On the Realization of Non-Linear Pseudo-Noise Generator for various Signal Processing and Communication Applications

Javaid A. Sheikh[1,] Shabir A. Parah[1] G. Mohiuddin Bhat[2]
[1] Post Graduate Department of Electronics and Instrumentation Technology, University of Kashmir-Srinagar-190006
[2]University Science Instrumentation Centre, University of Kashmir- Srinagar
Corresponding Author: Javaid A. Sheikh email: sjavaid_29ku@yahoo.co.in

Abstract

In digital communication systems and digital signal processing, the design of pseudo-noise (PN) sequences having good correlation properties has been one of the most important development steps. Its well-known application areas include spread spectrum communications, Multiuser Communications, Digital Signal Processing for reduction of power spectral density, mitigation of Multiple Access Interference (MAI) and improvement of signal to noise ratio (SNR) respectively. In this paper a performance of non- linear PN code generator for interference rejection improvement of signal to noise ratio in signal processing applications have been studied. The signal of interest can be considered to be a digitally controlled wide band digital chaotic signal, which has been implemented by conventional PN code generators. The proposed technique can be used as an alternative code for improvement in signal to noise ratio, interference rejection, spreading code for various signal processing and communication applications. The proposed scheme has been implemented using matlab as a simulation tool. Power spectral density, auto-correlation and cross-correlation property have been thoroughly studied and has been compared with conventional scheme and are presented in the paper.

Keywords: PN Code Generator, Spread Spectrum Modulation, Auto-correlation, Cross-correlation, Power Spectral Density.

1. Introduction

The signal processing is concerned with time varying signal modeling, non-linear modeling and processing, signal compression and applications of DSP in communication by way of channel equalization, error correction and modulation/ demodulation. An essential aspect of signal processing is modeling and analysis of signals [1]. The analysis, manipulation and processing of signals is fundamental to radio communication systems, multimedia systems, medical and biological systems etc., each presenting unique technical challenges. The signal processing for communications deals with signal processing aspects of radio communication, biological, multimedia and sensor system. The emergence of distributed image communication systems with multiple visual sensors have created the need for new signal processing and networking algorithms that are able to cope with the specific constraints imposed by the distributed architectures. They require in particular that the images are processed and transmitted without any global knowledge of the signals, or that of the full system. Distributed processing, coding and communication of visual information have thus recently gained much interest from the research community. In communications, the speech signal is processed and transmitted over a communication channel. Speech signals contain information about the time varying characteristics of the excitation source and position of the time-domain window. When transmitted over a communication channel it is corrupted by noise and hence signal to noise ratio gets reduced. Thus some form of channel coding is used to accentuate signal-to-noise (SNR) of the signal prior to its transmission over a noisy channel. One way to accomplish the required channel coding is to spread the spectrum of the signal in order to reduce the effect of channel noise after de-spreading the signal at the receiver. The spectrum spreading is achieved by the use of a typical spreading code with unique features [2]. This paper presents a non-linear method for the generation of a typical spreading code which enjoys the following features.

a: Good auto- correlation property
b: Low power spectral density
c: more complex (wide-band chaotic signal)

d: Easy to implement

2: Pseudo-noise (PN) codes)

Pseudo-random codes serve an important role in signal processing. Since the classic work of Golomb [1], numerous mathematical techniques have been developed for the generation of code families with high auto- and cross-correlation performance. With few exceptions though researchers in the field have been interested in the development of the algebraic aspect of the theory of code design. The goal of the present paper is to demonstrate how analytical techniques can provide higher flexibility to build different requirements into the algorithms. In order to achieve this, we propose here a technique which make extensive use of tools from Muliti-resolution Harmonic Analysis as well as a general result of Benke regarding the fundamental construction of Rudin-Shapiro Polynomials. More specifically, we consider codes and code-families as finite approximants of bases in infinite-dimensional function spaces. An approximation scheme is exhibited with the desired asymptotic properties. We then obtain a variety of new code generation and provide some explicit estimates for their performance. To motivate our approach to the design problem of coding sequences, we will follow the historical development of the subject through the theory of Shift Register Sequences a widely used spreading code in signal processing and communication applications.

