ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 7, July 2014

Hardware efficient watermarking technique for finite state sequential circuit using STG

Jeebananda Panda[1], Ankur Bharadwaj[2], Neeta Pandey[3], Asok Bhattacharyya[4]

Associate Professor, ECE Department, Delhi Technological University, Delhi, India[1,3]

Assistant professor, ECE Department, JPIIT, Noida, India[2]

Professor, ECE Department, Delhi Technological University, Delhi, India[4]

Abstract: Intellectual Property Protection (IPP) is very important for a design created by IP owner. For this, IP owner embeds watermark in its design. One such type of technique is suggested by Oliviera, in which modification of State Transition Graph (STG) of a digital circuit takes place in such a way that it is not possible for the intruder to find that there is a watermark embedded in the circuit. It is also possible to prove the piracy of the design in court-of-law. A method for state reduction in the watermarked circuit has been proposed in this paper. The comparison of simulation of non-watermarked, watermarked circuit with existing technique and the modified reduced state watermarked circuit is done using ModelSim Simulator. The Detection of Piracy can be done by using a counter circuit.

Keywords: Intellectual Property Protection, State Transition Graph, Watermark, Finite state machine, Signature sequence

I. INTRODUCTION

There are various watermarking techniques for watermarking a sequential design. Finite State Machines are of two types: Completely specified and incompletely specified. Incompletely specified machines contain unused transitions which may be used for embedding watermark [3]. We are considering the watermarking of completely specified machines. In completely specified machines we can add extra input and output pairs to the original FSM [4] such that on the application of a particular input which only owner knows, piracy can be detected by observing the output sequence. But in complex designs finding such an input sequence is itself a tough task and it also adds to design overhead. Another method of watermarking includes embedding a signature in the design by state encoding [6].Oliviera [1] gave various techniques to embed digital watermark in sequential circuits, which include adding extra states in the original design. But, still the design overhead caused in the watermarking of a circuit is an important problem.

In this paper we propose a technique which can reduce the overhead caused due to watermarking of the sequential design. The synthesis results of the proposed technique have shown significant reduction in hardware overhead.
Different simulation tools are available for simulating a physical design before actually implementing them which made complex design of systems easy to test. But these designs can be easily stolen and used for unintended purposes without taking permission from IP owners. So, there has to be a method for protecting and tracking the ownership of such complex designs. Also, if necessary there should be a method of proving the ownership.

For this purpose, Oliviera[5] had suggested a watermarking algorithm in which State Transition Graph of a sequential circuit is modified in such a way that only owner knows its internal transitions and the user of that circuit can't even know that there is any watermark in the circuit. But, the watermarking algorithm used by Oliviera[5]adds some redundant states to the original STG which adds to the design overhead in complex designs. These redundant states can be reduced to certain extent depending upon the characteristics of State Transition Graph and choosing the signature sequence carefully. We have simulated watermark circuit with reduced number of redundant states and compared it with original watermarked circuit. We found that there was a reduction in number of flip-flops required to watermark same sequential circuit design.

II. WATERMARKING OF FINITE STATE MACHINES

Oliviera[5] proposed a technique for watermarking a completely specified FSMs. In this technique the STG is modified in such a way that authentication of the design can be proved by applying a signature sequence in addition to the input sequence of arbitrary length. The procedure for modification of STG[5] is explained below for reference-

1. Copy STG V for original STG Q in a way such that there is a corresponding qi ϵ Q state for every vi ϵ V state.
2. Create STG R with state ri, ($1 < I \leq k$) by copying state qti and all its outgoing edges, where qti refers to the state reached in STG Q at time t when the signature sequence is applied to STG Q.
   Here,
   k=(No. of bits in signature/No. of input bits)
   Note that r0 = q0
3. For each value of i such that $1 \leq i \leq k$, state qti has one of its incoming edges which now originates in state r(i - 1) and terminates at ri. For the input sequence

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 7, July 2014

corresponding to the signature, the edge originating in state r(i - 1) terminates at ri only. If the input sequence does not correspond to the signature, then the state reached from ri will be one of the states in the original STG Q for i < k while that in the duplicated STG V for i ≥ k so that the design conserves its functionality.

