CSK BASED SECRET COMMUNICATION

N.R.Raajan, S.Praveen, J.Sushidhar, K.S.Mathavan, K.Karthikeyan, M.Malligaraj, P.Praveenkumar
Dept. of ECE, School of EEE, SASTRA University,
Thanjavur, TamilNadu,INDIA.
nrraajan@ece.sastra.edu,praveenanu26@gmail.com,sushidhar26@gmail.com, ksmaddy91@gmail.com,
m.malligaraj@gmail.com, krishkarthikeyan1991@gmail.com, praveenkumarvps@gmail.com

***Abstract*-The notion of non-linear dynamics has become an energetic and fashionable field of work that is having a thoughtful effect on a wide variety of topics in present day technology. One such evolution of non-linear dynamics is the chaos theory. It is not about disorder, rather is about very complicated systems of order. However, the point of interest lies in bridging the gap between random nature of chaotic signals and the demanding needs of Information safety. Hence, Safety via ambiguity is employed to ensure correct and complete transaction of data. A good solution to bring ambiguity is to materialize the message signal as unsystematic information. Consequently, Safety via ambiguity is resolved by a technique called Chaos shift keying. The technique is all about replacing one's and zero's of the message signal by the chaotic signals. The simulated results and future scope are discussed. It has been found that CSK modulated waveform looks exactly like a wideband noise. Hence even if a third party tries to hack the system, nobody can be able to judge any significant information is present or not.**

Keywords- Information safety, non-linear dynamics, Chaos, Chua Circuit, Chaos shift keying, Modulation, Demodulation.

I. INTRODUCTION

Communication is the act by which the sender and the receiver of the message will be tuned to a particular message or a series of messages. The same was defined by Ban and Hawkins as the process of sending and receiving messages through channels which establish common meaning between a source and a receiver. The study of communication has revealed that it is not only a vital but complicated process too. There are numerous definitions, theories and researches available about communication. But our main intention is primarily focused on how to communicate "safe and sound". There comes the need for Information security. Several people are misjudged by the name of Information security. People visualize safety of the information with restricted number of single events such as website hacking, procuring credit card details etc. The reality is that these are only tips of Information security. There is lot to explore in Information security rather than just restricting our views with respect to the IT industry. Classic examples include smokes produced by Red Indians to communicate among themselves, ancient rulers used to trim their soldier's head and inscribe the information onto their heads and pass to their neighbor's country. The above examples have set a tone that even the day to day activities has to be carefully looked upon for safe exchange of information. Thus there is certainly an alarming issue in developing Information security. As long as we keep our Information sheltered, the concept of eavesdropping remains dumb.

II. CHAOS

So what precisely chaos is? As the name suggests, Chaos means a state of confusion or unclear. The name "chaos theory" comes from the idea that the systems depict it as deceptively disordered, but chaos theory is actually about finding the underlying order in apparently random data. In technical aspect, Chaos is a random, aperiodic, noise like structured waveform. The history of chaos goes back to the experiment performed by Edward Lorenz. In 1960, he was working on the problem of weather indication. He designed a set of twelve equations to predict weather pattern which was actually a failure as it was not able to exactly predict the weather on a given day. In the following year, he wanted to see the particular sequence again. But this time he started in the middle of the sequence, rather than in the beginning. He saved the number separately and executed the sequence. After an hour or so, it was surprising to see that the sequence has evolved differently. The new original pattern was found to be entirely different from the old pattern. This effect came to be popularly known as the Butterfly effect which explains the dependence on the initial conditions. Any small changes in the initial conditions can change the entire output. This led to the impact that chaos theory is "sensitive to initial conditions". The amount of difference in the initial conditions is so small that it is comparable to butterfly flapping its wings. Just a small change in the initial conditions can drastically change the long-term behavior of a system.

A perfect analogy for the chaos theory is the motion of a double pendulum. Similar to the fact that chaos waveforms do not trace the same path again; the trajectory of the double pendulum is distinctive for every starting points. There are lots of technical facts about Chaos to be understood which are given below.

