Low-Overhead Robust RTL Signature for DSP Core Protection: New Paradigm for Smart CE Design

Anirban Sengupta
Computer Science and Engineering
Indian Institute of Technology Indore
asengupt@iiti.ac.in

Dipanjan Roy
Computer Science and Engineering
Indian Institute of Technology Indore
phd1501201007@iiti.ac.in

Saraju P. Mohanty
Computer Science and Engineering
University of North Texas, Denton, USA
saraju.mohanty@unt.edu

***Abstract*—The design process of smart Consumer Electronics (CE) devices heavily relies on reusable Intellectual Property (IP) cores of Digital Signal Processor (DSP) and Multimedia Processor (MP). On the other hand, due to strict competition and rivalry between IP vendors, the problem of ownership conflict and IP piracy is surging. Therefore, to design a secured smart CE device, protection of DSP/MP IP core is essential. Embedding a robust IP owner's signature can protect an IP core from ownership abuse and forgery. This paper presents a covert signature embedding process for DSP/MP IP core at Register-transfer level (RTL). The secret marks of the signature are distributed over the entire design such that it provides higher robustness. For example for 8th order FIR filter, it incurs only between 6% and 3% area overhead for maximum and minimum size signature respectively compared to the non-signature FIR RTL design but with significantly enhanced security.**

I. Introduction

In the design process of current smart Consumer Electronics devices, use of DSP and MP based reusable IP cores has become inevitable. The use of reusable DSP IP core decreases the design cycle immensely thus speeds up the design productivity [1]. The reason is that, once a DSP/MP IP core is designed with a certain specification and technology for a smart CE device, the same IP core can be used for other CE devices which employ the same specification and technology. For example, JPEG CODEC IP core for digital cameras can be reused in smart-phones or tablets. However, due to these advantages and strong market competition between IP vendors, DSP/MP IP cores are susceptible to major threats like unauthorized reuse and false claim of ownership [2], [3], [4], [5]. Therefore, to invalidate the ownership abuse and establish authorization, embedding owner's secret mark (as signature) in the IP core design is vital.

II. Related Prior Research

Secret mark for an IP core should be imperceptible and obscure in nature for an adversary. Moreover, it should not incur too much design overhead while preserving the correct functionality of an IP core. Few IP core ownership protection approaches for DSP cores during different phases of High-level Synthesis (HLS) are discussed in [6], [7], [8], [9]. In [6] a dual variable encoding scheme is proposed to embed secret mark for an IP core. In this approach, owner's secret mark is embedded during register allocation phase of HLS. In [8], a input output mapping based IP core secret mark embedding process is proposed. Both these approaches embed owner's secret mark in single phase of HLS. In [7], a robust secret mark embedding approach is proposed, where the owner's secret mark is embedded in three different phases of HLS. In [9] ownership protection for both the IP owner and IP user is also proposed. None of these approaches embeds owner's secret mark during RTL. The benefit of embedding owner's secret mark during RT level is that the detection and authentication of signature for a genuine owner is simpler and less cumbersome compared to embedding at architecture level. Fig. 1 depicts the overview of possible attacks on a DSP/MP IP core and the proposed approach to shield it.

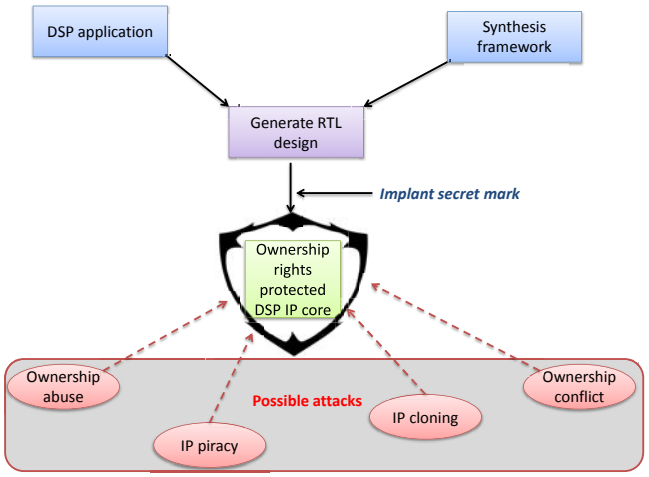

Fig. 1. Overview of the possible threats and proposed approach.

