HLS Based Hardware Watermarking of Blur, Embossment and Sharpening Filters Using Fused Ocular Biometrics and Digital Signature

Presented in IEEE 37th International System-on-Chip Conference (SOCC)

Vishal Chourasia, Anirban Sengupta and Rrahul Chaurasia, "HLS based Hardware Watermarking of Blur, Embossment and Sharpening Filters Using Fused Ocular Biometrics and Digital Signature," IEEE 37th International System-on-Chip Conference (SOCC), Dresden, Germany, pp. 143-148, 2024.

INTRODUCTION

- Need of reusable intellectual property (IP) core.
- Importance of HLS in secure IP design.
- Why securing image filter ?
- Globalization of design supply chain.
- Limitation of traditional watermarking method.

Fig. 1 : Hardware (IC) design process

PREVIOUS WORKS

Sr. No.	Existing Work	Technique Used	Remarks
1.	J. Chen et. al., [1] (2021)	presented a watermarking technique through functional unit (FU) binding	however, [1] imposes significant design overhead while embedding even a smaller size ASCII code driven watermark key as compare to proposed approach.
2.	F. Koushanfar et al. [4] (2005)	auxiliary signature Variables-based Watermarking	[4] they are capable of generating digital evidence of low strength and also incurs design overhead, unlike the proposed approach.
3.	E. Castillo et. al., [5] (2008)	automatic signature insertion strategy	[5] presents strategy for generating watermarked design corresponding to combinational logic patterns.

NOVEL CONTRIBUTIONS

- This work introduces a hardware watermarking framework that uses an IP vendor's ocular biometrics and encoded digital signature to enhance IP security, particularly for piracy detection and verification of IP ownership.
- The framework utilizes HLS-based ocular biometric watermarking, which maps critical ocular features of the IP vendor into covert, imperceptible watermark constraints, without adding significant design cost overhead.
- Experimental results show that this approach achieves higher robustness in tamper tolerance and a lower probability of coincidence compared to recent watermarking techniques, with secure digital image filters embedded at the register transfer level.

THREAT MODEL

IP Piracy

IP Counterfeiting: Copied IP design under the same brand name by an attacker.

IP Cloning: Copied IP design under a different brand name by an attacker.

Presence of malicious logic (Hardware Trojans): Counterfeited IPs are not rigorously tested as genuine ones. Therefore, it may contain malicious logic which can cause safety hazards for both the SoC integrator and the end consumer.

