INTERNATIONAL JOURNAL OF COMMUNICATIONS
Issue 2, Volume 2, 2008

Chaotic Sequences Implementations on Residue Number Spread Spectrum System

M. I. Youssef, M. Zahara, A. E. Emam, and M. Abd ElGhany

***Abstract*—** In this paper, the performance of chaotic code generators implemented in spread spectrum communication system is analyzed and compared to those using conventional pseudo random code generators as maximum length, gold code generators. Image is used as a data source and the histogram of the spreaded image is analyzed. Applicability of different types of generators are studied by examining their autocorrelation, cross-correlation performance and the bit error rate for the communication system is evaluated for various codes. Finally, a residue number arithmetic is added to the system; this system is evaluated and compared to that of non residue number system, measuring the histogram of the spreaded image and the probability of error for the system is measured.

***Keywords*—** Image encryption, Spread spectrum communication, chaotic sequence generator, and Residue number system.

I. Introduction

Spread Spectrum (SS) [1] – [5] has been defined as a means of transmission in which the signal occupies bandwidth much in excess of the minimum necessary to send the information, the band spread is accomplished by utilizing a "code" which is independent of the data and a synchronized reception with the code at the receiver is used for de-spreading and subsequent data recovery.

The SS Communications are widely used today for Military, Industrial, Avionics, Scientific, and Civil uses. The advantages of using SS include the following: [3]

- Low power spectral density.
  - As the signal is spread over a large frequency-band, the Power Spectral Density is getting very small, so other communications systems do not suffer from this kind of communications. However the Gaussian Noise level is increasing.
  - The ability to utilize the Satellite payload channels, which is achievable as the transmitted signal is spread in such away that it become noise like and thus would not interfere with the payload traffic.
- Interference limited operation.
- Privacy due to unknown random codes. As the applied codes are - in principle - unknown to a hostile user. This means that it is hardly possible to detect the message of another user.
- Applying spread spectrum implies the reduction of multi-path effects.
- Random access possibilities. As users can start their transmission at any arbitrary time.
- Good anti-jam performance.

The cost paid is the need of a larger bandwidth which already present due to the usage of the existing communication channels and the need for good synchronization at the receiver to detect the reception of the signal.

The "code" [6] used for spreading the signal is a pseudo-random or pseudo-noise (PN) code that is mixed with the data to spread the signal in a statistically random matter. These codes are considered fast codes as they run the information bandwidth or data rate many times.

The conventional PN sequence is generated by linear shift registers which generate a cost problem for making the period of the PN long because a large amount of storage capacity and a large number of circuits is required. It is also it is not considered secure for transmission systems as it can be easily described once a short sequential set of chips (2L+1) from the sequence is known. This is why non-conventional techniques as the use of chaos generators [8] – [11] to spread and de-spread the signal is actively being considered for spread-spectrum communications [8].

The performance of image encryption [12] – [14] using different types of spreading sequences is analyzed and a comparison is performed between chaotic sequence as a spreading code and conventional Pseudo-noise code generators.

Then a residue number system (RNS) is added to the chaotic communication system in order to add more features to the communication system. The usage of RNS adds more security to the system through encrypting the data signal and converting arithmetic of large numbers to arithmetic on small numbers, thus improving the signal-to-noise ratio of the received signal and decreasing the bit error probability

Following the introduction, in part two of this paper, a brief description of spread spectrum systems is provided. In part three a description of the conventional Pseudo-noise generators are provided, part four provides a definition of chaotic sequence, part five defines the method for generating the chaotic sequence, In part six an introduction to residue number system is provided, part seven provides system model description, part eight shows the simulation results, and finally in part nine the conclusion and future work in this field are indicated.

Manuscript received January 20, 2008.
* M. I. YOUSSEF is with the Al-Azhar University, Cairo, Egypt
* M. ZAHARA is with the Al-Azhar University, Cairo, Egypt
* A. E. EMAM is with the Al-Azhar University, Cairo, Egypt
* M. ABD ELGHANY is with the Al-Azhar University, Cairo, Egypt, mohamedgheth@yahoo.com

II. Direct Sequence Spread Spectrum Technique

There are many types of spread spectrum techniques [1], [2] as: Direct sequence (DS), frequency hopping, time hopping and hybrid system. Direct sequence (Fig 1) contrasts with the other spread spectrum process, in which a broad slice of the bandwidth spectrum is divided into many possible broadcast frequencies. In general, frequency-hopping devices use less power and are cheaper, but the performance of DS-CDMA systems is usually better and more reliable [8]. Thus, in this paper we will deal only with direct sequence method.

In Direct Sequence-Spread Spectrum the base-band waveform is XOR by the PN sequence in order to spread the signal. After spreading, the signal is modulated and transmitted. The most widely modulation scheme is BPSK.

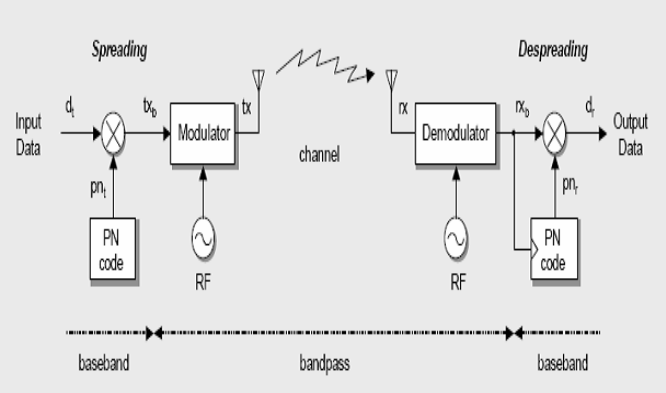

Fig.1 DS - SS block diagram

The bandwidth expansion factor - also called the Processing Gain (*K*) -, can be defined as the ratio between the transmitted spread spectrum signal bandwidth (*B*) and the bandwidth of the original data sequence ($B_{message}$) where the Processing Gain is approximately the ratio of the spread bandwidth to the information rate *R* (bits/s) and it is much greater than unity.

$$K = \frac{B}{B_{message}} \approx \frac{B}{R} \quad (1)$$

Spread Spectrum transmitters use similar transmits power levels to narrow band transmitters. Because Spread Spectrum signals are so wide, they transmit at a much lower spectral power density, than narrowband transmitters. Spread and narrow band signals can occupy the same band, with little or no interference. Interference rejection capability arises from low mutual correlation between the desired signal and the interfering signal ensured by the codes. This capability is the main reason for all the interest in Spread Spectrum today.

The equation that represents this DS-SS signal is shown in equation (2), and the block diagram is shown in Fig. 2.

$$S_{ss} = \sqrt{(2 E_s/T_s)}\,[m(t) \otimes p(t)] \cos(2 \pi f_c t + \theta) \quad (2)$$

Where:
m(t) is the data sequence,
T_s is duration of data symbol.
p(t) is the PN spreading sequence,
f_c is the carrier frequency,
θ is the carrier phase angle at t=0.

