HLS driven Hybrid GA-PSO for Design Space Exploration of Optimal Palmprint Biometric based IP Watermark and Loop Unrolling Factor

Presented in IEEE-iSES 2024

Anirban Sengupta, Vishal Chourasia and Nitish Kumar, "HLS driven Hybrid GA-PSO for Design Space Exploration of Optimal Palmprint Biometric based IP Watermark and Loop Unrolling Factor," IEEE International Symposium on Smart Electronic Systems (iSES), New Delhi, India, 2024, pp. 134-139, 2024

INTRODUCTION

- High-Level Synthesis (HLS) is a method widely used to create optimized, cost-effective hardware designs tailored for data-intensive tasks.
- It allows designers to navigate complex tradeoffs, like area and latency, to develop efficient hardware architectures.
- In HLS, DSE involves balancing multiple objectives like design area, latency, hardware security, and cost.
- This exploration is complex, especially when considering trade-offs between orthogonal parameters such as security versus cost or area versus latency.

INTRODUCTION

- **Hardware Security**: concerns arise when using third-party IP cores, as vulnerabilities related to piracy and ownership claims may surface.
- Hardware watermarking provides a strong defense against these threats but often comes with increased design costs, area, and latency overhead.
- **Hybrid GA-PSO Framework**: The paper introduces a novel approach that uses a hybrid Genetic Algorithm and Particle Swarm Optimization (GA-PSO) framework to optimize both watermark embedding (for security) and loop unrolling factor, effectively addressing the tradeoff between watermark strength, area, latency, and cost during HLS.

PREVIOUS WORKS

- **Existing Security Methods**: Prior methods for securing hardware IP typically involve embedding secret signatures as watermarks to prevent piracy and ownership claims.
- **Limitations of Previous Approaches**: These techniques often lack robustness against brute force attacks and watermark collisions, leading to lower security and higher design costs.
- **Advantages of the Proposed Approach**: The new framework optimizes palmprint-based IP watermarks and loop unrolling factors, offering stronger security and cost-effective solutions compared to previous methods.