To advance the state-of-art in CE hardware ownership, in this paper, we propose a novel low-overhead, highly robust, secret signature embedding process to protect owner's right in a DSP/MP IP core. The rest of the paper is organized as follows: section III discusses the novel contributions of the paper. Section IV highlights the proposed signature based secret mark for DSP core protection. Section V presents the experimental results, while section VI concludes the paper.

III. Contributions of This Paper

In this paper, we propose a novel low-overhead, highly robust, secret signature embedding process to protect owner's

right in a DSP/MP IP core. In proposed work, the owner's signature contains three different encoding variables, which have to be decoded to obtain the secret mark. Moreover the secret marks in proposed approach are distributed over the entire design as well as incur minimal hardware overhead without disturbing the IP core functionality. Therefore, it satisfies all the required quality of an ideal secret mark for DSP/MP IP core ownership protection. The **novel contribution of this paper can be summarized as follows:**

- A novel signature encoding RTL-based secret mark is proposed which is distributive and exclusive by nature.
- A covert signature embedding process is proposed which provides high robustness/security.
- It is the first contribution on secured RTL watermark for DSP cores.
- This secret mark embedding technique incurs very nominal area overhead while embedding maximum possible signature strength.

IV. Proposed Signature based Secret Mark for DSP Core Protection

This paper proposes a novel RTL based signature encoding process for DSP core protection which is highly robust and distributive by nature. This secret mark is based on encoding of three variables where each variable indicates a decoded meaning. For example in proposed approach, the secret mark constraints could indicate covert embedding through changing of the multiplexer and de-multiplexer sizes used in the design and sharing of intermediate registers during scheduling. Though identifying these secret marks for the original IP owner is simple and straight-forward, however is extremely challenging for an adversary.

A. Problem Formulation

Given a Data Flow Graph (DFG) of a DSP core as input, design a low-cost secret mark embedded DSP core at RT level using optimal hardware configuration; where each hardware configuration ((X_i)) can be expressed as follows:

$(X_i) = N(R_1), N(R_2), ..N(R_D)$,

where $N(R_D)$ is the number of resources of resource type R_D. Thus, in this process following are the i/ps and o/ps:

Inputs: (a) DSP/MP core (b) optimal hardware configuration (c) owner's signature

Output: Low-cost secret signature embedded RTL design of DSP core.

B. Proposed signature based secret mark

A low-cost secret signature embedding technique for DSP core is proposed here, where the IP owner's signature is embedded during register-transfer level. This is achieved by forced breakup of the multiplexer and de-multiplexer into its next hierarchical size and by forced change in the sharing of intermediate registers used in the design. Breaking component size by a designer to decrease design complexity is a common de-facto practice. Moreover, sharing of the intermediate register can be done in multiple ways, hence detecting the presence of watermark in both these case is highly difficult for an adversary. Therefore, these are very covert ways of inserting a secret mark (or watermark) in the RTL design of a DSP core. As mentioned earlier, in the proposed secret signature embedding technique, IP owner's signature consist of three variables, i.e.: 'θ', 'ϕ', and 'ω'. The flow diagram of proposed secret signature embedding process is shown in Fig. 2.

