ABSTRACT

The integration of the important functional components of an entire end product into a single chip called System-on-Chip (SoC) has emerged as the most promising key. To mitigate the cost and time of the development of SoC, design-for-reuse technique becomes essential in which an intellectual Property (IP) core acts as an indispensible part. The effort in designing of SoC can be reduced and the chance of a first-time right implementation can be increased by means of re-using the modules. In the field of Electronic Design Automation (EDA), the protection of IP cores is very important. IP core piracy accounts for the major revenue loss as it is more vulnerable to dangers such as copyright fraud, attack, cloning, and reverse engineering. Hence, the assurance on the avoidance of illegal redistribution by consumers is highly needed by the designers of IP cores.

The three main approaches namely deterrent, protective and detection approach have been identified by the working community of the Virtual Socket Interface Alliance (VSIA) IP protection development group for securing the IP cores. They have been modeled in such a way that both the legal and illegal usages of the designs like watermarking and finger printing can be detected and traced by the owner. The clarity of this tracking could well-suffice as evidence if needed for the court hearing. Field Programmable Gate Array (FPGA) IP core protection can be implemented in various design

levels of Very Large Scale Integration (VLSI). It can be either in the form of circuit description in hardware description language (hard IP) or in any of the form of the netlist, placed and routed design (firm IP) and design layout in hardware description language (soft IP). Recently, a novel technology that is gaining attention towards IP protection is a watermarking technique as it hides ownership information in design thus providing convincing evidence.

In order to protect FPGA IP Cores at the behavioral level, this study provides an efficient novel watermarking technique by means of embedding watermark in Finite State Machine (FSM). Conventional techniques used to hide watermark in inputs/outputs of transitions in State Transition Graph(STG). Those are also not suitable for larger designs thus becoming a major drawback. Hence, the proposed method tends to split the states in (STG) in a hierarchial manner so as to hide the watermark bits in the output of FSM. The proposed hierarchical FSM work written in VHDL is synthesized by Xilinx ISE 13.2 for Spartan 3E FPGA and simulated by ModelSimSE5.7g. The performance of the proposed approach has evaluated using three set of watermark bits as 16 bit, 32bit and 64 bits based on the occupancy of number of Look up tables (LUTs), number of slices and number of slice Flip Flops (FFs) for the watermark. Further, the standard cell approach evaluation has been performed. The comparison of the performance of proposed watermarking approach with existing watermarking approach is been done. The robust solution for IP core protection against unauthorized use even at

behavioral level has been experienced from the proposed method based on the experimental results on MCNC, IWLS'93 and open core benchmark circuits.

Netlist represents the description of design into a list of logic gates and their interconnections. By means of watermarking netlist time delays, the IP Core protection at netlist level is achieved. The embedding of the watermark bit into the design by modifying timing constraints of the netlists has been carried out in this proposed approach. The existing conventional technique needs m number of netlists for hiding m number of watermark bits. However, the proposed technique groups the hashed output of IP core developer's identification into three bits for the generation of the signature digits which means that one netlist time delay variation corresponds to three watermark bits. To check the time constraints, the watermarked design is again place and routed. Then, the timing analyzer provided by Xilinx ISE is used to obtain the static timing analysis data on all the nets. This modification in net time delay has been carried out by Xilinx ISE's Timing Constraints Editor tool The proposed technique improved the processing time constraints and introduces no resource overhead.

In terms of security, conventional SRAM FPGAs have the lowest performance. This is due to easy copying of bitstream as the pirates can easily read the bitstream with a simple probe. Hence, these circuits need a bitstream transfer from a ROM at power up and are also feasible to improve security level with bitstream encryption. Advanced techniques are required beyond

bitstream encryption to ensure FPGA bitstream IP design security. Static Random Access Memory (SRAM) based FPGA is always unstable and hence the necessity of configuring on each power-up leads to retrieval of bitstream by the attackers. For protecting FPGA IP core, the Secure Start Hardware (SSH) approach uses a technique ensures FPGA design security beyond bitstream encryption. The implementation of an effective protocol for protecting IP core developer information in bitstream of VLSI design flow has been focused in this proposed work. Using a novel hardware SSH in the FPGA, high security is provided to IP cores. Moreover, the introduction of cryptographic protocol in SSH approach represents an authenticated channel between the IP core developer and SSH.

IP core protection at various VLSI design levels based on three different methodologies has been aimed in this research. It was observed that embedding capacity of watermark along with possession of low area and all the proposed IP core watermarking methods simultaneously increased the embedding capacity of watermark along with possession of low area and timing overhead.