Securing Reusable Hardware IP cores using Palmprint Biometric

Rahul Chaurasia, Anirban Sengupta

Indian Institute of Technology Indore, India

IEEE computer society

The IEEE Computer Society Technical Committee on VLSI

7th IEEE International Symposium on Smart Electronic Systems (iSES)

Platinum Sponsor	Gold Sponsor	Silver Sponsor
Qolsys QUALITY OF LIFE	Mentor A Siemens Business	Genus energizing lives

Introduction

- The digital signal processing (DSP) based intellectual property (IP) cores integrated in consumer electronic systems are used to facilitate applications such as image, audio and video processing with higher efficacy and low cost [1].
- Involvement of multiple offshore entities during design process of Integrated circuits (ICs) to minimize the overall design complexity, design cost and time-to – market, poses serious hardware threats of IP piracy or counterfeiting [2].
- Counterfeited IPs integrated may contain the malicious logic (hardware Trojans) hidden inside. These Trojan infected IPs or ICs are unreliable and unsafe for end consumers, when integrated in consumer electronics (CE) systems [3], [4].
- The proposed approach is capable of generating non-replicable and non-vulnerable secret biometric palmprint constraints that are embedded in DSP designs to detect counterfeited versions, thereby enabling the integration of only authentic IPs in the CE systems.

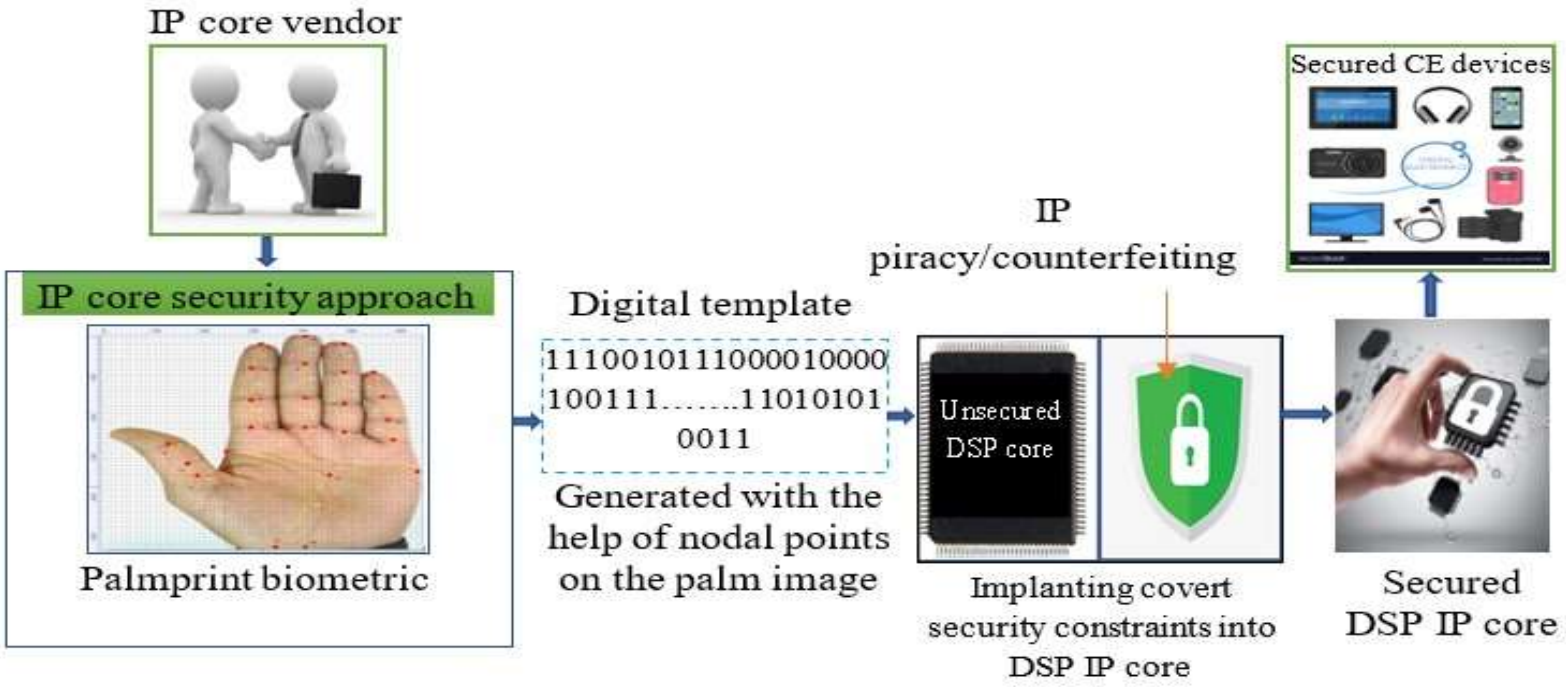
Literature Review

- **Hardware steganography** [5] based security approach to address the IP counterfeiting threat.
- However if the encoding rules and the secret value of chosen entropy threshold are leaked to an adversary, then the secret stego-mark may become weak.

