Symmetrical Protection of Ownership Right's for IP Buyer and IP Vendor using Facial Biometric Pairing

Authors: Rahul Chaurasia, Anirban Sengupta

Outline

- Introduction
- Contemporary Approaches
- Overview of Proposed Approach
- Discussion on Proposed Approach
- Results and Analysis

Introduction

- The digital signal processing (DSP) intellectual property (IP) cores are the integral part of consumer electronic systems, used to facilitate **applications such as image, audio and video processing** etc. with higher efficacy and low cost [1],[2].
- The DSP IP cores such as **JPEG, MPEG, DCT** and digital filters like **FIR, IIR** are widely **used** in several electronic gadgets such as **digital camera, cellular phones, smart watches** etc.
- **High demand of hardware accelerators**.
- Therefore, in order to tradeoff the supply and demand, these hardware accelerators are **developed and delivered by the third-party vendors** (sellers), this scenario indeed **may lead the major security concerns to end consumer along with IP buyer and seller** [7].

Contemporary Approaches

- The **watermarking approach:** [3], embeds the signature during lower abstraction level of the design. It provides the piracy detection by embedding the watermark of IP vendor only, but is incapable of tracing the illegal distribution of IP cores.
- [4], Protects the rights of IP buyer and seller but at lower abstraction level of the design.

- **Multivariable fingerprint and watermark** [5] embeds the multi variable finger print of IP buyer and watermark of IP seller during HLS.
- However, is not robust as the proposed facial biometric pairing-based approach.

- **Hardware steganography** [6] address the IP counterfeiting threat by embedding the secret stego-constraints into the design .
- 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.

Overview of Proposed Approach

- This paper presents a robust security methodology for protecting the rights of IP vendor along with IP buyer, in hardware IP cores using facial biometric.
- The approach, firstly embeds the facial biometric signature of IP buyer**.**
- Subsequently, post obtaining the embedding design with **IP buyer** signature, the facial biometric signature of **IP vendor** is embedded.
- **Offerings:**
- Symmetrical protection of ownership rights with zero design cost overhead.
- The embedded signature of IP vendor can also be used to detect the pirated IPs.
- Higher security in terms of lesser probability of coincidence (Pc) than state of the art approaches.

