International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

A Hardware Efficient Watermarking Technique Based on LFSR

Ankur Bhardwaj, Shamim Akhter

Abstract- Watermarking has been used for many years to protect data in the form of images, text etc. With the increasing use of semiconductor Intellectual Property(IPs) by industries to develop various products, this concept of watermarking has been applied by semiconductor industries as well to protect the VLSI designs which use these semiconductor IPs. There are many watermarking techniques for IP protection of VLSI designs, out of which watermarking of Finite State Machine(FSM) based design is research area. Watermarking technique implemented in this paper uses a Linear Feedback Shift Register (LFSR) to watermark a FSM based design. The LFSR based watermarking is applied successfully on a sequence detector and is compared with other FSM watermarking techniques. The simulation and synthesis of LFSR based watermarking is performed using ModelSim and Xilinx ISE tool respectively. Results show improvement in Hardware utilization as compared to other FSM watermarking techniques available in literature.

Index Terms: Watermarking, Intellectual Property, Finite State Machine, Linear Feedback Shift Register, Hardware utilization .

I. INTRODUCTION

With the advancement in VLSI Technology, size of transistors used in integrated circuits have been reduced significantly. Devices like FinFET working on 7 nm technology have made it possible to place whole system on a chip. A system on chip (SOC) required many independent semiconductor modules to be Inter-connected and function together as a system. These modules are designed by different parties and are their intellectual property(IP). These IPs are distributed to semiconductor industries and are used in many applications. The distribution of these IPs to different industries poses a risk of their misuse. Copying, redistribution and damaging the original IP is very common. So, it becomes very important to protect the IP from such misuse. Watermarking is one such method which involves embedding some information in the IP in such a way that no one else can see it[1]. This hidden information is extracted when authentication of the IP is required before court of law.

Manuscript published on 30 September 2019
* Correspondence Author
Ankur Bhardwaj*, Electronics and Communication Engineering, Jaypee Institute of Information Technology, Noida, India. Email:ankur.bhardwaj@jiit.ac.in
Shamim Akhter, Electronics and Communication Engineering, Jaypee Institute of Information Technology, Noida, India. Email: shamim.akhter@jiit.ac.in

There are three popular watermarking techniques available in the literature[2]. First is Constraint based watermarking[3] where extra constraints are considered in the design. These constraints may be added at any level of design flow. Second one is DSP watermarking, in which watermark is created by making some changes in filter parameters[4]. It can only be applied at the algorithmic level of the design process. Final one is Finite State Machine (FSM) based watermarking, which created watermark by modifying the state transitions or states of a FSM. FSM based watermarking may be done by property Implanting[5] or with the help of unused transitions[6]. In property Implanting FSM watermarking, the watermark is embedded as the property of FSM whereas the latter method uses unused transitions in an state transition graph (STG) of FSM to insert a watermark. In property implanting method, if an attacker tries to remove the watermark by removing the states, the original functionality of design will cease to occur. State transition graph does not always contain unused transitions, in that case extra states may be added to create watermark. Property Implanting and unused transitions method can be combined to get the advantage of both the methods[7]. But combining both the methods increase hardware overhead as compared to the original design. In this paper, an FSM based watermarking technique is analyzed which uses Linear Feedback Shift Register (LFSR) to create the watermark. This technique utilize same Flip Flops that are used in original FSM design and later modify the connections to work as LFSR when watermark is needed to be checked.
The paper is divided into five sections: Section II explains the related work and the problems in existing work, Section III explains the proposed technique, Section IV shows the simulation and synthesis results and section V concludes the paper.

II. RELATED WORK

As FSM is an integral part of almost every digital design nowadays, it makes FSM based watermarking a popular choice for IP protection of a design. Oliviera[5], gave an algorithm for creating a watermark by property implanting. This algorithm uses few extra states and a signature sequence to create a watermark. This technique was implemented on a sequence detector whose STG is shown in fig.1[8]. The algorithm works by copying all the “q” states. The copied states are “v” states and connecting the original and copied states are “r” states as shown in fig 2. These connection of there “r” states depends on the signature sequence chosen to watermark the circuit. The “r” states are traversed only when signature sequence is given, which help in detecting the watermark. The disadvantage of this technique is the used of extra copied states and need of a separate detector circuit to detect the watermark.

To reduce the number of states used in property implanting technique, counter based watermarking was proposed by Siddhant[9] as shown in fig.3.