Chaotic systems are deterministic as well as dynamic in nature. Controlled change in the output of the chaotic system with regard to time makes it special in the present communication era. These non-linear systems can be represented by means of either differential or difference equation.

This Deterministic dynamical system exhibits different steady state behaviors such as:

1. A DC Component
2. Periodic signals such as sinusoidal, cosine waveform and
3. A haphazard aperiodic non-repetitive continuous noise-like structured waveform.

This third component is in fact is the Chaos. As elucidated in the preceding portions, two chaos waves produced with small varying starting condition will have no relationship between them.

Chua's circuit is one of the better ways for producing chaotic waveforms. This circuit consists of Chua (chaotic) diode, active elements such as inductors and capacitors and non-linear resistors. It is evident that formulating the inductors in an IC is a difficult task, Chua's circuit without inductor has been recommended by numerous researchers.

A collection of non-linear differential equations can be used to epitomize the dynamics chaotic system:

$da/dt = \alpha*(b-a-h)$

$db/dt = a - b+ c$

$dc/dt = -\beta *b$

where a(t) and b(t) are the voltages taken at the capacitors and c(t) is the current density across the inductor present in the circuit

A dynamic system is said to be chaotic if it meets the underlying conditions:

1. It must be susceptible to starting conditions
2. It must be topological transitivity i.e. system must develop as time progresses
3. Its orbits must be intense.

Chua circuit's chaotic response is shown below:

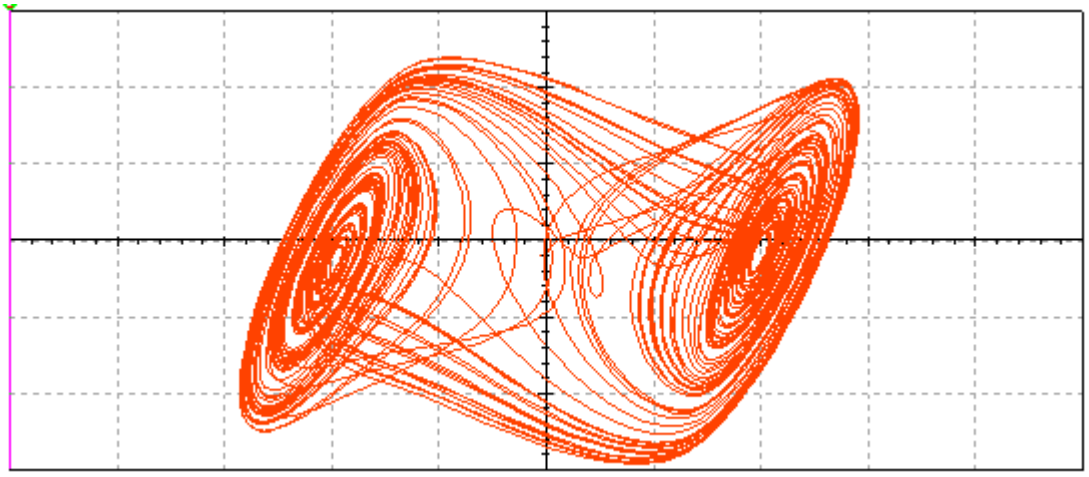

Fig.1 Simulated Chaotic wave

III. MODULATION

As said in the earlier section, waveforms produced by the Chua circuits will be appearing like a noise to the layman's eye and are supposed to have null auto correlation. The biggest advantage of chaotic waveforms is to force a communicator's signal to look like a wideband noise. The above referred modulation concept can be realized by the modulator circuit given below.