PROPOSED WORK : Design Flow

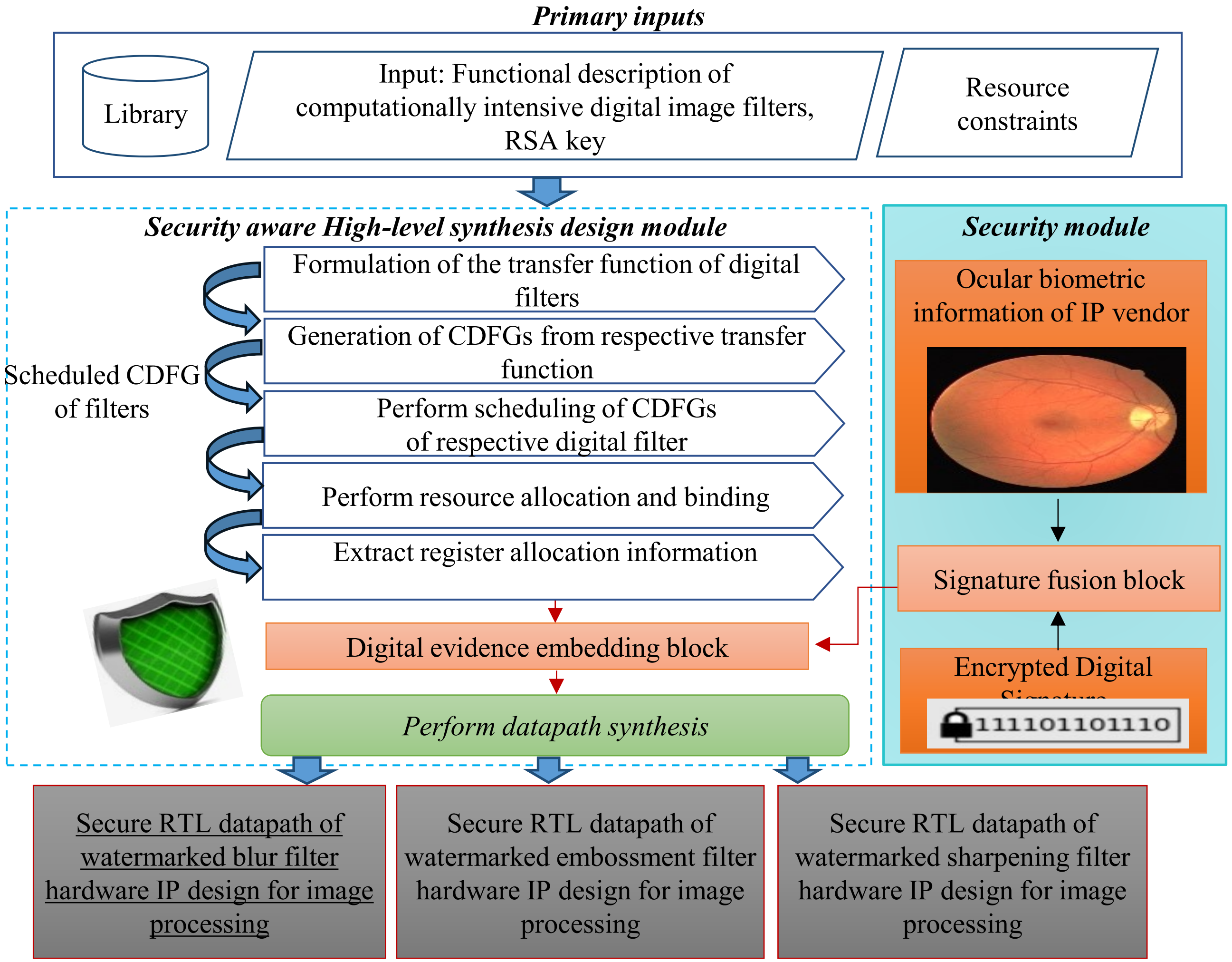

Fig. 2. Proposed HLS based design flow for generating ocular biometric based watermarked IP design