Thus the state transitions take place in STG Q or Q & R for i ≤ k and in STG Q, R and V for i ≥ k. In both cases the functionality obtained is the desired one. So, it is not possible to know for the intruder that STG has been modified. However, owner can detect the piracy by using the Piracy detection Circuit.

Design and Implementation of non – watermarked and watermarked circuit (As proposed by Oliviera [5]).
To elaborate the Oliviera [5] scheme, the STG by of Fig. 1 is considered. Following the steps outlined above, the STG of Fig. 1 modifies to STG of Fig. 2 for signature sequence '010'.

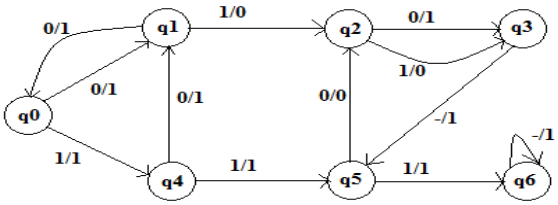

Fig.1 STG proposed by Oliviera[5].

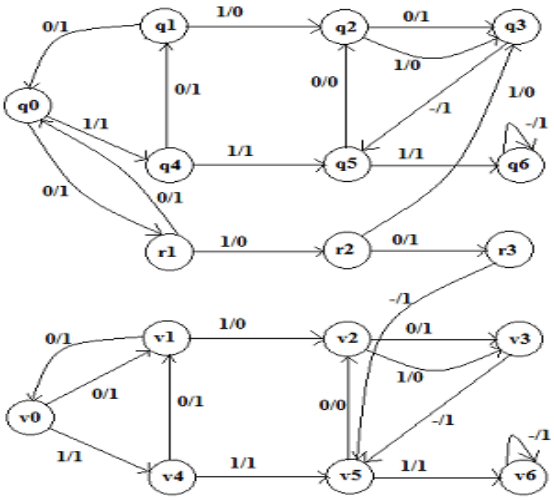

Fig.2 Watermarked STG consisting of 17 states [5]

It may be noted from Fig. 2 that all the states of the original STG are copied in the modified STG, which becomes a large hardware overhead in complex systems. However, It is not necessary to copy all the states of STG in some conditions. Given that the starting state is q0, the traversal is made via states r1, r2 and r3 on receiving the input sequence '010'. Subsequent inputs will make state transition to v5 for STG of Fig. 2 and thereafter vi states are traversed. The proposed technique is based on the fact that the state transitions, after watermark is detected and one duplicate state is reached, may be routed via an appropriate state of original STG. This transition may be used to set counter for the first time signature states are traversed and thereafter increasing the counter.

The above discussion indicates that the STG of Fig. 2 can be redrawn as Fig. 3 while maintaining the original functionality intact. The number of states is reduced from 17 states in Fig. 2 to 11 states in Fig. 3. Therefore the proposed scheme reduces hardware overhead caused by watermarking.

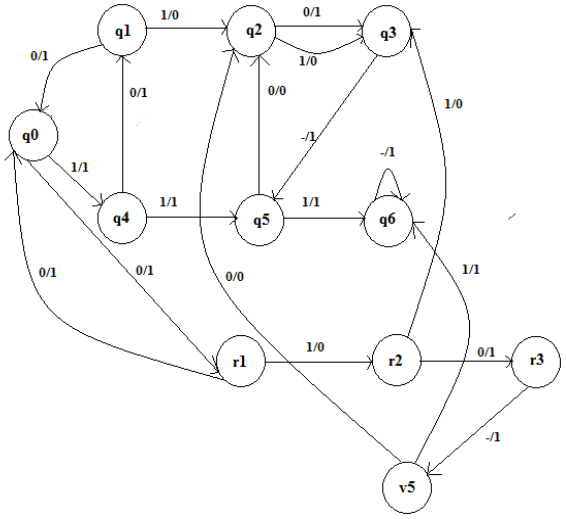

Fig.3 Proposed Reduced State watermarked circuit

Once state v5 is traversed in Figs. 3, there is no input sequence that can lead FSM to go to starting state q0 so, if until a reset is applied, circuit will not traverse ri states again even if signature is applied again and circuit will perform normally. This means that we can test the watermarked circuit only once after application of signature input, until we apply reset signal. This property was present in the original watermarked circuit of Oliviera [5] shown in Fig. 2 also.