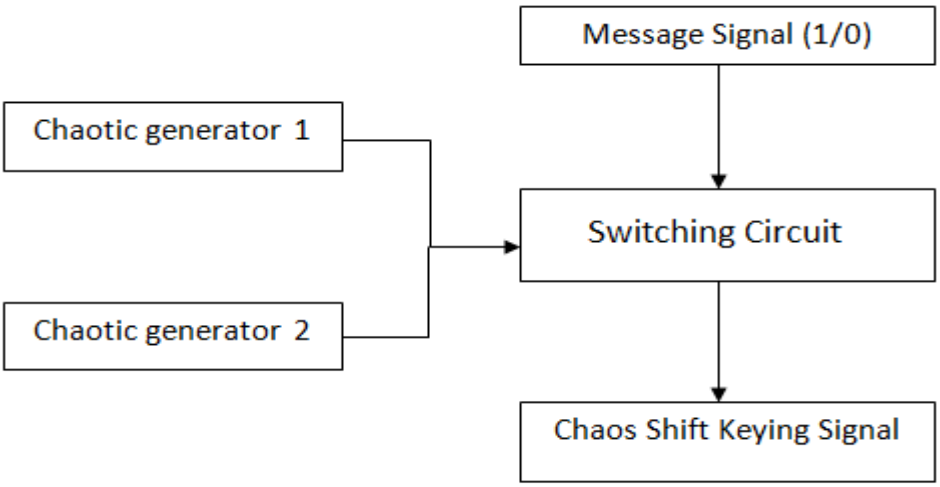

Fig.2 Modulator circuit generating CSK signal

It is obvious from the above diagram that modulator is simply a button that toggles between the output of the chaotic generators, nothing but the Chua circuit. Based on the input from the user, the button switched between the two generators.

There are different ways for producing two dissimilar chaotic waveforms

1. By using different Chua's circuits.

2. Same Chua circuit with diverse starting conditions

3. Same Chua circuit and same starting conditions but being multiplied by different constants.

Chaos Shift keying is achieved by using two different chaos wave generated from their respective chaotic generators. The message signal could be either '1' or '0', where '1' and '0' are represented by different chaotic waves. Based upon the message signal, two chaotic generators will be selected and fed to the Switching circuit.

Chaos wave produced from chaotic generator 1 is used to denote 1's of the message signal and chaos wave produced from chaotic generator 2 is used to denote 0's of the message signal. This will make the interloper to be ignorant of the exchange of information as the chaotic modulated wave will look like noise, as shown below