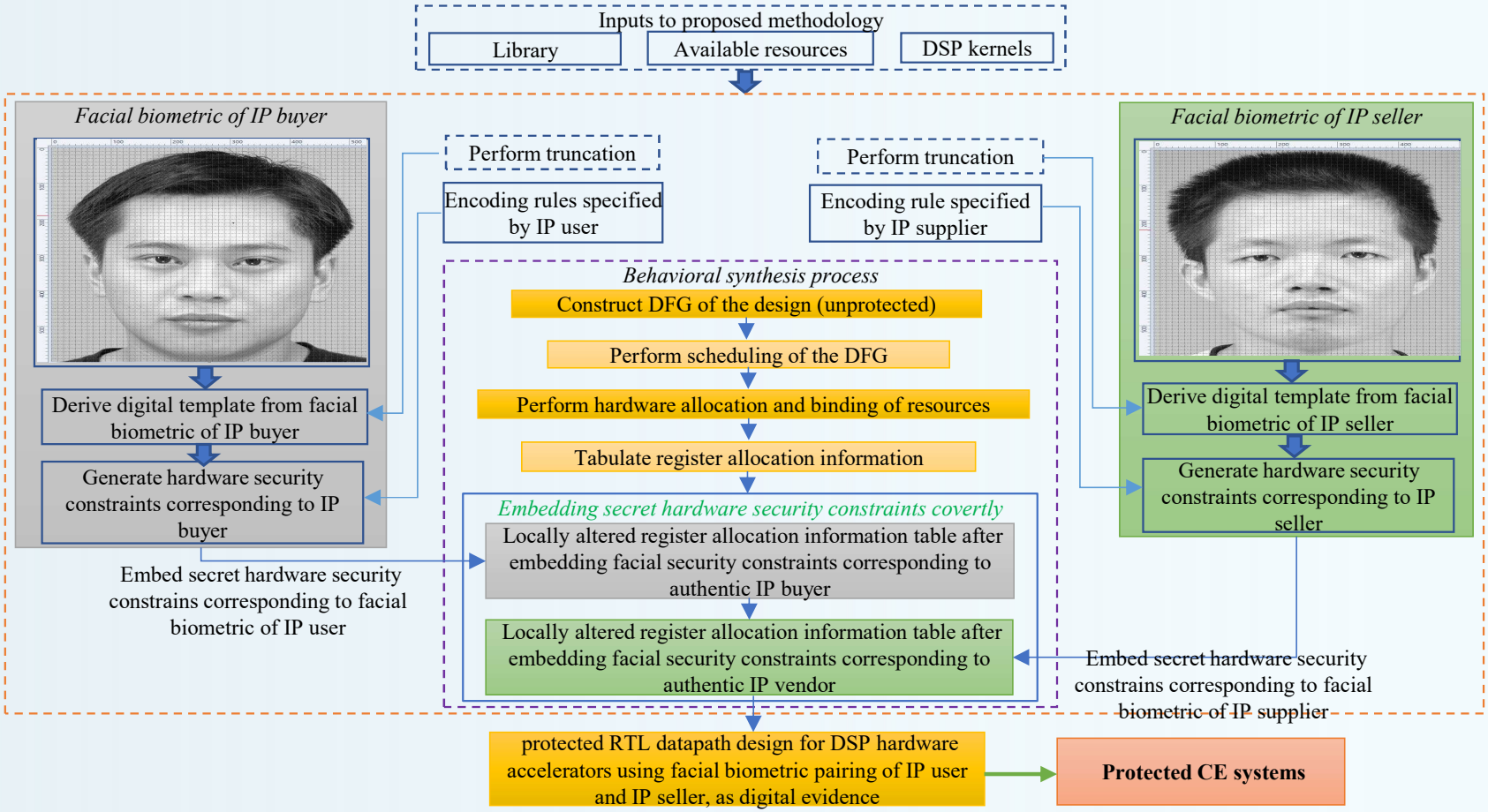
Threat Model

- ***Threat to IP seller***:
- An IP buyer may falsely claim the IP ownership rights, post receiving the IP. Therefore, a robust security mechanism must be integrated in order to safeguard the rights of IP seller.

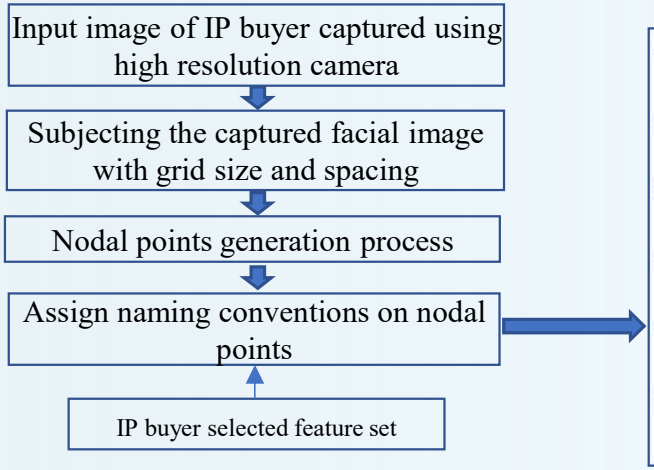
- ***Threat to IP buyer***:
- An untrustworthy IP seller may distribute/ sell the illegal copies of custom IP (designed based on the IP buyer specification).
- An adversary in offshore design house may counterfeit the design without the knowledge of original IP seller.
- This may lead to illegal use of custom IPs.