PROPOSED WORK : Flow Diagram and Genomic sequence

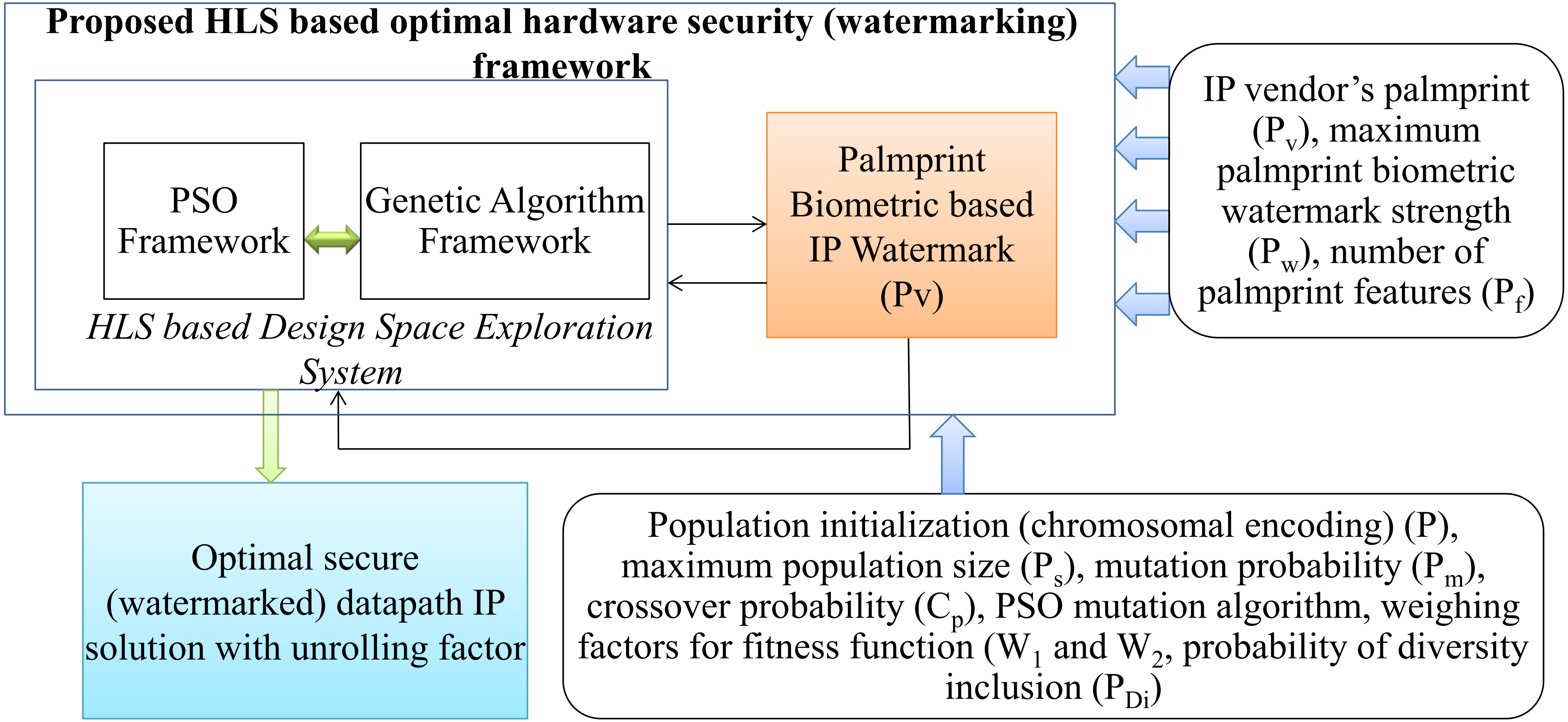

Fig. 1. Overview of proposed approach

PROPOSED WORK CONTINUE…

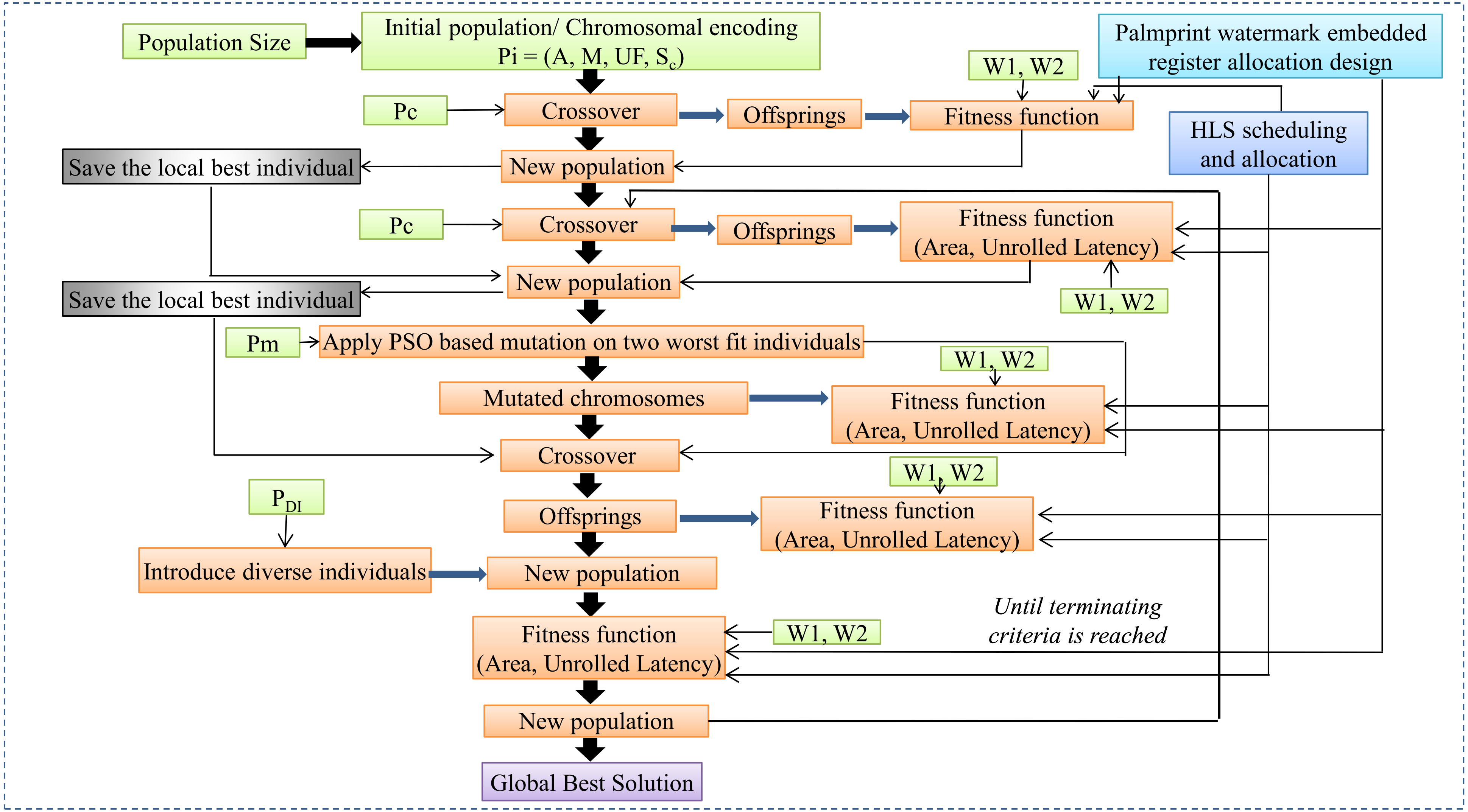

Fig. 2. HLS based Design Space Exploration System

PROPOSED WORK: Chromosomes and palmprint approach

Input block

P_1= A_{max} | M_{max} | UF_{max} | SC_{max} (Max. values)

P_2= A_{min} | M_{min} | UF_{min} | SC_{min} (Min. values)

P_3= A_{avg} | M_{avg} | UF_{avg} | SC_{avg} (Avg. values)

P_4= A_{rnd} | M_{rnd} | UF_{rnd} | SC_{rnd} (Random values) b/w Min and Max

Fig. 3. Generation G0 Population Chromosomes

Populations	A	M	UF	Sc
P_1 and P_2: O_1	A_{max}	M_{max}	UF_{min}	SC_{min}
P_1 and P_3: O_2	A_{max}	M_{max}	UF_{avg}	SC_{avg}
P_1 and P_4: O_3	A_{max}	M_{max}	UF_{rnd}	SC_{rnd}
P_2 and P_1: O_4	A_{min}	M_{min}	UF_{max}	SC_{max}
P_2 and P_3: O_5	A_{min}	M_{min}	UF_{avg}	SC_{avg}
P_2 and P_4: O_6	A_{min}	M_{min}	UF_{rnd}	SC_{rnd}
P_3 and P_1: O_7	A_{avg}	M_{avg}	UF_{max}	SC_{max}
P_3 and P_2: O_8	A_{avg}	M_{avg}	UF_{min}	SC_{min}
P_3 and P_4: O_9	A_{avg}	M_{avg}	UF_{rnd}	SC_{rnd}
P_4 and P_1: O_{10}	A_{rnd}	M_{rnd}	UF_{max}	SC_{max}
P_4 and P_2: O_{11}	A_{rnd}	M_{rnd}	UF_{min}	SC_{min}
P_4 and P_3: O_{12}	A_{rnd}	M_{rnd}	UF_{avg}	SC_{avg}