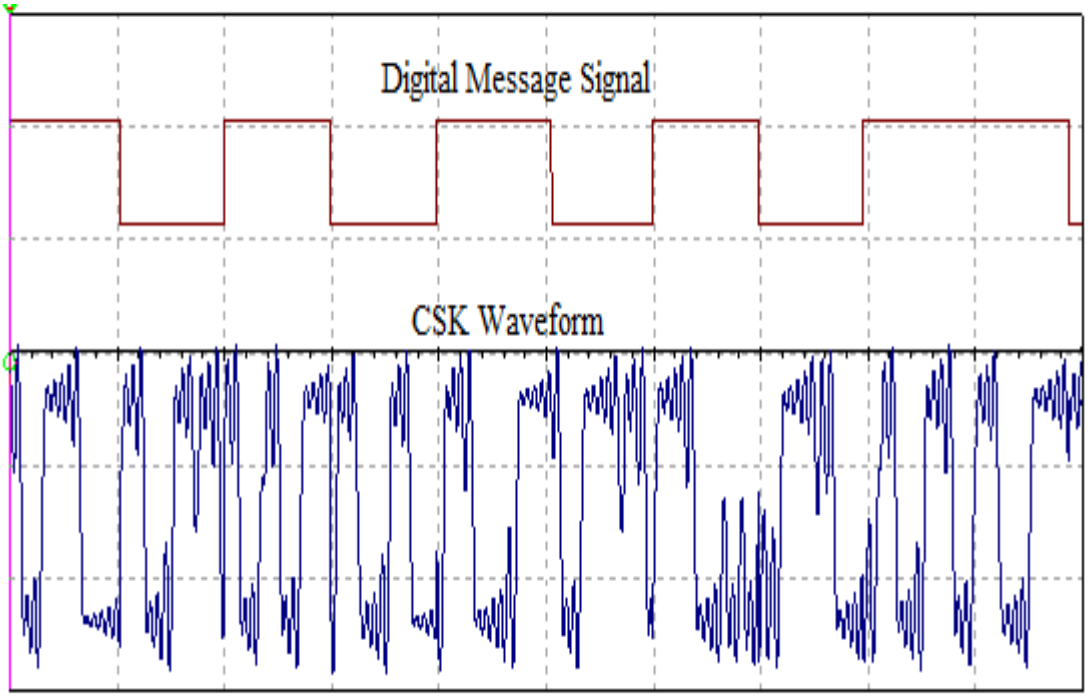

Fig.3 CSK Waveform with its corresponding input message signal

IV. DEMODULATION

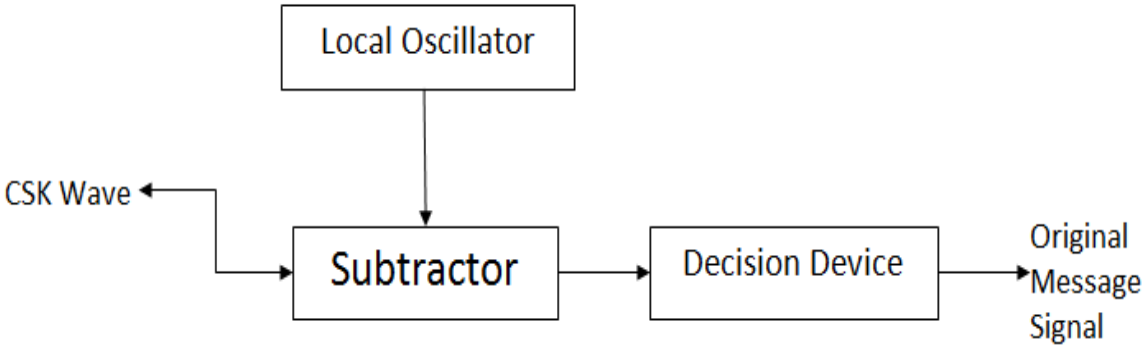

Fig.4 Demodulator circuit retrieving the original message signal from received CSK signal

Complement of the modulator circuit is shown above. The circuit consists of a subtractor and a decision device, also known as the Threshold Detector. The output of the subtractor is the given as input to the decision device. Finally the original message signal which was given from the information source at the beginning can be retrieved back from the output of the decision device.

