that map nicely with cryptographic requirements such as confusion, diffusion, deterministic pseudo-randomness, algorithm complexity. Furthermore, the possibility of chaotic synchronization, where the master system (transmitter) is driving the slave system (receiver) by its output signal, made it probable for the possible utilization of chaotic systems to implement security in the communication systems. Many methods like chaotic masking, chaotic modulation, inclusion, chaotic shift keying (CSK) had been proposed.

WORKING PRINCIPLE

The principle of chaotic masking hints at the larger issue of communication secrecy. Certainly, fundamental properties of chaotic systems seem to make them ideal for this purpose. Chaotic systems are inherently unpredictable. Their dynamics are a periodic and irregular. A small message added to or modulated onto unpredictable a periodic and irregular wave forms could be difficult to decipher without a second chaotic system, identical to the first, which can synchronize to the transmitter. Concealment, privacy, and encryption these aspects can be interpreted in the context of chaotic communication. Concealment of a message using chaotic carrier signals is possible because the carrier is irregular and a periodic. The presence of a message in the chaotic fluctuations may not be obvious. According to Shannon, the second aspect, communication privacy, occurs for systems in which special equipment is required to recover the message. This situation is present with chaotic communication systems because an eavesdropper must have the proper receiver system, with matched parameter settings, to decode the message. Finally, encryption occurs naturally in chaotic communication techniques. In conventional encryption techniques, a key is often used to encrypt the message. If the transmitter and receiver share the same encoding key, the scrambled message can be recovered by the receiver. In chaotic systems, the transmitter itself acts as a dynamical key. The receiver must be able to synchronize to the transmitter's dynamical parameters. A direct application of chaos theory to telecommunication systems appears in a conventional digital spread spectrum, where the information is spread over a wider band by using a chaotic signal instead of the usual periodic sequence, called Pseudo-noise (PN) sequence, the latter is generated, for instance, by linear shift registers. The problem with a linear shift register generator is that the price paid for making the period of the PN long increases sharply because a large amount of storage capacity and a large number of logic circuits are required. This imposes a practical limit on how large the period of the PN can actually be made. This can be overcome by the use of digital chaotic sequence generators. A classic, efficient, and well-studied method of generating a sequence of pseudo random bits is the linear feedback shift register.

A shift register is a very simple electronic device, which produces a very fast pseudo random sequence. Basically, this device is formed by a sequence of adjacent bits in a register and at each clock signal the sequence is shifted a position to the right. The right-most bit is the output. To the left, one additional bit is introduced which is computed by a function, named feedback function, of the previous contents of the registers. The binary storage elements are called the stages of the shift register, and their contents are called the state of the shift register. After starting the shift register in any initial state, it progresses through some sequence of states; hence a periodic succession ultimately results. This succession is used in the XOR operation to produce the ciphered message. When the feedback function is linear, the shift register is called a linear shift register and using the theory of polynomials over finite fields, it is possible to discover how to design a device that produces a sequence whose period is very long and has good randomness properties. But, it is important to stress that the linear feedback shift register is insecure for cryptographic purposes.

II. METHODS AND MATERIAL

A. How to achieve chaotic behaviour?

Chaotic behaviour can be obtained by using different mapping techniques [4].In this paper we are using tent mapping technique.

TENT MAP: The following is a tent map equation.

$$x_{n+1} = \begin{cases} \mu x_n & \text{for } x_n < 0.5 \\ \mu(1 - x_n) & \text{for } x_n \gg 0.5 \end{cases}$$

Where m=1.9 and x(0)=0.4142. A code illustrating chaotic behaviour is given below:

$$x(0) = 0.4142;$$
$$\text{for } i = 1{:}\,1{:}\,1000$$
$$\text{if}(x(i-1) \leq 0.5)$$
$$x(i) = 1.9 * x(i-1);$$
$$\text{else}$$
$$x(i) = 1.9 * (1 - x(i-1));$$

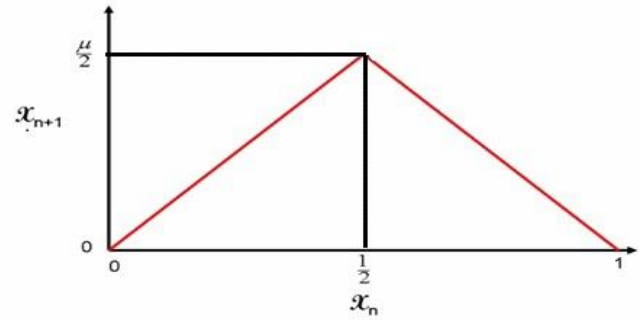

Figure 1: Tent map

CHAOS BASED COMMUNICATION SYSTEM USING REED SOLOMON (RS) ENCODER & DECODER

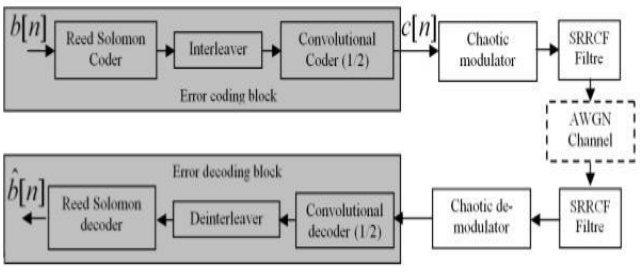

Figure 2 : Baseband chaotic communication system with error coding and decoding block