It uses a counter to count the number of times signature is applied. At a predefined count an output "Z" is set to 1, showing the detection of the watermark. This technique reduces the hardware requirements of watermarking as compared to property implanting for same signature sequence length. But this technique also has some drawbacks. There was large possibility of false watermark detection. This problem was removed by modified counter based approach[10] as shown in fig. 4, which uses a sequence detector to keep a track on signature sequence and avoid the false detection of watermark. This technique reduces the hardware overhead as compared to property implanting technique with more security. As the design complexity increases, modified counter based technique starts to utilize more hardware. This problem is solved by the proposed LFSR based watermarking, which greatly reduces the hardware overhead due to watermarking in complex designs.

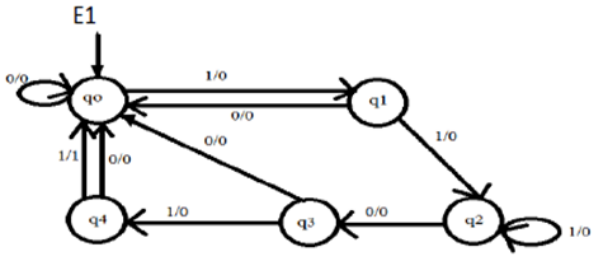

Fig. 1 STG of sequence detector[10]

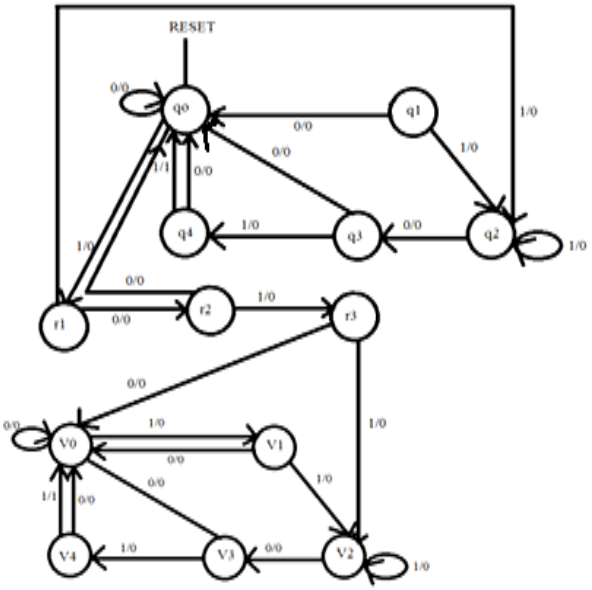

Fig 2. STG of sequence detector with property implanting watermarking[10]

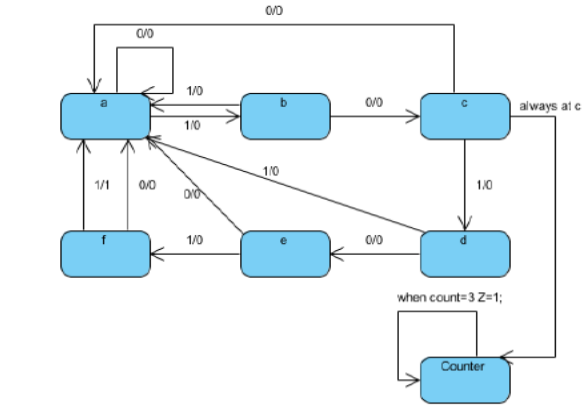

Fig. 3 STG with counter based watermarking[9]

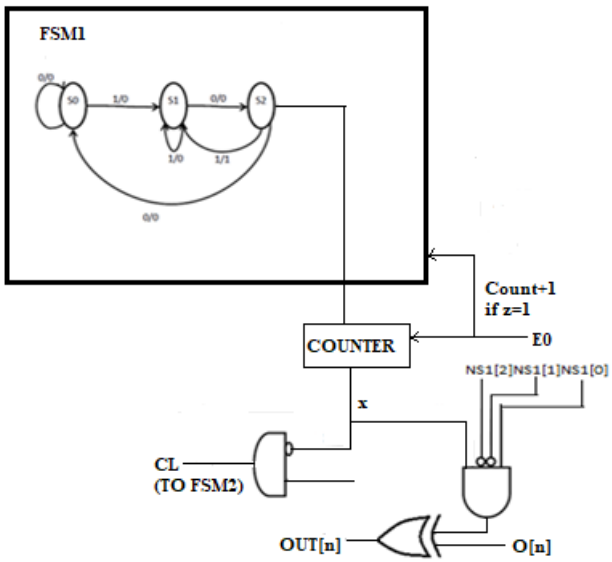

Fig. 4 Watermark embedding circuit for modified counter watermarking[10]