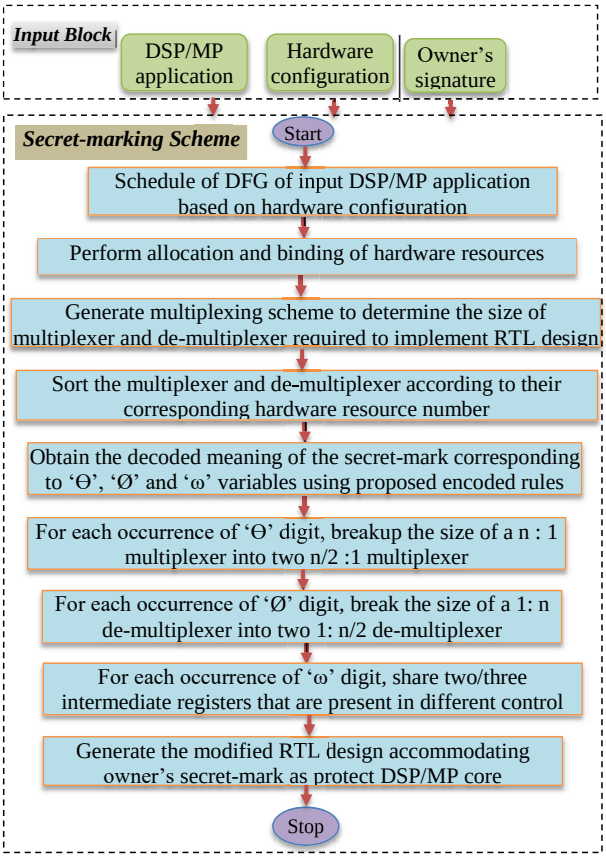

Fig. 2. Proposed secret signature embedding process for DSP core.

1) Signature Encoding: A novel triple variable encoded signature for secret mark embedding methodology is proposed to protect the IP owner's legal ownership in a DSP core. The encoded meaning of each signature variable is defined below:

- 'θ' = Encoded digit forcing breakup of multiplexer size into next hierarchical level at RTL.
- 'ϕ' = Encoded digit forcing breakup of de-multiplexer size into next hierarchical level at RTL.
- 'ω' = Encoded digit allocating sharing of min 2 - max 3 intermediate registers executing in different control step during scheduling.

2) Signature Embedding Steps: The proposed approach uses a low-cost hardware configuration (e.g., # of adders, # of multipliers, etc.) explored through Particle Swarm Optimization (PSO) [9] to design the given DSP core. Additionally, the owner's signature as a combination of 'θ,' 'ϕ,' and 'ω' variable

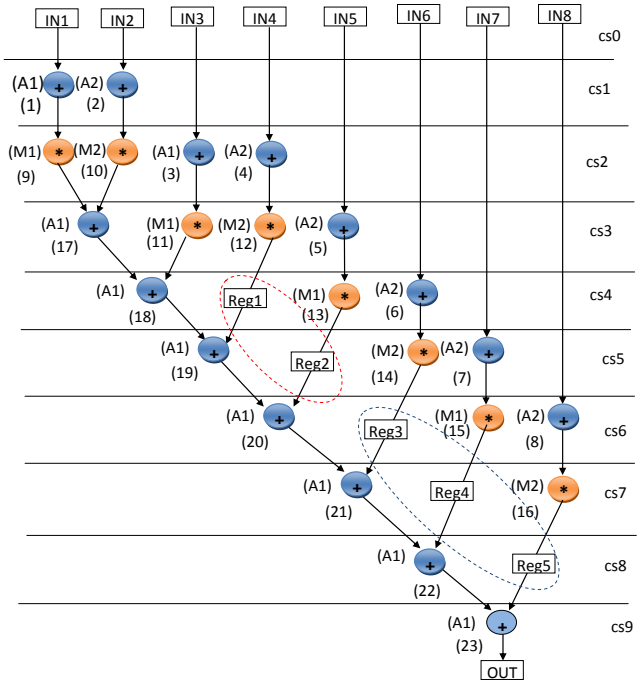

Fig. 3. Scheduled DFG of FIR using 2 adders and 2 multipliers where due to signature digits '$\omega\omega$', Reg1 & Reg2 must be executed through a single register and Reg3, Reg4, & Reg5 must be executed through another register).

is further taken as input. To insert the owner's signature, the following steps need to be followed:

1) Schedule the DFG of the input DSP core based on low-cost hardware configuration.
2) Perform hardware allocation and binding of resources.
3) Determine the size of multiplexer and de-multiplexer required to implement RTL design.
4) Sort the multiplexer and de-multiplexer in ascending order based on their corresponding hardware resource number (multiplexer for Adder_A1 to Adder_Ak, Multiplier_M1 to Multiplier_Mk etc.; de-multiplexer for Adder_A1 to Adder_Ak, Multiplier_M1 to Multiplier_Mk etc. and so on).
5) Decode the secret signature from the encoded meaning of each signature variable.
6) According to the encoded meaning, for each occurrence of 'θ' digit, breakup the size of a n:1 multiplexer into two n/2:1 multiplexer and one 2:1 multiplexer.
7) According to the encoded meaning, for each occurrence of 'ϕ' digit, breakup the size of a 1:n de-multiplexer into two 1:n/2 de-multiplexer and one 1:2 de-multiplexer.
8) According to the encoded meaning, for each occurrence of 'ω' digit, share two/three intermediate registers that are present in different control step during scheduling.

