Secure and Optimized IP design using Key-driven Cipher-Based Multi-layer Encrypted HLS Watermarking integrated with FA based Exploration

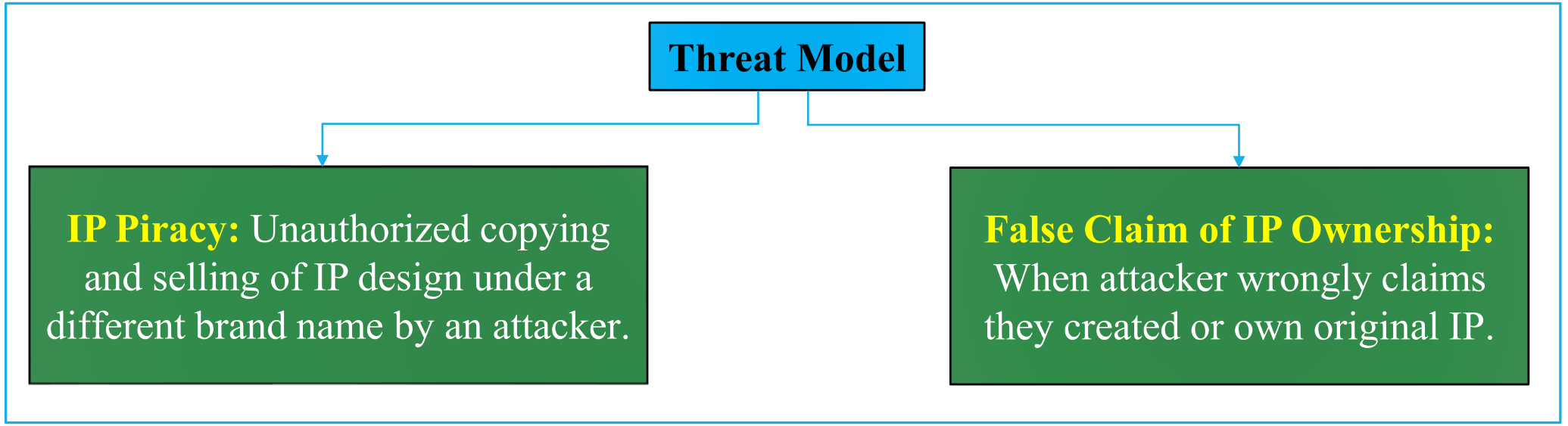
Presented in IEEE International Conference on Mechatronics (ICM'25)

Authors: Anirban Sengupta, Vishal Chourasia and Nabendu Bhui

• Introduction

- In electronic system designs, system-on-chips, comprising of several reusable intellectual property (IP) blocks.
- These are fundamental as they provide efficient optimized solutions for critical applications ranging from image processing, video compression, signal filtering, to machine learning, medical image analysis etc.
- To satisfy these market needs, IP designers heavily depend on reusable IP cores.
- such hardware IPs are prone to external hardware threats due to globalization in the design supply chain.

• Threat Model



- Attacker → An untrustworthy entity
- Defender → A genuine IP designer

• Related Works

Sr. No.	Existing Work	Technique Used	Remark
1.	J. Chen and B. C. Schafer, [1] (2021)	employs pragma insertion within the allocation stage of functional units	[1] technique is ineffective for generating extensive/large watermark constraints
2.	A. Sengupta et.al.,[2] (2021)	Facial biometric based hardware watermarking	[2] preprocessing steps for watermark generation
3.	M. Rostamiet.al., [3] (2014)	provide a detailed catalogue of different hardware security techniques along with countermeasures.	[3] However, it fails to discuss optimization of secure IP designs.

[1] J. Chen and B. C. Schafer, "Watermarking of Behavioral IPs: APractical Approach," *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Grenoble, France, pp. 1266-1271,2021.

[2] A. Sengupta and M. Rathor, "Facial Biometric for Securing Hardware Accelerators," *IEEE Transaction on Very Large Scale Integration (VLSI) Systems*, vol. 29, no. 1, pp. 112-123, Jan. 2021.