Thematic Design Flow

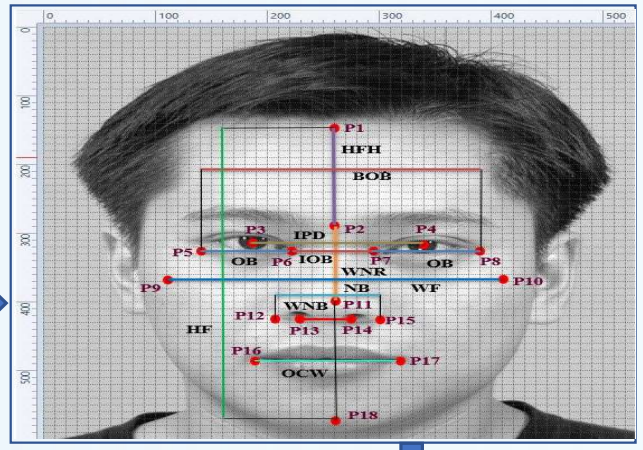
Design Flow of Proposed Work



Generating Hardware Security Constraints for Facial Biometric of the IP Buyer



Generate the facial image with chosen features



Calculating the Feature Dimensions of Chosen Features

Facial features	Naming convention of points	Co-ordinates (x1, y1)-(x2, y2)	Feature dimension evaluated using Manhattan equation (|x2-x1|+|y2-y1|)	Binarize feature magnitude
Face Height (HF)	(P1) & (P18)	(260, 145) & (260,570)	425	110101001
Height of Forehead (HFH)	(P1) &(P2)	(260, 145) & (260, 290)	145	10010001
Nasal Ridge Width (WNR)	(P2) & (P11)	(260, 290) & (260, 400)	110	1101110
Inter Pupillary Distance (IPD)	(P3) & (P4)	(185, 315) & (340, 315)	155	10011011
Ocular Breadth (OB)	(P5) & (P6)	(140, 325) & (220, 325)	80	1010000
Bio- Ocular Breadth (BOB)	(P5) &(P8)	(140, 325) & (390, 325)	250	11111010
Inter – Ocular Breadth (IOB)	(P6) & (P7)	(220, 325) & (295, 325)	75	1001011
Face Width (WF)	(P9) &(P10)	(110, 370) & (410,370)	300	100101100
Nasal Breadth (NB)	(P12) & (P15)	(205, 425) & (300, 425)	95	1011111
Nasal Base Width (WNB)	(P13) & (P14)	(230, 425) & (275, 425)	45	101101
Oral Commissure Width(OCW)	(P16) & (P17)	(190, 485) & (320, 485)	130	10000010

Cont.

- For example, if IP buyer selects following facial features among the total specified features, in the following concatenation order such as:

  "HF→WNR→OB→IOB→NB→OCW→WNB→WF→BOB".

- ✓ Then, the generated facial signature will be as follows:

  1101010011101110101000010010111011111100000101011011001011001111 1010

- Subsequently, hardware security constraints are generated based on following inputs:
  - Facial signature,
  - Scheduled DSP design and its register allocation information,
  - Encoding rule specified by the **IP buyer**.

