $R = S + \text{AWGN} = \left[r_0, r_1, r_2, r_3, \ldots, r_{K \times N}\right]$ is the received signal block that is passed as input to the algorithm to recognize transmitted symbols and to perform error correction. The value of the transmitted data is unknown to the non-coherent receiver, as it only deals with the sort of chaotic map used by the transmitter.

3. Detection Algorithm

To discriminate the transmitted symbol, the sub-optimal receiver estimates the probability density function (PDF) by computing the minimum distance between the chaotic map and the received signal. To be more exact, the receiver uses N_d sequential signals received ($N_d \leqslant N$) for com-

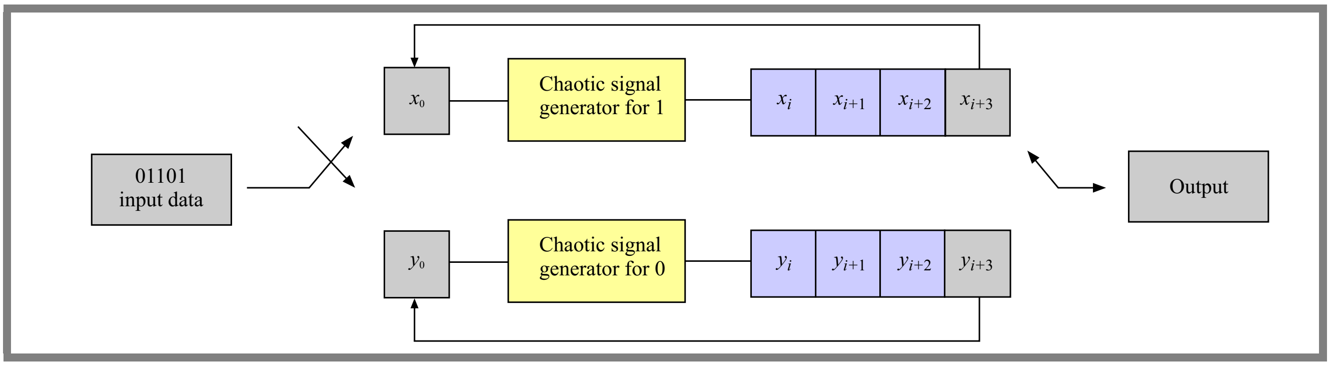

Fig. 3. CSK encoder proposed for error correction.

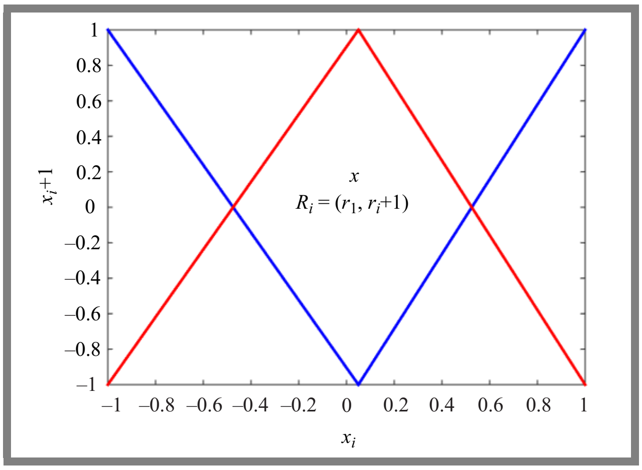

Fig. 4. N_d in 2D space.

puting the minimum distance between the chaotic map and the received signal in an N_d-dimensional space ($N_d = 2, 3, \ldots$). Figure 4 shows the tent maps in 2D space, with the coordinates corresponding to two subsequent signals received $R = (r_i, r_{i+1})$, $i = 1, 2, \ldots, N{-}1$. In the 2D space shown in Fig. 4, the minimum distance between the point and the map is calculated with the goal of selecting the map that is closest to point R. The receiver calculates the shortest distance with the use of a scalar product. Two vectors are required for the scalar product.