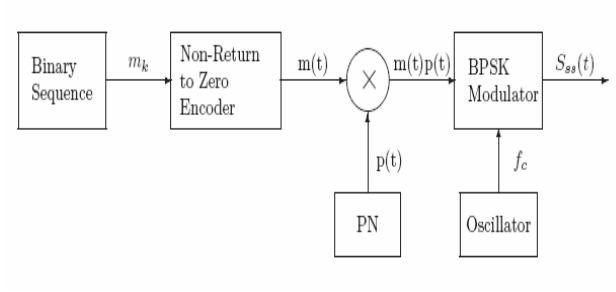

Fig. 2 DS- SS Transmitter block diagram

The demodulator, de-modulates the modulated (PSK) signal first, low Pass Filter the signal, and then de-spreads the filtered signal to obtain the original message. The process is described by the following equation (3) and the block diagram is shown in Fig. 3.

$$m(t) = [\, S_{ss} * \cos(2 \pi f_c t + \theta)\,] \otimes p(t) \quad (3)$$

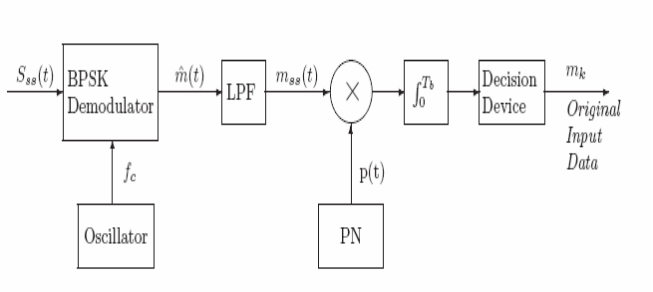

Fig. 3 DS- SS Receiver block diagram

It is clear that the spreading waveform is controlled by a Pseudo-Noise (PN) sequence which is a binary random sequence. This PN is then multiplied with the original base-band signal, which has a lower frequency, which yields a spread waveform that has noise-like properties. In the receiver, the opposite happens, when the pass-band signal is first demodulated, and then de-spreaded using the same PN waveform. An important factor here is the synchronization between the two generated sequences.

III. Pseudo-Noise Code Generator

PN is the key factor in DS-SS systems (Fig 1). A Pseudo Noise or Pseudorandom sequence is a binary sequence with an autocorrelation that resembles, over a period, the autocorrelation of a random binary sequence. It is generated using a Shift Register, and a Combinational Logic circuit as its feedback. The Logic Circuit determines the PN words.

Due to the usage of the PN code, the spread spectrum technique has the ability to discriminate interference signals and detect the received signal by matching received PN code with the local PN code and measuring the number of chips of the code delay between the signal being transmitted and received, and thus determine uniquely the range from the transmitter to the receiver without ambiguity [3]. Consequently the spread spectrum technique has its advantage in that its phase is easily resolved.

There are three basic properties that can be applied to a periodic binary sequence (PN sequence) as a test of the appearance of randomness, they are:

1. *Balance Property*: Good balance requires that in each period of the sequence, the number of binary *Ones* differs from the number of binary *Zeros* by at most one digit.

2. *Run Property*: A run is defined as: sequence of a single type of binary digits. The appearance of the alternate digit in a sequence starts a new run. It is desirable that about one half the runs of each type is of length 1, about one fourth of length 2, one eighth is of length 3, and so on.

3. *Correlation Property*: If a period of the sequence is compared term by term with any cyclic shift of itself, it is best if the number of agreements differs from the number of disagreements by not more than one count.

The PN (Pseudo Noise) codes used for DSSS require certain mathematical properties.

1. Maximum Length Sequences: These are PN sequences that repeat every 2^n -1, where n is an integer. These sequences can be implemented using shift registers. The PN sequences must exhibit good correlation properties. Two such sequences are Barker Codes, and Willard Codes.

2. Maximum Auto-Correlation: When the received signal is mixed with locally generated PN sequence, it must result in maximum signal strength at the point of synchronization.

3. Minimum Cross-Correlation: When the received signal with a different PN sequence than that of the receiver, is mixed with the locally generated PN sequence, it must result in minimum signal strength. This would enable a DSSS receiver to receive only the signal matching the PN code. This property is known as Orthogonality of PN Sequences.

The M-Sequence and Gold sequences are the most popular conventional spreading sequences in spread spectrum systems. The M-sequences have very desirable autocorrelation properties. However, large spikes can be found in their cross-correlation functions especially when partially correlated. Another limiting property of M-sequences is that they are relatively small in number. Therefore, the number of sequences is usually too small and not suitable for spread spectrum systems. On the other hand, the Gold sequences have better cross-correlation properties than M-sequences; they are constructed by taking a pair of specially selected M-sequences.

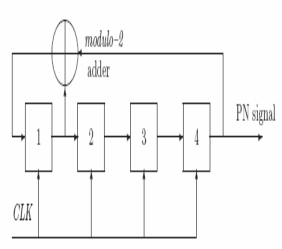

Fig. 4.a PN Generator block diagram m-sequence code

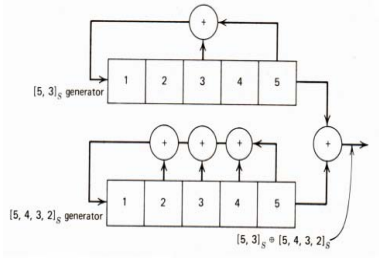

Fig. 4.b PN Generator block diagram Gold code

In this paper, the so called Maximum–Length PN sequence is used, generated by a linear feedback shift register, which has feedback logic of only modulo–2 adders (XOR Gates).

IV. Chaotic sequence code generator

Chaotic theory has been established since 1970s from many different research areas, such as physics, mathematics, biology and chemistry, ,..etc. The most well-known characteristics of chaos are the so-called "butterfly-effect" (the sensitivity to the initial condition), and the pseudo-randomness generated by deterministic equations.

A chaotic dynamical system [8] – [10] is an unpredictable, deterministic and uncorrelated system that exhibits noise-like behavior through its sensitive dependence on its initial conditions which generates sequences similar to PN sequence. The chaotic dynamics have been successfully employed to various engineering applications such as automatic control, signals processing and watermarking.

Since the signals generated from chaotic dynamic systems are noise-like, super sensitive to initial conditions and have spread and flat spectrum in the frequency domain, it is advantageous to carry messages with this kind of signal that is wide band and has high communication security. For this reason, numerous engineering applications of secure communication with chaos have been developed.

A direct application of chaos theory to telecommunication systems appears in a conventional digital spread spectrum [10], [11], where the information, is spread over a wider band by using a chaotic signal instead of the usual periodic PN sequences.

The chaotic sequences have Noise-like waveform, and Wide band spectrum properties [10] in comparison with the periodic pseudo number sequence. These properties have the following advantages:

- Sensitive dependence on the initial conditions which is desirable for multi-user communication and also for secure communication.
- Infinitely long period without increasing the generator which is desirable for multi-user communication and also secure communication.

The disadvantage of such system is the complexity to synchronize the receiver chaos sequence with local generated at the receiver end.

V. Generation of chaotic sequence

Various non-linear dynamic systems are used in order to generate the chaotic sequence as: Tent map, logistic map, quadratic map and Bernoulli map [16], [17]. In this paper the generation of chaotic sequence using the logistic and tent maps is studied through the analysis of the bifurcation diagram for each of them.

The state space description of the logistical map is:

$$x_{n+1} = r\, x_n (1 - x_n) \qquad 0 \le x_n \le 1,\ 0 \le r \le 4 \qquad (4)$$

Where;

r is called the bifurcation parameter.

The state space description of the tent map is:

$$F(x_n) = x_{n+1} = k (1 - | 1 - 2 x_n |) \quad (5)$$

Where;

F is the transformation mapping function,

k is arbitrary constant that is selected by the designer to make a chaotic system.

One major difference between chaotic sequences and PN sequences is that the generated chaotic sequences are not binary. Therefore chaotic sequences must be transformed into binary sequences.

In order to transfer the real valued chaotic sequence (x) to binary sequence, a threshold function $\theta_t(x)$ is defined as,

$$\theta_t(w) = \begin{cases} 0 & , x < t \\ 1 & , x \geq t \end{cases} \quad (6)$$

Where

t is the threshold value

The threshold value is chosen as an arithmetic mean of a large number of conservative values of x. Thus a binary sequence is obtained and is referred to as a chaotic threshold sequence.