[3]. M. Rostami, F. Koushanfar and R. Karri, "A Primer on Hardware Security: Models, Methods, and Metrics," in *Proceedings of the IEEE,* vol. 102, no. 8, pp. 1283-1295, Aug. 2014.

• The Proposed Methodology

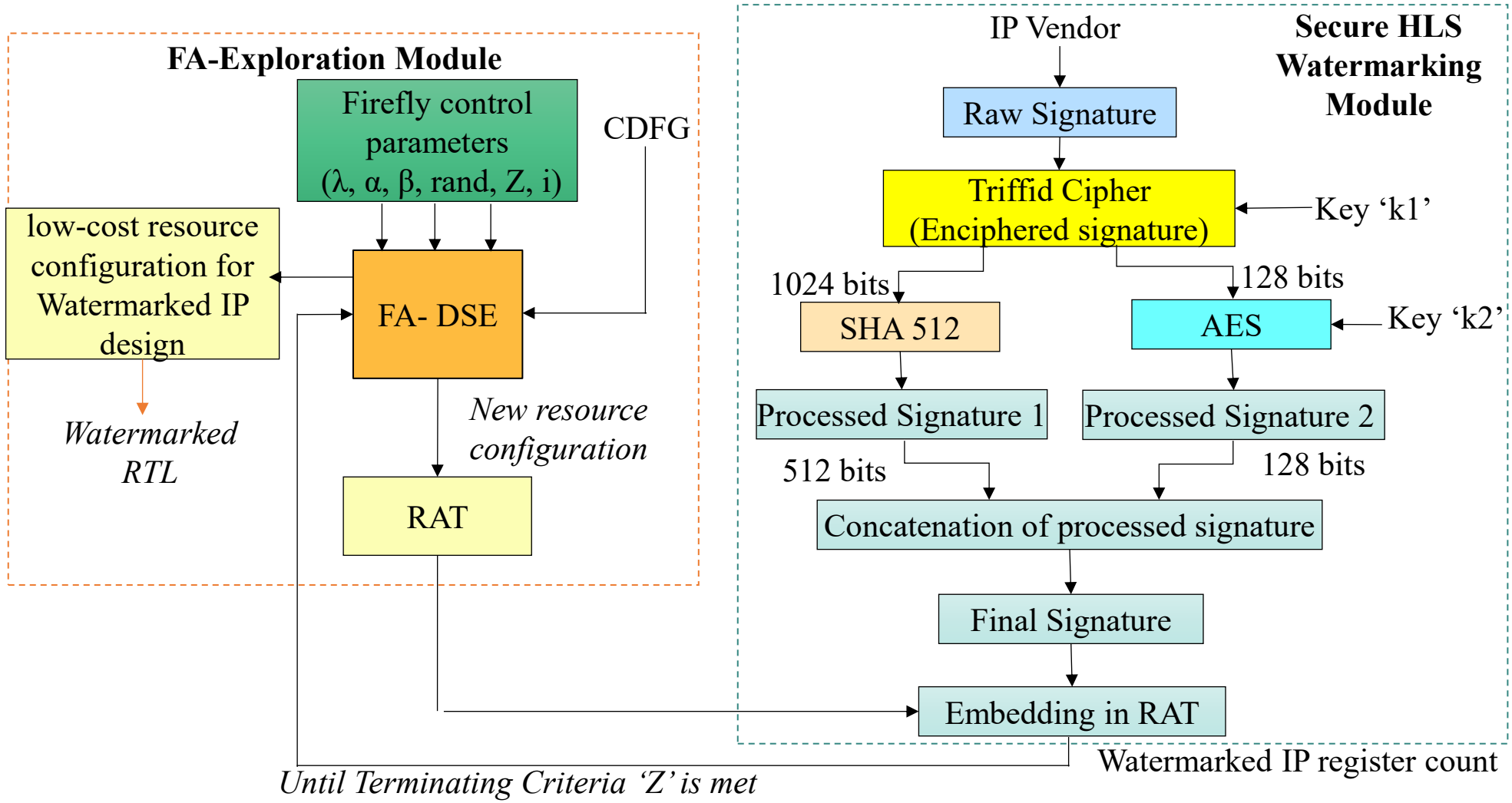