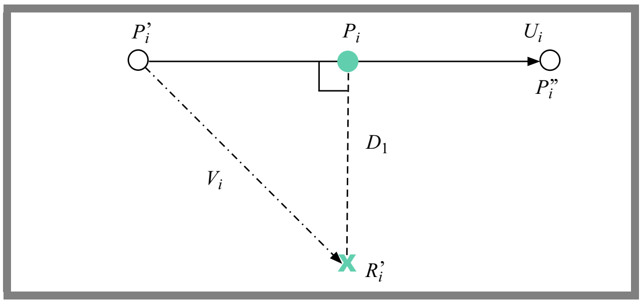

Fig. 5. Calculation of the shortest distance.

Minimum distance D between the nearest point $P = (x, y)$ and R, as illustrated in Fig. 5, has been determined using the equations below, regardless of which 2 points of $P_0 = (x_0, y_0)$ and $P_1 = (x_l, y_l)$ are selected from any curved line in the space shown in Fig. 4 [6]–[9]:

$$A = \sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2}\,, \tag{3}$$

$$u = (l,\, m) = \left(\frac{x_1 - x_0)}{A}\,, \frac{y_1 - y_0}{A}\right)\,, \tag{4}$$

$$v_0 = (r_i - x_0,\; r_{i+1} - y_0)\,, \tag{5}$$

$$T = l(r_i - x_0) + m(r_{i+1} - y_0)\,, \tag{6}$$

$$P = (x, y) = (T_l + x_0, T_m + y_0)\,, \tag{7}$$

$$D = \sqrt{(x - r_i)^2 + (y - r_{i+1})^2}\,. \tag{8}$$

Each symbol in the 2D space has two straight lines. The shortest distance is determined by the lowest value of the two distances, in which D_1 is related to symbol 1 and D_0 is related symbol 0. D_0 and D_1 are both evaluated for each of the k values and their summation calculations ΣD_0 and ΣD_1 are discovered. Finally, the decrypted symbol is specified as 0 (or 1) based on whether $\Sigma D_1 < \Sigma D_0$ or $\Sigma D_0 < \Sigma D_1$.

4. Error Correction for CSK

The error correction algorithm has been designed using chaotic dynamics. It follows sub-optimal detections, as shown in Fig. 6. The fundamental principle of the error correction pattern is presented in Fig. 7, with $K = 5$ and $N_d = 2$. The chaotic series samples for 1 and 0 data are represented by x_i and y_i, respectively. The sequence samples are combined, in turn, every two symbols ($N_d = 2$). In such mixed chaotic series, the chaotic dynamics regarding a few sequential samples are lost. For instance, y_0 is not the result of x_0 and x_1, nor is it the result of similar chaotic dynamics. It is possible to avoid such a loss of chaotic dynamics if a suitable criterion is used. This is caused by the fact that by analyzing chaotic dynamics for samples in the mixed chaotic series, the initial chaotic series may be reconstructed.

As illustrated in Fig. 8, the error correction mechanism used in the previous technique from [14] is based on correcting each bit in the stream.

5. Proposed Error Correction Algorithm

The proposed algorithm uses only the preceding and the following 1 and 0 symbols from the current symbol in the

