PERFORMANCE ASSESSMENT OF CHAOTIC SEQUENCE DERIVED FROM BIFURCATION DEPENDENT LOGISTIC MAP IN CDMA SYSTEM

Oluyemi E. Adetoyi[1] and Solomon A. Adeniran[2]

[1] Electrical and Electronic Engineering Department, University of Ibadan, Nigeria

[2] Electronic and Electrical Engineering Department, Obafemi Awolowo University, Ile-Ife, Nigeria

ABSTRACT

In CDMA system, m-sequence and Gold codes are often utilized for spreading-despreading and scrambling-descrambling operations. In a previous work, a design framework was created for generating large family of codes from logistic map, which have comparable autocorrelation and cross correlation to m-sequence and Gold codes. The purpose of this work is to evaluate the performance of these chaotic codes in a CDMA environment. In the bit error rate (BER) simulation, matched filter, decorrelator and MMSE receiver have been utilized. The received signal was modelled for synchronous CDMA uplink for simulation simplicity purpose. Additive White Gaussian Noise channel model was assumed for the simulation.

KEYWORDS

CDMA, Chaotic codes, Linear Receivers, Logistic Map, Lyapunov exponent

1. INTRODUCTION

Code Division Multiple Access (CDMA) capacity is dependent on a number of factors, of which spreading code plays a crucial role (Meenakshi & Chawla, 2014). Lot of efforts has been made towards developing optimal codes both for synchronous and asynchronous CDMA. The m-sequence, Gold sequence and Kasami sequence that are currently used asynchronously in CDMA, all have limitations. M-sequence has small set and poor cross correlation; Gold codes have poorer correlation than m-sequence, but larger set. Small Kasami has better correlation than Gold, but small set; while large Kasami has poorer correlation values than Gold, but contain more sequences (Meenakshi & Chawla, 2014) (Sawlikar & Sharma, 2011) (Pickholtz, Milstein, & Schilling, 1982). The essence of this research work is to create a framework for generating large sets of optimal codes for asynchronous CDMA. Recent researches have shown that apart from linear shift registers sequences (m-sequences, gold sequences etc), chaotic sequences have good correlation properties and large family size (Umeno & Kitayama, 1999) (Vladeanu, Banica, & Assad, 2003) (Zhang, Guo, Wang, Ding, & Chen, 2000). The low autocorrelation side-lobes of these chaotic sequences allow for easy synchronization with the receiver; while the low cross correlation reduces the multiple access interference. They have been considered as good candidate

DOI: 10.5121/ijcnc.2016.8506

for application in DS-CDMA system. In (Adetoyi & Adeniran, 2016), we presented a method for generating chaotic sequences by exploiting the bifurcation control of the logistic map. The BER performance of these bifurcation dependent sequences, in a DS-CDMA environment, is exploited in this paper.

2. RELATED WORK

In (Umeno & Kitayama, 1999), chaotic sequence was generated from second order Chebyshev polynomial ($X_{j+1} = 2X_j - 1$), which is one form of logistic map. The real valued chaotic sequence was obtained by calculating the periodic points, which was translated to corresponding binary sequence using the well established symbolic dynamics correspondence ($S_j = sgn[X_j]$). Here sgn(x) = 1 for x > 0 and sgn(x) = -1 for x < 0. Two sequences of period 15 and three sequences of period 7 were generated using this method. The normalized autocorrelation and cross correlation for 7-bit length was 0.5221 and 0.6757 as against 0.72143 for Gold. The 15-bit length normalized autocorrelation and cross correlation was 0.3314 and 0.3293 as against 0.3333 and 0.4667 for small Kasami set.

The generation of OverSampled Chaotic Map binary sequences was presented in (Zhang, Guo, Wang, Ding, & Chen, 2000), where Chebyshev map was also used. The generalized OSCM is

$$x = f^{(p)}(x_n) \quad (p = 2,3,4,\ldots.) \tag{2.17}$$

where p = 1 is the parent map.

The binary sequence was obtained by using threshold and also by writing the absolute value of x in a floating point number with m-bits:

$$|x| = 0.b_1(x)\, b_1(x)\, b_2(x)\ldots.. b_i(x)\ldots b_{m1}(x) \qquad b_i(x) \in \{0,1\} \tag{2.18}$$

It was found that the balance property of the sequences produced by both methods was worse than Gold sequences or Kasami Sequences, except the period is very large. The sequences were considered good candidate for CDMA and W-CDMA. It is doubtful if large family can be realized.

In (Vladeanu, Banica, & Assad, 2003), a method of selecting optimal sequences from sequences generated in (Umeno & Kitayama, 1999) was presented. A best limit value of $min\{max\{C_A, C_C\}\} = 5$ was imposed on the binary pn sequences; as such only chaotic sequences that presents less than this value were selected. This produced smaller set of sequences than in (Umeno & Kitayama, 1999).

In (Pareek, Patidar, & Sud, 2010), a method to generate random sequences from two logistic maps connected in cross-coupled manner was presented. The bit sequence was generated by comparing the outputs of both the logistic maps in the following way:

$$g(X_{n+1}, Y_{n+1}) = \begin{cases} 0 \text{ if } X_{n+1} > Y_{n+1} \\ 1 \text{ if } X_{n+1} \leq Y_{n+1} \end{cases} \tag{2.19}$$

The set of initial conditions (X_0, Y_0 ,ϵ (0,1) and $X_0 \neq Y_0$) serves as the seed for the PRBG, it produces the same bit sequence if exact same seed was used, due to the deterministic procedure.