It should be noted that two inputs of each hardware resources come via two multiplexers and the corresponding output goes out via one de-multiplexer. Therefore, each signature must contain twice the number of 'θ' digits than 'ϕ' digits.

3) Design of IP core with embedded Secret Signature: In this paper we discuss secret signature embedding technique for a given owner's signature through Finite Impulse Response (FIR) filter. To perform that a 7th order FIR filter is taken as input in the form of DFG [10]. The DFG is then scheduled using 2 adders (Adder_A1, Adder_A2) and 2 multipliers (Adder_M1, Adder_M2) which is explored through a PSO-driven design space exploration framework. Allocation of hardware and binding of each resource is performed on the scheduled DFG. The scheduled and hardware allocated DFG of FIR filter is shown in Fig. 3. As shown in the figure it has 8 primary inputs (IN1-IN8), one primary output (OUT), five intermediate register (Reg1-Reg5), total 8 multiplication operations (orange nodes) and 15 addition operations (blue nodes). In can be observed that out of total 8 multiplication operation opn. 9, opn. 11, opn. 13, and opn. 15 are executed through multiplier M1 and rest i.e. opn. 10, opn. 12, opn. 14, and opn. 16 are executed through multiplier M2. Similarly opn. 1, opn. 3, opn. 17, opn. 18, opn. 19 opn. 20, opn. 21, opn. 22, and opn. 23 are executed through adder A1 and rest i.e. opn. 2, opn. 4, opn. 5, opn. 6 opn. 7, and opn. 8 are executed through adder A2. Therefore, to implement this design in RTL two 16:1, two 8:1, and four 4:1 multiplexer and one 1:16, one 1:8, and two 1:4 de-multiplexer is required. The datapath of unprotected (without embedded signature) FIR filter is shown in Fig. 4.

Now let's assume a 14-digit signature : '$\theta\theta\theta\theta\theta\theta\theta\phi\phi\phi\phi\omega\omega$' is provided by an original DSP IP owner. According to the encoded meaning of 'θ' variable, a multiplexer present in the original/unprotected FIR design (shown in Fig. 4) must be implemented using next hierarchical size multiplexer. For example, due to the first digit of the signature i.e. 'θ', the first 16:1 multiplexer of Adder 'A1' must be implemented using two 8:1 and one 2:1 multiplexer. Similarly, according to the encoded meaning of 'ϕ' variable, a de-multiplexer present in the original/unprotected FIR design (shown in Fig. 4) must be implemented using next hierarchical size de-multiplexer. For example, due to the ninth digit of the signature i.e. 'ϕ', the 1:16 de-multiplexer of Adder 'A1' must be implemented using one 1:2 de-multiplexer and two 1:8 de-multiplexers. Further, due to the thirteenth digit of the signature i.e. 'ω', two intermediate registers 'Reg1' and 'Reg2' must be implemented through a common register as both are used in different control steps (see Fig. 3). Finally, due to the last digit of the signature i.e. 'ω', rest of the intermediate register 'Reg3', 'Reg4' and 'Reg5' must be implemented through a common register as all are present in different control steps (see Fig. 3). The datapath of the signature (secret mark) embedded FIR filter is shown in Fig. 5. As shown in the figure, due to eight θ' digits the size of eight multiplexers are broken into next hierarchical size. Further, due to four ϕ' digits the size of four de-multiplexers are broken into next hierarchical size. Finally, due to two consecutive 'ω' digits 'Reg1' & 'Reg2' are executed through a single register 'Reg1' while 'Reg3', 'Reg4' & 'Reg5' are executed through another distinct register 'Reg2'.