- The **watermarking approaches** [6], [7] insert original signature into the target design in the form of watermark.
- However, in the watermarking approaches, the chosen signature is vulnerable if the relevant information such as digit encoding into security constraints, signature size and combinations of digits are leaked to an adversary, s/he can replicate and re-use it. This renders the watermark a weaker secret mark.

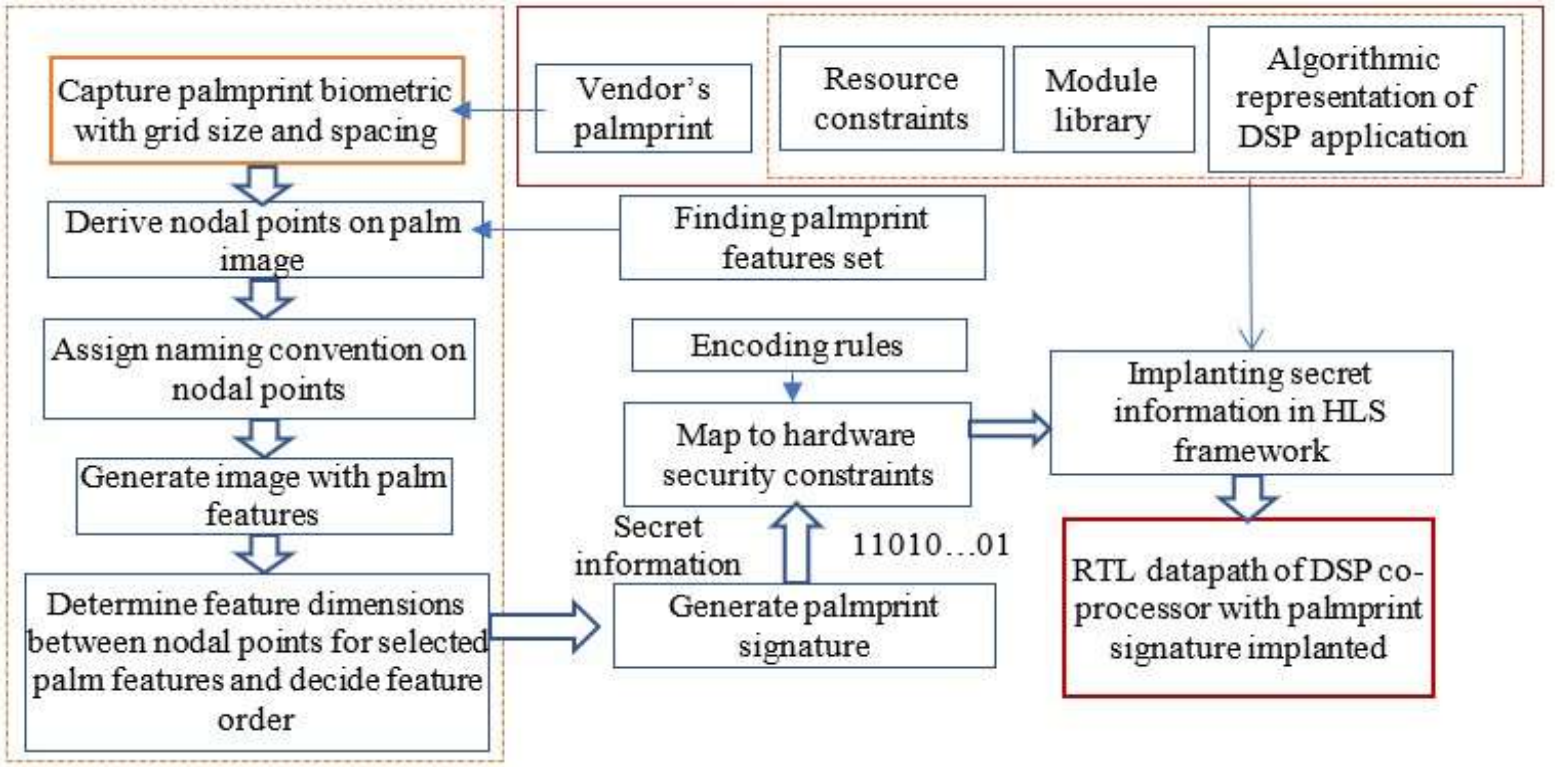
- **Fingerprint biometric** [8] based hardware security approach embeds IP vendor's authentic fingerprint biometric constraints into the design.
- However, the fingerprint approach is not contact-less as it depends on optical scanner during both fingerprint implantation and verification. The generated fingerprint constraints using minutiae points are also affected by external environmental factors such as dirt and grease etc.