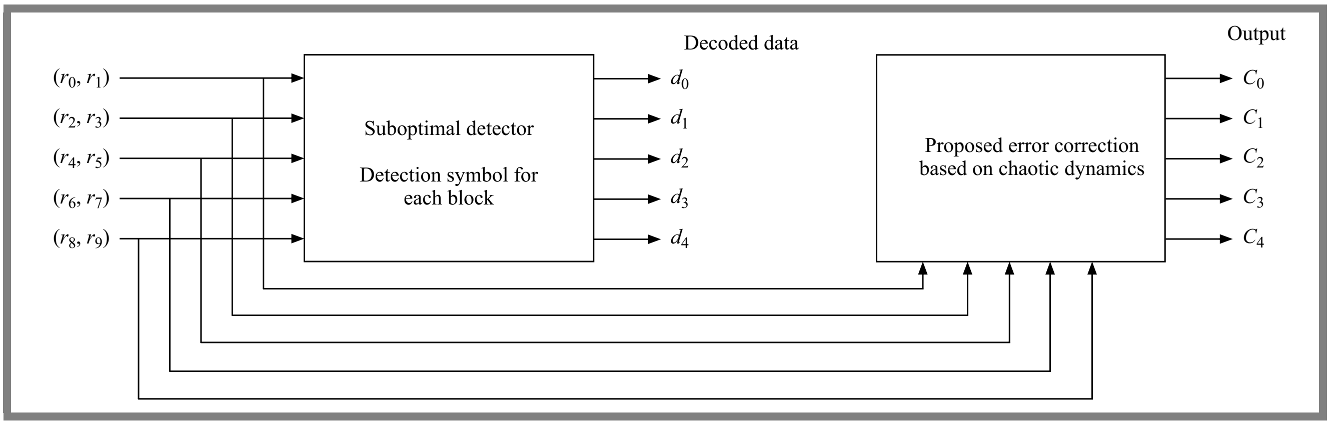

Fig. 6. Error correction algorithm diagram.

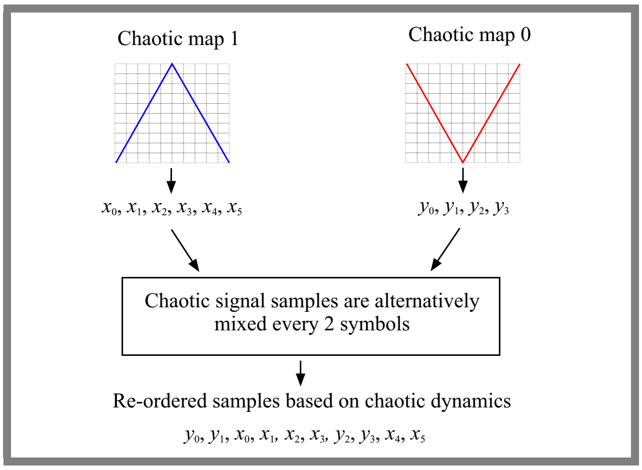

Fig. 7. Concept of the suggested error correction approach.

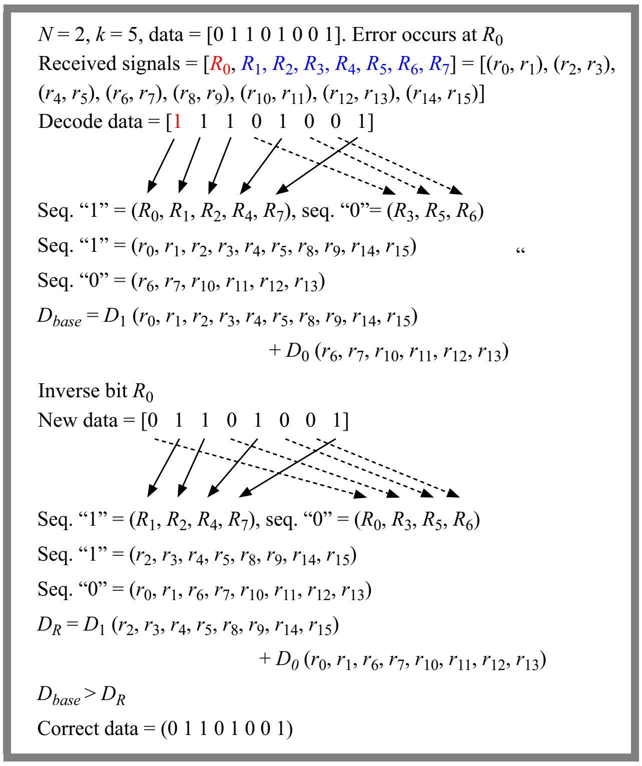

Fig. 8. Error correction algorithm method from [14].