VI. Residue Number System (RNS)

A residue number system (RNS) [18], [19] represents a large integer using a set of smaller integers, so that computation may be performed more efficiently. It relies on the Chinese remainder theorem of modular arithmetic for its operation, a mathematical idea from Sun Tsu Suan-Ching (Master Sun's Arithmetic Manual) in the 4th century AD.

The residue number system is defined by the choice of v positive integers m_i (i = 1, 2, 3 … v) referred to as moduli. If all the moduli are pair-wise relative primes, any integer N, describing a non-binary message in this letter, can be uniquely and unambiguously represented by the so-called residue sequence (r_1, r_2 ..r_v) in the range $0<N<M_I$,where $r_i = N \pmod{m_i}$ represents the residue digit of N upon division by m_i, and $M_I = \prod m_i$ is the information symbols' dynamic range. Conversely, according to the Chinese Reminder Theorem, for any given v-tuple (r_1, r_2..r_v) where $0 \leq r_i < m_i$; there exists one and only one integer N such that $0 \leq N < M_i$ and $r_i = N \pmod{m_i}$ which allows us to recover the message N from the received residue digits.

Residue number system has two inherent features that render the RNS attractive in comparison to conventional weighted number systems, such as for example the binary representation. These two features are [18]:

- The carry-free arithmetic and,
- Lack of ordered significance amongst the residue digits.

The first property implies that the operations related to the individual residue digits of different moduli are mutually independent because of the absence of carry information. The second property of the RNS arithmetic implies that some of the residue digits can be discarded without affecting the result, provided that a sufficiently "high dynamic range" is retained in the "reduced" system in order to unambiguously contain the result.

VII. System Model

In this paper, a Lena image as shown in Fig 5.a, is used as a data source and is encrypted using direct sequence spread spectrum technique and based through AWGN channel, as shown in Fig 5.b. The encrypted image is analyzed when the system is designed with conventional PN sequence, and with chaotic sequence, finally RNS is added and the system performance is measured.

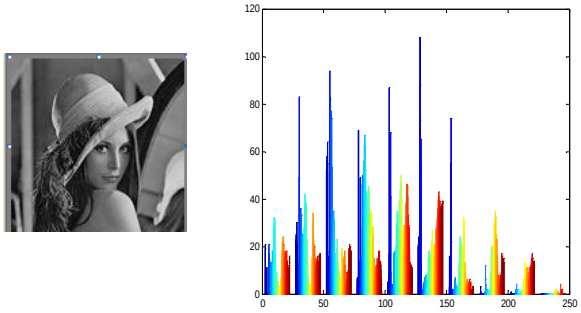

Fig. 5.a Lena image and its histogram before encryption

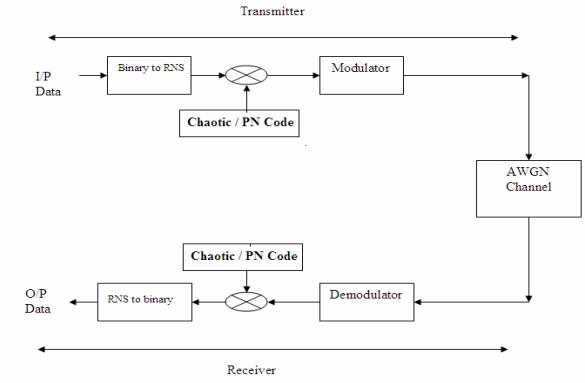

Fig. 5.b Direct Sequence Spread Spectrum system with RNS

The bit error probability (P_e) [2] for BPSK system is used as a reference for comparisons between various schemes.

$$P_e = \begin{cases} Q\,[1/\sqrt{((K-1)/3N + N_o/2E_b)}] & , \text{M, Gold} \\ Q\,[1/\sqrt{((K-1)/\sqrt{3}N + N_o/2E_b)}] & , \text{Chaotic} \end{cases} \quad (7)$$

The reason for the presence of different bit error probability as shown in equation (7) is due to the decrease of the multiple access interference (MAI) when utilizing chaotic code generators.

The equation that measures the autocorrelation and cross correlation functions is as shown in equation (8) and (9).

$$r_{xx}(l) = \Sigma\ x(n).\ x(n-l) \quad (8)$$

$$r_{xy}(l) = \Sigma\ x(n).\ y(n-l) \quad (9)$$

Where;

r_{xx} , is the auto correlation for discrete functions.

r_{xy} , is the cross correlation for discrete functions.

VIII. SIMULATION RESULTS

Various simulations were performed for using chaotic and/or conventional pseudorandom sequence. System using chaotic sequence is also compared to with/without RNS.

The simulations are divided into nine sections. Section 1; show the bifurcation diagram and the histogram for two chaotic sequence generators. In section 2, the autocorrelation and cross correlation for conventional and chaotic code generators are provided. Section 3; study the randomness of the chaotic sequence through plotting the frequency, time distribution and its power spectral density. In section 4, the histogram for the spreaded using chaotic code and conventional PN code generators are analyzed. In section 5 the sensitivity towards the initial value in chaotic sequence generator is shown, and in section 6 the effect of number of chaotic sequence on the system performance is provided. In section 7 the histogram of the spreaded image using RNS is evaluated. Section 8 measures the nit error probability when using various code generators and finally, section 9 measures the bit error probability for Logistic map generator implemented in a SS system with and without RNS.

A. The bifurcation and chaotic maps:

The bifurcation and histogram for each of the chaotic generators: The logistic map and the tent map are drawn to show its random performance.