Proposed Work (Thematic Representation)



Securing reusable DSP IP core used in CE systems

Proposed Work (Overview)

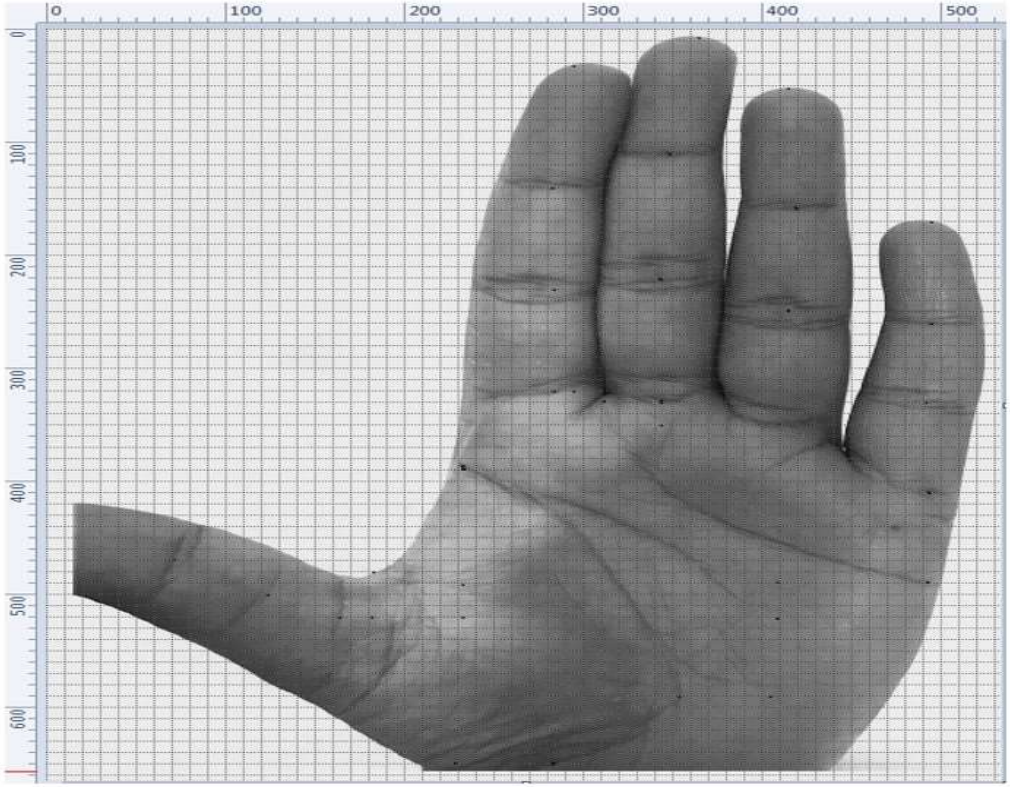


Proposed palmprint biometric for securing DSP co-processors

Proposed Work (Cont.)