III. PROPOSED TECHNIQUE

Proposed technique uses FSM to be watermarked (fig 1.) to function as a sequence detector in normal mode and an LFSR when watermark detection is needed. A LFSR is a shift register whose input is the linear combination of its previous state. This linearity is achieved with the help of XOR gates as shown in fig. 5. LFSR generates Pseudo random sequences depending on the combination of XOR gates applied in the feedback path. In this paper, The LFSR is used as Output Response analyser(ORA). The input to the ORA is the modulo 2 sum of feedback response and an external input "I" as shown in fig 6. The external input sequence applied at the ORA input decides the state of LFSR for a particular feedback combination. For a particular input sequence, we can predict the LFSR state. This sequence is called signature and can be used to watermark any FSM[11].

Fig. 7(a) shows the three flip flops used in designing the sequence detector of fig 1.The values input signals "j", "k" and "l" are used to decide whether the flip flops will work as sequence detector or LFSR. Fig. 7(b)-7(d) shows the three multiplexers used generate the inputs to flip flops. Fig. 7(e) shows the circuit for detection of watermark. The steps involved in watermark detection are as follows-

- FSM to be watermarked is converted into LFSR according to the value of TEST input.
- If TEST = 0, FSM works in normal mode.
- If TEST =1 FSM works as LFSR.
- 2:1 mux is used to select the mode of operation.
- To detect the watermark, TEST is made high and Input signature is given at I pin.
- Output(OUT) becomes high when complete signature sequence is given.
- Under LFSR mode OUT becomes high on different state when compared to normal operation mode indicating watermark detection.

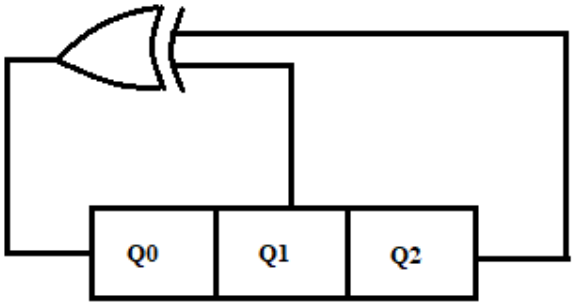

Fig. 5 Example of LFSR

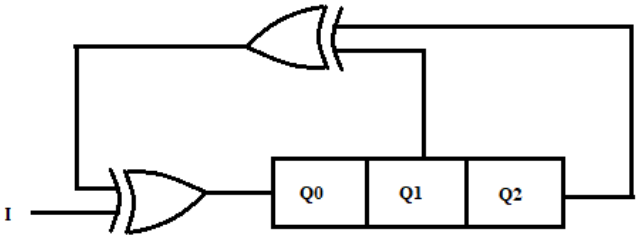

Fig. 6 LFSR as ORA

The schematic diagram of Watermarked circuit is illustrated in fig. 7-fig. 11 sequentially.