But in case the original STG is such that after vi states circuit reaches on q0 state by applying some sequence of input, then there is a possibility to traverse R states again. To avoid this situation, following additional steps may be used:

(i) Use a test signal which becomes high when state vi is reached in the watermarked circuit.
(ii) When state q0 is reached and test signal is high, next state from q0 on application of the first bit of the signature will be q1 instead of r1. So the ri states are not traversed again once state V is reached.
(iii) (iii)This test signal can be disabled again when we apply low reset signal.

A close inspection of STG of Fig.2 reveals that state v5 is traversed after r3 state irrespective of the input sequence. This may not be true, in general, for every STG. To elaborate on this, the STG of a sequence detector [2] is considered. This circuit detects the sequence "11011" and it is an overlapping sequence detector. Fig.5 shows the watermarked circuit for a signature sequence "101". Here states v0 and v2 are traversed after watermarked state r3, both the states are therefore retained in reduced STG. The modified STG is drawn in Fig. 6 where the state transitions from v0 and v2 In this case when we reduce

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 7, July 2014

number of only two vi states are important i.e. v0 & v2. Now, the STG with reduced number of states is shown in Fig. 6.

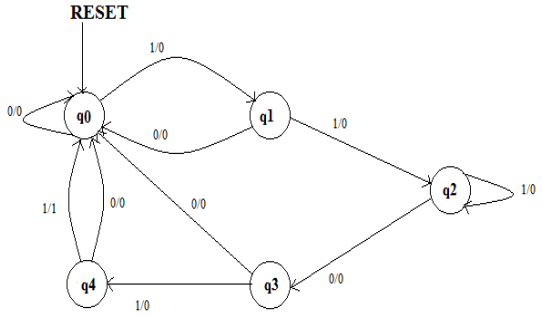

Fig.4 STG of Sequence Detector proposed by Subbaraman [2]

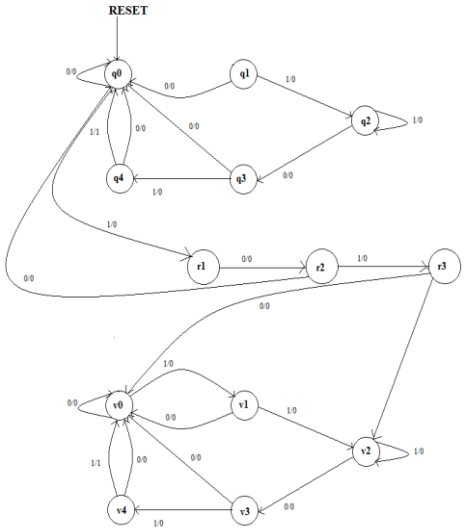

Fig.5 Watermarked STG of sequence Detector by Subbaraman[2]

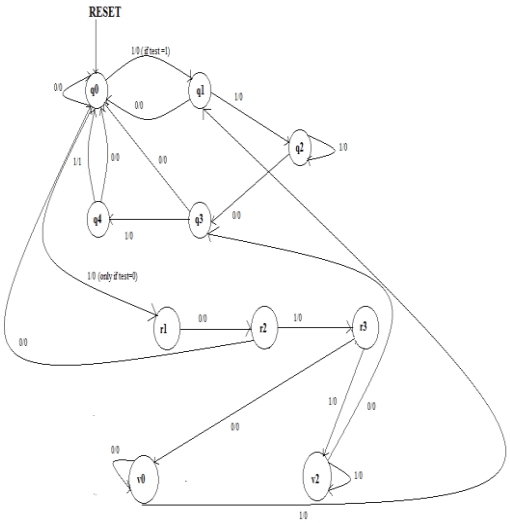

Fig.6 Reduced state watermarked STG of Sequence Detector (Proposed design)

In Fig. 6, when suppose state v0 is reached now, if we apply input '10' circuit will reach on q0 and if accidently signature is applied at this stage the R states will be traversed again, similarly if state v2 is reached after r3 and sequence '00' is applied, circuit will reach on q0 state and there is a possibility of traversing ri states. So, to eliminate this situation a test signal will be used. When state v0 or v2 is reached test signal will be '1' and remain high until reset is applied. Now if present state is q0 and test is '0' then next state will be r1 if input '1' is applied, if test is '1' then next state will be q1 and circuit will not go in STG R even if signature is applied accidently. To reduce the number of vi states, the last part of the signature sequence should be chosen in such a way that there are minimum numbers of transitions to the different vi states from final ri state.