Two thousand sequences having one million bits length were subjected to NIST randomness test and nine test results were presented. The proportion of sequences that passed the test at a significant level (α) of 0.01 is at least 98.6%. The sequences are considered good enough for secure cryptosystem.

In (Spinsante, Andrenacci, & Gambi), De Bruijn sequences generated from combinatorial mathematics was presented. Although the family size is large, the generation process is complex. The analysis was shown only for De Bruijn sequences with a length of 32 bits. The normalized radar ambiguity diagrams of De Bruijn and the chaotic sequences was compared, the differences in their performance, with respect to distance and doppler resolution determined by the main peak level, and the sidelobes level on the plane, were not significant. Results show that in some scenarios, and with given assumptions, De Bruijn sequences may provide improved performance with respect to systems adopting chaotic sequences. It was suggested that it can be used in DS-CDMA if the correlation selection criteria is defined, then its performance will be comparable to currently used CDMA codes.

In (Suneel, 2009), the sequences generated from Henon map was considered random enough and having large key space to be used for cryptographic applications. Henon map is a two-dimensional discrete-time nonlinear dynamical system represented by the state equations:

$$x_{k+1} = -\alpha x_k^2 + y_k + 1 \tag{2.20a}$$

$$y_{k+1} = -\beta x_k \tag{2.20b}$$

Generating a pseudorandom binary sequence from the orbit of a chaotic map essentially requires mapping the state of the system to $\{0, 1\}$. The two bits b_x and b_y derived respectively from the *x* and *y* state-variables are as follows:

$$b_x = \begin{cases} 1 & \text{if } x > \tau_x \\ 0 & \text{if } x \leq \tau_x \end{cases} \tag{2.21}$$

$$b_y = \begin{cases} 1 & \text{if } y > \tau_y \\ 0 & \text{if } y \leq \tau_y \end{cases} \tag{2.22}$$

Here, τ_x and τ_y are appropriately chosen threshold values for state-variables *x* and *y,* such that the likelihood of $x > \tau_x$ is equal to that of $x \leq \tau_x$ *and* $y > \tau_y$ is equal to that of $y \leq \tau_y$. Therefore the median of large consecutive values of *x and y were used*. Thus, two streams of bits $S_x = \{b_x^i\}_{i=1}^{\infty}$ and $S_y = \{b_y^i\}_{i=1}^{\infty}$were obtained from the map. Bit-streams B_x *and* B_y are formed by choosing every *P*th bit of S_x *and* S_y *respectively* and the jth bit of these two sequences are $B_x(j)$ and $B_y(j)$. Then, the pseudo-random output bit *O* is chosen as per the following rule:

$$O(j) = \begin{cases} B_x(j) & \text{if } B_y(j-2) = 0 \text{ and } B_y(j-1) = 0; \\ \overline{B}_x(j) & \text{if } B_y(j-2) = 0 \text{ and } B_y(j-1) = 1; \\ B_y(j) & \text{if } B_y(j-2) = 1 \text{ and } B_y(j-1) = 0; \\ \overline{B}_y(j) & \text{if } B_y(j-2) = 1 \text{ and } B_y(j-1) = 1; \end{cases} \tag{2.23}$$

A multilevel spreading codes for DS-CDMA using ternary and quaternary Gray Inverse Gray (GIG) codes was proposed in (Usha & Sankar, 2013). The 3-level, 6-length ternary and 4-level, 8-length quaternary GIG codes obtained have autocorrelation and cross correlation that is better than Gold.

3. BIFURCATION DEPENDENT CHAOTIC SEQUENCES – A REVISIT

The method for generation of the bifurcation dependent sequences has been fully described in (Adetoyi & Adeniran, 2016). The discrete form of the original logistic map was modified to accommodate the bifurcation control in Equation 1.

$$x_{n+1} = r_u x_n (1 - x_n) \tag{1}$$

where u denotes the number of sequences that take integer values; n is the length of the sequence and also an integer and x_0 is the initial condition for the special case when $n = 0$. The real sequences were generated using the first domain D_1 of Figure 1, out of the ten purely chaotic domains created from the chaotic region of the logistic map using Lyapunov exponent estimation. The logistic map was iterated in the D_1 domain for different values of bifurcation parameter taken with an accuracy of 10^{-4}, but fixed initial condition of 0.7. The choice of the initial condition was arbitrary, since it is fixed for all bifurcation values. Since it usually takes finite length of time for the sequences to be uncorrelated, in this case approximately ten iterates; then to generate N-bit length sequences, the map was iterated *N + 20* times and the first twenty iterates were discarded. Two-bit encoding of the real chaotic sequences was done, in order to reduce quantization error. The threshold for taking encoding decision was determined by subjecting a training sequence to Lloyd compression algorithm, which optimizes the partition quantization parameter. The encoding of the real value sequence x_{n+1} was done for 2-bit encoding according to the decision

$$x_i = \begin{cases} 00 \; if \; x_{n+1} \leq \quad LT1 \\ 01 \; if \; LT1 < x_{n+1} \leq LT2 \\ 10 \; if \; LT2 < x_{n+1} \leq LT3 \\ 11 \; if \; x_{n+1} > LT3 \end{cases} \tag{2}$$

where, LT1, LT2 and LT3 are three partitions obtained from Lloyd algorithm.