Fig. 1. Proposed secure and optimized HLS watermarking methodology

• The Proposed Methodology

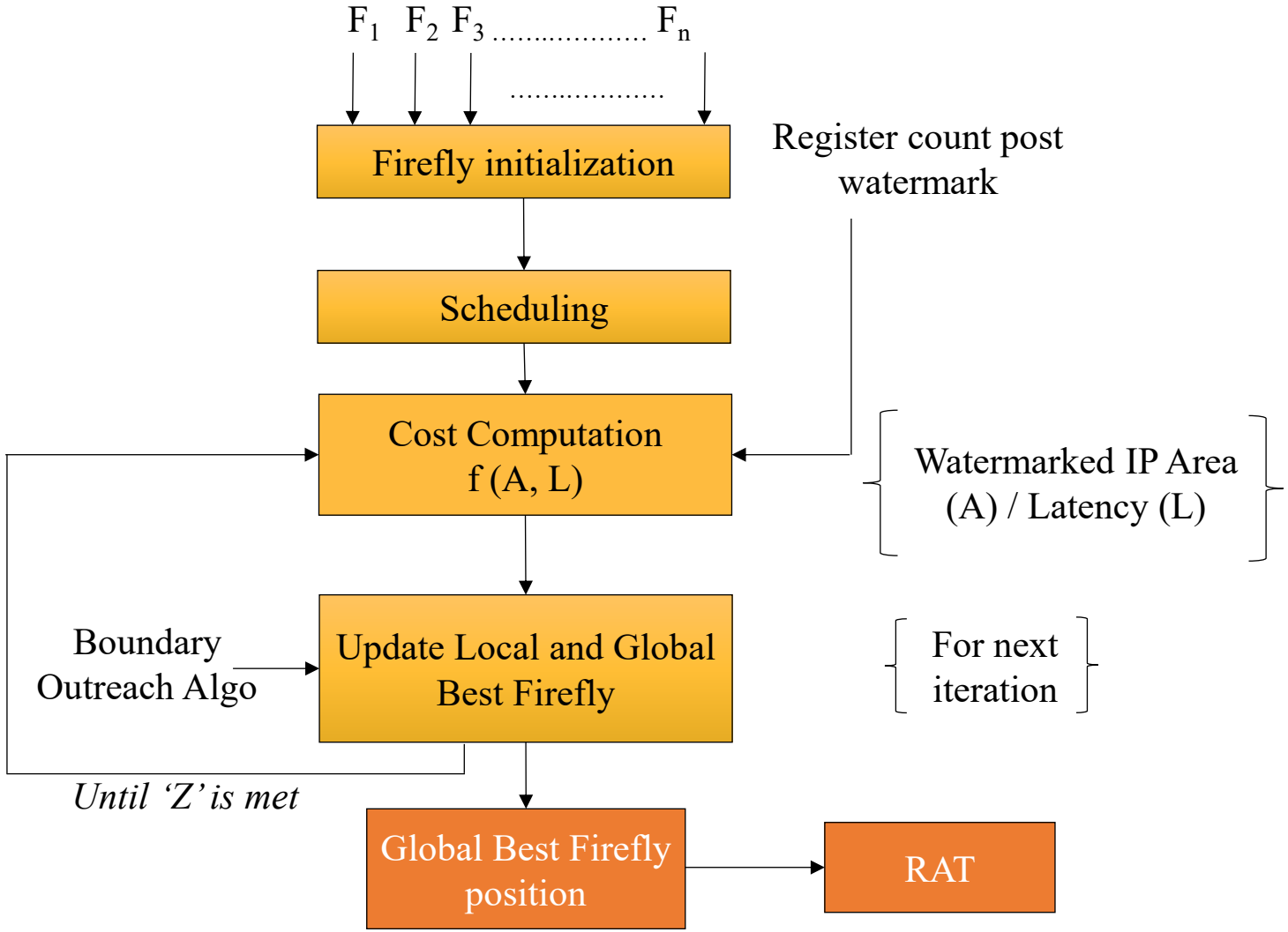


Fig. 2. The proposed FA-DSE integrated with the HLS IP watermarking framework

• The Proposed Methodology

The first firefly position is initialized as:

$F_1 = (S1_{min}, S2_{min}, \ldots\ldots\ldots\ldots, Sn_{min})$ (1)

The second firefly position is initialized as:

$F_2 = (S1_{max}, S2_{max}, S3_{max}, \ldots, Sn_{max})$ (2)

The third firefly's position is initialized as:

$F_3 = [((S1_{min}+S1_{max})/2), ((S2_{min}+S2_{max})/2), ((S3_{min}+S3_{max})/2),$
$((Sn_{min}+Sn_{max})/2_{max})]$ (3)

The rest of the fireflies (F_4, ..., F_n) are initialized as:

$M_{id} = (c+d)/2 \pm \alpha$ (4)

where 'c' is minimum resource value, 'd' is maximum resource value and 'α' is a random value between 'c' and 'd'.

• The Proposed Methodology

Each firefly position is updated using eqns. (5), (6), and (7) respectively.

$$Q_i^{t+1} = Q_i^t + \left(\beta\left(Q_j + Q_i\right) + \alpha\left(rand - \frac{1}{2}\right)\right) \quad (5)$$

where the attractiveness b is given by,

$$\beta = \beta_0 e^{-\lambda r^2 ij} \quad (6)$$

The distance between any two fireflies i and j, located at positions Qi and Qj, respectively, is calculated using the Cartesian distance, defined as:

$$r_{ij} = \left|Q_i - Q_j\right| = \sqrt{\sum_{k=1}^{d}(Q_{i,k} - Q_{j,k})^2} \quad (7)$$

The firefly positions (F_1,F_2,…,F_n) are utilized for scheduling of CDFG. The scheduled information, along with the register count after watermarking, is employed to compute the cost. The cost (fitness) function comprises of the watermarked IP area (A) and latency (L) as shown in eqn. (8).

$$C_f = 0.5 * \left(\frac{A_w}{A_{max}}\right) + 0.5 * \left(\frac{L_w}{L_{max}}\right) \quad (8)$$