➢ Capturing palm image

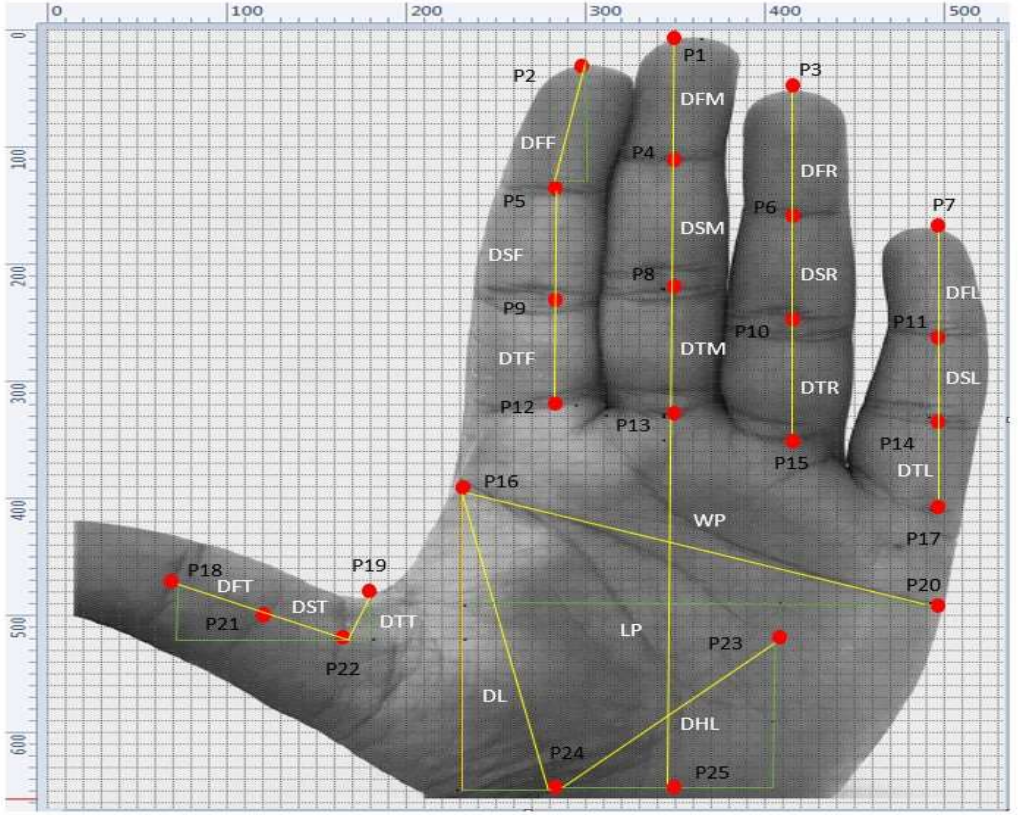
- At first the palmprint biometric of the authentic vendor or designer is captured and subsequently image of the captured palmprint is subjected to a specific grid size/spacing.
- This helps in generating the nodal points precisely.



Proposed Work (Cont.)

➢ **Generating image with chosen palm features and nodal points**

- Finding Palmprint Feature Set and Deriving Nodal Points for Captured Palmprint Biometric.
- Assigning Naming Convention and Deriving Palmprint Image with Selected Feature set.



Proposed Work (Cont.)

➢ **Finding Feature Dimensions and Deriving Palmprint Signature Based on the Selected Feature Order**

- For example, a palmprint signature for the selected order of palmprint features ("DL╪ DHL --- ╪ DTT". Where, '╪' represents the concatenation operator) after concatenation is as follows:
- Palmprint Signature:

"100001001.1110110000.1110100011110101111.---.11111"

FEATURE DIMENSION AND CORRESPONDING BINARY REPRESENTATION OF CHOSEN PALMPRINT FEATURES

Feature #	Feature name	Feature dimension	Binary representation
F1	DL	265.75	100001001.11
F2	DHL	176.91	10110000.111010001111010111
F3	WP	283.24	100011011.0011110101110000101
F4	LP	325	101000101
F5	DFF	101.11	1100101.00011100001010001111
F6	DSF	100	1100100
F7	DTF	90	1011010
F8	DFM	105	1101001
F9	DSM	110	1101110
F10	DTM	105	1101001
F11	DFR	110	1101110
F12	DSR	85	1010101
F13	DTR	110	1101110
F14	DFL	95	1011111
F15	DSL	70	1000110
F16	DTL	70	1000110
F17	DFT	55.90	110111.111001100110011
F18	DST	51.45	110011.011100110011
F19	DTT	42.72	101010.101110000101000111111

Note: Size of the palmprint signature varies based on the number of chosen palm features by the vendor for signature generation (depending on the required security strength corresponding to target application).

Proposed Work (Cont.)

➢Deriving the Covert Security Constraints and Implanting into Target IP core Design

- Post obtaining the digital template of palmprint signature, corresponding hardware security constraints are generated based on the encoding rules.
- The encoding rules for the signature bits are as follows:

The bit '1' embeds an edge between node pair (odd-odd), bit '0' embeds an edge between node pair (even-even). Moreover, the binary bit '.' embeds an edge between node pair (0, integer) into the CIG of target DSP design.