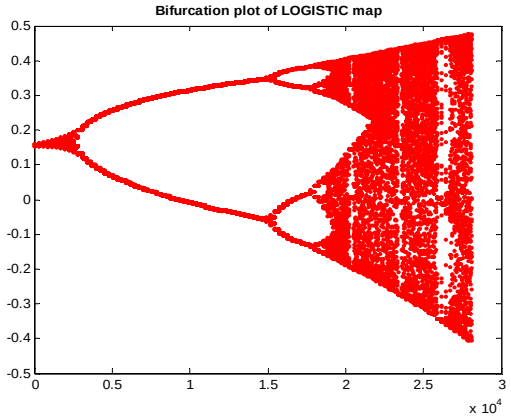

Fig. 6.a bifurcation diagram for Logistic map, x_0=-0.35

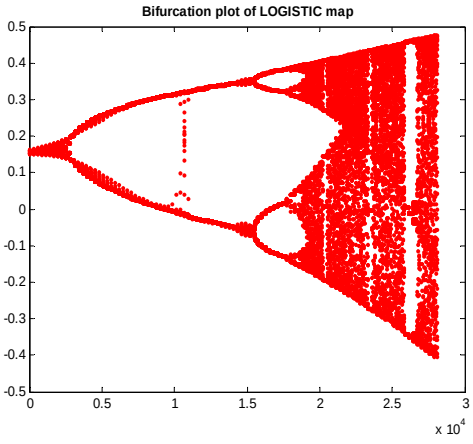

Fig. 6.b bifurcation diagram for Logistic map, x_0=0.1

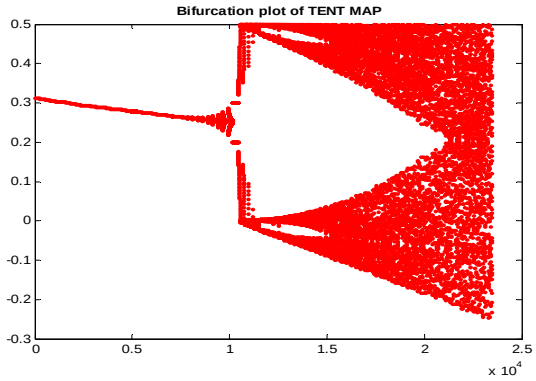

Fig. 6.c bifurcation diagram for Tent map, x_0 = 0.5

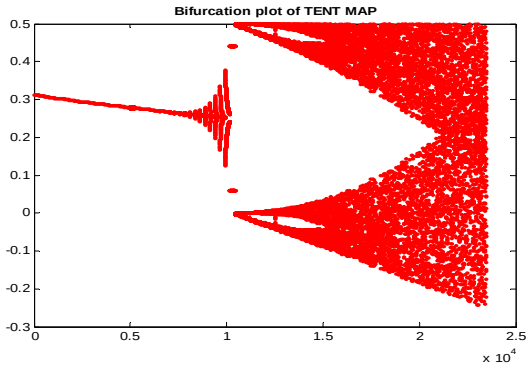

Fig. 6.d bifurcation diagram for Tent map, x_0 = 0.1

From Fig. 6, it show the sensitivity of the chaotic maps towards its initial value x_0 and also indicate that depending on the value of r, the dynamics of system can change attractively exhibiting periodicity or chaos.

The logistic and tent maps are drawn by geometry in-order to demonstrate their chaotic performance, as shown in Fig 7.

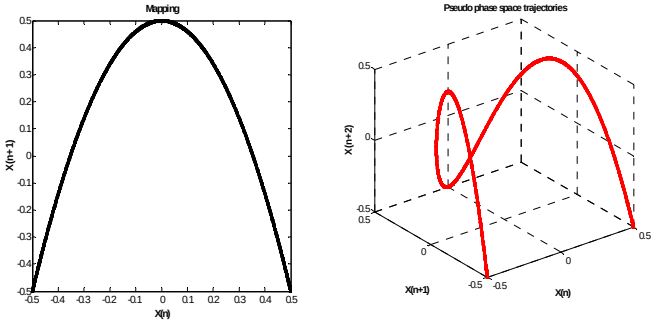

Fig. 7.a Graph of the Logistic Map function for one dimension and phase space trajectories

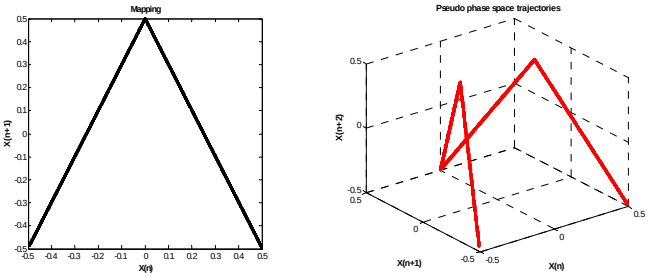

Fig. 7.b Graph of the Tent Map function for one dimension and phase space trajectories

The histogram for the chaotic sequences: Logistic map and the tent map are drawn as shown in Fig 8.

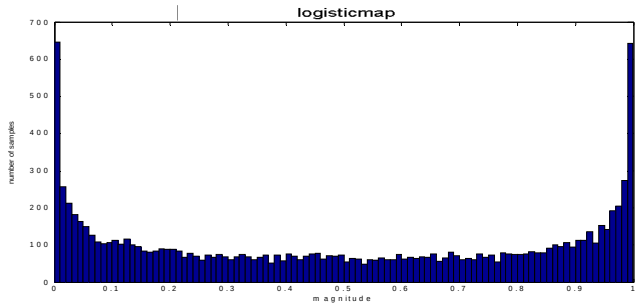

Fig. 8.a Histogram for Logistic map - x_0 =0.1

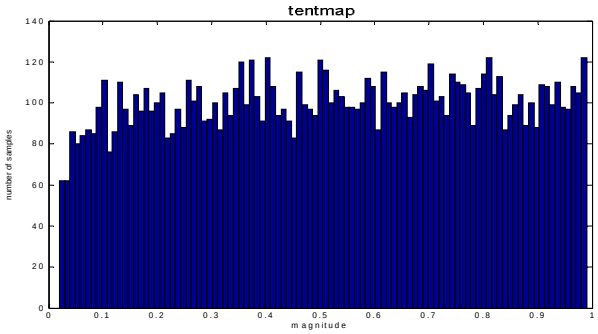

Fig. 8.b Histogram for Tent map - x_0 =0.1

Fig. 8 shows that the chaotic sequences generators – especially that generated through the Tent map – have a well distributed probability function which is required for random umber generation.

B. The autocorrelation and cross-correlation function:

In the next simulations the autocorrelation and cross correlation performance for each of the chaotic and conventional random sequences are analyzed.

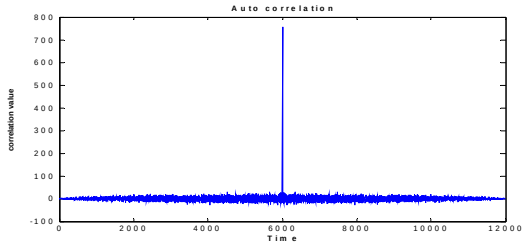

Fig. 9.a Autocorrelation function for Logistic map

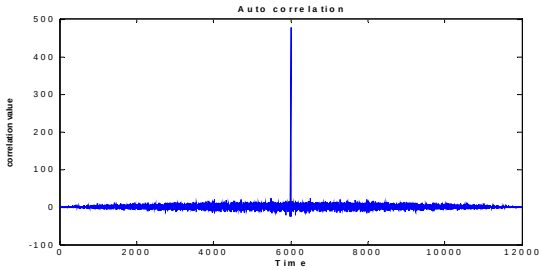

Fig. 9.b Autocorrelation function for Tent map

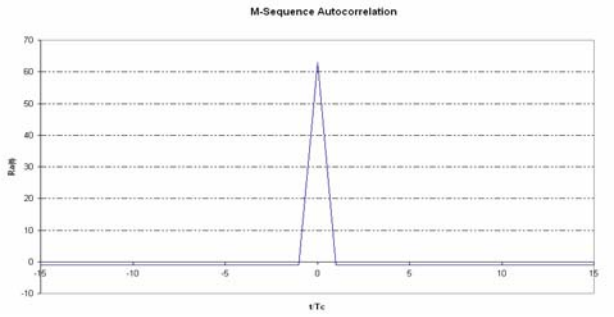

Fig. 9.c Autocorrelation function for M- Sequence

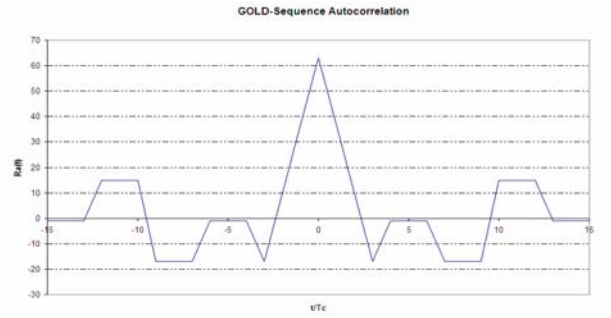

Fig. 9.d Autocorrelation function for Gold sequence

Fig. 9 shows the autocorrelation function for the chaotic sequence is highly compared to that of the conventional PN code generators.

In order to demonstrate the extreme sensitivity of the chaotic logistic map the next analysis will study the cross correlation between two codes generated by Logistic map with difference of 0.000000001 in the initial condition and for the conventional PN code generators, is as shown in Fig 10.