III. RESULTS

Synthesis and Simulations are performed using Xilinx ISE 6.1i EDA tool with its built in synthesis tool IST and Modeltech's Modelsim 5.4a. The simulations and results of non-watermarked, watermarked and watermarked circuit with reduced states are shown in next section.

An input sequence "0101010101010….." which includes signature "010" as first three bits is applied to STG of Figs. 1-3 and the simulation results are depicted in Figs. 7-9 respectively. It may be noted that similar output characteristics are obtained for each case. Only the state transitions differ in watermarked and non- watermarked circuit. In case of non - watermarked circuit, for the given input sequence circuit traverses STG Q, but in case of watermarked circuit of Fig. 2 for the first three bits of input, its traverses STG R, and after that circuit enters in STG V which are replica of original STG and remain in STG V until reset is applied.

State assignment for Fig.1 – q0=000, q1= 001, q2= 010, q3=011, q4=100, q5=101, q6=110

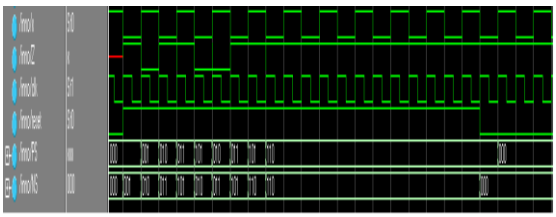

Fig. 7 Simulation of original STG of Fig.1

State assignment for Fig.2 q0=00000, q1=00001,q2=00010,q3=00011,q4=00100,q5=00101,q6=00110 r1= 00111, r2 =01000,r3=01001,v0=01010,v1=01011,v2=01100,v3=01101,v4=01110,v5=01111,v6=10000

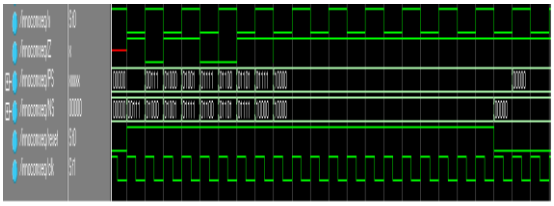

Fig. 8 Simulation of watermarked STG of Fig.2

Sate Assignment for Fig.3 – q0=0000, q1=0001, q2=0010,q3=0011,q4=0100,q5=0101,q6=0110,r1=0111,r2 =1000,r3=1001,v5=1010

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 7, July 2014

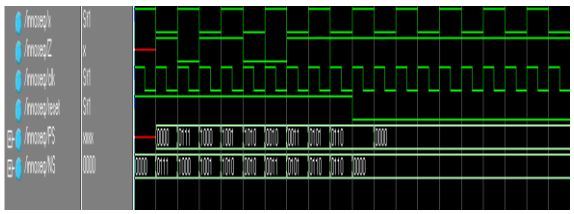

Fig. 9 Simulation of watermarked STG with reduced states of Fig. 3

In simulation of Fig.3, when the signature ”010” is applied the circuit traverses STG R as in the case of Fig.2. After that it enters the next vi state(v5) for any input applied to r3. Now, if the input is applied when present state is v5, the next state will be one of the qi states and then circuit remains in qi states until reset signal is applied.

Similarly the simulations of sequence detector of Figs. 4-6 are shown in Figs. 10-12.

State assignments for fig.4- q0=000,q1=001,q2=010,q3=011,q4=100

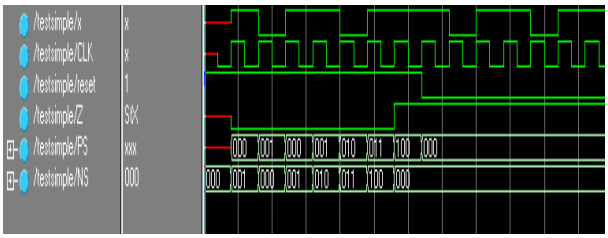

Fig. 10 Simulation of original sequence detector

State assignments for Fig.5 – q0=0000,q1=0001,q2=0010,q3=0011,q4=0100,r1=0101,r2 =0110,r3=0111,v0=1000,v1=1001,v2=1010 v3=1011, v4=1100