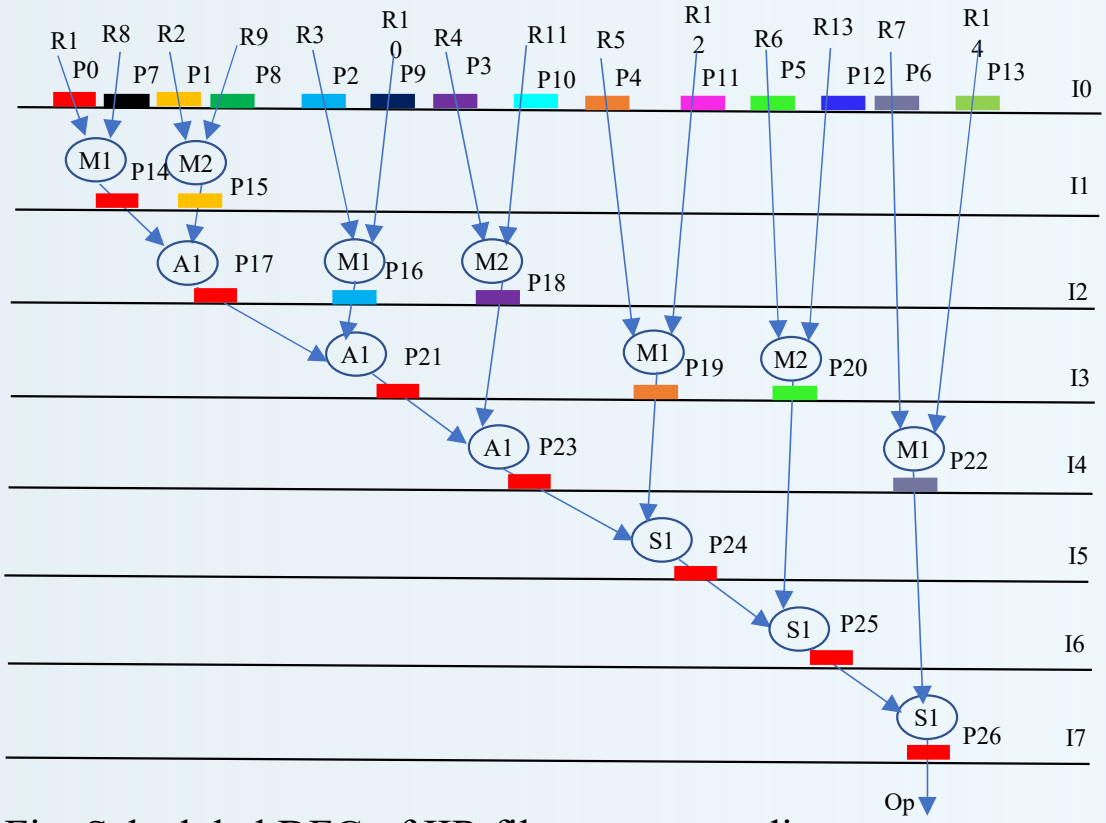


Fig. Scheduled DFG of IIR filter corresponding to resources (one adder, two multipliers and one subtractor)

➢ ***Encoding rule***:

- For signature bit '0' implant the security constraints between the storage variable pairs where both the variables (P) are even.
- For bit '1' implant the security constraints between the storage variable pairs where first variable is 0 and second variable can be of any unused available integer value.

***Hardware security constraints (for IP buyer)*:**

- For signature bit '0'→(P0-P2), (P0-P4), (P0-P6), (P0-P8), (P0-P10), (P0-P12), (P0-P14), ,..……..,(P4-P14),
- For signature bit '1'→(P0-P1), (P0-P3), (P0-P5),…..(P0-P25).

Generating security constraints corresponding to Facial biometric IP seller

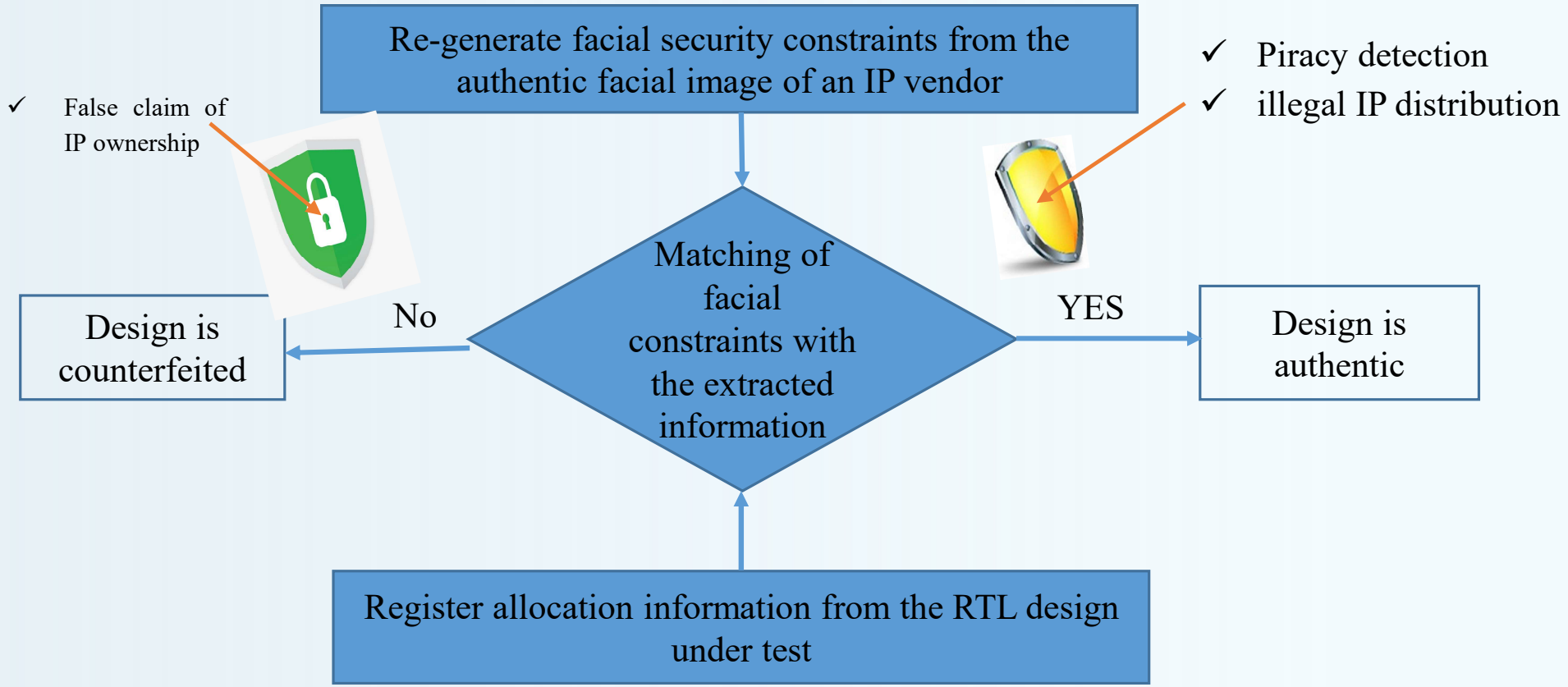
- Generate hardware security constraints are generated based on :
- Facial biometric signature of **IP seller**,
- Scheduled DSP design and its register allocation information,
- Encoding rule specified by the **IP seller**.