To simplify the implementation process of a complex

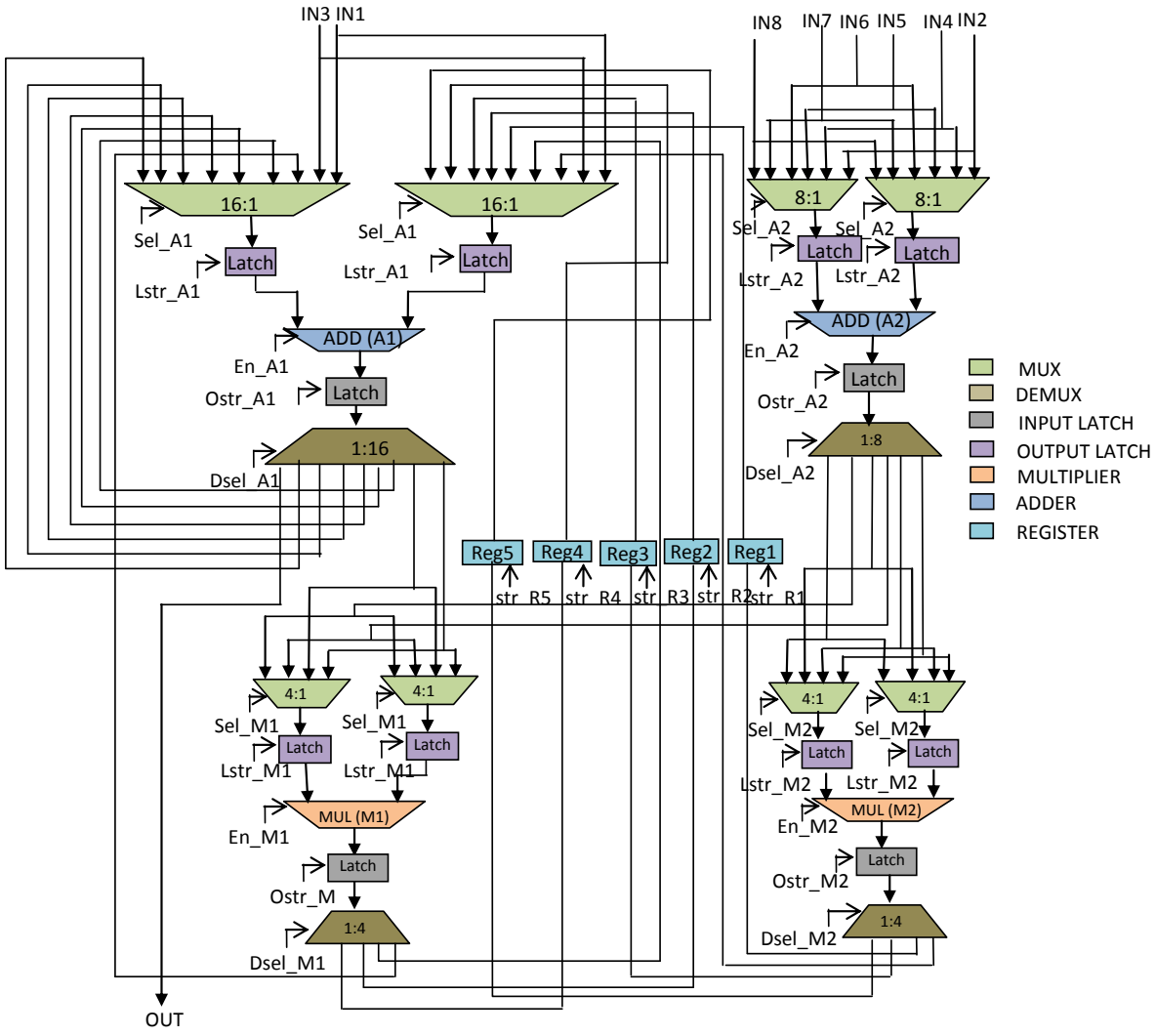

Fig. 4. RTL datapath of unprotected FIR filter.

DSP core, breaking the component size into multiple sub-components is a common de-facto practice. Additionally, sharing of registers is also an industry de facto. Therefore, an adversary would not be able to identify this hierarchical breakup of multiplexer/de-multiplexer size and register sharing as secret mark and confuse as a normal design.

C. Proposed Signature detection

a) Inspection: The IP controller is re-developed through inspecting appropriate data of the received IP such as structural characteristics, technical specifications etc.; b) Signature Verification: in re-developed data-path and controller, existence of owner's signature is verified by detecting the presence of embedded secret constraints.