Fig. 4. Generation 1 Populations Chromosomes

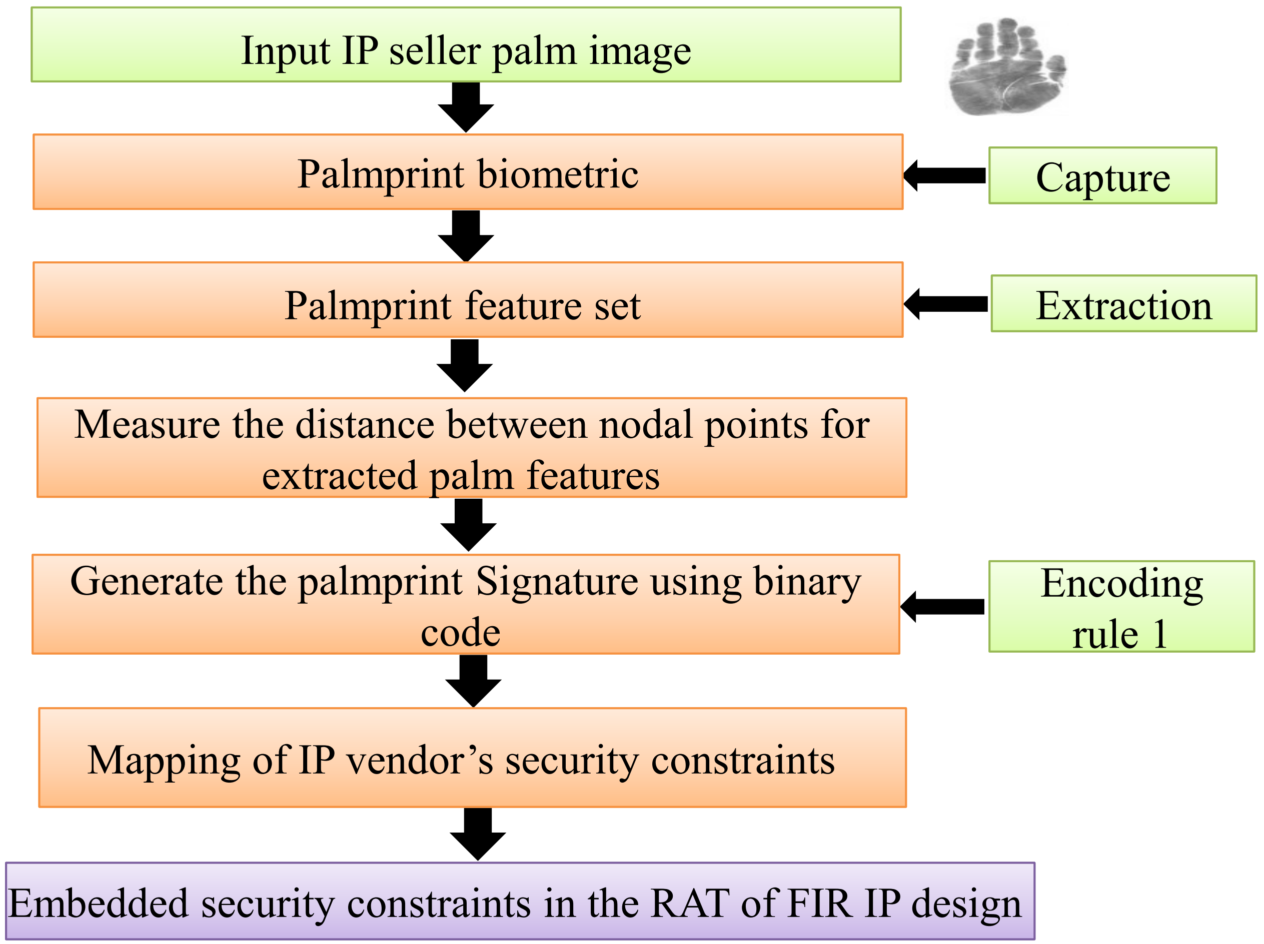

Fig. 5. Proposed IP seller palmprint approach

PROPOSED WORK: FIR SDFG and RAT

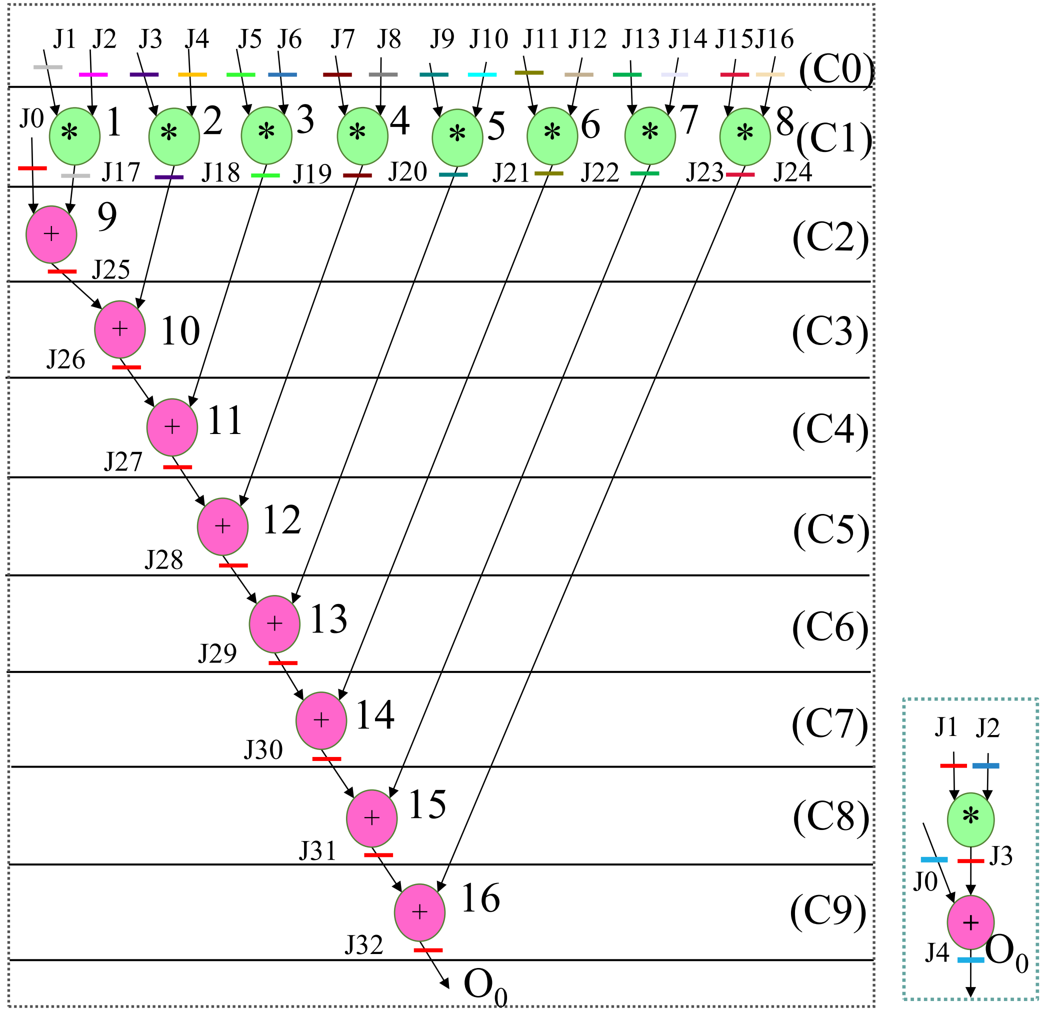

Fig. 6. Scheduled DFG using 8M,4A, UF8 and 1M,1A UF1

TABLE 1. RAT BEFORE AND AFTER EMBEDDING PROPOSED PALMPRINT BIOMETRIC WATERMARK CONSTRAINTS

Registers	Red(R)	Silver(S)	Purple(P)	Indigo(I)	Orange(O)	Lime(LI)	Blue(B)	Maroon(M)	Gray(GY)	Teal(T)	Aqua(A)	Olive(OL)	Khaki(K)	Green(G)	Lavender(L)	Crimson(C)	Wheat(W)
CO		J1	J2	J3	J4	J5	J6	J7	J8	J9	J10	J11	J12	J13	J14	J15	J16
C1	J0	J17		J18		J19		J20		J21		J22		J23		J24	
C2	~~J25~~	J25		J18		J19		J20		J21		J22		J23		J24	
C3	~~J26~~	J26				J19		J20		J21		J22		J23		J24	
C4	~~J27~~	J27						J20		J21		J22		J23		J24	
C5	~~J28~~	J28								J21		J22		J23		J24	
C6	~~J29~~	J29										J22		J23		J24	
C7	~~J30~~	J30												J23		J24	