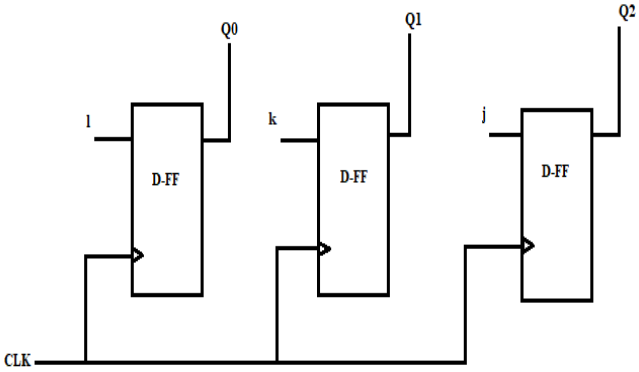

Fig. 7(a) Flip flops used in designing the sequence detector

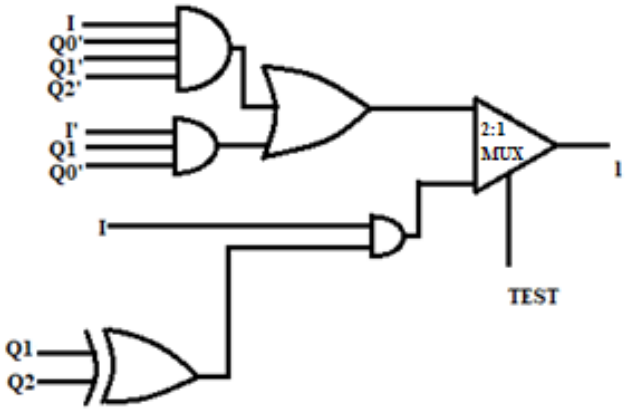

Fig. 7(b) Circuit to generate "l" input

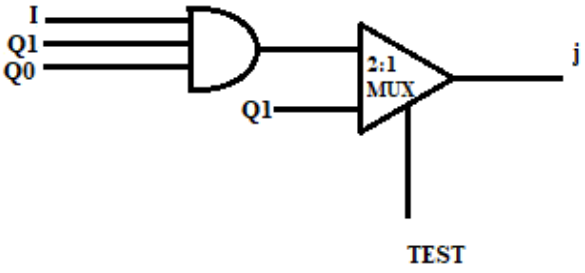

Fig. 7(c) Circuit to generate "j" input

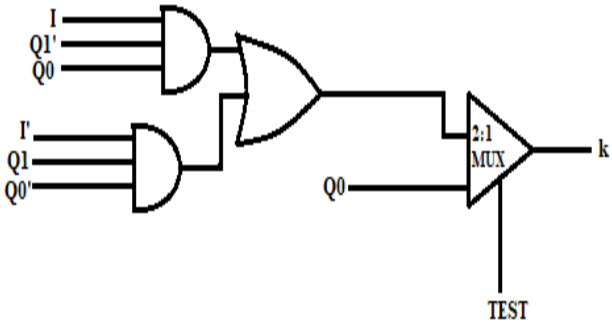

Fig. 7(d) Circuit to generate "k" input

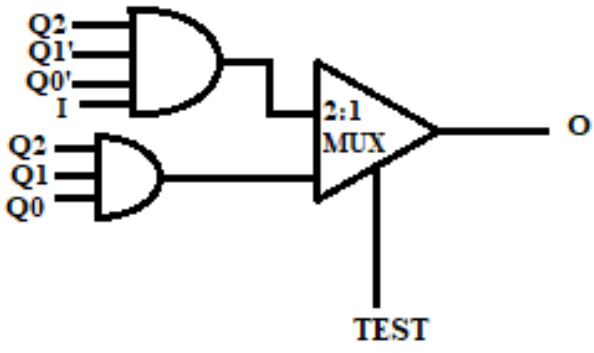

Fig. 7(e) Circuit to generate Output.

In this paper, watermarking is applied to a sequence detector whose STG is shown in Fig 1. This sequence detector gives a high output when "11011" is given as input(I). When normal operation of sequence detector is required, TEST = 0 is given in fig 8 – fig 11 and the multiplexer selects the circuit for sequence detector.

When watermark detection is required TEST signal is made high and multiplexer selects circuit for a LFSR. Signature sequence is chosen to be "110". When TEST is high and signature sequence is given, the states traversed by LFSR would be different than the states traversed when normal the circuit is working in normal mode. After the complete signature sequence is given the output (O) will become high, indicating detection of watermark. In complex designs there are large number of states in FSM, there is very low probability of false detection of watermark for an input sequence other than signature sequence. Security of less complex designs can be improved by adding extra flip- flop in the circuit of fig. 7(a) which will become active only during testing the watermark.