• The Proposed Methodology

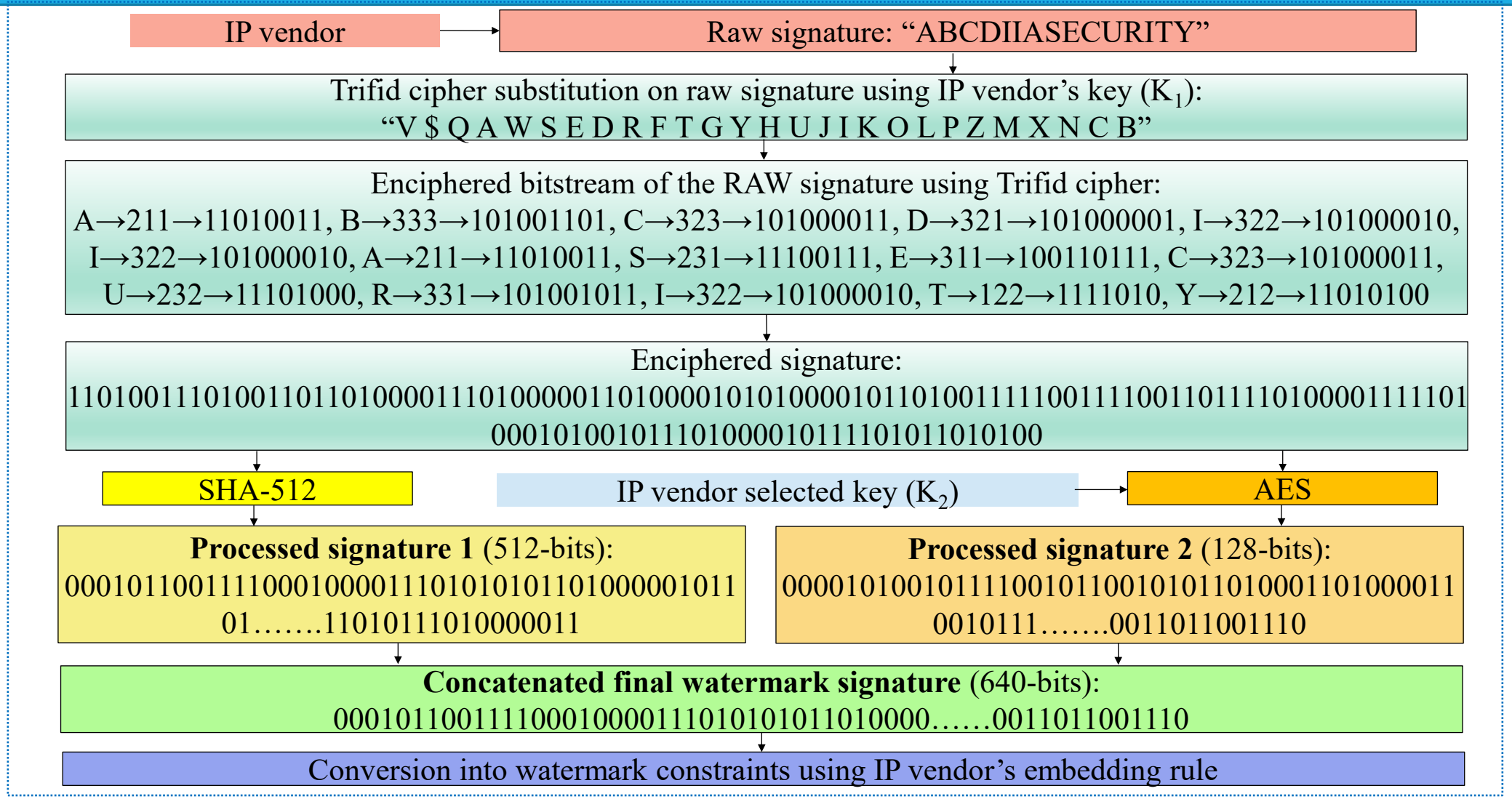


Fig. 3: Demonstration of the proposed approach

• The Proposed Methodology

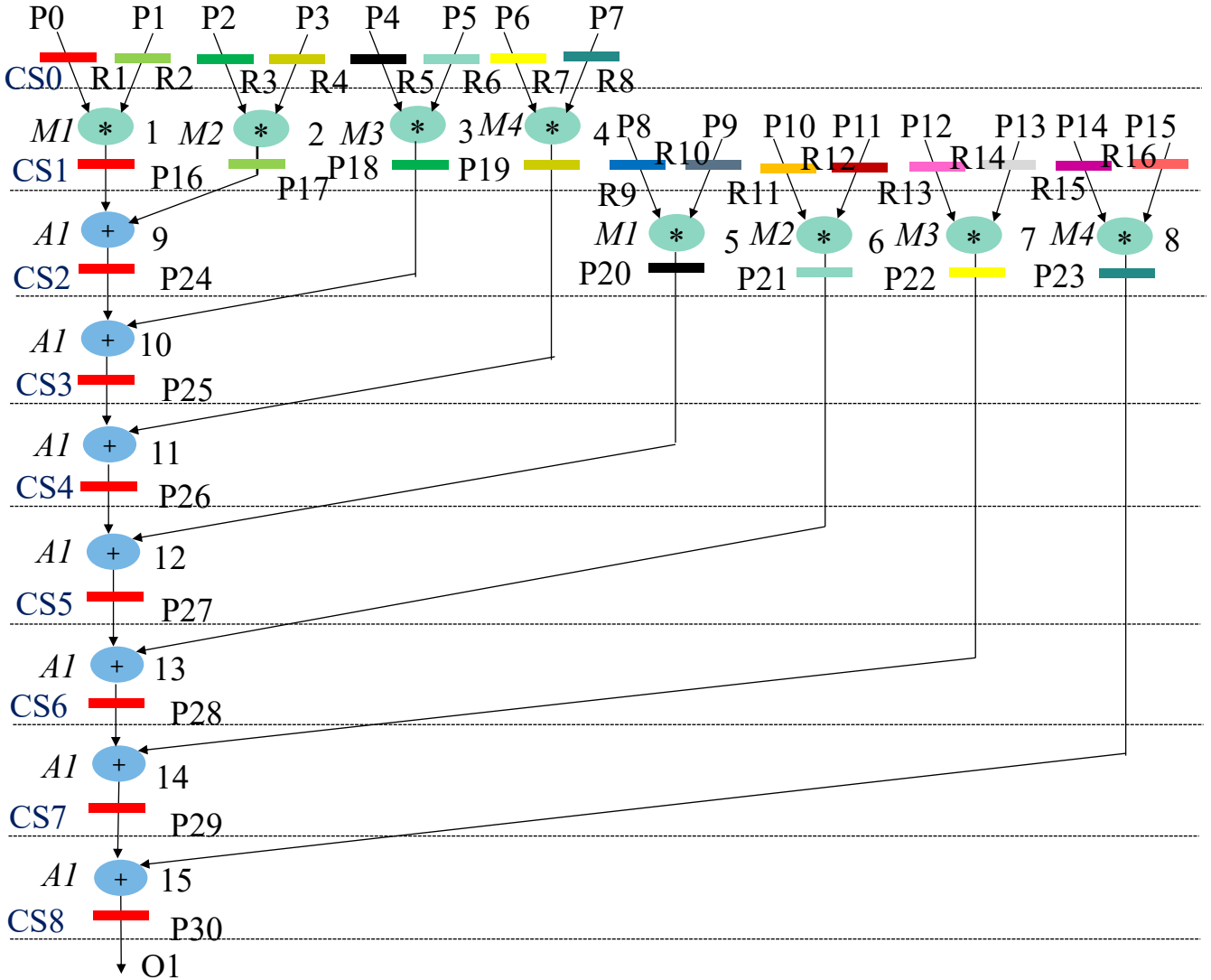


Fig. 4: SDFG of 8-point DCT with 1A (+) and 4M (*)

• Results and Analysis

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16
CS0	P0	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15
CS1	~~P16~~ **P19**	~~P17~~	~~P18~~	~~P19~~ **P18**	-	**P16**	**P17**	-	P8	P9	P10	P11	P12	P13	P14	P15
CS2	~~P24~~ **P19**	**P24**	~~P18~~	~~P19~~ **P18**	~~P20~~	~~P21~~	~~P22~~	~~P23~~	-	-	**P21**	-	**P23**	**P20**	-	**P22**
CS3	~~P25~~ **P19**	-	-	~~P19~~	~~P20~~	~~P21~~	~~P22~~	~~P23~~	**P25**	-	**P21**	-	**P23**	**P20**	-	**P22**
CS4	~~P26~~	-	-	-	~~P20~~	~~P21~~	~~P22~~	~~P23~~	-	**P26**	**P21**	-	**P23**	**P20**	-	**P22**
CS5	~~P27~~	-	**P27**	-	-	~~P21~~	~~P22~~	~~P23~~	-	-	**P21**	-	**P23**	-	-	**P22**
CS6	~~P28~~	-	-	-	-	-	~~P22~~	~~P23~~	-	-	-	**P28**	**P23**	-	-	**P22**
CS7	~~P29~~	-	-	-	**P29**	-	-	~~P23~~	-	-	-	-	**P23**	-	-	-
CS8	~~P30~~	-	-	-	-	-	-	**P30**	-	-	-	-	-	-	-	-