Transmitter Structure

1. Error coding block

The data information symbols are firstly coded by a Reed Solomon (RS) coder [6]. RS are powerful error correcting codes that can be employed in a wide variety of digital communication systems. The RS (255, 239, 8) is used in this project. Interleaving is a technique commonly used in communication systems to overcome correlated channel noise such as burst errors or fading. As a result of interleaving, correlated noise introduced in the transmission channel appears to be statistically independent at the receiver and thus allows better error correction. Without an interleaver, the RS decoder cannot correct more than 8 errors in code words. At the output of the interleaver, the symbols are coded with a convolution coder (7, 1/2) with code rate R=1/2.

2. Chaotic modulator

The main goal of using a chaotic modulator is to have a highly secure transmission with small complexity and low cost of implementation. By introducing this simple modulator, the system can benefit of all the features offered by the chaotic signal. After coding the information bits $b[n]$, the output symbols $c = [c[1] \ldots . c[N]^T$ are transmitted using a chaotic signal. Then

$$s(n) = s[N - n] = 1 + 2c(n), 1 + 2c(n), 1 \ll n \ll N$$

According to the above equation, the generated chaotic signals can take place in the two regions for $(s = 1, s = 3)$. The inner regions $= 2$, is used as a guard region to ensure a minimum distance between the two waveforms associated to $c = 0$ and $c = 1$. Finally, the transmitted baseband signal is

$$x(n) = x(N - n) = f_{s(n)}^{-1}[x(n - 1)]$$

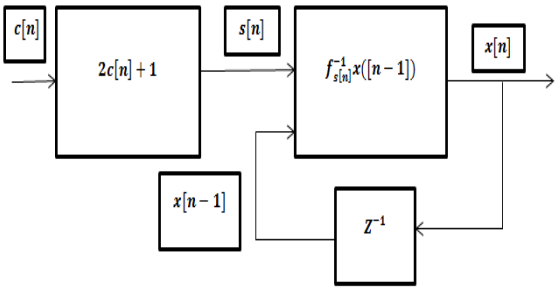

Figure 3: Chaotic modulator

Figure 3 shows the chaotic modulator. Note that this baseband chaotic signal at the output of the modulator can be moved to any desired frequency band for a pass band transmission. A square root raised cosine filter is used as pulse shape filters for the chaotic symbolic samples.

Receiver structure

After passing through an AWGN channel, the received signal is

$$y(n) = x(n) * n[n - T] + w(n)$$

Where h[n] is the pulse shaping filter, w[n] is an additive white Gaussian noise with power spectral density equal to $N_0/2$, T is the period of dynamic symbols, and $*$ denotes the discrete time convolutional operator. We assume that we have a perfect clock synchronisation on the receiver side which means that the sampling at the output of the matched filter is synchronized with the sampling period of the received signal. The demodulation of the received chaotic signal is achieved by the chaotic demodulator. Finally it is decoded by an RS decoder to estimate the emitted bits $b[n]$. The proposed scheme has been verified in Rayleigh Fading channel also.

Chaotic Demodulator

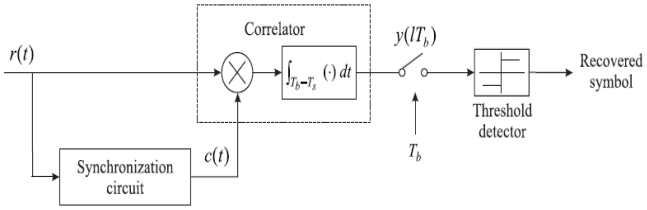

Figure 4: Coherent antipodal CSK system demodulator.

Assuming that the transmitted signal is corrupted by additive noise, the received signal is given by

$$r(t) = s(t) + n(t)$$

where $n(t)$ denotes the noise signal. At the receiver, a self-synchronization circuit will be used to reproduce the chaotic signal. The reproduced signal then correlates with the received signal r(t).

The output of the correlater is given by

$$y(lT_b) = \int_{(l-1)(T_b+T_s)}^{lT_b} r(t)c(t)dt$$

Where T_s is the acquisition time to achieve synchronization.

The output of the correlator is compared with the threshold (zero in this case) to determine whether a "+1" or "−1" has been received. If the correlator output is larger than zero, a "+1" is detected. Otherwise, a "−1" is decoded.