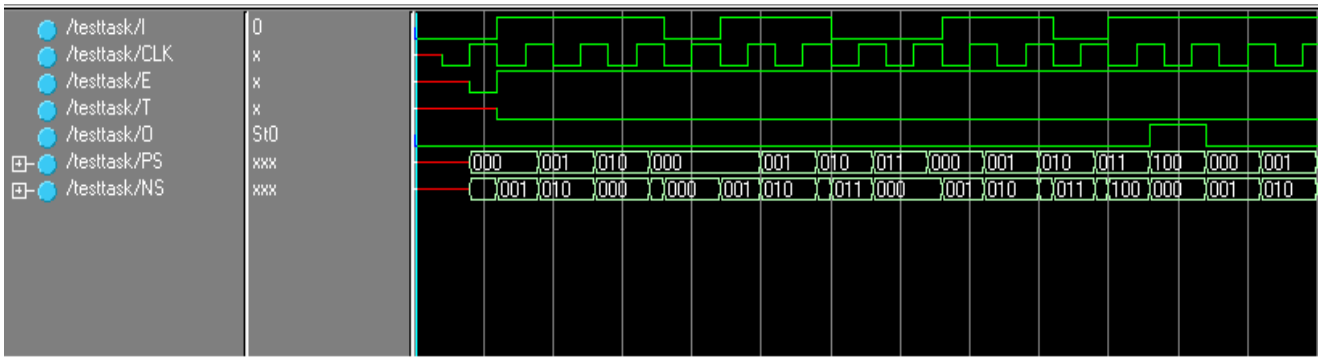

Fig 8(a) Simulation result for normal operation mode

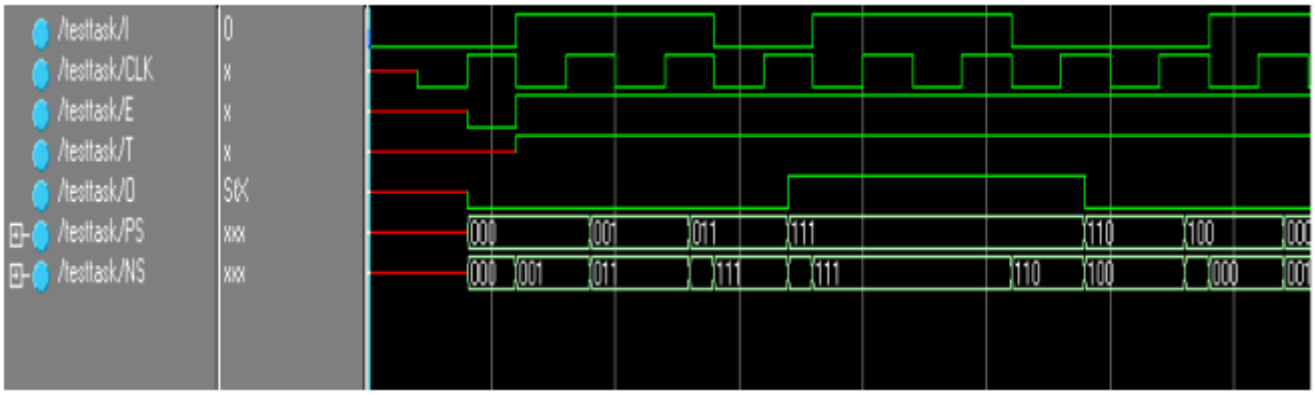

Fig. 8(b) Simulation result of watermark detection for signature"110"

Table. 1 Cell Usage Comparison

Cell Usage	Property Implanting(watermark creation)[1,3]	Added states property implanting[7]	Modified counter based technique[9]	LFSR based watermarking(proposed technique)
BEL	21	54	23	8
FLIP FLOPS/LATCHES	13	20	12	3
CLOCK BUFFERS	2	2	2	1
IO BUFFERS	2	9	3	4

IV. SIMULATION AND SYNTHESIS RESULTS

Fig. 8(a) shows the simulation result of the sequence detector working in normal mode. TEST signal is denoted by "T". Since circuit is in normal mode T is kept low. Enable signal is denoted by E, Clock by "CLK", and Present states and next states by "PS" & "NS" respectively. After an input sequence "11011" is given, output becomes high indicating detection of sequence.

Fig. 8(b) shows the simulation result of the watermark detection in the sequence detector FSM. For watermark detection, signature sequence given at I is "110" and TEST is kept high. It can be seen that output becomes high at different sequence than the sequence required for sequence detector, indicating the detection of watermark.

Table 1. compares the hardware utilization of proposed algorithm with Property Implanting watermarking, added states watermarking and modified counter based watermarking.

The BELs used in proposed technique are reduced by 85% as compared to added states property implanting technique, 65% as compared to modified counter based technique and 62% as compared to property implanting technique. Number of flip flops used in proposed technique are reduced by 85% as compared to added states property implanting technique, 77% as compared to modified counter based technique and 75% as compared to property implanting technique.