V. Experimental Results

This section presents the experimental results of the proposed approach in terms of security analysis and design cost analysis.

A. Security Analysis

In this section, we discuss the attacker's perspective regarding the difficulty level in removing the owner's secret signature and its associated complexity level. To remove the secret signature from a DSP IP core an attacker needs to identify the owner's signature size (w) and the number of variables used to encode it. He/she then has to know the interpretation rule of each variable. After knowing that, he/she can then launch brute-force attack (analyzing exhaustive possibilities) to obtain the 'decoded signature digits' and verify its presence in the golden DSP IP core. The details of the attacking steps is shown in Fig. 6.

The maximum possible signature combinations generated through encoding variables (v) for different signature size (w) is reported in Table I. A secret signature is claimed to be highly tampered tolerant (T_t) if identifying its exact match from

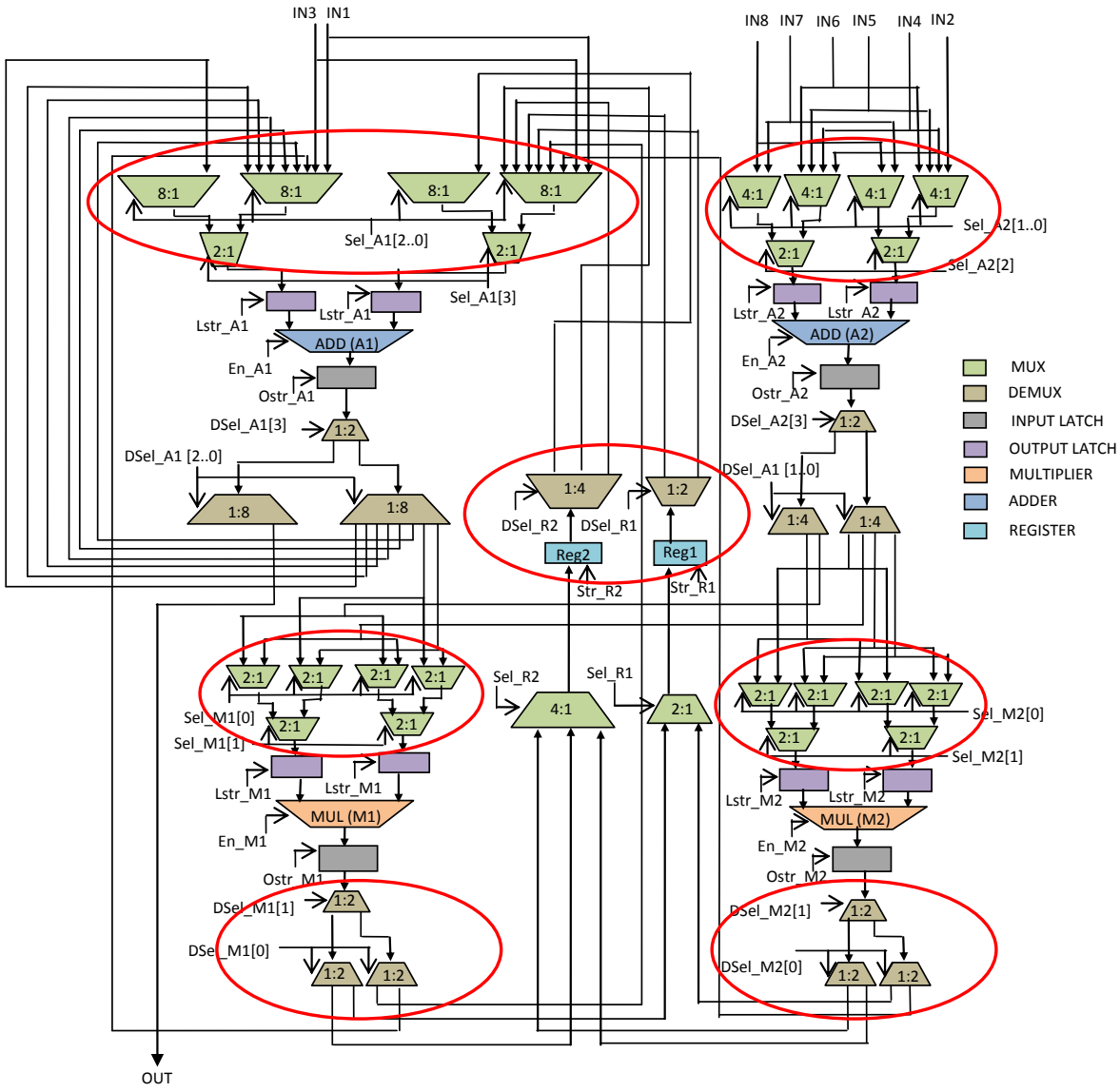

Fig. 5. RTL datapath of FIR filter with embedded Secret Signature = "$\theta\theta\theta\theta\theta\theta\theta\phi\phi\phi\phi\omega\omega$".