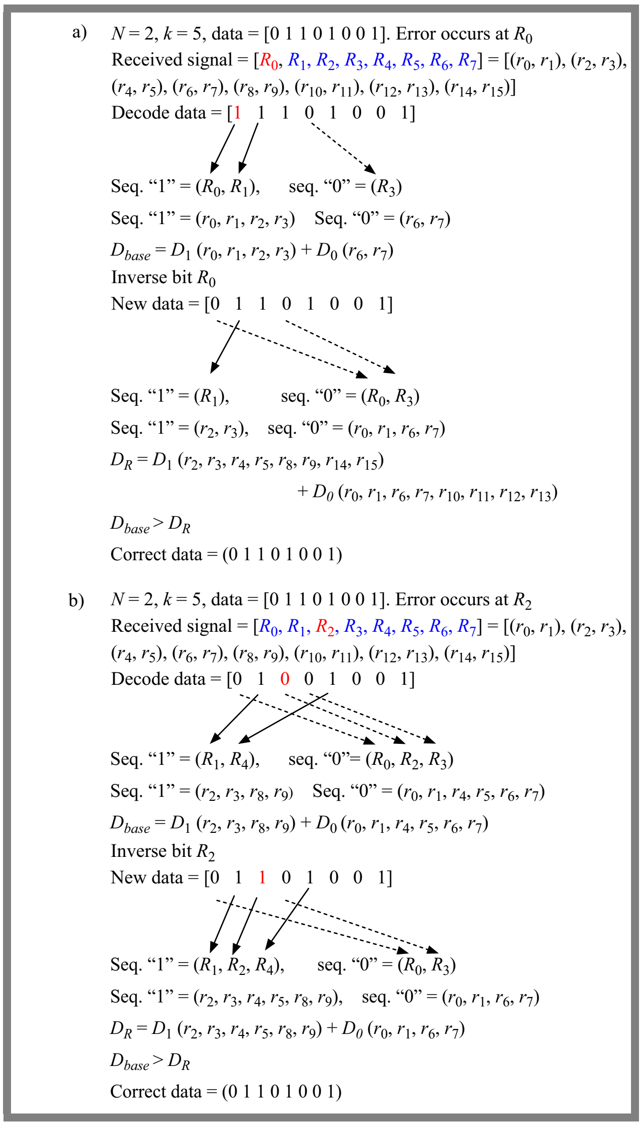

Fig. 9. Error correction algorithm used in the proposed approach: a) error occurs in the first bit, b) error occurs in the third bit.

error correction procedure. The recipient arranges the received samples based on the decrypted symbols, with the process yielding 2 sequences, i.e. seq. "1" from the previous 1 to the next 1 and seq. "0" from the next 0 to the previous 0.

The categorization blocks' depends on the case in which the current symbol 1 is mixed with seq. "1" otherwise with seq. "0" is the examination of the received series' chaotic dynamics. The sorted seq. "1" or seq. "0" aggregates two chaotic series that differ in chaotic dynamics if an error occurs while the receiver is detecting symbols. When it comes to error correction, such chaos aspects are crucial. The receiver then employs the sub-optimal detection algorithm which includes computation of the minimum distance D1 (seq. "1") between the chaotic map for symbol 1 and seq "1" as well as computation of the minimum distance D_0 (seq. "0") from the chaotic map to seq. "0" for symbol 0. For the purpose of studying chaotic dynamics, a reference distance D_{Base} is also defined as:

$$D_{Base} = D_1\big([Seq.\,1(.)]\big) + D_0[Seq.\,0(.)]\,. \qquad (9)$$

The receiver reverses the decoded symbols and then reorganizes seq. "1" and seq. "0" in accordance with the current opposite symbol. For new series, the receiver employs suboptimal computation and detection using the shortest distance. In order to investigate chaotic dynamics, a new assessment distance is specified as $D_R(m)$, in which $m = 0, 1, \ldots, K{-}1$, where subscript R denotes the reverse initial character. In a case in which the chaotic map conforms to its series and m-th decrypted symbol is inverted, $D_R(m)$ denotes the minimum distance between the series that have been arranged. An error correction algorithm defined in such a manner is depicted in Fig. 9.

6. Simulation Results

To evaluate the efficiency of the proposed error correction approach, Matlab was used with $K = 32$ and a chaotic map with $a = 4$. For each 1 bit, the length of the chaotic series is $N = 4$. We used $N_d = 2, 3$, and 4 to calculate the shortest distance. The process was repeated 10,000 times in order to achieve acceptable level of precision of BER calculations. For $N_d = 2, 3, 4$, and $N = 4$, BER for E_b/N_0 with N as the structure for a sub-optimal receiver devoid of error correction is illustrated in Fig. 10. It is evident from the figure that in the case of $N_d = 4$ (i.e. when $N = N_d$), error correction performance is considerably improved. When $\mathrm{BER} = 10^{-3}$ is used, E_b/N_0 increases by 1.6 dB with $N_d = 4$ instead of $N_d = 2$. Higher N_d increase the precision of computing the distance between the received point and the trajectory of the skew tent map.