The family of sequences generated, by the perturbation of the bifurcation parameter can be represented in matrix form for *k* number of sequences of length *n* each, as

$$S(t) = \begin{pmatrix} S_{11} & S_{12} & \dots & S_{1n} \\ S_{21} & S_{22} & \dots & S_{2n} \\ \vdots & \vdots & \dots & \vdots \\ S_{k1} & S_{k2} & \dots & S_{kn} \end{pmatrix} \tag{3}$$

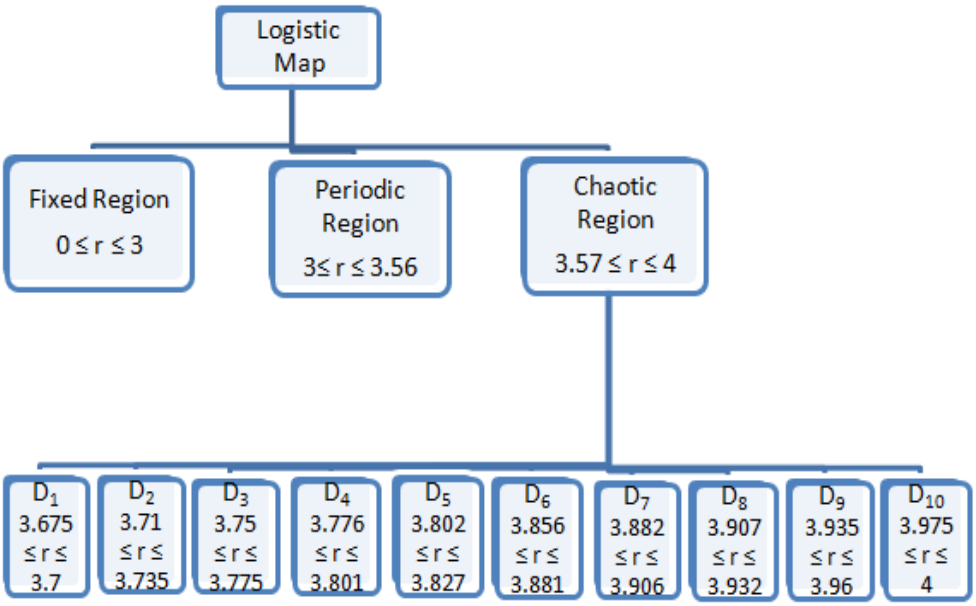

Figure 1. Chaotic domains creation based on Lyapunov exponent estimation

4. CDMA RECEIVED SIGNAL MODEL

While transmission from mobile to base station is done asynchronously, it is often the case to model it, as synchronous CDMA for simulation and analysis purpose (Liu). A CDMA channel with K users sharing the same bandwidth is shown in Figure 1. In this model, all the users simultaneously access a communication channel. The users of the system are identified at the base station by their unique spreading code $S_k(t)$. The signal that is transmitted by any user consists of the user's data b_k that modulates its spreading code. Baseband transmission was employed. Then the received signal is

$$\mathbf{r(t)} = \sum_{\mathbf{k=1}}^{\mathbf{K}} \mathbf{b_k C_k S_k(t)} + \mathbf{n(t)}, \mathbf{t} \in [\mathbf{0}, \mathbf{T}] \quad (4)$$

where, K is the total number of users, C_k is the channel attenuated amplitude, n(t) is the additive white Gaussian noise with σ^2 as variance, b_k and $S_k(t)$ are as defined above

5. LINEAR RECEIVERS

These are sub-optimal multiuser receivers. The general form of a linear receiver is given by $\hat{b}$ = sgn(w^T.y). The *sgn(.)* function returns the sign of the operand and the filter weight vector $\boldsymbol{w}$ is often chosen to minimize a cost function of the difference metric between the original data bit and estimated data bit, while $\hat{b}$ is the estimated transmitted bit of the desired user data b and y is the received signal. The receivers utilized in the simulation are sub-optimal multiuser receivers.