the all possible signature combinations (i.e. Brute-force) is extremely challenging. Therefore, more the number of possible signature combinations more the time required to identify it which indicates higher temper tolerance ability. The maximum number of possible signatures can be calculated from the following equation [7]:

$$T_t = v^w \tag{1}$$

TABLE I
TAMPER TOLERANCE ABILITY OF PROPOSED APPROACH FOR DIFFERENT SIGNATURE SIZES

Signature size	Signature combination	Tamper-tolerance(T_t)
3	$\theta\theta\phi$	27
6	$\theta\theta\theta\theta\phi\phi$	729
8	$\theta\theta\theta\theta\phi\phi\omega\omega$	6561
14	$\theta\theta\theta\theta\theta\theta\theta\phi\phi\phi\phi\omega\omega$	4782969

B. Design Cost Analysis

We have implemented both the unprotected and secret signature embedded 8th order FIR filter in a standard FPGA device of a modern RTL tool. The overhead analysis in terms of Logic Elements (LE) is performed with respect to unprotected RTL design after embedding maximum and minimum size signatures. The device utilization summary of unprotected FIR filter is reported in Table II. The device utilization summary after embedding maximum and minimum possible signature in FIR filter is reported in Table III. It can be observed from the table that LE overhead of proposed approach is trivial and lies between 6% - 3%.

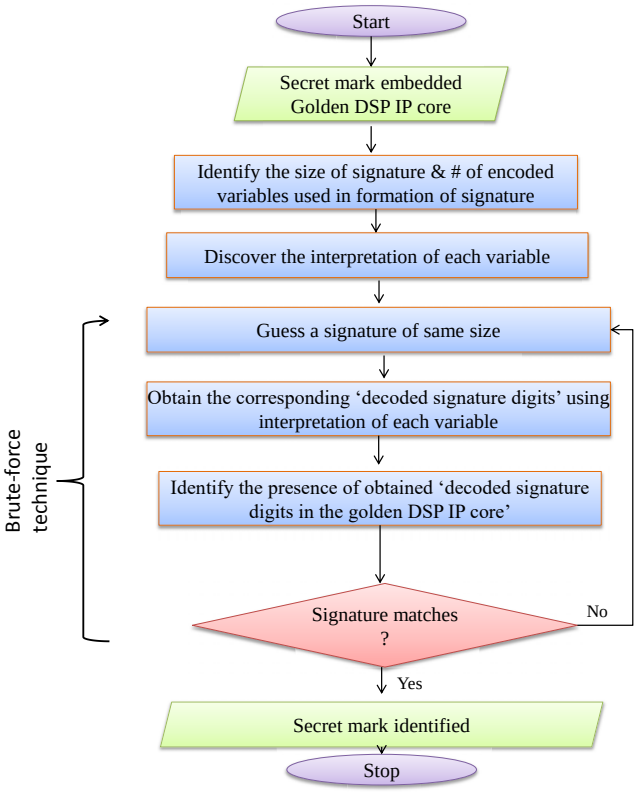

Fig. 6. Flowchart of secret signature detection process through Brute-force attack.