Linear shift registers are very important for the algebraic theory of error correcting codes. In a shift register (SR), eventually, a sequence will repeat. This is because for a binary SR sequence, there are only 2r possible states (either on or off, for each tube). So, a repetition occurs in the first 2r states. However, we can improve on that bound, since if we have a state of all 0's, the shift register will continue producing 0's, which means its period is just 1. So, the period of a binary shift register is at most 2r − 1. A sequence generated by an r-tube shift register will be said to have maximum length if its period is p = 2r − 1. Lemma also in case of PN codes, any r inputs and r outputs of a maximum length r-tube shift register sequence completely determine all of the outputs. Since a computer is a finite state machine, true randomness cannot be produced on it. Hence, there is a need to produce sequences that appear random. A good model for binary random sequences is flipping a fair coin. From statistics, there are certain things one would expect from such a model:

- The number of +1's (heads) is about the same as the number of −1's (tails).

- Short runs (consecutive streaks of heads or tails) are more likely to occur than long runs. Precisely, half the runs have length 1, one fourth has length 2, one eighth have length 3, etc.

- There is also a certain property about the autocorrelation of such sequences.

Autocorrelation measures how similar a sequence is to a shift of itself. One would expect that the autocorrelation peaks at no shift (being identical to itself), and is smaller for positive shifts. The auto-correlation function r(i) of any PN sequence of length N is given by

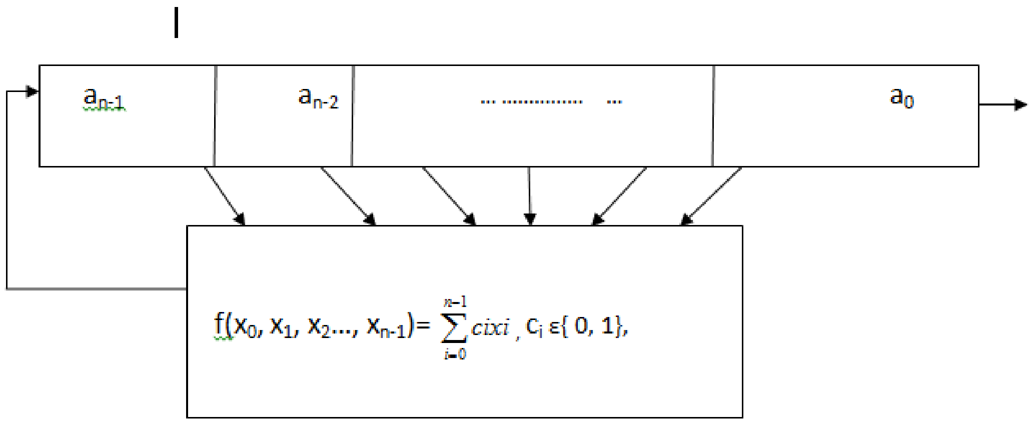
$r(i) = \{ 1$ for $i = 0$

$-1/N$ for $1 \leq |i|\ N-1$

These properties make PN sequences efficient for speech encryption. However, due to third property, adjacent bits correlation becomes considerably less, thereby making the PN sequences more effective to be used in systems like CDMA. Therefore, useful PN sequences must have very good auto-correlation and cross-correlation properties as well as maintaining some randomness property. The Welch bound places a lower limit on the maximum level of the correlation function (auto-correlation of side lobes and cross-correlation levels). The Welch bound for a set K sequences with each sequences of length (N ≥ K) is defined as

$$\Phi\text{max} \geq \sqrt{N-K/NK-K}$$

and such a bound is no longer achievable when N > K(K+1)/2 for real cases. Note that, in the sequel, sometimes we shall represent binary sequences using zeros and ones and in other cases +1's and -1's and ones are mapped to -1's. Block diagram of the binary LFSR is given below.


a_{n-1}
a_{n-2}
... .
a_0
$f(x_0, x_1, x_2..., x_{n-1}) = \sum_{i=0}^{n-1} c_i x_i$, c_i ε{ 0, 1},

So it is a finite state machine consisting of inner states, update function which modifies the inner state between two outputs and output function that computes the next output bit from the current inner state. The initial inner state is known as the initial content or seed which is required to start the machine. The feedback function of the LFSR can be chosen in such a way that the inner states iterates through all 2^n-1 possibility. It is called M − LFSR. The majority of modern signal processing techniques use several LFSRs as building blocks. In this direction combiner generators and clock-controlled generators are two main classical methodologies. It uses two or more M - LFSRs whose lengths are pair-wise co-prime and having different feedback functions. The key stream is generated as a linear / non-linear Boolean function f of the outputs of these LFSRs.