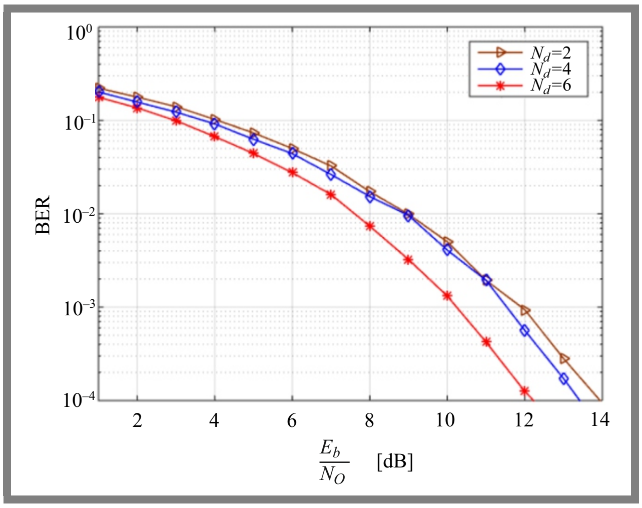

Fig. 10. BER for various N_d values.

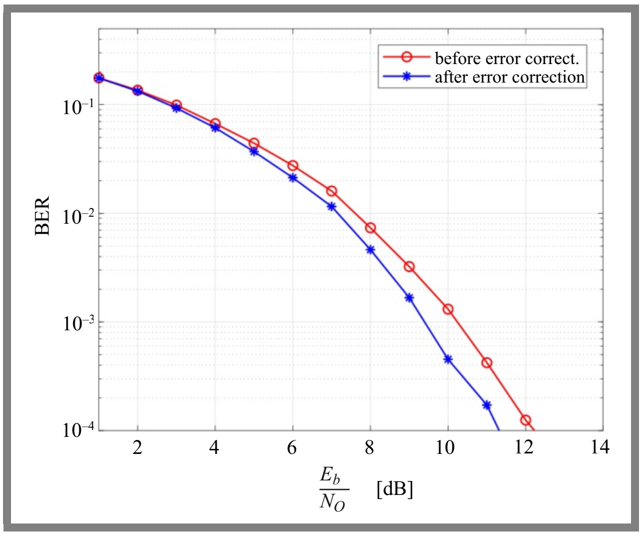

Fig. 11. BER after and before error correction, $N_d = 4$.

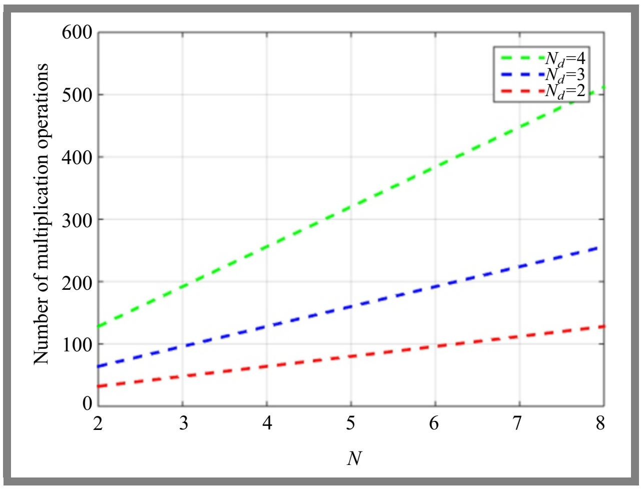

Fig. 12. Chaotic coding complexity as a function of N.

Such an enhancement is caused by the increase in the chaotic signal's spreading factor, but there is a drawback in the form of increased complexity of mathematical operations. Fig. 11 shows BER versus E_b/N_0 for $N = 4$ and $N_d = 4$ using the proposed approach to show the suboptimal receiver performance before error correction. The improvements in E_b/N_0 for $N_d = 4$ equal 0.4 dB, based on this figure, at $\mathrm{BER} = 10^{-3}$. In spite of the fact that the values achieved by the coding scheme are low, overall performance is considered to be excellent, since it eliminates the need for adding redundant bits in the error correction mechanism. Moreover, it is expected that performance will improve even more with a further N_d increase, however increasing N_d by more than 4 may make the system more difficult to compile.