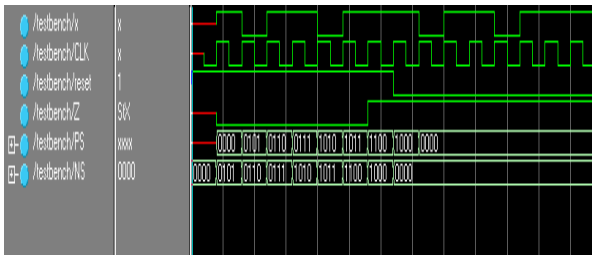

Fig. 11 Simulation of watermarked sequence detector

State assignments for Fig.6
q0= 0000, q1=0001, q2=0010, q3=0011, q4=0100,r1=0101,r2=0110,r3=0111,v0=1000, v2=1001

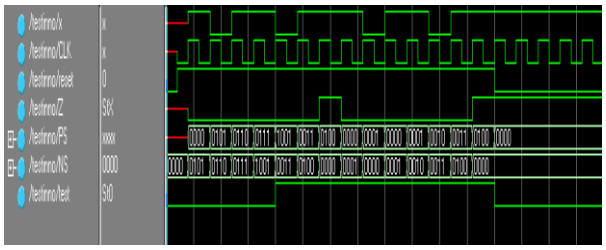

Fig. 12 Simulation of reduced state watermarked circuit.

In Fig. 12 it may be noted that, when test signal became high, circuit reaches in state v0. If test signal is high and q0 state is reached the next state from q0 with input ‘1’ is q1 not r1. So this proves the functionality of reduced state watermarked circuit explained in previous section.

TABLE I
SYNTHESIS REPORT OF STG USED BY OLIVIERA[5]

Details	Original Design (fig.1)[1]		Watermarked Design(fig. 2)[1]		Proposed Watermarked Design (fig. 3)	
IOs	4		4		4	
Flip Flops/Latches	FDC	8	FDC	15	FDC	12
Cell Usage	BELS	11	BELS	20	BELS	18
Clock Buffers	BUFGP	2	BUFGP	2	BUFGP	2
IO Buffers	IBUF	1	IBUF	1	IBUF	1
	OBUF	1	OBUF	1	OBUF	1

TABLE II
SYNTHESIS REPORT OF SEQUENCE DETECTOR IMPLEMENTED BY SUBBARAMAN[2]

Details	Original Design (fig.4)[6]		Watermarked Design(fig. 5) [6]		Proposed Watermarked Design (fig. 6)	
IOs	4		4		4	
Flip Flops/Latches	FDC	6	FDC	13	FDC	12
Cell Usage	BELS	9	BELS	21	BELS	19
Clock Buffers	BUFGP	2	BUFGP	2	BUFGP	2
IO Buffers	IBUF	1	IBUF	1	IBUF	1
	OBUF	1	OBUF	1	OBUF	1

The synthesis report shows that no. of latches/flip flops are reduces in case of Fig.3 as compared to Fig.2. The hardware requirement of watermarked circuit is much more as compared to non- watermarked circuit. The timing report for STG of Figs. 1-3 and Figs. 4-6 are respectively summarized in Tables 3 and 4.

TABLE III
TIMING SUMMARY OF STG USED BY OLIVIERA[5]

	Original Design (fig. 4)	Watermarked Design(fig. 5)	Watermarked Design (fig. 6)
Maximum Frequency	264.340 MHz	264.340 MHz	264.340 MHz

TABLE IV
TIMING SUMMARY OF SEQUENCE DETECTOR

	Original Design	Watermarked Design(fig. 2)	Watermarked Design (fig. 3)
Maximum Frequency	231.267 MHz	231.267 MHz	231.267 MHz

The maximum operating frequency in the reduced state watermarked circuit is same as that of original STG. This is an important result as this helps in maintaining the secrecy of watermarked design.

IV. DETECTION OF WATERMARK

The detection of watermark can be done using a Counter circuit as suggested by Subbararaman[2]. When the state

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 7, July 2014

transition occurs in STG Q count value becomes "00", as the signature sequence is applied count value increases for each state transition through ri states. After final ri state the next state is a vi state and counter retains its previous value indicating that whole signature sequence has been traversed.