3. Proposed non-linear Pseudo-noise (PN) Signal Generator

The proposed generator is based on the combination of number of sub-generators in a determined form. By combining a number of these, a complex structure is obtained that can produce a big number of un-correlated PN sequences of the same (and maximum) period with remarkable random properties. In this technique a set of PN generators have been taken, for this if aij is the feed-back coefficients and rij as the content of the cells of the shift register (aij, rij ε G) of the number of generator rij(t) is the content of the cell rj of LFSR after the ith pulse. We denote the feedback function as Zi(t) = ai0ri0(t) + ai1ri1(t) +…………………+ aiL-1-riL-1(t) where + denotes modulo-two addition. Assume that ai0= 1 riL-1(t) depends on ri0(t) otherwise we would not exploit the length of the LFSR's. aij =1 denotes a closed connection and aij = 0 denotes an open connection. In the proposed scheme, a non-linear combiner generator in which several LFSR's are combined through a non-linear function. The block diagram of the said scheme is shown in Fig.2, and its implementation is shown in Fig.3. It consists of four LFSR's whose lengths L1, L2, L3, L4 are pair-wise relatively prime. The non-linear combiner function is controlled by LFSR and a feedback from its own output, this feedback element makes the proposed scheme more complex and good auto-correlations and cross-correlations properties as shown in Figures 4-7 respectively. The power spectral density is also shown in Figure 8-9. The proposed scheme can be considered to one of the main methodology for preventing to destroy the inherent linearity property of a LFSR and thus considered to be a best tool for various communications and signal processing applications [3]. The Performance of Proposed Scheme have been compared with the conventional scheme with that of auto and cross correlation and power spectral density and are found satisfactory to conformity

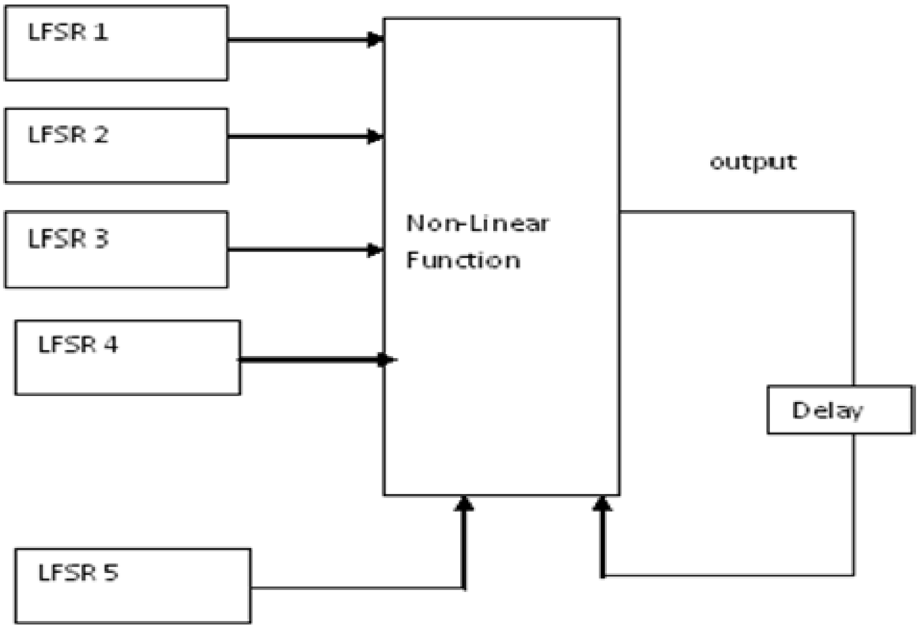


Fig. 2. Proposed Non-linear Pseudo noise Generator

.