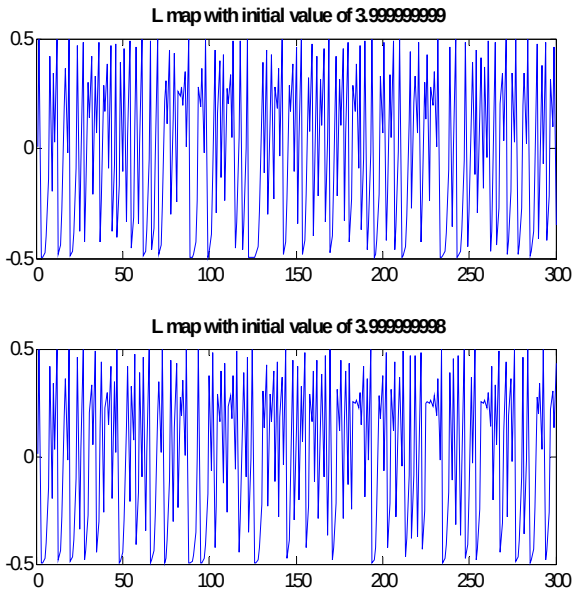

Fig. 10 Code 1 and Code 2 generated by the logistic map

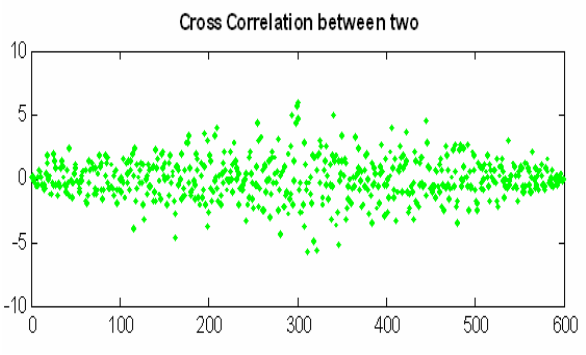

Fig. 11.a The cross correlation between the two chaotic codes

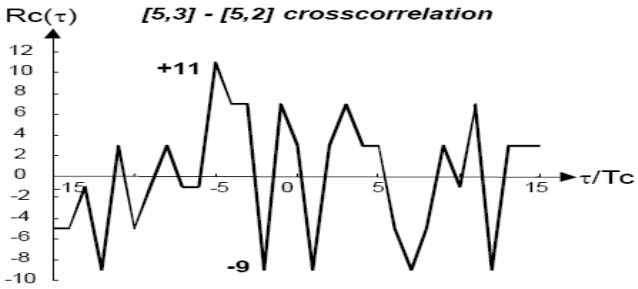

Fig. 11.b Cross-correlation function for the M- Sequence

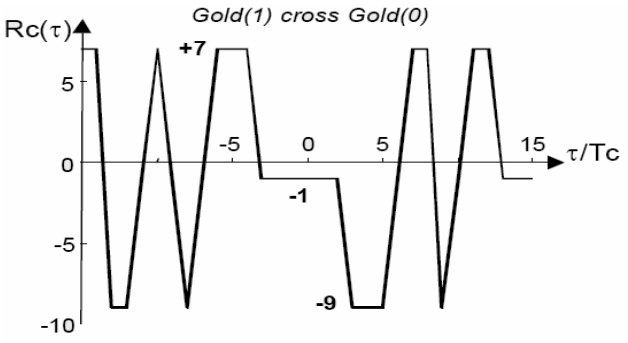

Fig. 11.c Cross-correlation function for the M- Sequence

Fig. 11 shows that chaotic sequences have very low values of the cross correlation function. This is an important issue with regards to security, because the receiver cannot be figured out from a few points of the chaotic sequence. Consequently, the chaotic sequence also permits more users in the communication system and the system obtains a greater security.

C. Frequency and time distribution

In order to see the randomness of the chaotic sequence, the time and frequency distribution of the code are shown in Fig.12 for both the Logistic map and Tent map. The power spectral density for the Logistic map is drawn in comparison with a purely random sequence as foreseen in Fig. 13.

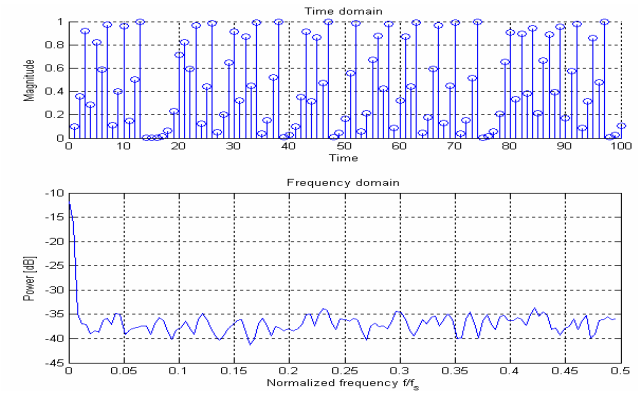

Fig 12.a Logistic map in the time and frequency domain, , x_0= 0.1

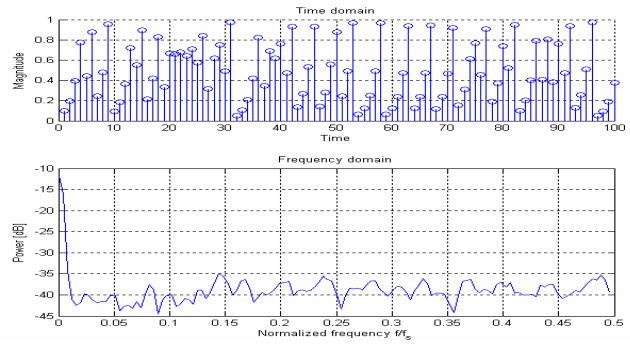

Fig 12.b Tent map in the time and frequency domain, x_0= 0.1

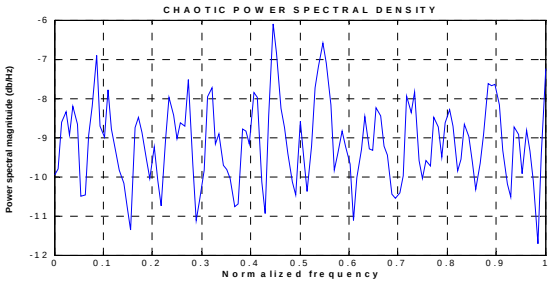

Fig. 13.a Power Spectral density for Chaotic sequence,

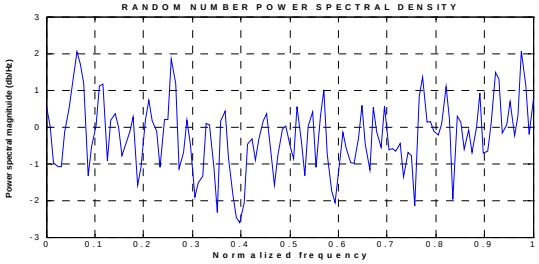

Fig. 13.b Power Spectral density for random sequence

It is shown from Fig. 13 that the density of the chaotic code is close to that of a purely random code sequence. These results suggest that chaotic codes generated by Logistic map satisfy the basic requirements for secure spread spectrum communication.

D. *Encryption using chaotic sequence and PN sequence*

The histogram of the encrypted image (Lena) using first chaotic sequence and again using conventional code generator for equal code length (N = 3) is as shown in Fig 14.