Fig. 5: RAT for 8-point DCT before & after embedding security constraints

Table 1: Comparison of the proposed approach with similar approaches

Security (Watermarking) approaches	T_T	D_E	C_P			
			8-Point DCT	Sharpening Filter	JPEG-CODEC	Cardiac Pacemaker
Proposed approach	4.56E+192	2.79E-104	4.94E-07	7.26E-05	9.1E-03	2.0E-07
Genomic Signature, 2024 [3]	3.4E+38	2.93E-39	2.58E-04	7.26E-05	3.9E-01	4.58E-02
Pragma based watermarking, 2021 [1]	NA	1.73E-18	1.02E-02	1.15E-03	5.94E-01	1.81E-01
Facial biometric, 2021 [2]	9.67E+24	NA	4.72E-03	3.67E-04	5.44E-01	1.35E-01
FSM watermarking, 2022 [4]	3.40E+38	2.93E-39	2.58E-04	7.26E-05	3.92E-01	4.58E-02

• The Proposed Methodology

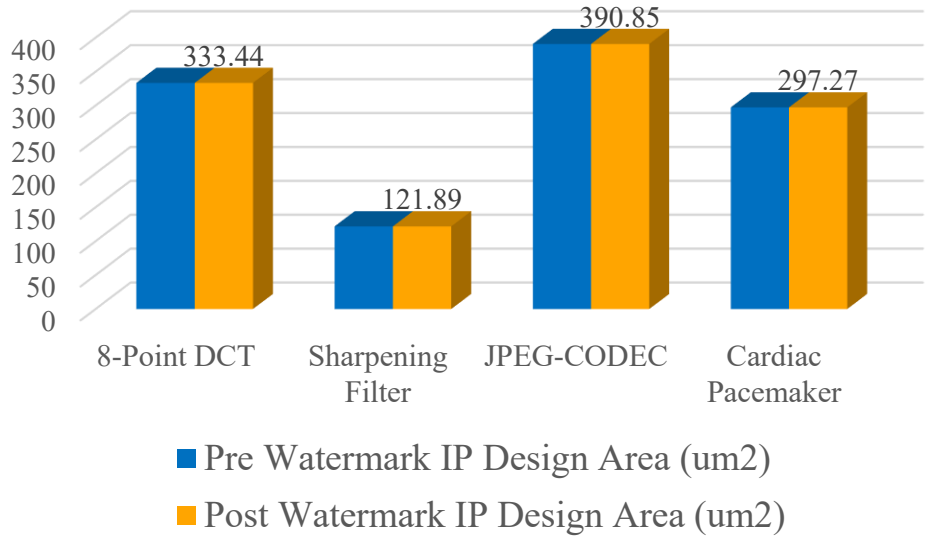


Fig. 6: Comparison of pre watermark IP area vs. post watermark IP area for different benchmarks
(indicating zero area overhead post embedding proposed watermark)

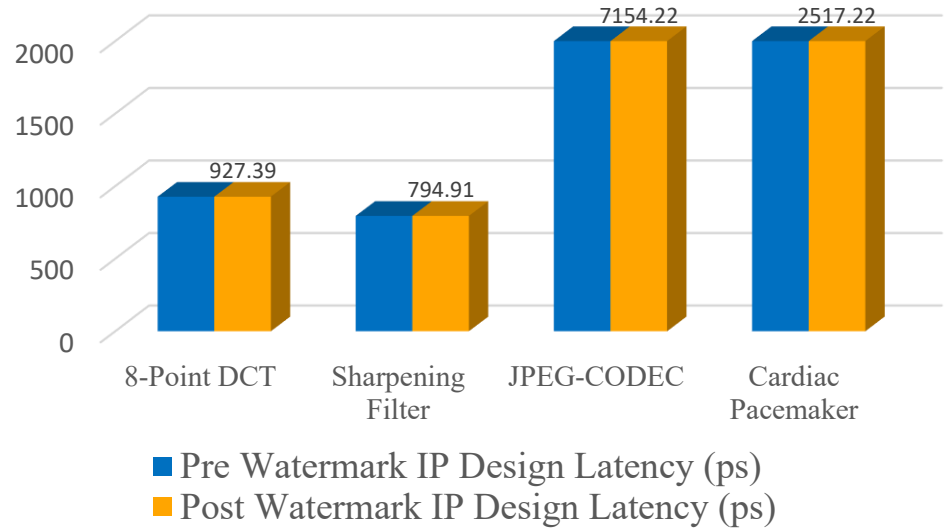


Fig. 7: Comparison of pre watermark IP latency vs. post watermark IP latency for different benchmarks
(indicating zero latency overhead post embedding proposed watermark)