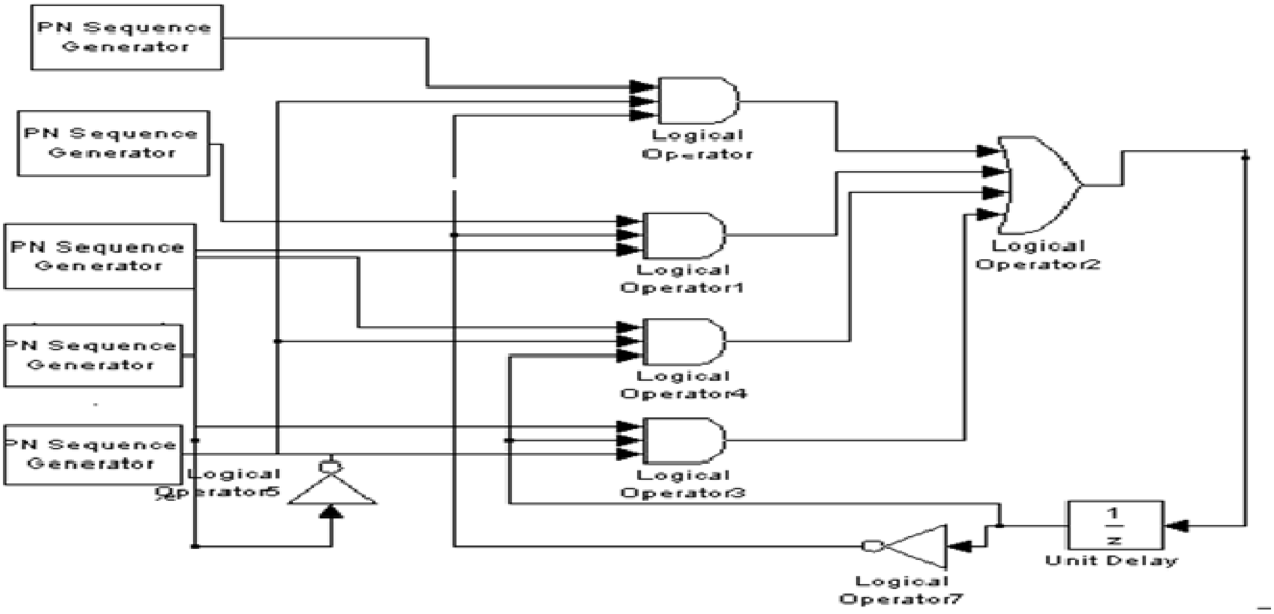


Fig.3. Implementation of Proposed Scheme

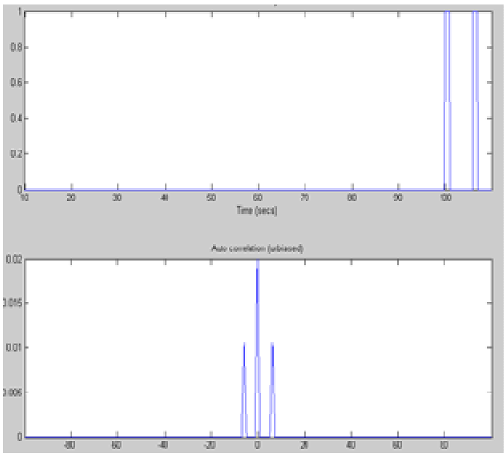


Fig.4. Auto-Correlation of Conventional Scheme

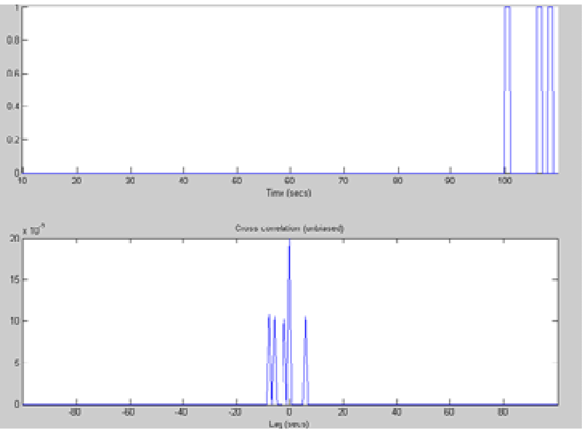


Fig.5. Cross Correlation of Conventional Scheme

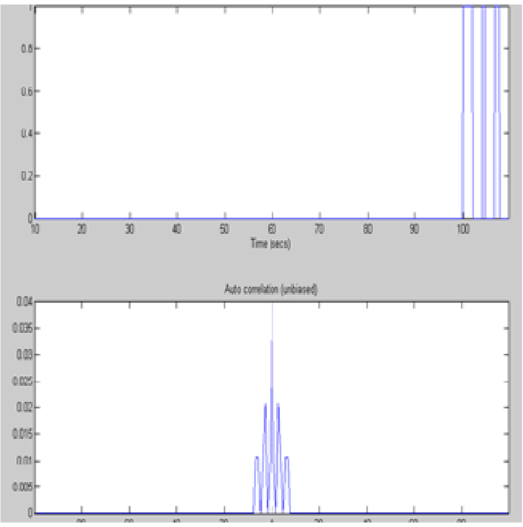


Fig.6. Auto-Correlation of Proposed Scheme

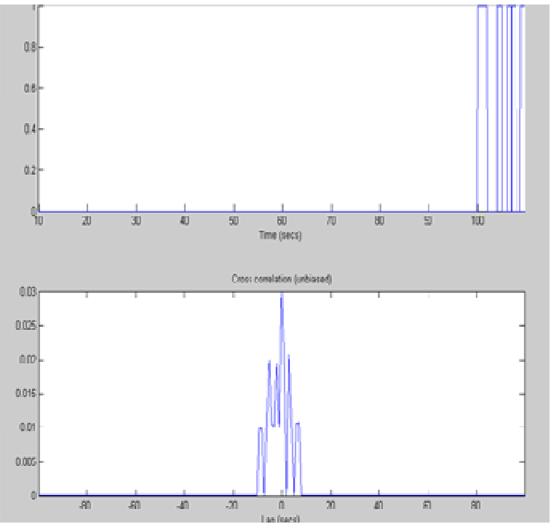


Fig.7 . Cross-Correlation of Proposed Scheme

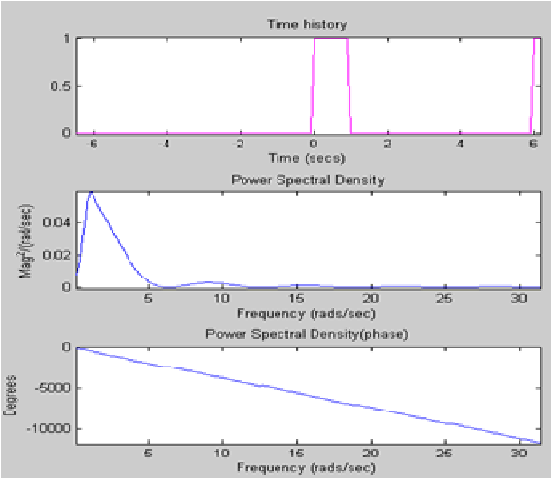


Fig.8. Power Spectral Density of conventional Scheme

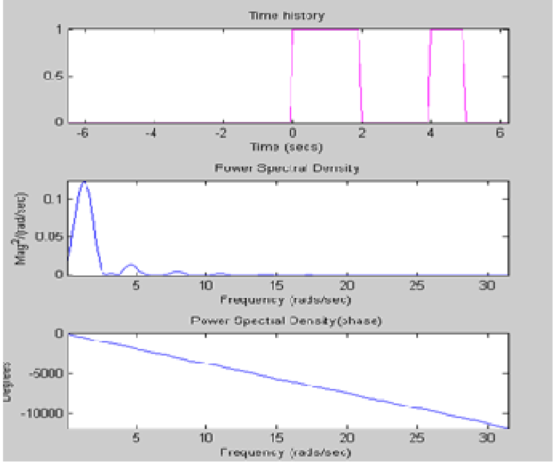


Fig.9. Power Spectral Density of Proposed Scheme

5. Conclusion

A new non-linear PN sequence has been proposed which is shown to have bounded cross-correlation value, better than the existing code. It is expected that this new code would be explored in CDMA and other signal processing applications. The proposed scheme is also capable of providing a range of applications in spread spectrum modulation, Global positioning system and other cellular and multimedia applications. Moreover the proposed technique has a potential of introducing a high degree of security with low complexity. The results obtained after simulation have been compared with conventional scheme and has proved the efficacy of the proposed scheme. The auto-correlation, cross-correlation and power spectral density of the proposed scheme have also been verified.

References

[1] Sucheteta Chakraborti and S.K.Pal "A new approach for identification scheme of LFSR based Pseudo-random generator". IJSDIA International Journal of Secure Digital Information age, vol.1,No 1, June, 2009.

[2] G.M.Bhat, Javaid Ahmad, Shabir Ahmad " On the design and realization of Chaoitic Spread Spectrum Modulation technique for Secure Data Transmission", published in IEEEXplore, Volume, issue, 14-16 March, 2009, pp 241-244.