PROPOSED WORK : Watermark Generation

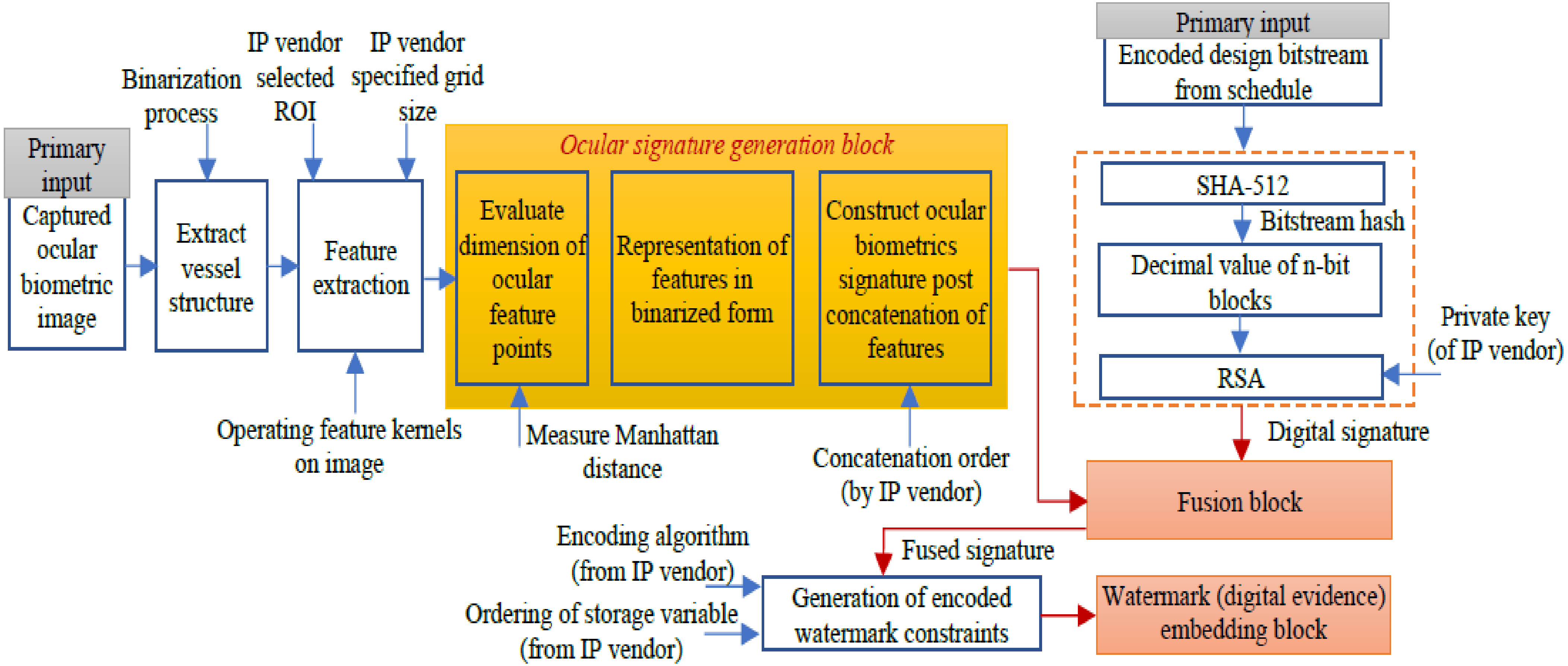

Fig. 3 Details of the proposed fused watermarking process with IP vendor’s ocular biometric and encoded hash