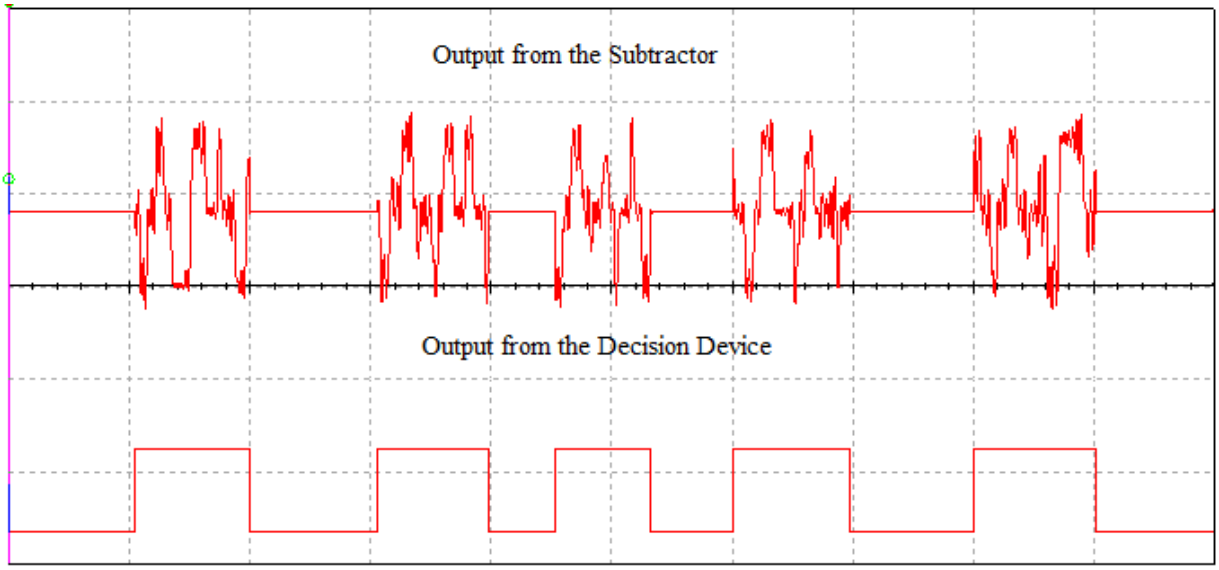

Fig.5 Output of the demodulator circuit

V. EXPERIMENTAL RESULTS

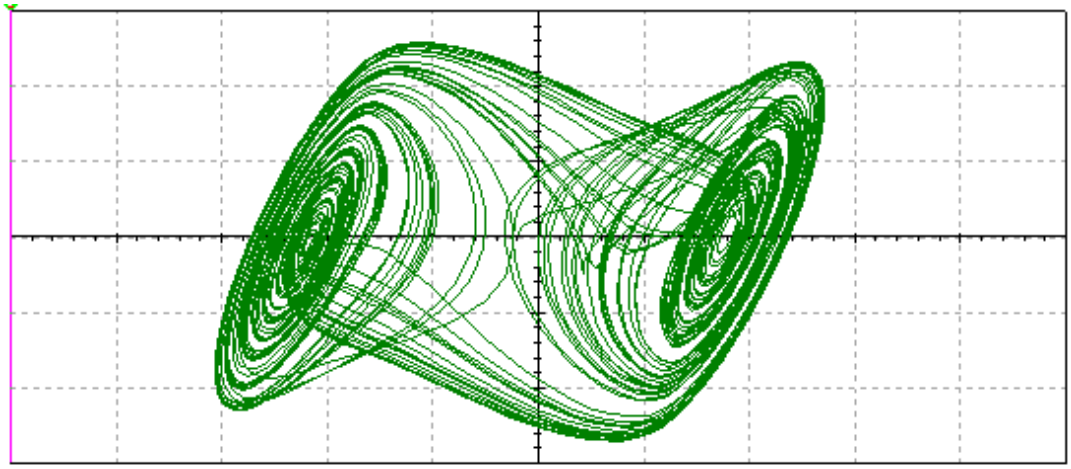

Fig.6 Chaos wave from generator1 –Phase domain

The above figure shows the chaos wave emitted from the output of the transmitter system. The above is attained by blending the waves in Fig. 7 and observing it in Phase domain. The figure resembles like a double-scroll that are being connected by swirling lines.