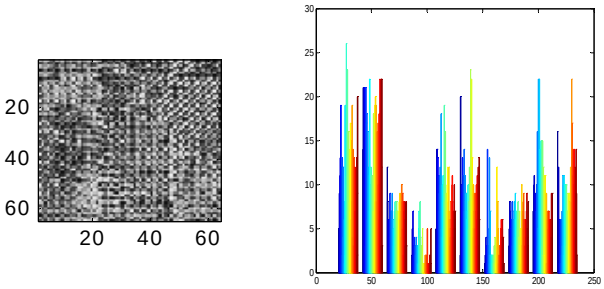

Fig. 14.a Image and its Histogram after encryption , using N = 3, Chaotic code – Logistic Map

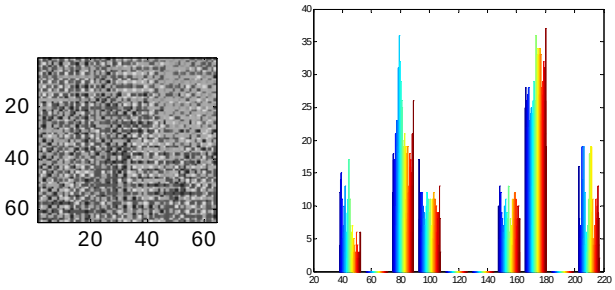

Fig. 14.b Image and its Histogram after encryption , using N = 3, Conventional PN code

From Fig 14, it is shown that chaotic sequence produce a more scrambled sequence compared to that of conventional code sequence.

E. *Effect of initial value of chaotic sequence*

Using chaotic numbers equal to three (N = 3) and changing the initial value x0 from -0.5 to 0.5 and seeing the change in the histogram of the spreaded image (Lena) as shown in Fig15

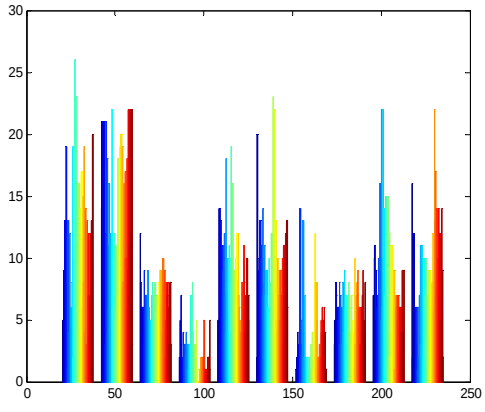

Fig. 15.a Histogram after encryption, x0 = -0.45

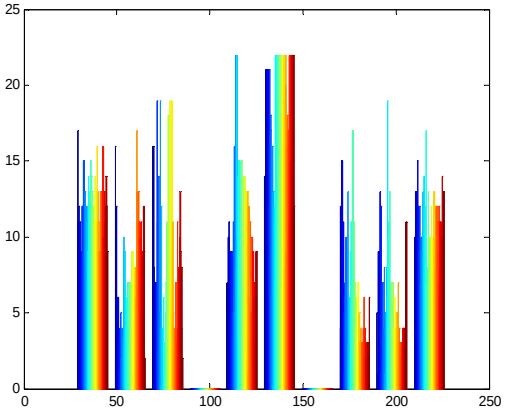

Fig. 15.b Histogram after encryption, x0 = -0.3

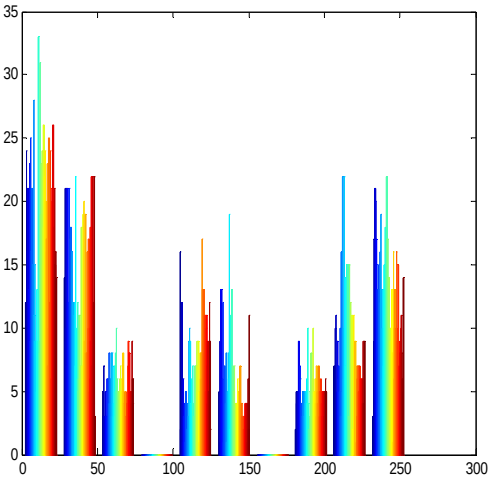

Fig. 15.c Histogram after encryption, x0 = 0.25

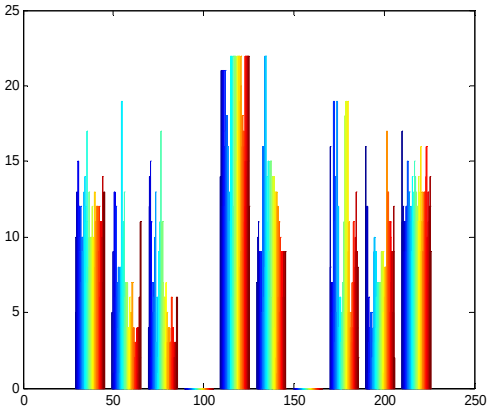

Fig. 15.d Histogram after encryption, x0 = 0.48

From Fig 15, it is shown that changing the initial condition value for the chaotic sequence would affect the histogram of the spreaded image.

Measuring the cross correlation of the image before and after spreading for various initial values, as shown in Fig 16,

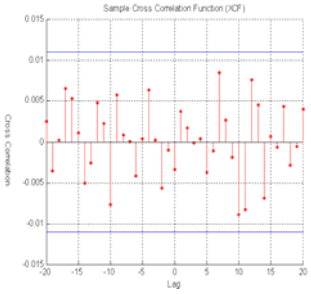

Fig16.a For x0 = -0.45

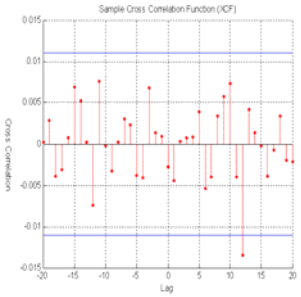

Fig16.a For x0 = -0.3

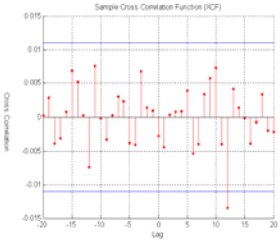

Fig16.a For x0 = -0.2

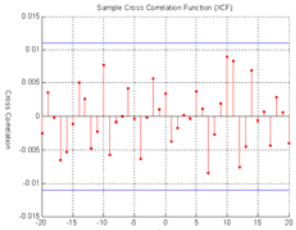

Fig16.a For x0 = -0.1

Fig 16 show that the cross correlation is minimum at certain initial condition values as at x0 = -0.45 and x0 = -0.1.

F. Effect of increasing number of chaotic sequence

Increasing number of chaotic sequence (N) and see the effect on the spreaded image (Lena) and it's histogram as shown in Fig 17.

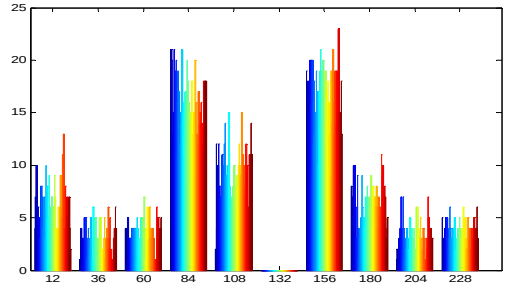

Fig. 17.a Histogram after encryption, using N= 2

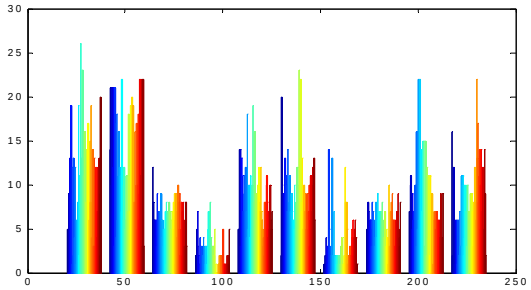

Fig. 17.b Histogram after encryption, using N= 3

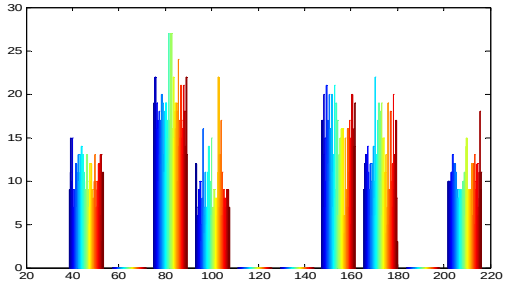

Fig. 17.c Histogram after encryption, using N= 5

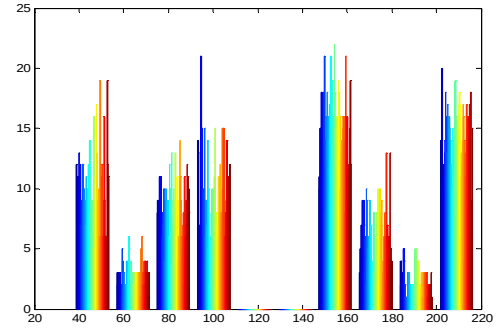

Fig. 17.d Histogram after encryption, using N= 7

The probability of error measured for various chaotic lengths as shown in Fig. 18.