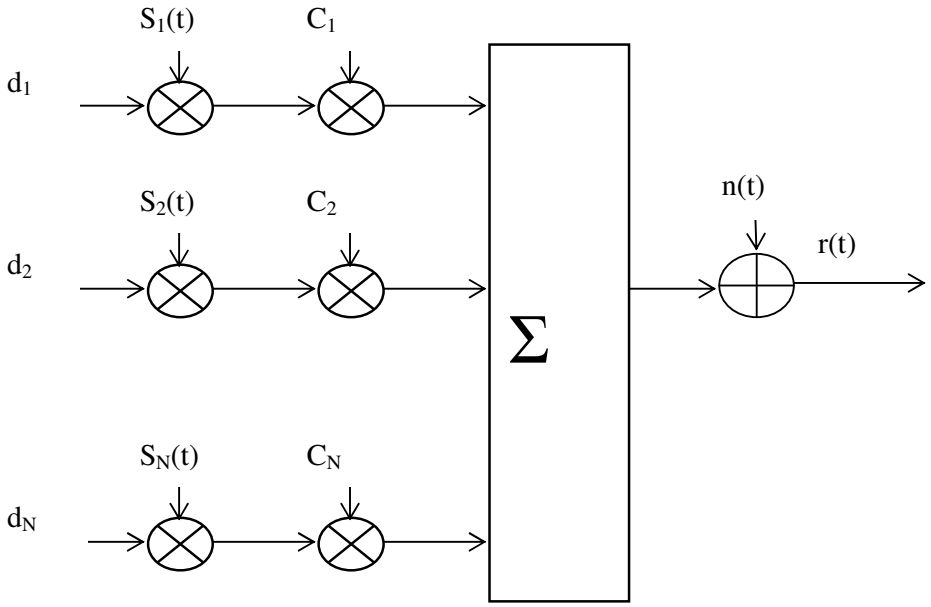

Figure 2. Received signal model for forward and reverse links

5.1. Matched Filter

Matched filter bank, which is depicted in Figure 3, is the simplest receiver and usually the first stage in the base band signal detection. Almost all modern multi-user detection techniques deal with the output of the matched filter bank and the cross-correlation information of all users in the system (Venkateswarlu, Sandeep, & Chakravarthy, 2012). Matched filter was designed for orthogonal signature waveforms, which correlates the received waveform with the suitably delayed version of the spreading code. It does not cancel the effect of interference from other users, which is a main drawback of its use in CDMA system. Each of the filters weight is matched to the signature waveforms assigned to the users. It is an optimum receiver of known signal in Additive White Gaussian Noise (AWGN) environment. But in CDMA systems, matched filter is not the optimum receiver because the power of system's MAI signal is very high at output of matched filter. Received signal at base band is given by Equation 1. The output of each matched filter can be represented as $y_1(t)$, $y_2(t)$, …, $y_k(t)$. The output can be defined for the K-th user matched filter (Liu), as

$$y_k = \int_0^T r(t)S_k(t)dt = \int_0^T S_k(t)\left[\sum_{j=1}^K A_j b_j S_j(t) + n(t)\right]dt \quad (5a)$$

$$= A_k b_k + \sum_{j=1 j\neq k}^K A_j b_j \int_0^T S_k(t)S_j(t)dt + \int_0^T S_k(t)n(t)dt \quad (5b)$$

The crosscorrelation between the kth and jth user spreading sequences can be defined as

$$\rho_{kj} = \int_0^T S_k(t)S_j(t)dt \quad (6)$$

The decision is made by taking the signum of the matched filter output as follows

$$\hat{b}_k = \mathrm{sgn}(y_k) \tag{7}$$

From equation 5b, the outputs of the matched filters for all users in matrix form is

$$y = RAb + n \tag{8}$$

where **R** is the normalized crosscorrelation matrix whose diagonal elements are equal to 1 and non-diagonal elements is equal to the cross-correlation ρ_{kj},

$\mathbf{A}=\mathrm{diag}\{A_1, \ldots, A_k\}$; $\mathbf{y}=[y_1, \ldots, y_k]^T$; $\mathbf{b}=[b_1, \ldots, b_k]^T$

and **n** is a Gaussian random vector with zero mean and covariance matrix $\sigma^2 R$.

5.2. Decorrelator

The decorrelator is shown in Figure 4. It is a linear detector which applies a linear transformation to the matched filter output to eliminate the effect of multiple access interference, thus providing unbiased estimates (Venkateswarlu, Sandeep, & Chakravarthy, 2012). The transformation R^{-1}, which is the correlation matrix inverse, is applied (Liu). It does not require prior knowledge of the received power and its performance is independent of the power of interfering users so that it solves the near-far problem. The main problem in the decorrelator detector is the neglect of noise term in the data estimate *b*, which leads to noise enhancement. Moreover, the structure of this detector needs to know the entire signature codes of the system's users and this makes the structure complex. The decision for the kth user is made based on

$$\hat{b}_k = \mathrm{sgn}(R^{-1}y_k) \tag{9a}$$

$$= \mathrm{sgn}(R^{-1}(RAb + n)_k) \tag{9b}$$

$$= \mathrm{sgn}((Ab + R^{-1}n)_k) \tag{9c}$$

.

5.3. MMSE Detector

The minimum mean square error (MMSE) receiver, shown in Figure 5, has simpler structure than the decorrelator detector. The MMSE detector is an adaptive algorithm detector that compromises between the matched filter detector and the decorrelator detector (Venkateswarlu, Sandeep, & Chakravarthy, 2012). It solves the matched filter detector problems by minimizing the MAl signals' powers and the noise power jointly at the output of the detector (Liu). The motivation for the use of adaptive algorithms lies in the desire to make the individual taps of the receiver filter to respond to changes in the communication channel. The traditional implementation of adaptive receivers is that a sequence of a priori known training data is incorporated into the data stream at prearranged times. However, this effectively reduces the overall data rate of the system, which is the main drawback of this approach. The MMSE can be implemented as a receiver, with transformation $T = (R + \sigma^2 A^{-2})^{-1}$ at the matched filter output, in order to minimize the mean square error between its estimated data and the original data. As the background noise goes to zero, the MMSE detector converges in performance to the Decorrelator detector. As the noise grows large, it is reduced to the matched filter receiver. Some other drawbacks of this receiver are