PROPOSED WORK : Automated Retinal Feature extraction

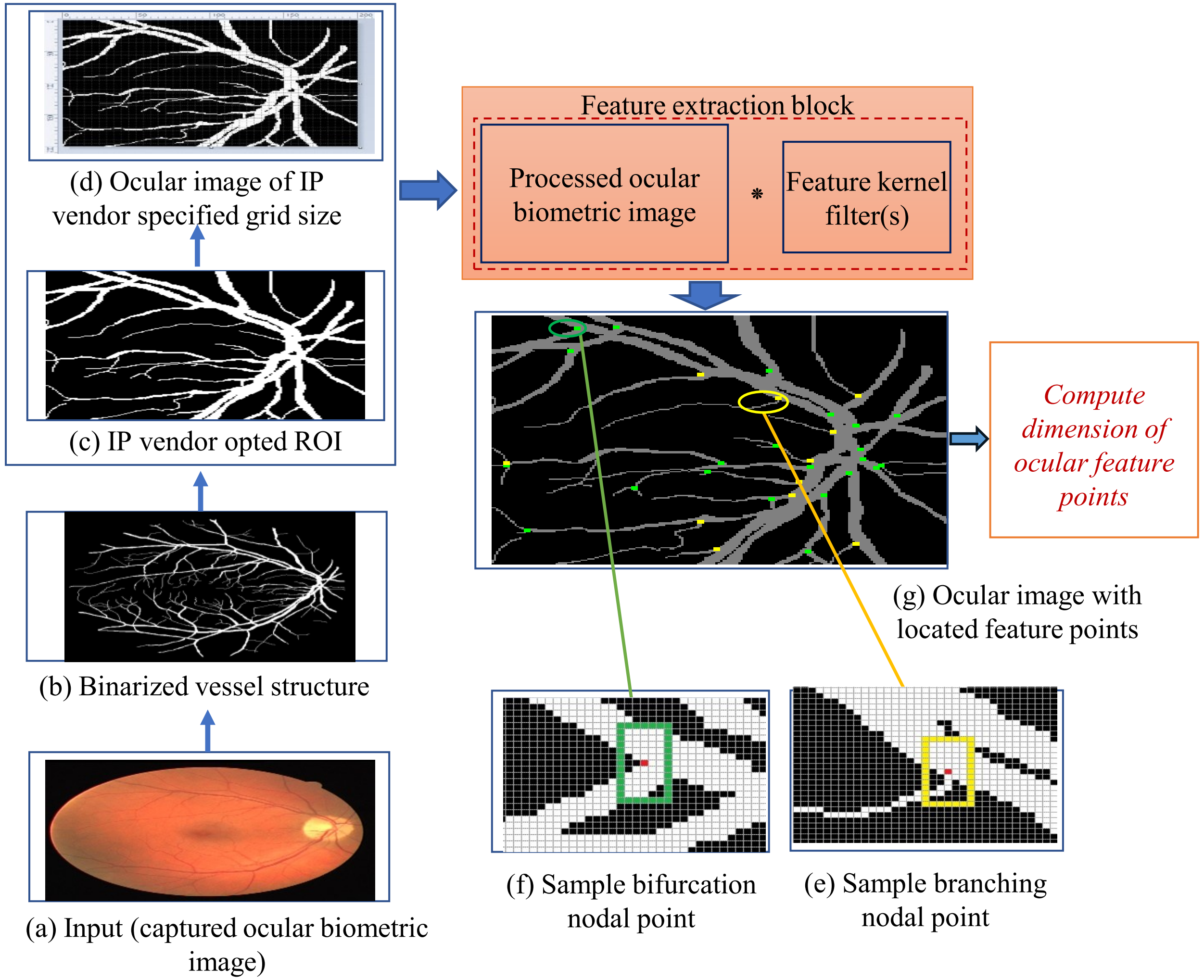

Fig. 4 Feature extraction from IP vendor's captured ocular biometric image

The generated ocular signature is: 110111.11100110011001100111100111.1100001010001111011------1101011.011010001111010111.

The encoded hash is generated post employing SHA-512 and RSA security modules. The generated encoded hash signature is: 1000000100000111111111011-----------1101011100010 (128 bits).