C8	~~J31~~	J31														J24	
C9	~~J32~~	J32															

RESULT AND ANALYSIS

TABLE 2. SENSITIVITY ANALYSIS FOR FIR FILTERS FOR PROPOSED

Bench-marks	P=4		P=6		P=8	
	Rgb	C_F	Rgb	C_F	Rgb	C_F
8 Tap	[2,2,4,140]	-0.21	[2,2,2,140]	-0.21	[1,2,2,154]	-0.23
20 Tap	[3,4,15,150]	-0.29	[1,4,10,161]	-0.28	[1,5,10,161]	-0.28
60 Tap	[1,5,1,173]	-0.36	[3,5,3,172]	-0.36	[3,6,40,152]	-0.33
100 Tap	[1,7,62,144]	-0.38	[1,7,20,156]	-0.37	[1,7,40,140]	-0.38

TABLE 3. PARETO OPTIMAL SET GENERATION OF THE PROPOSED

Benchmarks	P=4	P=6	P=8
8 Tap FIR	233	264	178
20 Tap FIR	406	343	391
60 Tap FIR	503	719	471
100 Tap FIR	565	1088	1036

TABLE 4. CONVERGENCE ANALYSIS OF PROPOSED APPROACH

Benchmarks	P=4		P=6		P=8	
	Ic	Tc(ms)	Ic	Tc(ms)	Ic	Tc(ms)
8 Tap FIR	G5	170.64	G7	413.79	G1	69.62
20 Tap FIR	G9	705.73	G5	519.28	G3	398.65
60 Tap FIR	G15	3226.50	G11	2355.0	G5	1013.27
100 Tap FIR	G11	2807.86	G19	8519.4	G25	13692.03