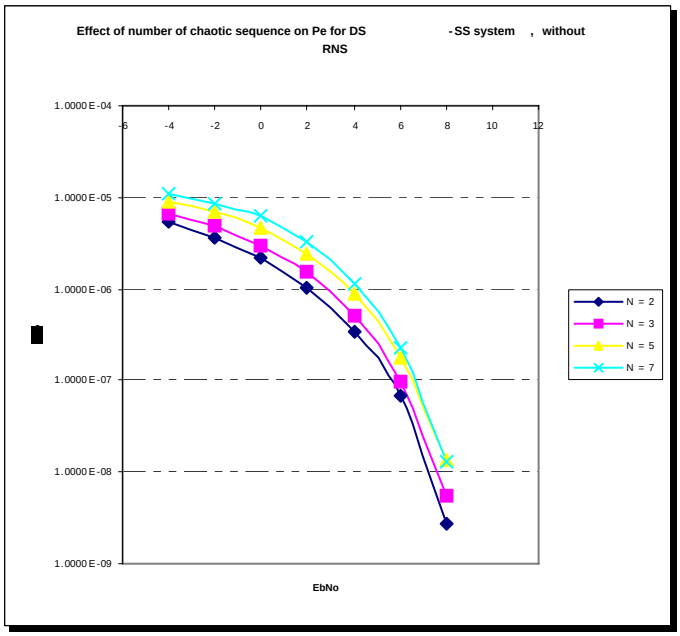

Fig. 18 Probability of error for various lengths of chaotic sequences

From Fig. 17 and Fig. 18, it is shown that as the number of chaotic sequence increases leading to an increase in the spreaded sequence but this consequently leads to a decrease in the performance due to the need of a larger channel bandwidth.

G. *Image Histogram with and without RNS*

The histogram for the spreaded signal is studied with RNS [9 7 5] and without RNS for both chaotic sequence and conventional PN code generators. Taking initial value x0= -0.45 and number of chaotic sequence = 3.

G.1 for Chaotic code generators

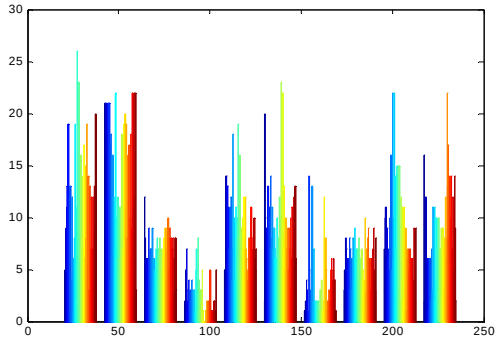

Fig. 19.a Histogram after encryption ,without RNS

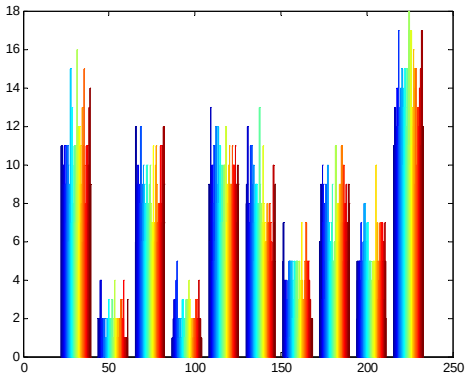

Fig. 19.b Histogram after encryption ,with RNS

From Fig 19.a and 19.b, it is shown that using RNS would produce a more spreaded sequence of the data and the image is more scrambled, thus it provides more secure transmission.

G.2 for Conventional PN code generators

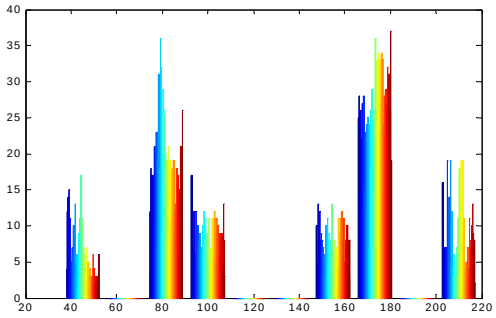

Fig. 20.a Histogram after encryption ,without RNS

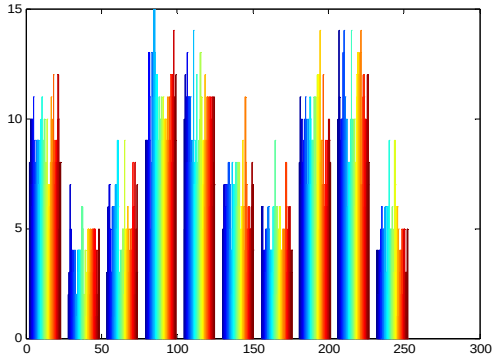

Fig. 20.b Histogram after encryption ,with RNS

From Fig 20.a and 20.b, it is shown that using RNS would produce a more spreaded sequence of the data and the image is more scrambled, thus it provides more secure transmission.

H. *The bit error probability for various code generators:*

In this section, the system performance is measured through the probability of error for both M-sequence and Logistic map code generators.

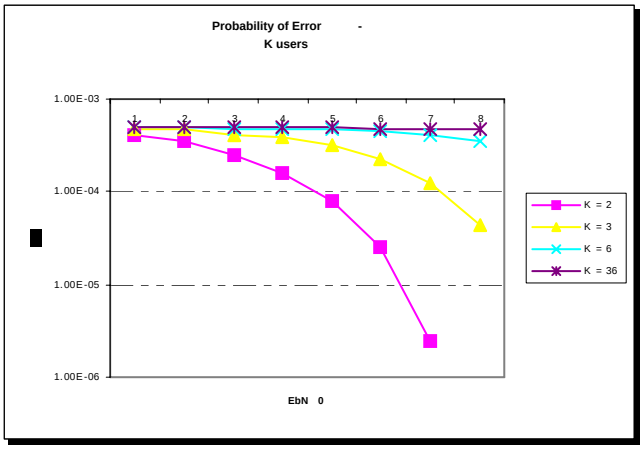

Fig. 21.a bit error probability for K- user DS-SS system using M-Sequence

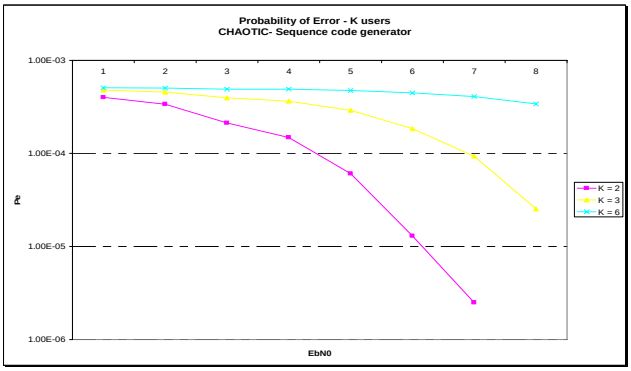

Fig. 21.b bit error probability for K- user DS-SS system using Logistic map

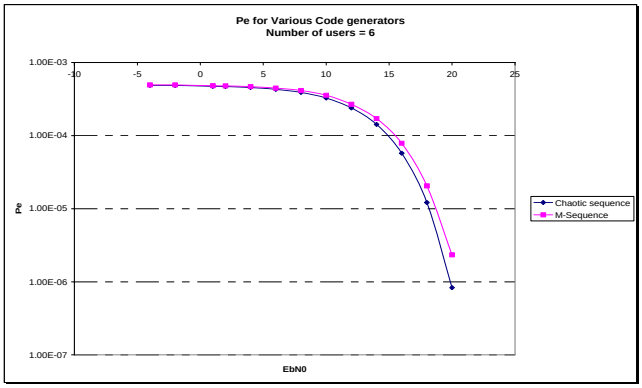

Fig.21.c bit error probability for 6- user DS-SS system using: M-Sequence / Logistic map code