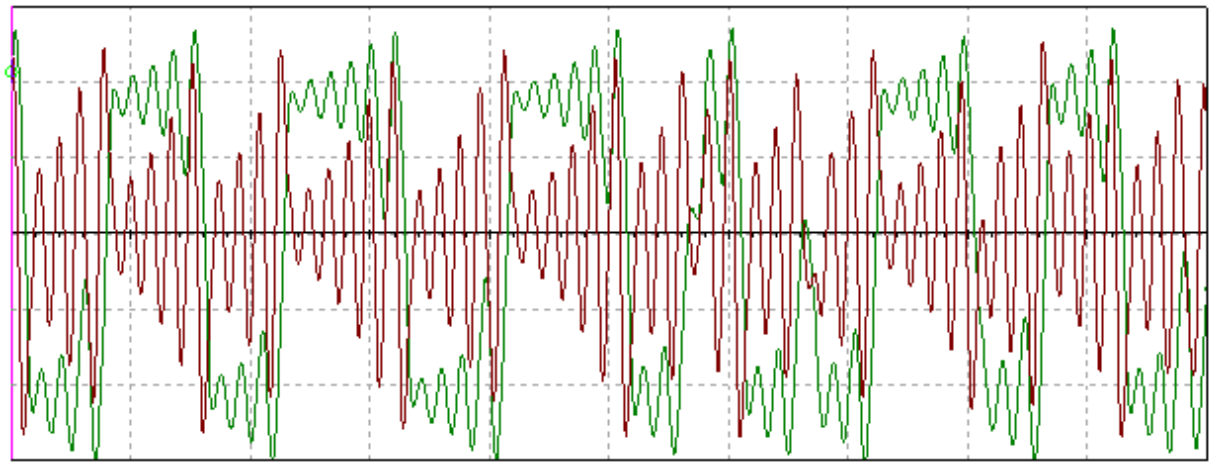

Fig.7 Chaos wave from generator1 –Time domain

The output will be taken across the capacitors. It is known fact that chaos waves are sensitive to initial conditions. Sensitivity to initial conditions is made with respect to the capacitance values. Even the minute changes in the magnitude values of the capacitances can lead to different chaotic waveforms. The following figure is the one which is obtained by changing the magnitude of the capacitance values used in the first circuit by one percent proves the above said statement.

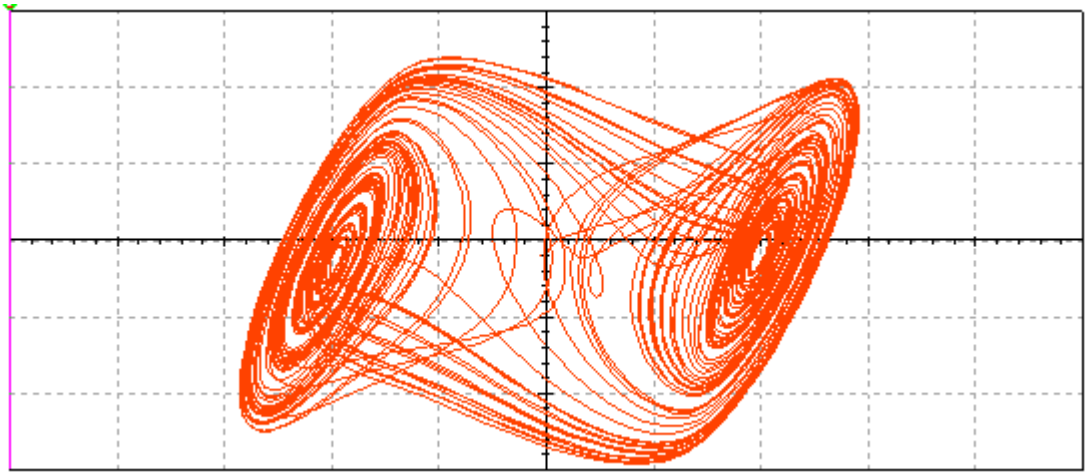

Fig.8 Chaos wave from generator2 –Phase domain

The plots in the figure may look alike but actually it will not be the same due to minute changes in the initial conditions.