that its performance depends on the powers of the interfering users. Therefore, there is some loss of resistance to the near-far problem as compared to the Decorrelator detector and it requires estimation of the received amplitudes (Mahtab, Ahmed, Hussain, & Hasan, 2005). The decision for the kth user is based on

$$\hat{b}_k = \text{sgn}((R + \sigma^2 A^{-2})^{-1} y_k) \quad (10a)$$

$$= \text{sgn}((R + \sigma^2 A^{-2})^{-1} (RAb + n)_k) \quad (10b)$$

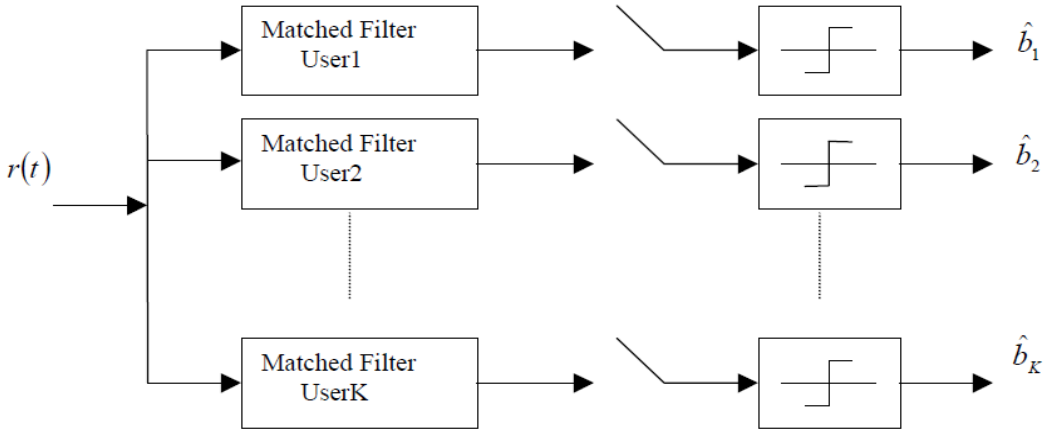

Figure 3. Conventional matched filter receiver for multiple user detection

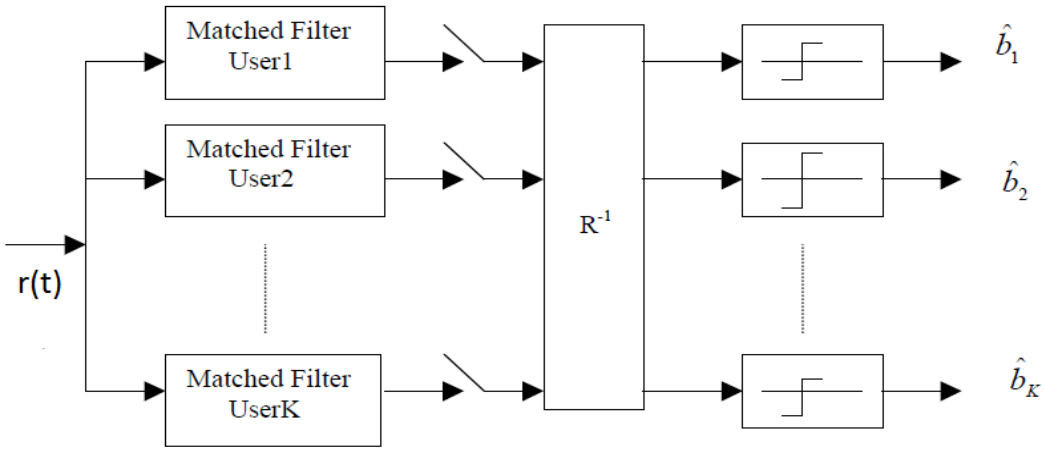

Figure 4. Decorrelating detector

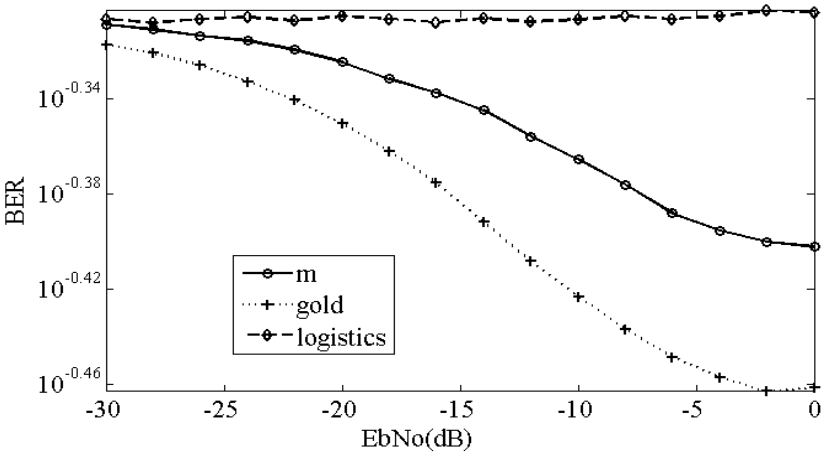

Figure 5. Six users BER performance of M, Gold and Logistic sequence for matched filter receiver