The bit error probability for Chaos-based spreading sequence is improved by around 15% at EbNo = 15 db, thus at any fixed BER their > 15% more users can be allocated for free for chaotic-based codes.

I. Bit error probability for Logistic map code generator implemented in SS system with and without RNS:

Using Lena image as an input data source and transfer it through a direct sequence spread spectrum system using chaotic sequence generator.

The system is implemented twice, the first using RNS transformation of the binary sequence of the image and the second without RNS conversion.

The probability of error is measured for various bit energy to noise ratio with and without residue number system.

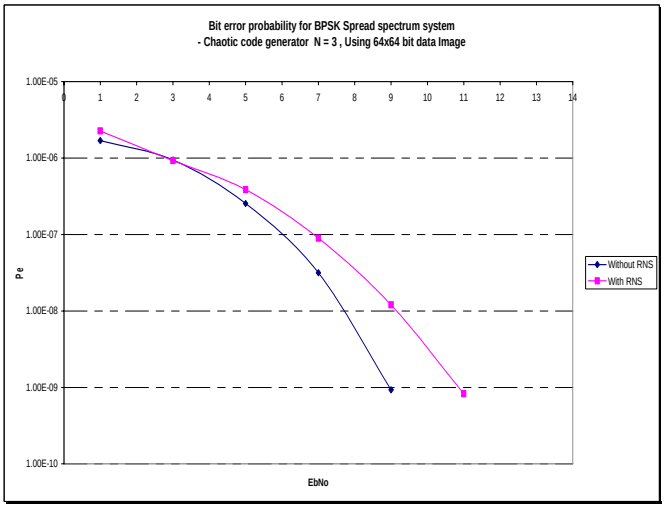

Fig. 22 Bit error probability for DS-SS system using chaotic sequence generator: With and without RNS

It is deduced from Fig. 22 that the performance of system with RNS is comparable with that without RNS, although it was seen previously that RNS system produce a more scrambled image and thus provide improved secure transmission.

IX. Conclusion

In comparison to conventional codes, chaotic codes, not only have better autocorrelation and cross-correlation performance and lower probability of error for multi-user communication, but also have some properties superior to the former.

Firstly, conventional codes generated by linear shift register generators are easily decipherable once a short sequence set of bits from the sequence is known. In contrast, security of the chaotic sequence is considered extremely high. Secondly, for an m-stage linear shift register generator and Gold sequence, there is a limit on the number of maximum length sequences. In contrast, for the chaotic sequence any change of the initial conditions or parameters will generate a new sequence, thus theoretically there exist an infinite number of sequences that can be generated.

Also, chaotic sequence provides a well distributed spreaded signal histogram which indicates a more signal randomness and thus more security compared to PN code sequence.

Thus, due to the above advantages that the use of chaotic sequence provides, it is considered a best choice for secure data communication.

In this paper an image is used instead of binary data for digital transmission, this open the way for encrypted image transmission over a channel through spreading the information using not only well known maps as logistic or tent maps but also through the usage of modified maps through addition of some constants to the state space equations of the maps to be used as a secret key.

And, finally adding RNS to the model in order provide better security and encryption to the transmitted data as seen from the histogram of the encrypted information.

References

[1] N.B chakrabarti , A. K . Datta, “introduction to the principles of digital communication", New Age Publishers, 2007.

[2] Erik Storm, Tony Ottosson, Arne Svensson, “An introduction to spread spectrum systems”, Department of signals and systems, Chalmers university of technology, Sweden, 2002.

[3] Raymond L. PICKHOLTZ, “Theory of spread spectrum communication – A tutorial”, IEEE Trans. Communication, vol. 30, No.5, May 1982.

[4] Ryuji Kohno, Reuven Meidan, and Laurence B. Milstein, “Spread Spectrum Access Methods for Wireless Communications”, IEEE Communication magazine, January 1995.

[5] Yong Luo, “Spread Spectrum Ranging System – Analysis and Simulation”, Master Thesis in Electronic systems engineering – University of Regina, Saskatchewan, March 1998.

[6] Ipsita Bhanja, “Performance comparison of various spreading codes in spread spectrum modulation in ranging technique”, Proc of national conference on range technology, pp30-35, 2006

[7] Carl Andren, “A Comparison of Frequency Hopping and Direct Sequence Spread Spectrum Modulation for IEEE 802.11 Applications at 2.4 GHz” Harris Semiconductor, Palm Bay, Florida Nov. 1997.

[8] S. Mandal and S. Banerjee, "A chaos-based spread spectrum communication system," Nat. Conf. Nonlinear Sys. Dynamics, IndianInstitute of Technology, Kharagpur, Dec 28-30, 2003.

[9] Predrag Cvitanović, Roberto Artuso, Ronnie Mainieri, Gregor Tanner, Gábor Vattay, Niall Whelan and Andreas Wirzba, "Chaos: Classical and Quantum", ChaosBook.org version12.3, Sep 30 2008.

[10] Peter Stavroulakis, “Chaos Applications in telecommunication,” Taylor and Francis Group, LLC, 2006.

[11] Zbigniew Kotulski, Janusz Szczepański, Biuletyn Wat, "Application of discrete chaotic dynamical systems in cryptography", DCC method, Int. J. Bifurcation and Chaos, PP.111-123, 1999.
[12] Shujun Li, Xuan Zheng, "On the security of an image encryption method", in Proc. IEEE Int. Conference on Image Processing (ICIP'2002).
[13] Shujun Li, Xuan Zheng, "Cryptanalysis of a chaotic image encryption method", In Proceedings of 2002 IEEE International Symposium on Circuits and Systems (ISCAS 2002).
[14] Jui-Cheng Yen, Jiun-In Guo, "A new chaotic key-based design for image encryption and decryption", In Proceedings of 2000 IEEE International Conference on Circuits and Systems (ISACS 2000.
[15] Mario Martelli, "Introduction to discrete dynamic systems and chaos," Wiley, Inter-science, 1999
[16] Wang Hai, Hu Jiandong. "Logistic-Map chaotic spread spectrum sequence" ACTA Electronica sinica, Vol.25 No. 1 19-23, 1997.
[17] Jessa, M. "The period of sequences generated by tent-like maps", IEEE trans. Circuits syst. I, Fundam. Teory appl., 2002, 49,(1), pp.84-88
[18] Lie-Liang, Lajos Hanzo, "Performance of residue number system based DS-CDMA over multipath fading channels using orthogonal sequences", department of electronics and computer science, university of Southampton, UK , July 1999.
[19] K. W. Watson, "Self-checking computations using residue arithmetic," *Proc. IEEE*, vol. 54, pp. 1920–1931, Dec. 1966.