Embedding Facial constraints of IP buyer and seller into design

Register Allocation Information Post Embedding the Facial Biometric Driven Security Constraints Corresponding to IP Buyer and IP Seller

CS (I)	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14
0	P0	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13
1	P15	P14	P2	P3	P4	P5	P6	P15	--	P9	P10	P11	P12	P13
2	P17	P17	P16	P16	P4	P5	P6	P18	P17	--	--	P11	P12	P13
3	P21	P21	P21	P18	P19	P20	P6	P18	--	--	--	--	--	P13
4	P23	P23	--	--	P19	P20	P22	--	--	P23	--	--	--	--
5	P24	P24	--	--	--	P20	P22	--	--	--	--	--	--	--
6	P25	P25	P25	--	--	--	P22	--	--	--	--	--	--	--
7	P26	P26	--	--	--	--	--	--	--	--	--	--	--	--

Nullifying False Ownership Claim and Detecting Piracy



Results and Analysis

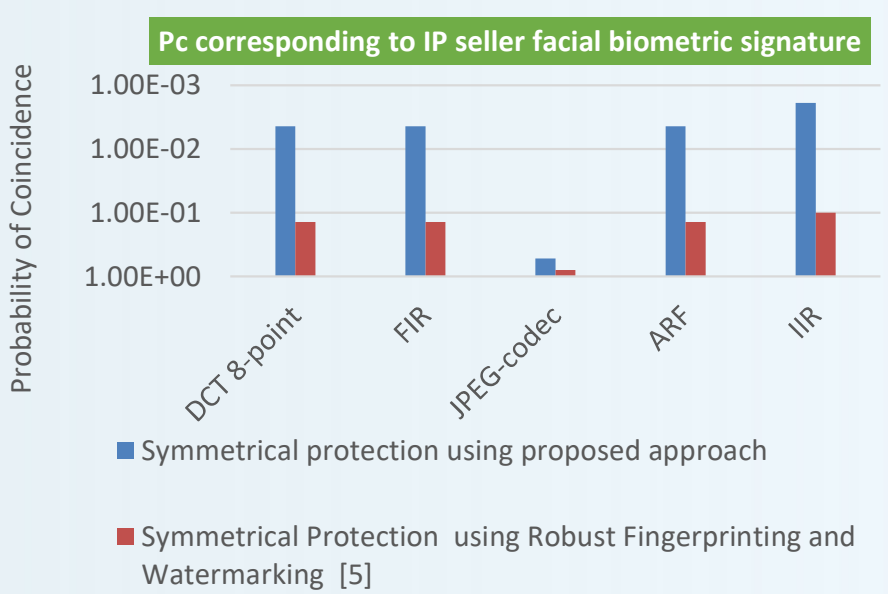
The proposed approach is analyzed in terms of security strength and design cost overhead.