V. CONCLUSION

Simulation and Synthesis results of the above method proved that there is no change in output response of the original, watermarked circuit as used by Oliviera[5] and Subbaraman[2] and the proposed reduced state watermarked circuit. But the number of states is considerably reduced in case of reduced state watermarked circuits thereby reducing the hardware overhead due to watermarking. Also the maximum operating frequency is same in all the cases. So we should explore two possibilities for state reduction:-

Firstly, the signature sequence should be chosen in a way that there is minimum number of transitions to vi states after final state of STG R. Secondly, the vi states to be copied from STG Q should be chosen in such a way that there is no possible state transition to initial state of STG Q, when we apply further input sequence after the arrival of vi states.

REFERENCES

[1] Arlindo L. Oliveira, "Techniques for the Creation of Digital Watermarks in Sequential Circuit Design," IEEE Transactions on Computer-aided Design of Integrated Circuits and Systems, Vol. 20, No. 9, September 2001.

[2] ShailaSubbaraman , and P. S. Nandgawe, "Intellectual Property Protection of Sequential Circuits Using Digital Watermarking", First International Conference on Industrial and Information Systems, ICIIS 2006, 8 - 11 August 2006, Sri Lanka

[3] J. Toruoglu, and E. Charbon, "Watermarking Based Copyright Protection of Sequential Functions", IEEE journal of Solid State Circuits, Vol. 35, No. 3,February 2000, pp434-440.

[4] Amr T. Abdel-Hamid, Sofi'eneTahar and El MostaphaAboulhamid, "IP Watermarking Techniques- Survey and Comparison ", Proceedings of The 3rd IEEE International Workshop on System-on-Chip for Real-Time Applications, ISBN 0- 7695-1929-6103 copyright 2003 IEEE.

[5] Arlindo L. Oliveira, "Robust Rechniques for WatermarlingSequential Circuit Designs", DAC 99, New Orleans, Louisiana c 1999 ACM 1-58113-109-7/99/06.

[6] M. Lewandowski, R. Meana, M. Morrison and S. Katkoori, "A Novel Method for Watermarking Sequential Circuits", International Symposium on Hardware-Oriented Security and Trust, 2012 IEEE.

BIOGRAPHIES

Jeebananda Panda Born on 15 th Feb, 1968 in Odisha , India . He got graduated in Electrical engineering and subsequently in electronics and Communication engineering in 1988 and 1989 respectively. He got his M.E degree in Applied Electronics specialization from Bharathiyar University in 1992. Presently working as an Associate Professor in the Department of Electronics and Communication Engineering, Delhi Technological University, Delhi, India. He is presently working for Ph.D in Dept. of Electronics in Engineering, Faculty of Technology, Delhi University. His field of research is Watermaking of Digital Data.

Ankur Bharadwaj Born on 04 January, 1990 in Meerut, Uttar Pradesh, India. Completed M.Tech in VLSI Design and Embedded Technology in year 2013 from Delhi Technological University, Delhi, India. Currently Ph.D from Jaypee Institute of Information Technology, Noida, India. Working as an Assistant Professor in Jaypee Institute of Information Technology, Noida since 2013.

Neeta Pandey Completed her M.E. in Microelectronics from Birla Institute of Technology and Sciences, Pilani and Ph.D. from Guru Gobind Singh Indraprastha University Delhi. She has served in Central Electronics Engineering Research Institute, Pilani, Indian Institute of Technology, Delhi, Priyadarshini College of Computer Science, Noida and Bharati Vidyapeeth's College of Engineering, Delhi in various capacities. At present, she is working as an Assistant Professor in ECE Department, Delhi Technological University. Her research interests are in analog and digital VLSI Design.

Asok Bhattacharyya Obtained M.Tech and Ph.D. degree from Institute of Radio Physics, Calcutta University, India in 1970 and 1981 respectively. He joined Delhi College of Engineering in May 1974. He has retired as Professor in E&C Engineering. He has worked in different fields- Digital System Design, Analog System Design, Easily testable and diagnosable Digital systems/ Fault tolerant Computing and Medical Image Processing area. He has authored two research monographs.