RESULT AND ANALYSIS

TABLE 5. PC AND TT COMPARISON WRT IP SELLER'S WATERMARK

Bench marks	Pre-embedding registers	Proposed approach Pc	Proposed approach TT	Physical level watermark [3]		Multilevel Watermarking [4]		Facial Biometric [5]		Automated Watermarking [6]		Dynamic IP Watermarking [7]	
				Pc	TT	Pc	TT	Pc	TT	Pc	TT	Pc	TT
8 tap FIR filter	17	8.81E-5	2.99E+73	6.15E-1	256	4.27E-1	16384	6.52E-3	9.67E+24	2.63E-2	1.52E+18	4.26E-4	3.40E+38
20 tap FIR filter	41	1.87E-2	6.55E+76	8.20E-1	256	7.07E-1	16384	1.28E-1	9.67E+24	2.27E-1	1.52E+18	4.26E-4	3.40E+38
60 tap FIR filter	121	2.37E-1	3.48E+82	9.35E-1	256	8.90E-1	16384	5.02E-1	9.67E+24	6.07E-1	1.52E+18	4.26E-4	3.40E+38
100 tap FIR filter	201	4.59E-1	2.69E+74	9.60E-1	256	9.32E-1	16384	6.61E-1	9.67E+24	7.41E-1	1.52E+18	4.26E-4	3.40E+38

RESULT AND ANALYSIS : Evaluation parameters

- **Tamper Tolerance :**

$$\mathbf{TT} = (V)^r$$

Where, V and r corresponds to types of watermark signature bits and generated watermarking strength of the corresponding security approach.

- **Probability of Coincidence :**

$$\mathbf{PC} = \left(1 - \frac{1}{C}\right)^r$$

Where, C corresponds to number of registers in the baseline design (pre-watermark embedding). The computed PC values of the proposed approach, corresponding to different filter designs is presented in Table 6.

TABLE 6. PROPOSED TT AND PC ANALYSIS

Benchmarks	**Register (c)**	**Pc**	**TT**
8 Tap FIR	17	8.81E-5	2.99E+73
20 Tap FIR	41	1.87E-2	6.55E+76
60 Tap FIR	121	2.37E-1	3.48E+82
100 Tap FIR	201	4.59E-1	2.69E+74

REFERENCE

[1] Anirban Sengupta, Reza Sedaghat, Zhipeng Zeng, "Rapid Design Space Exploration for multi parametric optimization of VLSI designs", Proc of 2010 IEEE International Symposium on Circuits and Systems (ISCAS), Paris, France, pp: 3164-3167, 2010.

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

[3] A. Sengupta and M. Rathor, "Enhanced Security of DSP Circuits Using Multi-Key Based Structural Obfuscation and Physical-Level Watermarking for Consumer Electronics Systems," IEEE Trans. on Consumer Electronics, vol. 66 (2), pp. 163-172, 2020.

[4] D. Roy and A. Sengupta, "Multilevel Watermark for Protecting DSP Kernel in CE Systems" in IEEE Consumer Electronics Magazine, vol. 8 (2), pp. 100-102, 2019.

[5] A. Sengupta, R. Chaurasia "Secured Convolutional Layer IP Core in Convolutional Neural Network using Facial Biometric", IEEE Trans. on Consumer Electronics, Volume: 68, Issue: 3, Aug 2022, pp. 291-306.

[6] A. Sengupta, D. Roy, "Automated low cost scheduling driven watermarking methodology for modern CAD high-level synthesis tools", Elsevier J. Advances in Engineering Software, vol 110, 2017, pp 26-33.

[7] F. Koushanfar, I. Hong, M. Potkonjak "Behavioral Synthesis Techniques for Intellectual Property Protection", ACM Transactions on Design Automation of Electronic Systems, Volume 10, Issue 3, pp 523–545

[8] Vipul Kumar Mishra, Anirban Sengupta, "MO-PSE: Adaptive Multi Objective Particle Swarm Optimization Based Design Space Exploration in Architectural Synthesis for Application Specific Processor Design", El sevier Journal on Advances in Engineering Software, Volume 67, January 2014, pp. 111-124.

Thank You!