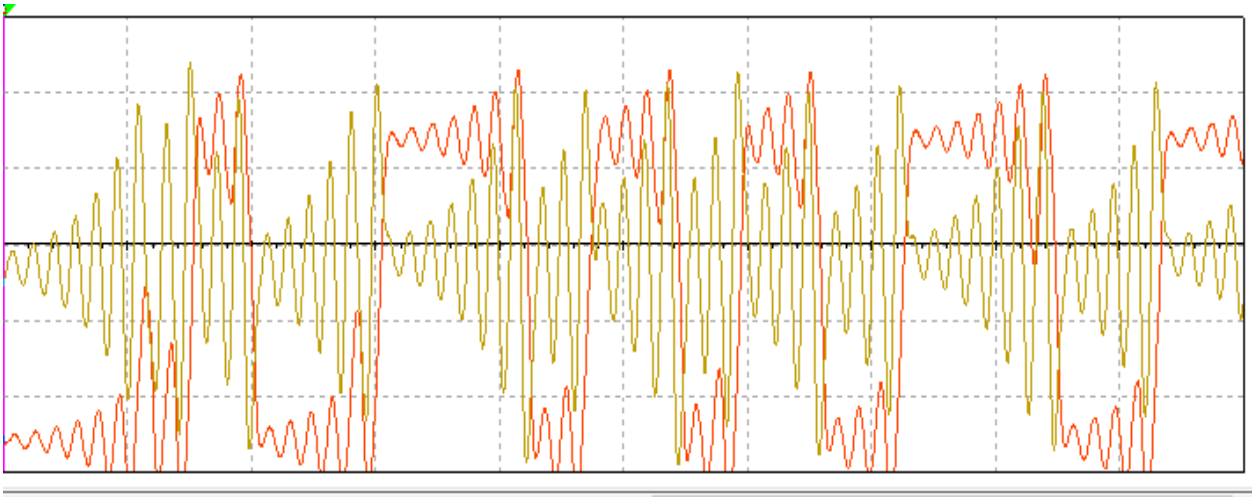

Fig.9 Chaos wave from generator2 –Time domain

The following figure is the CSK modulated waveform that replaces the input signal, which is transmitted through the open channel. This wave will not grab the attention of the hackers as each symbol in the digital signal is substituted with the waves shown in Fig. 7 and 9 that looks like noise.

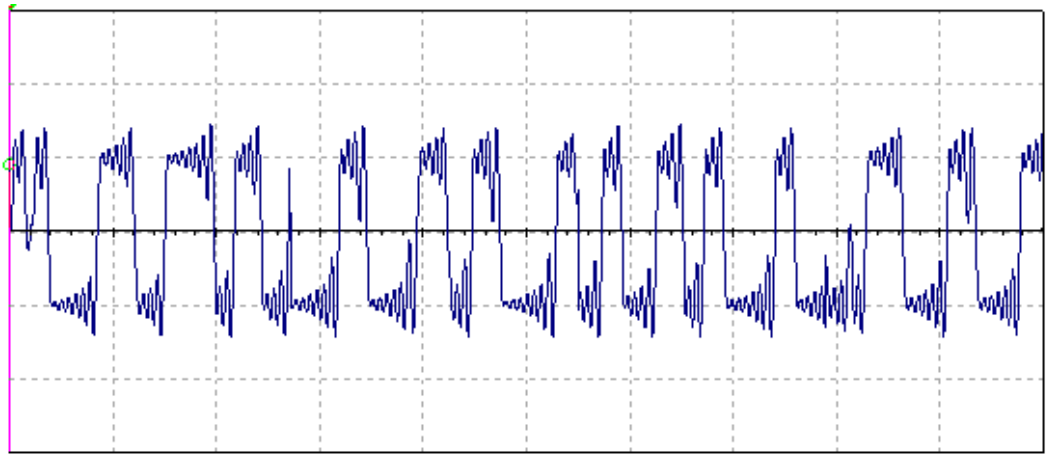

Fig.10 Chaos Shift keying waveform

The output from the demodulator part, which is shown below, is obtained feeding the subtractor circuit's output to the decision device. Based on the subtractor output, the threshold detector will determine the original message signal. For a good system, the input message signal can be retrieved back from the output of the decision device and it is shown in the figure.