6. SIMULATION RESULT

The three multiuser receivers has been chosen such that the performance of the sequences can be accessed under varying noise and interference conditions. The matched filter is the worst case scenario, since it does not provide means of reducing interference and noise. The decorrelator reduces interference, but enhances noise; while the MMSE provide means for mitigating both interference and noise. Equation 8, 9 and 10 corresponding to the mathematical model of the matched filter, decorrelator and MMSE respectively, were implemented with MATLAB sub-routines. All the six 63-bit M-sequences, first six out of sixty-five 63-bit Gold sequences and first six out of two hundred and forty-nine 62-bit bifurcation dependent logistic sequences generated

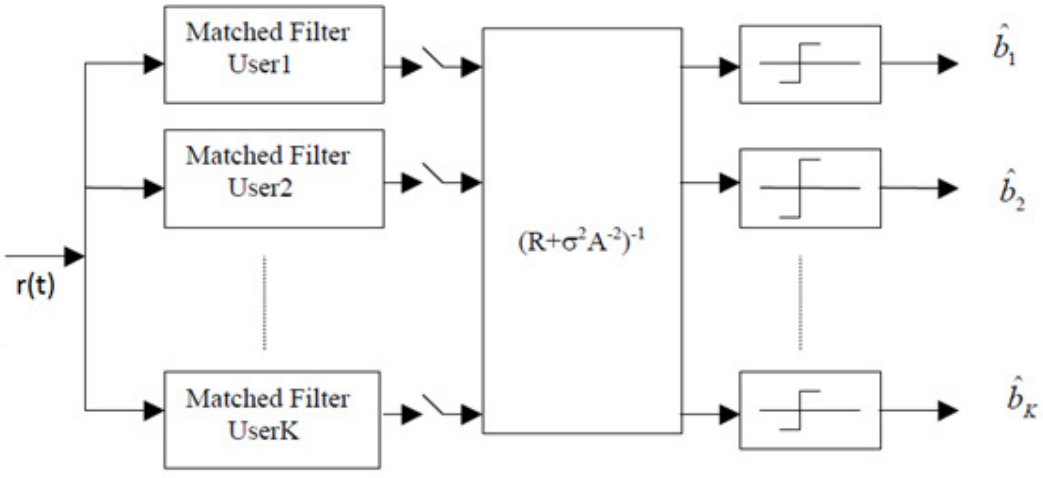

Figure 6. Six users BER performance of M, Gold and Logistic sequence for decorrelator receiver

from D_1 domain, were utilised for simulating six users transmission. Each of the six user transmission consists of 100,000 bits of data spread by his respective user code. The transmitted

data are corrupted by AWGN in the channel. The BER of logistic sequence was compared to Gold and m-sequence for the matched filter, decorrelator and MMSE receiver types, in a CDMA environment of six users as shown in Figures 6-8 respectively. In Figure 6, logistic sequence has worst BER performance for matched filter receiver; while it has best performance for decorrelator and MMSE as shown in Figure 7 and 8 respectively. In Figure 9, the BER performance of logistic sequence was considered for all the receiver types. It can be seen that decorrelator provides the best reception for logistic sequence. The spectral analysis of random sample logistic, Gold and m-sequences were conducted by taking the Fast Fourier Transform and shown in Figures 10-12.

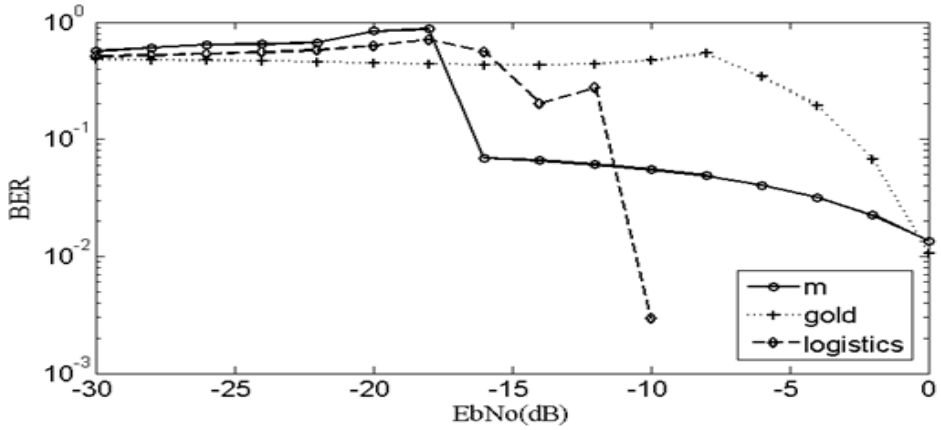

Figure 7. Six users BER performance of M, Gold and Logistic sequence for MMSE receiver