III. RESULTS AND DISCUSSION

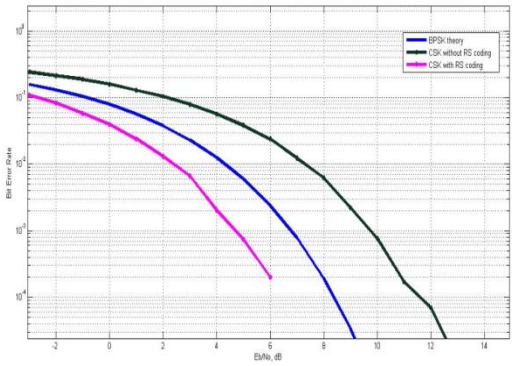

Figure 5 : Bit Error Rate (BER) calculation over AWGN channel for RS (7, 3) code.

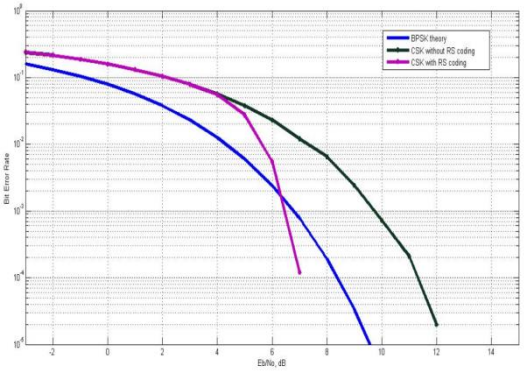

Figure 6: Bit Error Rate (BER) calculation over AWGN channel for RS (256,239) code.

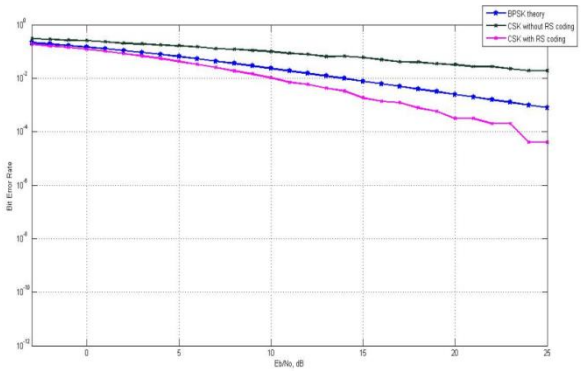

Figure 7: Bit Error Rate (BER) calculation over Rayleigh channel for RS (7,3) code.

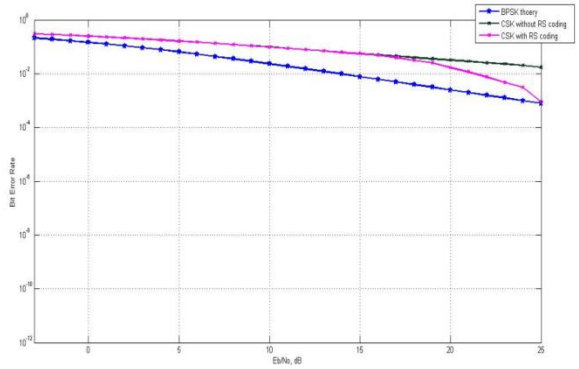

Figure 8: Bit Error Rate (BER) calculation over Rayleigh channel for RS (256,239) code.

IV. CONCLUSION

The objective of this paper was to explore techniques to exploit the properties of chaotic signals to implement secure communication. The facts that chaotic signals were aperiodic, broadband and sensitive to initial conditions/parameters mismatches were important for them to be utilized in security. Therefore the chaotic parameters acted some sort of hardware key and hence same dynamical system was necessary for the transmitter and the receiver with proper chaotic synchronization techniques. The implementation of the method was done mostly by using tent map therefore, the performance of the methods in other chaotic systems, preferably higher order systems, or time delay systems, can also be done in order to improve the security further.

Simulation results confirm the improvement of the performance of CSK by introducing the channel coding block, the degradation caused by the chaotic modulator is attenuated and performance becomes very close to non-secure binary coded BPSK.

V. REFERENCES

[1] C. Shannon, "Communication in the presence of noise," Proc. Inst. Radio Eng., vol. 37, pp.10–21, Jan 1947.

[2] L. Chua, "Dynamic nonlinear networks: State-of-the-art," IEEE Transactions on Circuits and Systems, vol. 27, pp. 1059–1087, Nov 1980.

[3] S. H. Strogatz, "Non linear dynamics and chaos," Preseus Books Publishing, LLC, 1994.

[4] P. Stavroulakis, Chaos applications in telecommunications. CRC press, 2005.

[5] G. Kolumban, M. Kennedy, G. Kis, and Z. Jako, "Fm-dcsk: A novel method for chaotic communications," in Circuits and Systems, 1998. ISCAS'98. Proceedings of the 1998 IEEE International Symposium on, vol. 4. IEEE, 1998, pp. 477–480.

[6] G. Kaddoum and F. Gagnon, "Error correction codes for secure chaos-based communication system," in Communications (QBSC), 2010 25th Biennial Symposium on. IEEE, 2010, pp. 193- 196.