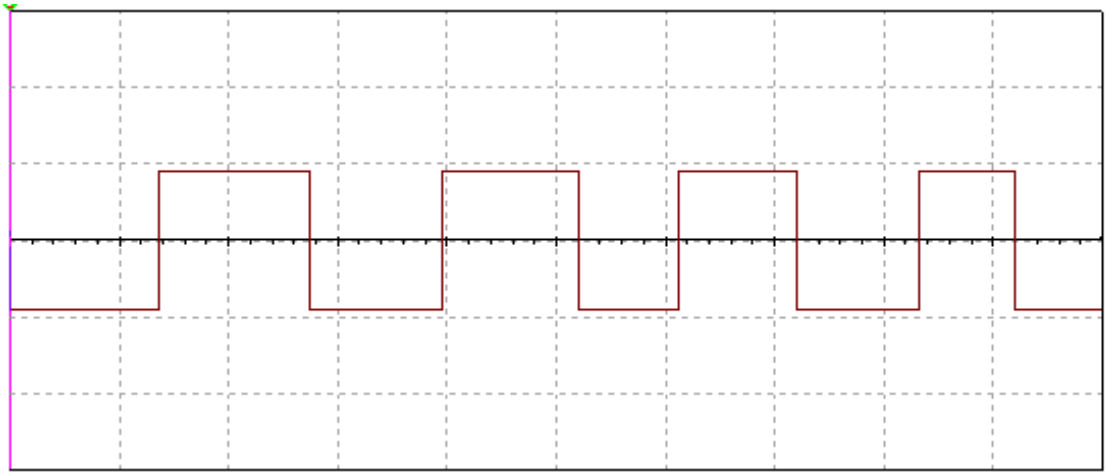

Fig.11 Output from the decision device

VI. CONCLUSION

Thus the urged mythos in this paper achieves data safety through equivocalness. Encumbrance of two chaotic waves can be completely kept off, as the chaos waves have zero correlation property, which are the major troubles in the current communication trend. Though the intruder seeks to attack the signal, one cannot trace the message signal as chaos wave produced is random and non-periodic as the produced wave is very sensitive to the initial condition. Though the groove is open and has high possibility for hackers to get through, this mythos doesn't create any hunch as this chaotic transmitted signal would not attract anyone's care. The initial conditions must be kept as clandestine and this should be disclosed only to the exact receiver via a secret channel for retrieving the original message. Further works can be explored in the fields like intervention free and more secured MC-CDMA, MIMO - OFDM and so on.

REFERENCES

[1] Chua,L.O, *Introduction to nonlinear Circuit theory*, McGraw-Hill, New York, 1969.

[2] Leon O. Chua, *The Genesis of Chua's Circuit*, Hirzel-Verlag, AEU, Vol. 46, No. 4, 1992.

[3] G. Kolumban and M. P. Kennedy, "The role of synchronization in digital communications using chaos-Part III: Performance bounds for correlation receivers", *IEEE Transactions on Circuits and Systems I: Fundamental Theory Application*, vol. 47, no. 12, pp. 1673-1683, Dec. 2000.

[4] N.R.Raajan, Krishnamourthy Karthikeyan, Malligaraj.M, Praveen.S et al, "Chaos Based Shift Keying for Covert Communication", *Article in Press.*

[5] Herve Dedieu, M.P.Kennedy, Martin Hassler, "Chaos Shift Keying: Modulation and Demodulation of a Chaotic Carrier using self-synchronizing Chua's circuits", *IEEE Transactions on Circuits and Systems-II: Analog and Digital Signal Processing*, Vol.40, No.10, October 1993.

[6] Yuu-Seng Lau and Zahir M. Hussain, "A New Approach in Chaos Shift Keying for Secure Communication, *Proceedings of the Third International Conference on Information Technology and Applications (ICITA)*, 2005.

[7] Sergio Callegari, Riccardo Rovatti and Gianluca Setti, “Spectral Properties of Chaos-Based FM Signals: Theory and Simulation Results”, *IEEE Transactions on Circuits and Systems—I: Fundamental Theory and Applications*, vol. 50, No. 1, January 2003
[8] L.M.Pecora and T.L.Caroll, “Driving Systems with Chaotic Signals”, Phys. Rev. A, vol.44, pp. 2374-2383, 1991.
[9] Michael Peter Kennedy, Geza Kolumban, “Digital Communication using chaos”, Signal Processing, Elsevier, vol.80, pp. 1307-1320, 2000.
[10] N.R.Raajan, B.Monisha, Niranjana Rangarajan, Vishnupriya.R, “ Secured OHWDM using Fractals”, *International Conference on Modeling Optimization and Computing (ICMOC)*, 2012.
[11] S.S. Haykin, Communication Systems, 3rd Edition, Wiley, New York, 1994.
[12] Michael Peter Kennedy, "Robust Op-Amp realization of chua's circuit", Frequenz, vol. 46, no.3-4, pp. 66-80 March-April 1992.
[13] Christopher P. Silva and Albert M. Young, "Introduction to Chaos-Based Communications and Signal Processing", *IEEE Aerospace Conference Reprint*, 2000.