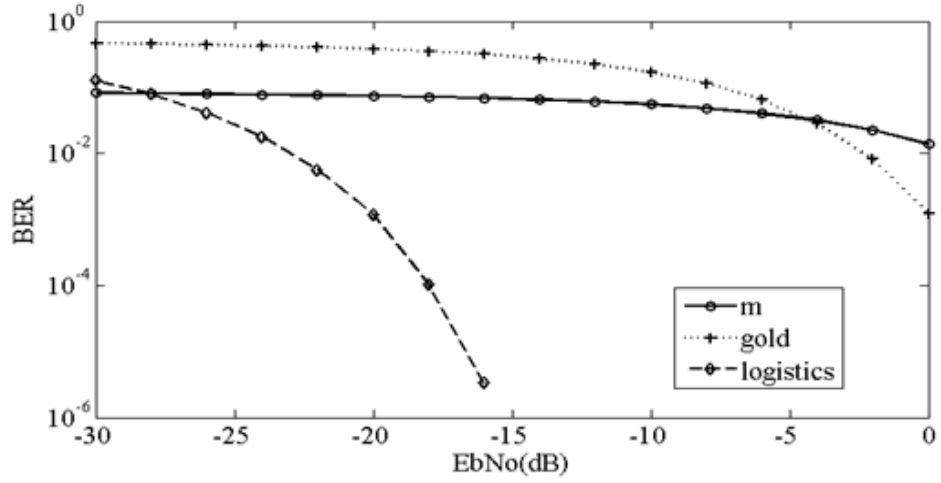

Figure 8. Six users BER performance of Logistic sequence for matched filter, decorrelator and MMSE receiver