Unfortunately, the increase in computational complexity caused by the number of the required multiplications when the dimension is increased, is one of the limitations of the chaotic coding scheme. The number of required multiplications is defined by Eqs. (3) and (8) and is equal to N. Consequently, the total number of multiplications in the two equations is $2N$, and such operations are repeated for each straight line. The number of straight lines is 2^{N_d-1}. Hence, $2N \times 2^{N_d-1}$ is the number of the required multiplication operations. For symbols 0 and 1, such a procedure should be applied to the chaotic map. As a result, the number of multiplications required is $4N \times 2^{N_d-1}$, and because the next and previous bits should be replicated, the total number of multiplications required is even higher and equals $8N \times 2^{N_d-1}$. The above-mentioned relation versus N with N_d as the parameter is shown in Fig. 12.

Figure 13 shows that the proposed approach outperforms the previous method with a similar $N_d = 4$ value as the delay parameter. To understand the number of multiplications

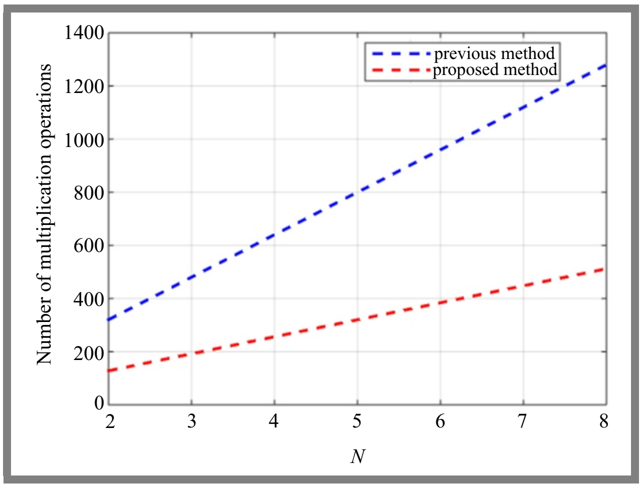

Fig. 13. Proposed and existing error correction method versus N parameter.

for the preceding techniques, Fig. 8 shows that multiplications will repeat for all k bits in the stream, resulting in $8N \times 2^{N_d-1} \times k$ multiplications. Table 1 shows the differences in the number of multiplications when the number of bits is 5 and $N_d = 4$.

Tab. 1. Number of required multiplications for proposed and previous error correlation methods.

N	Number of multiplication operations for the proposed method $8N \times 2^{N_d-1}$	Number of multiplication operations for the previous method $8N \times 2^{N_d-1} \times b$
4	320	800
5	384	960
6	448	1120
7	512	1280

7. Conclusions

Chaotic dynamics can be utilized as non-redundant error correction method. Such an error correcting system requires no redundant bit series due to the fact that it uses chaotic dynamics in the transmitted signal blocks. In terms of E_b/N_0 metrics, the system outperforms the traditional chaotic scheme with shift keying, and the advantage of the proposed method increases along with the number of series. The proposed error correction approach reduces operational delay when compared with other approaches, as the correction delay depends solely on calculations related to the preceding and following bits. The scheme's ability to correct errors without redundancy renders it worth considering as a performance improvement method.

References

[1] G. Kolumbán, B. Vizvári, W. Schwarz, and A. Abel, "Differential chaos shift keying: A robust coding for chaos communication", *in Proceedings of NDES'96 International Conference*, Jan. 1996, pp. 87–92 [Online]. Available https://www.researchgate.net/publication/239666158_Differential_chaos_shift_keying_A_robust_coding_for_chaos_communication.

[2] M.P. Kennedy and G. Kolumbán, "Digital communications using chaos", *Journal of Signal Processing*, vol. 80, no. 7, pp. 1307–1320, 2000 (https://doi.org/10.1016/S0165-1684(00)00038-4).

[3] M. Hasler and T. Schimming, "Chaos communication over noisy channels", *Int. Journal on Bifurcation and Chaos*, vol. 10, no. 4, pp. 719–735, 2000 (https://doi.org/10.1142/S0218127400000505).