Table 2: The convergence time and exploration time of the proposed DSE based watermarking approach

Benchmarks	Convergence time	Exploration time
8-Point DCT	0.103 sec	0.944 sec
Sharpening Filter	0.002 sec	0.305 sec
JPEG-CODEC	13.797 sec	82.999 sec
Cardiac Pacemaker	0.302 sec	3.906 sec

References

[1] J. Chen and B. C. Schafer, "Watermarking of Behavioral IPs: A Practical Approach," Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, pp. 1266-1271, 2021.
[2] A. Sengupta and M. Rathor, "Facial Biometric for Securing Hardware Accelerators," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 29, no. 1, pp. 112-123, Jan. 2021.
[3] A. Sengupta, V. Chourasia and A. K. Singh, "Gen-Sign: HLS Based Watermarking Using IP Vendor's Feistel Cipher Encrypted Genomic Signature for Protecting CNN and Image Processing Filter Cores Against Piracy," IEEE International Symposium on Smart Electronic Systems (iSES), New Delhi, India, pp. 128-133, 2024.
[4] R. Karmakar, S. S. Jana and S. Chattopadhyay, "A Cellular Automata Guided Finite-State-Machine Watermarking Strategy for IP Protection of Sequential Circuits," IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 2, pp. 806-823, 1 April-June 2022.
[5] Express Benchmark Suite, University of California Santa Barbara (UCSB), http://www.ece.ucsb.edu/EXPRESS/benchmark/, Sep. 2025.
[6] Silvaco's open cell library [Online], Available: https://si2.org/open-cell-and-free-pdk-libraries/, accessed on Sep. 2025.
[7] M. Potkonjak, "Methods and systems for the identification of circuits and circuit designs," US Patent, US7017043B1, 2006.
[8] M. Rostami, F. Koushanfar and R. Karri, "A Primer on Hardware Security: Models, Methods, and Metrics," Proceedings of the IEEE, vol. 102, no. 8, pp. 1283-1295, Aug. 2014.
[9] B. C. Schafer and Z. Wang, "High-Level Synthesis Design Space Exploration: Past, Present, and Future," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 39, no. 10, pp. 2628-2639, Oct. 2020.
[10] M. Rostami, F. Koushanfar and R. Karri, "A Primer on Hardware Security: Models, Methods, and Metrics," in Proceedings of the IEEE, vol. 102, no. 8, pp. 1283-1295, Aug. 2014.
[11] A. Sengupta and S. Bhadauria, "Exploring low cost optimal watermark for reusable IP cores during high level synthesis," IEEE Access, vol. 4, pp. 2198–2215, 2016.
[12] M. Rathor and G. P. Rathor, "Hard-Sign: A Hardware Watermarking Scheme Using Dated Handwritten Signature," IEEE Design & Test, vol. 41, no. 2, pp. 75-83, April 2024.
[13] R. Karmakar and S. Chattopadhyay, "Hardware IP Protection Using Logic Encryption and Watermarking," IEEE International Test Conference (ITC), Washington, DC, USA, 2020.
[14] A. -A. Koufopoulou, A. Papadimitriou, A. Pikrakis, M. Psarakis and D. Hely, "On the Prediction of Hardware Security Properties of HLS Designs Using Graph Neural Networks," IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Juan-Les-Pins, France, pp. 1-6, 2023.
[15] L. Collini, J. Ah-Kiow, C. Pilato, R. Karri and B. Tan, "Using Static Analysis for Enhancing HLS Security," IEEE Embedded Systems Letters, vol. 16, no. 2, pp. 166-169, June 2024.

THANK YOU