TABLE II
DEVICE UTILIZATION SUMMARY OF 8TH ORDER FIR FILTER WITH NO SECRET SIGNATURE

Resource type	Resource usage
Total Logic Elements	1370/68416 (2%)
Total Combinational Function	1369/68416 (2%)
Dedicated Logic Registers	65/68416 (<1%)
Total Registers	52
Total Pins	145/622 (23%)

TABLE III
DEVICE UTILIZATION SUMMARY OF 8TH ORDER FIR FILTER WITH MAXIMUM & MINIMUM SECRET SIGNATURE AND LE OVERHEAD COMPARED TO UNPROTECTED FIR FILTER

Signature & resource details	Details of maximum signature	Details of minimum signature
Signature size	14	3
Signature digits	$\theta\theta\theta\theta\theta\theta\theta\theta\phi\phi\phi\phi\phi\omega\omega$	$\theta\theta\phi$
Total logic elements	1461/68416 (2%)	1418/68416 (2%)
Total combinational function	1458/68416 (2%)	1417/68416 (2%)
Dedicated logic registers	65/68416 (<1%)	65/68416 (<1%)
Total register	52	52
Total pin	145/622 (23%)	145/622 (23%)
Overhead (%)	6%	3%

C. Comparative Perspective with Prior Related Research

There have been prior work on DSP/MP core protection using secret mark such as [6], [7], [8], [9]. However they have been embedded during HLS. On the contrary this is a novel methodology for protecting DSP/MP cores using signature implanted directly in RTL datapath. Thus the comparative perspective with baseline design (no secret mark) is presented in Table II and Table III. As observed LE overhead of proposed approach is nominal between 6% - 3%,, but offers strong security.

VI. CONCLUSION

This paper proposes a novel RTL signature-based low-overhead DSP IP core protection approach to preserve the ownership right. This secret mark is exclusive and distributed throughout the design. The area overhead in terms of LE for the 8th order FIR benchmark is between 6% and 3% with respect to maximum and minimum size signature compared to a an unprotected (baseline) design.

ACKNOWLEDGMENT

This work is financially supported by CSIR under sanctioned grant no. 22/730/17/EMR-II.

REFERENCES

[1] E. Castillo, U. Meyer-Baese, A. Garcia, L. Parrilla, and A. Lloris, "Ipp@hdl: Efficient intellectual property protection scheme for ip cores," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 15, no. 5, pp. 578–591, May 2007.

[2] A. Sengupta and D. Roy, "Antipiracy-aware ip chipset design for ce devices: A robust watermarking approach [hardware matters]," *IEEE Consumer Electronics Magazine*, vol. 6, no. 2, pp. 118–124, April 2017.

[3] R. Chapman and T. S. Durrani, "Ip protection of dsp algorithms for system on chip implementation," *IEEE Transactions on Signal Processing*, vol. 48, no. 3, pp. 854–861, March 2000.

[4] A. B. Kahng, J. Lach, W. H. Mangione-Smith, S. Mantik, I. L. Markov, M. Potkonjak, P. Tucker, H. Wang, and G. Wolfe, "Constraint-based watermarking techniques for design ip protection," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 20, no. 10, pp. 1236–1252, Oct 2001.

[5] D. Kirovski, Y.-Y. Hwang, M. Potkonjak, and J. Cong, "Intellectual property protection by watermarking combinational logic synthesis solutions," in *1998 IEEE/ACM International Conference on Computer-Aided Design. Digest of Technical Papers (IEEE Cat. No.98CB36287)*, Nov 1998, pp. 194–198.

[6] F. Koushanfar, I. Hong, and M. Potkonjak, "Behavioral synthesis techniques for intellectual property protection," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 10, no. 3, pp. 523–545, Jul. 2005.

[7] A. Sengupta, D. Roy, and S. P. Mohanty, "Triple-phase watermarking for reusable ip core protection during architecture synthesis," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 4, pp. 742–755, April 2018.

[8] B. Le Gal and L. Bossuet, "Automatic low-cost ip watermarking technique based on output mark insertions," *Des. Autom. Embedded Syst.*, vol. 16, no. 2, pp. 71–92, Jun. 2012. [Online]. Available: http://dx.doi.org/10.1007/s10617-012-9085-y

[9] D. Roy and A. Sengupta, "Low overhead symmetrical protection of reusable ip core using robust fingerprinting and watermarking during high level synthesis," *Future Generation Computer Systems*, vol. 71, pp. 89 – 101, 2017.

[10] "DSP benchmark suite." [Online]. Available: http://express.ece.ucsb.edu/benchmark/