[4] F.C.M. Lau and C.K. Tse, *Chaos-Based Digital Communication Systems*. Springer, 2003 (https://doi.org/10.1007/978-3-662-05183-2).

[5] F.C.M. Lau and C.K. Tse, "Approximate-optimal detector for chaos communication systems", *Int. Journal of Bifurcation and Chaos*, vol. 13, no. 5, pp. 1329–1335, 2003 (https://doi.org/10.1142/S0218127403007266).

[6] W.M. Tam, F.C.M. Lau, and C.K. Tse, "Generalized correlation-delay-shift-keying scheme for noncoherent chaos-based communication systems", *IEEE Trans. Circuits and Systems Part I*, vol. 53, no. 3, pp. 712–721, 2006 (https://doi.org/10.1109/ISCAS.2004.1329075).

[7] L.E. Larson, J-M. Liu, and L.S. Tsimring, *Digital Communications Using Chaos and Nonlinear Dynamics*. Springer, 2006 (https://doi.org/10.1007/0-387-29788-X).

[8] W.M. Tam, F.C. Lau, and K.T. Chi, *Digital Communications with Chaos: Multiple Access Techniques and Performance*. Elsevier, 2006 (https://www.elsevier.com/books/digital-communications-with-chaos/tam/978-0-08-045151-0).

[9] C.P. Silva and A.M. Young, "Introduction to chaos-based communications and signal processing", in *Proc. IEEE Aerospace Conference*, vol. 1, pp. 279—299 (https://doi.org/10.1109/AERO.2000.879402).

[10] P. Stavroulakis, Ed., *Chaos Applications in Telecommunications*, 1st ed. Boca Raton: CRC Press, 2005 (https://doi.org/10.1201/9780203025314).

[11] G. Kaddoum and F. Gagnon, "Error correction codes for secure chaos-based communication system", *25th Biennial Symposium on Communications*, Kingston, Canada, 2010, pp. 193–196 (https://doi.org/10.1109/BSC.2010.5472918).

[12] U. Parlitz, L.O. Chua, L. Kocarev, K.S. Halle, and A. Shang, "Transmission of digital signals by chaotic synchronization", *Int. Journal of Bifurcation Chaos*, vol. 2, no. 4, pp. 973–977, 1992 (https://doi.org/10.1142/9789812798855_0019).

[13] M. Hasler and T. Schimming, "Optimal and suboptimal chaos receivers", *Proceedings of the IEEE*, vol. 90, no. 5, pp. 733–746, 2002 (https://doi.org/10.1109/JPROC.2002.1015004).

[14] S. Arai, Y. Nishio, and T. Yamazato, "Error-correcting scheme based on chaotic dynamics and its performance for non-coherent chaos communications", *Nonlinear Theory and its Applications*, *IEICE*, vol. 1, no. 1, pp. 196–206, 2010 (https://doi.org/10.1587/nolta.1.196).

[15] H.N. Abdullah, T.R. Saeed, and A.H. Sahar, "Suboptimal Detection of Modified Logistic Map Based Chaos Shift Keying Modulation", *U.P.B. Sci. Bull.*, *Series C*, vol. 80, no. 3, 2018 (https://www.academia.edu/70642142/Suboptimal_Detection_of_Modified_Logistic_Map_Based_Chaos_Shift_Keying_Modulation).

[16] H.N. Abdullah, T.R. Saeed, and A.H. Sahar, "Efficient error correcting scheme for chaos shift keying signals", *IJECE*, vol. 9, no 5, pp. 3550–3557, 2019 (https://doi.org/10.11591/ijece.v9i5.pp3550-3557).

Asaad H. Sahar, Ph.D.
Assistant Lecturer at Department of Electronics and Communication Engineering
https://orcid.org/0000-0003-3655-0162
E-mail: asaad.ha87@gmail.com
University of Baghdad, Baghdad, Iraq

Hikmat N. Abdullah, Ph.D.
Professor at College of Information Engineering
https://orcid.org/0000-0002-1133-2057
E-mail: dr.h.abdullah@ieee.org
Al-Nahrain University, Baghdad, Iraq

Thamir R. Saed, Ph.D.
Assistant Professor at Department of Electrical Engineering
E-mail: thamir_rashed@yahoo.com
University of Technology, Baghdad, Iraq