V. CONCLUSION

As seen by the synthesis results of Table 1, the cell utilization has reduced significantly in the proposed technique when compared to the other techniques. Also there is no requirement of separate detector circuit to detect the watermark, hence lesser flip flops required. For complex designs, LFSR based watermarking technique is better than other techniques as the probability of false detection is very low. Hence this technique, removes the shortcomings of property implanting and counter based watermarking techniques and proves to be a better watermarking technique.

REFERENCES

1. Intellectual Property Protection Development Working Group, "Intellectual Property Protection: Schemes, Alternatives and Discussion," *VSI Alliance*, White Paper, Version 1.1, Aug. 2001.
2. Amr T. Abdel-Hamid, Sofi`ene Tahar, and El Mostapha Aboulhamid, "IP Watermarking Techniques- Survey and Comparison," in Proc. of The 3rd IEEE Int. Workshop on System-on-Chip for Real-Time Applications, Calgary, Alta., Canada, pp. 60-65, July 2003.
3. Andrew B. Kahng, John Lach, William. H. Mangione-Smith, Stefanus Mantik, Igor L. Markov, Miodrag Potkonjak, Paul Tucker, Huijuan Wang, and Gregory Wolfe, "Constraint-Based Watermarking Techniques for Design IP Protection," *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems*, pp. 1236-1252, Iss. 10, Oct. 2001.
4. Roy Chapman and Tariq S. Durrani, "IP Protection of DSP Algorithms for System on Chip Implementation," IEEE Trans. on Signal Processing, Vol. 48, Iss. 3, pp. 854-861, Mar. 2000.
5. Arlindo L. Oliveira, "Techniques for the Creation of Digital Watermarks in Sequential Circuit Designs," IEEE Trans. on Computer-aided Design of Integrated Circuits and Systems, Vol. 20, Iss. 9, pp. 1101- 1117, Sep. 2001.
6. I. Torunoglu and E.Charbon, "Watermarking-Based Copyright Protection of Sequential Functions," *IEEE Journal of Solid-State Circuits*, Vol. 35, No. 3, pp. 434-440, Feb. 2000.
7. Ankur Bhardwaj and Shamim Akhter," IP Protection of Sequential Circuits Using Added States Watermark with Property Implantation", Advances in Signal Processing and Communication- Select Proceedings of ICSC 2018, pp. 521-528.
8. Shaila Subbaraman , P. S. Nandgawe," Intellectual Property Protection of Sequential Circuits Using Digital Watermarking", First International Conference on Industrial and Information Systems, ICIIS 2006, Sri Lanka, pp.556-560, 8 - 11 August 2006.
9. Siddhant Malik," Counter based approach to intellectual property protection in sequential circuits and comparison with existing approach", 2014 International Conference on Circuits, Systems, communication and Information Technology Applications(CSCITA),pg. 48-53, 2014.
10. Ankur Bhardwaj and Shamim Akhter," Modified Counter Based Approach for Digital Watermarking of Sequential Circuits" International Journal of Innovative Technology and Exploring Engineering, Vol.8, June 2019, pp 3409-3413.
11. M.L. Bushnell and V.D. Agarwal, Essentials of Electronic Testing for Digital, Memory and Mixed-Signal VLSI Circuits, Springer, 2005, ISBN 0-7923-7991-8.

AUTHORS PROFILE

Ankur Bhardwaj was born at Meerut, Uttar Pradesh, India on January 04,1990. He received B.Tech degree from Gautam Buddh Technichal University, Lucknow (June 2011), M.tech degree from DTU Delhi(2013) and currently pursuing PhD degree from Jaypee Institute of Information Technology, Noida**.** He joined Jaypee Institute of Information Technology, Noida, in July 2013 as a Lecturer. Presently he is Assistant Professor in the Department of Electronics and Communication Engineering, Jaypee Institute of Information Technology, Sector 62, Noida.

Shamim Akhter was born at Chittaranjan, West Bengal, India on January 15, 1979. He received B.Tech degree from ZHCET, AMU(June 2001), M.Tech degree from IIT Delhi (Dec 2002) and Ph.D degree from Jaypee Institute of Information Technology, Noida, India(March 2015). He joined Jaypee Institute of Information Technology, Noida, in April 2003 as a Lecturer. Since then he is engaged in teaching, research and development in the field of VLSI digital circuits design. He has published research papers in reputed International Journals. Besides he has also published papers in International Conferences in India and abroad. Presently he is Assistant Professor in the Department of Electronics and Communication Engineering, Jaypee Institute of Information Technology, Sector 62, Noida.