- For example, for a sample design having 31 storage variables (T0 to T30) executing through 8 registers (R1 to R8), the generated security constraints corresponding to the zeros are: <T0, T2>, <T0, T4>---<T16, T28>, the security constraints corresponding to ones are: <T1, T3>, -----<T27, T29> and corresponding to the binary points are: <T0, T1>, <T0, T3>, -- -, <T0, T11>.

TABLE I
REGISTER ALLOCATION OF A TARGET HARDWARE IP CORE POST IMPLANTATION

Registers	i0	i1	i2	i3	i4	i5	i6	i7	i8	i9
R1	T0	T8	T17	T24	T25	T26	T27	T28	T29	T30
R2	T1	T9	T16	--	--	--	--	--	--	--
R3	T2	T11	T18	T18	--	--	--	--	†	--
R4	T3	T10	T19	T19	T19	--	--	--	--	--
R5	T4	T4	T13	T20	T20	T20	--	--	--	--
R6	T5	T5	T12	T21	T21	T21	T21	--	--	--
R7	T6	T6	T15	T22	T22	T22	T22	T22	--	--
R8	T7	T7	T14	T23	T23	T23	T23	T23	T23	--
R9	--	T8	T19	T19	T19	--	--	--	--	--
R10	--	T9	--	T24	--	T26	--	T28	--	T30
R11	--	--	T18	T18	T25	--	--	--	--	--
R12	--	--	--	T20	T20	T20	T27	--	--	--
R13	--	--	--	T22	T22	T22	T22	T22	T29	--
R14	--	--	--	T21	T21	T21	T21	--	--	--
R15	--	--	--	T23	T23	T23	T23	T23	T23	--

RESULTS AND DISCUSSION

- The proposed palmprint biometric approach is analyzed in terms of security and design overhead.

Security Analysis:

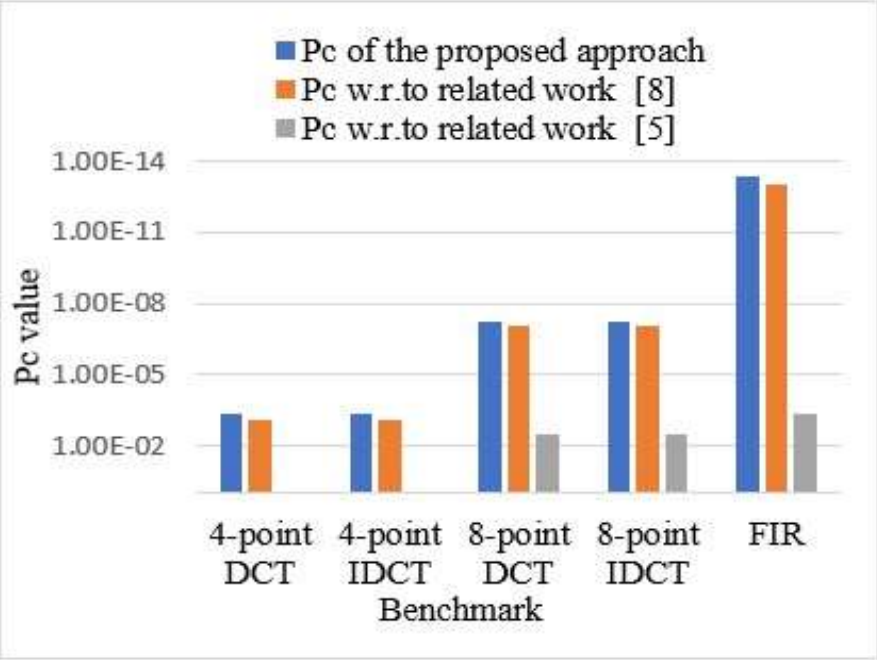
- The security of the proposed approach is analyzed in terms of probability of coincidence (Pc) and temper tolerance (TT) ability.
- The Pc metric is formulated as follows:

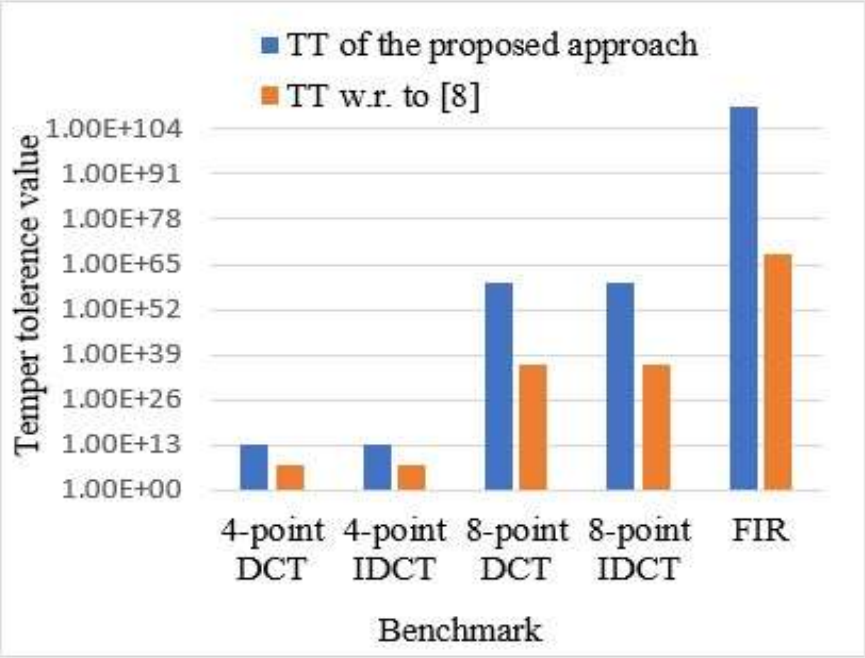
$$\mathrm{Pc} = \left(1 - \frac{1}{\tau}\right)^{S} \qquad (1)$$

- The TT metric is formulated as follows:

$$\mathrm{TT} = P^{Q} \qquad (2)$$

Comparison of Probability of Coincidence and Tamper Tolerance Ability with Previous Works





Design Cost Overhead Post Implanting the Palmprint Signature

Design cost Analysis:

Design cost can be measured using the following metric:

$$Z = h1\frac{\nabla t}{\nabla max} + h2\frac{\Delta t}{\Delta max} \qquad (3)$$

- Design cost overhead post implanting the palmprint signature into the design is minimal (0.2%-0.8%) as evident from Table II.

TABLE II

DESIGN COST PRE AND POST EMBEDDING PALMPRINT BIOMETRIC CONSTRAINTS

Benchmarks	Design cost of baseline	Design cost of palmprint implanted design	% Cost overhead
4-pointDCT	0.5611	0.5623	0.2%
4-point IDCT	0.5611	0.5623	0.2%
8-pointDCT	.4721	.4740	0.4%
8-point IDCT	.4721	.4740	0.4%
FIR	.4443	.4479	0.8%

Conclusion

- This paper presents a novel contact-less palmprint biometric security approach for securing the reusable hardware IP core.
- The proposed approach enables the seamless detection of pirated/counterfeited DSP IPcores used in CE systems, thus ensuring consumers safety and protecting IP/brand value, returning revenue and resolving traffic bleed.
- Any DSP based intellectual property (IP) core can be embedded with proposed palmprint signature to distinguish between authentic and its fake versions.
- The biometric palmprint constraints generated through the proposed approach is non-replicable and non-vulnerable as compared to hardware steganography and hardware watermarking approaches.
- The proposed work presents stronger security and minimal design overhead in parallel, compared to the existing state of the art approaches.

References

[1] R. Schneiderman, “DSPs evolving in consumer electronics applications,” IEEE Signal Process. Mag., vol. 27, no. 3, pp. 6–10, 2010.

[2] F. Koushanfar et al., “Can EDA combat the rise of electronic counterfeiting?,” DAC Design Automation Conference, San Francisco, CA, 2012, pp. 133-138.

[3] B. Colombier and L. Bossuet, “Survey of hardware protection of design data for integrated circuits and intellectual properties,” IET Computers & Digital Techniques, vol. 8, no. 6, pp. 274-287, 2015.

[4] 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, 2005.

[5] A. Sengupta and M. Rathor, “IP core steganography for protecting DSP kernels used in CE systems,” IEEE Trans. Consum. Electron., vol. 65, no. 4, pp. 506-515, 2019.

[6] B. Le Gal and L. Bossuet, “Automatic low-cost IP watermarking technique based on output mark insertions,” Design Autom. Embedded Syst., vol. 16, no. 2, pp. 71–92, 2012.

[7] D. Ziener and J. Teich, “Power signature watermarking of IP cores for FPGAs,” J. Signal Process. Syst., vol. 51, no. 1, pp. 123–136, 2008.

[8] A. Sengupta and M. Rathor, “Securing hardware accelerators for CE systems using biometric fingerprinting,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 28, no. 9, pp. 1979-1992, 2020, doi: 10.1109/TVLSI.2020.2999514.

Thank you