[3]. N.Bonneau, M.Debbah and E. Altman, "Spectral Efficiency of CDMA Downlink Cellular networks with matched filter"., volume 2006, Article 1D 74081,pages 1-10 EURASIP Journal on wireless Communications and Networking.

[4] A.Hjorungnes and M.Debbah, "Minimum BER detector for uplink DS-CDMA systems," EURASIP Journal on Wireless Communications and Networking", VOL.2008, Article 1D 462710, 12 pages, 2008

[5] Q. Zhang and J.Zhang, "Choice of Chaoitic spreading sequences for asynchronous DS-CDMA Commuinications,". Proc. of IEEE Asia-Pacific Conference on CAS., pp 6245-6250,2000

[6] Abhijit Mitra. "On Pseudo –Random and Orthogonal Binary Spreading Sequences" International Journal of Information Technology, Vol 4 Number 2, 2007

[7] J. L.Masscy " Shift Register Synthesis and BCH decoding", IEEE Trans on information Theory, Vol. IT-15, Nov, June 1976.

[8] Chaotic Sequences for spread spectrum: An alternative to PN Sequences," Proc of the IEEE Intel Conf on selected topics in wireless comm., Vancourver, B.C., Canada, pp. 437-440.

[9] H. Nijmuijer and I.M.Y. Moreels, "An observer looks at synchronization," IEEE Trans on circuits and sys-1 vol.44,pp.882-890,1997.

[10] E. R. Berlekamp, R.E. Peile, and S.P. Pope, "The applications of error control to communications", IEEE Communications Magzine, Vol.25, no.4, pp 44-57, Apr. 1987.

[11] R.Gold, "Optimal Binary Sequences for Spread Spectrum Multiplexing", IEEE Trans, 1967. IT-13 (5). PP. 619-621.

[12] S. Junfu- Analysis of the complexity and random properties of Geffe,s Binary Sequence Generator, Journal of Electronics, vol.1 no.4,1984,pp.234-243.

[13] W. Chambers- Clock Controlled Shift Registers in Binary Sequence Generators, IEEE proceedings on Computer and Digital techniques, vol. 135, no-1 1985 pp17-24.

[14] C.-F. Hong and G.-C. Yang, "Concatenated prime codes," IEEE Commun. Lett., vol. 3, pp. 260–262, Sept. 1999.

Dr. Javaid A. Sheikh has completed his M.Sc., M. Phil and Ph. D in Electronics from University of Kashmir, Srinagar in the year 2004, 2008 and 2012 respectively in the field of communications and Signal Processing. He is working as Assistant Professor in the department of Electronics and I. T University of Kashmir, Srinagar. His field of interest are Wireless Communications, design and development of efficient MIMO- OFDM based wireless communication techniques, Spread Spectrum modulation, Digital Signal Processing, Electromagnetics. Besides teaching and research, Dr. Javiad A. Sheikh has guided about thirty five projects. He has published about twenty five research papers in International and National journals and conference proceedings.

Shabir A. Parah has completed his M. Sc and M. Phil in Electronics from University of Kashmir, Srinagar in the year 2004 and 2010 respectively in the field of Signal processing and Embedded systems. He is presently perusing Ph. D in the field of Signal processing and data hiding. He is working as Assistant Professor in the department of Electronics and I. T University of Kashmir, Srinagar. His field of interest are Signal Processing, Embedded Systems, Secure Communication and Digital design. Mr. Shabir A. Parah has guided about fifteen projects. He has published about twenty three research papers in International and National journals and conference proceedings.

Prof. G. Mohiuddin Bhat obtained his M.Sc. (Electronics) from the University of Kashmir, Srinagar (India) in 1987, M.Tech. (Electronics) from Aligarh Muslim University (AMU), Aligarh (India) in 1993 and Ph.D. Electronics Engg. from AMU, Aligarh, (India) in 1997. The major field of research of Dr. Bhat is Signal Processing Techniques and Secure Message Communication.
He has served as Assistant Professor, Associate professor and now as Professor & Director, University Science Instrumentation Centre (USIC), University of Kashmir. He has published many research papers on his area of interest. He has worked in the area of Mobile Radio Communication, Spread Spectrum Communication and Neural Networks and has guided many research degrees leading to the award of M.Phil and Ph.D. His present research interest include Secure Message Communication, Neural networks and Signal Processing techniques for communication.