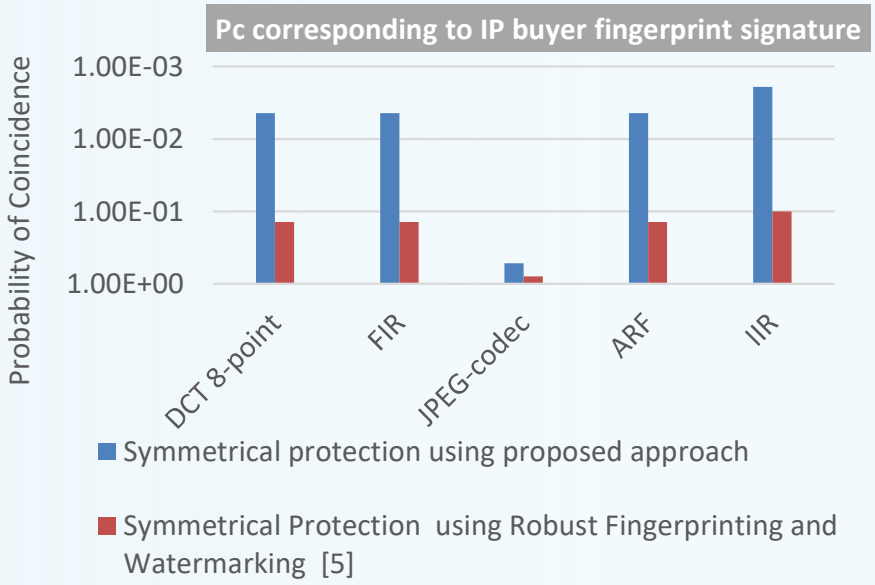
➢ *Security Analysis:*

The security of the proposed approach is analyzed in terms of probability of coincidence (Pc).

- The Pc metric is formulated as follows [5]:

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





Results and Analysis

➢ *Design cost Analysis:*

- Design cost (Φ) for enabling the symmetrical protection of IP rights for buyer and seller by integrating the security during higher abstraction level of the design process, is formulated as follows:

$$\Phi = \eta 1 \frac{\Omega_A}{\Omega_{Max}} + \eta 2 \frac{\upsilon_D}{\upsilon_{Max}} \quad (3)$$

TABLE IV
Design Cost of the Proposed Approach Post Embedding Facial Biometric Signature of IP buyer and then of IP Seller into the Design

DSP benchmarks	No. of registers (**δ**)	Resource configuration	Design cost of baseline design	Design cost after embedding facial biometric of IP buyer	Design cost after embedding facial biometric of IP seller	% Design cost overhead
DCT-8point	16	1(+), 2(*)	0.447	0.447	0.447	0.00%
FIR	16	1(+), 3(*)	0.5697	0.5697	0.5697	0.00%
JPEG-codec	129	3(+), 3(*)	0.2178	0.2178	0.2178	0.00%
ARF	16	2(+), 4(*)	0.4121	0.4121	0.4121	0.00%
IIR	14	1(+),2(*),1(-)	0.5247	0.5247	0.5247	0.00%

References

1. C. Pilato, S. Garg, K. Wu, R. Karri and F. Regazzoni, “Securing hardware accelerators: a new challenge for high-level synthesis,” *IEEE Embedded Syst. Lett*., vol. 10, no. 3, pp. 77-80, Sept. 2018.
2. X. Wang, Y. Zheng, A. Basak and S. Bhunia, “IIPS: Infrastructure IP for Secure SoC Design,” *IEEE Trans. Comput*., vol. 64, no. 8, pp. 2226-2238, 1 Aug. 2015.
3. S. Rai, A. Rupani, P. Nath and A. Kumar, “Hardware Watermarking Using Polymorphic Inverter Designs Based On Reconfigurable Nanotechnologies,” *2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2019, pp. 663-669.
4. J. Lach, W.H. Mangione-Smith, M. Potkonjak, Fingerprinting techniques for field-programmable gate array intellectual property protection, *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst*. 20 (10) (2001) 1253–1261.
5. D. Roy, A. Sengupta "Low Overhead Symmetrical Protection of Reusable IP Core using Robust Fingerprinting and Watermarking during High Level Synthesis", *Elsevier Journal on Future Gener. Comput. Syst*., Volume 71, June 2017, pp. 89–101.
6. 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.
7. A. Sengupta “Frontiers in Securing IP Cores - Forensic detective control and obfuscation techniques”, *The Institute of Engineering and Technology (IET)*, 2020, ISBN-10: 1-83953-031-6, ISBN-13: 978-1-83953-031-9.
8. CAD for Assurance, IEEE Hardware Security and Trust Technical Committee, https://cadforassurance.org/tools/ip-ic-protection/faciometric-hardware-security-tool/, accessed on March 2022.