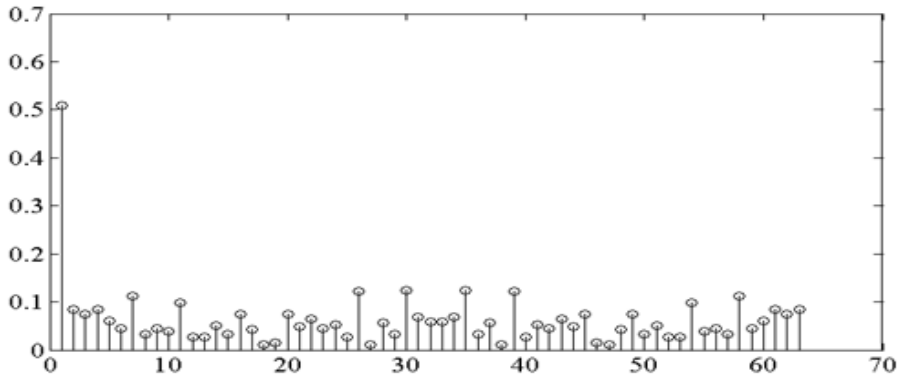

Figure 9. Spectrum of 63-bits Gold Sequence

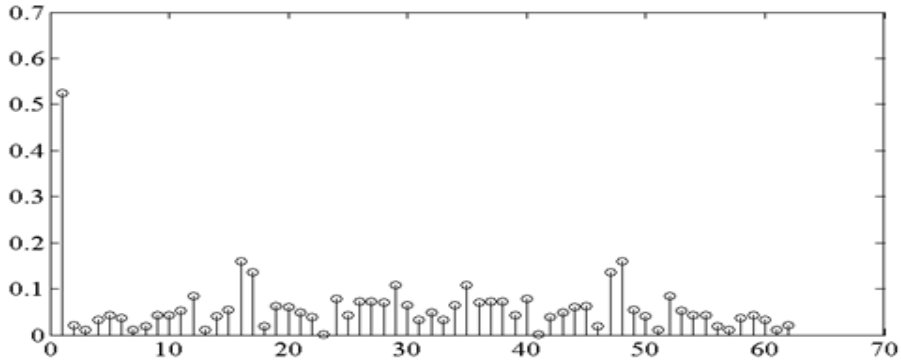

Figure 10. Spectrum of 63-bits Gold Sequence

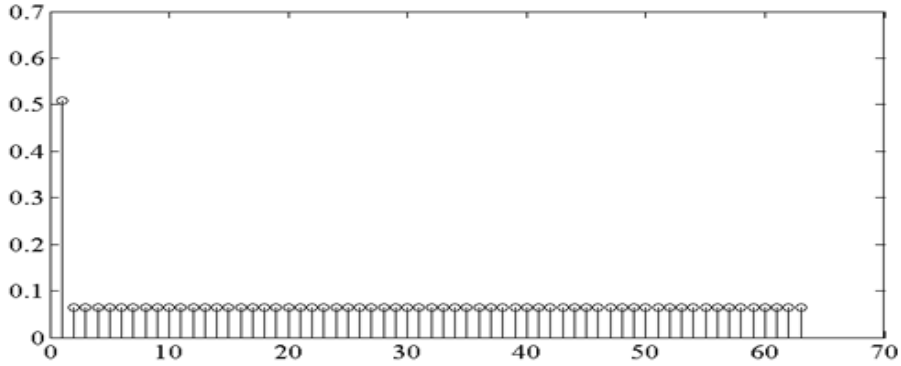

Figure 11. Spectrum of 62-bits Logistic Sequence

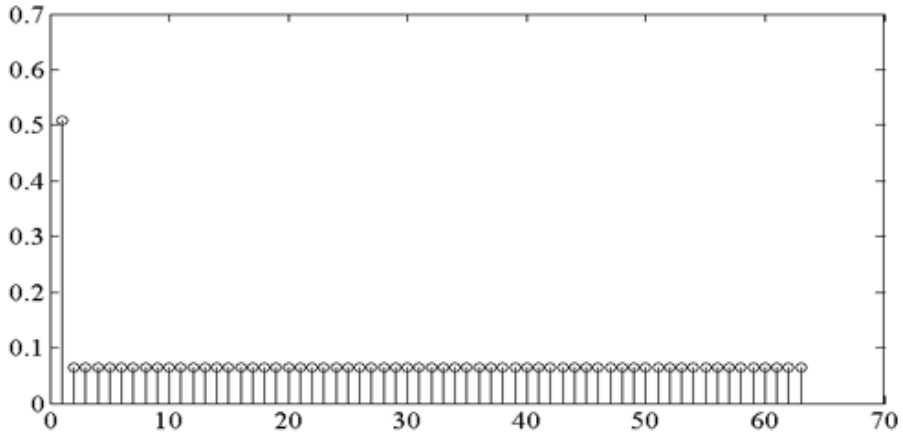

Figure 12. Spectrum of 63-bits M-Sequence

6. CONCLUSIONS

It can be observed from the result that logistic sequences show better BER performance than Gold and m-sequences for Decorrelator and MMSE receiver. Also, the decorrelator receiver proves to be an optimal receiver for logistic sequences, compared to matched filter and MMSE receiver. Furthermore the frequency spectrums of the logistic sequences are wideband, due to the low MSAAC values. However the spectrums of the logistic sequences are not as flat as m-sequence, but the flatness is comparable to Gold sequences.

ACKNOWLEDGEMENTS

This work was supported by the Nigerian Tertiary Education Trust Fund under academic staff training and development programme.

REFERENCES

[1] Meenakshi and M. P. Chawla, "A review comparison of different spreading codes for DS CDMA," IJSRD - International Journal for Scientific Research & Development|, vol. 2, no. 2, pp. 995-999, 2014.

[2] A. Sawlikar and M. Sharma, "Analysis of different pseudo noise sequences," International Journal of Computer Technology and Electronics Engineering (IJCTEE), vol. 1, no. 2, pp. 156-161, 2011.

[3] R. L. Pickholtz, L. B. Milstein, and D. L. Schilling, "Theory of spread-spectrum communications-A tutorial," IEEE Transactions on Communications, vol. com-30, no. 5, pp. 855-884, May 1982.

[4] K. Umeno and K. Kitayama, "Spreading sequences using periodic orbits of chaos for CDMA," Electronic Letters, vol. 35, no. 7, pp. 545-546, April 1999.

[5] C. Vladeanu, I. Banica, and S.El. Assad, "Periodic chaotic spreading sequences with better correlation properties than convectional sequences-BER performances analysis," in Signals,Circuits and Systems, 2003. SCS 2003.International Symposium on, vol. 2, Iasi,Romania, 2003, pp. 649-652.

[6] H. Zhang, J. Guo, H. Wang, R. Ding, and W Chen, "Oversample chaotic map binary sequences: Definition, performance and realization," in Circuits and Systems, 2000. IEEE APCCAS 2000., Tianjin, 2000, pp. 618-621.

[7] O. E. Adetoyi and S. A. Adeniran, "Chaotic Sequence Derived from Bifurcation Dependency," International Journal of Scientific & Engineering Research , vol. 7, no. 4, pp. 165-169, April 2016.

[8] N. K. Pareek, V. Patidar, and K. K. Sud, "A random bit generator using chaotic maps," International Journal of Network Security, vol. 10, no. No.1, pp. 32-38, 2010.
[9] S. Spinsante, S. Andrenacci, and E. Gambi, "De Bruijn Sequences for Spread Spectrum Applications: Analysis and Results".
[10] M. Suneel, "Cryptographic pseudo-random sequences from the chaotic," Sadhana, vol. 34, no. 5, pp. 689-701, October 2009.
[11] K. Usha and K. J. Sankar, "New Multi Level Spreading Codes for DS CDMA Communication," in Conference on Advances in Communication and Control Systems (CAC2S 2013), 2013, pp. 154-159.
[12] Y. Liu. Simulation Comparison of Multiuser Receivers in DS/CDMA Systems. [Online]. http://plaza.ufl.edu/yongliu/projectreport.PDF

[13] Y. Venkateswarlu, K. Sandeep, and A.S.N. Chakravarthy, "CDMA and MAI problem elimination methods," International Journal of Scientific and Research Publications, vol. 2, no. 7, pp. 1-13, 2012.
[14] Z. Mahtab, S.J. Ahmed, S.S. Hussain, and S. Hasan, "CDMA based wireless transceiver system matlab simulation and FPGA implementation," in Engineering Sciences and Technology,2005.SCONEST 2005. Student conference on, Karachi, August 2005, pp. 1-9.

AUTHORS

Oluyemi Adetoyi obtained her B.Sc. degree in Electrical and Electronic Engineering from University of Ibadan, Nigeria. Her M.Sc. degree in Electronic and Electrical Engineering was obtained from Obafemi Awolowo University, Ile-Ife, Nigeria. She was a lecturer at different time at Adekunle Ajasin University in Nigeria and at Babcock University between. Currently, she is a lecturer with University of Ibadan, Nigeria. She is currently pursuing her PhD in Communication Engineering at Obafemi Awolowo University, Ile-Ife, Nigeria. Her research interest is in wireless communication and data security.

Solomon Adeniran is a lecturer with the Department of Electronic and Electrical Engineering, Obafemi Awolowo University, Nigeria. His area of research work spans passive components for microwave networks, DSP and communication systems.