PROPOSED WORK: Schedule IP design

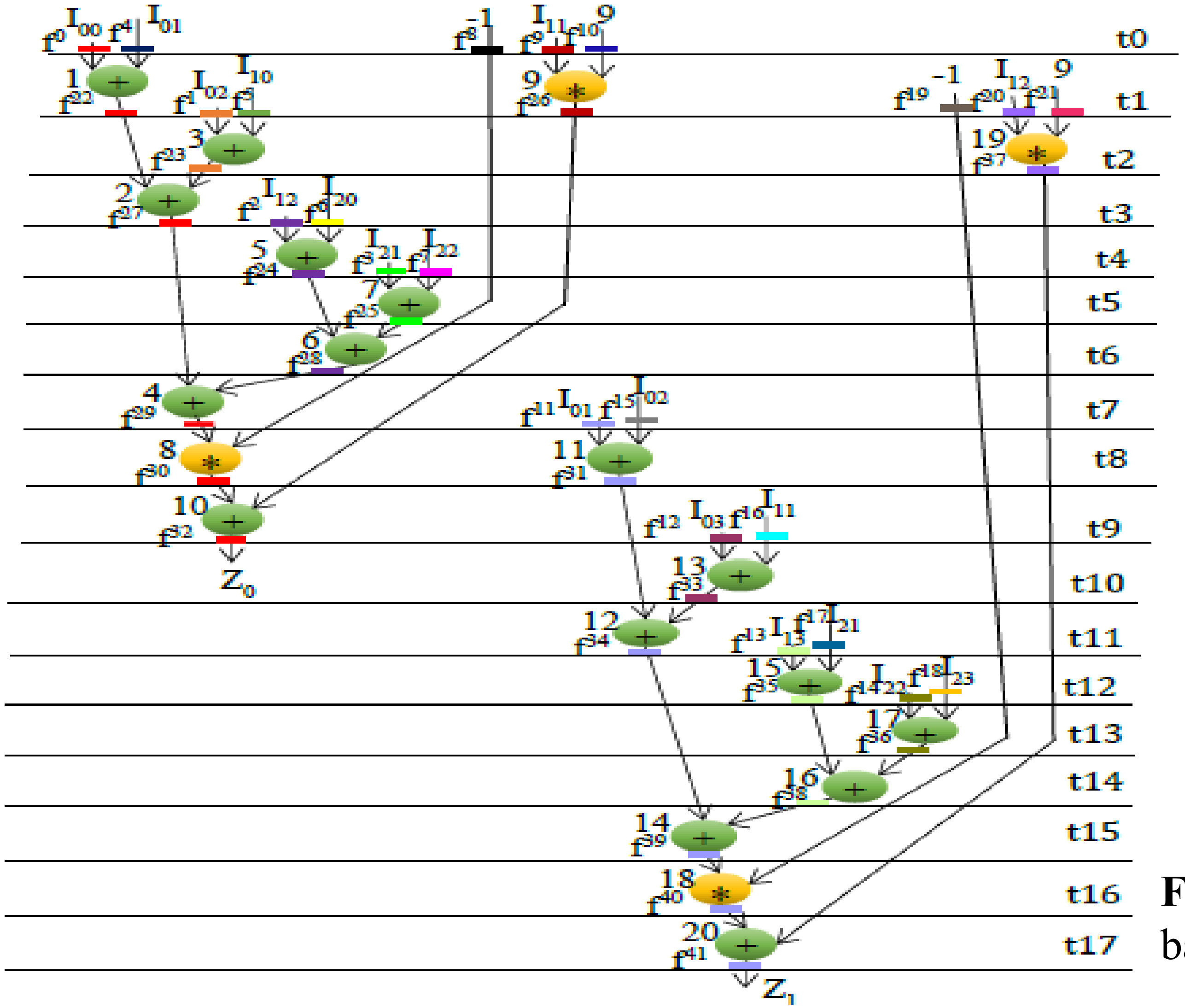

Fig. 5 Scheduled DFG of sharpening filter based on 1 adder and 1 multiplier

PROPOSED WORK: Encoding Rule and Watermark Constraints

- The encoding algorithm embeds fused watermark signature bits into watermark constraints as follows:

  - For bit ‘0’: Pair storage variables with <even-even> indices and alter the respective registers while avoiding conflicts.
  - For bit ‘1’: Pair storage variables with <odd-odd> indices.
  - For bit ‘.’: Pair storage variables with <zero-integer> indices.

- The watermark constraints generated using the encoding algorithm are as follows:

- For bit ‘0’- <f0,f2>, <f0,f4>, <f0,f6>,-----<f0,f40>, <f2,f4>, <f2,f6>,--

- For bit ‘1’-<f1,f3>, <f1,f5>, <f1,f7>, <f1,f9>---<f1,f41>, <f3,f5>,---

- For bit ‘.’-<f0,f1>,<f0,f3>,<f0,f5>--------.

PROPOSED WORK: Watermark Embedding Process during RA

TABLE 1. REGISTER ALLOCATION INFORMATION OF SHARPENING FILTER DESIGN POST EMBEDDING OCULAR WATERMARK (PARTIAL VIEW)

Registers	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
t0	f^{0}	f^{4}							f^{8}	f^{9}	f^{10}											
t1	f^{22}	f^{22}	f^{1}	f^{5}					f^{8}	f^{26}	-									f^{19}	f^{20}	f^{21}
t2	f^{22}	f^{22}	f^{23}	-					f^{8}	f^{26}	-									f^{19}	f^{37}	-
t3	f^{27}	-	-	-	f^{2}	f^{6}			f^{8}	f^{26}	-									f^{19}	f^{37}	-
t4	f^{27}	-	-	-	f^{24}	f^{24}	f^{3}	f^{7}	f^{8}	f^{26}	-									f^{19}	f^{37}	-
t5	f^{27}	-	-	-	f^{24}	f^{24}	f^{25}	-	f^{8}	f^{26}	-									f^{19}	f^{37}	-
t6	f^{27}	-	-	-	f^{28}	f^{28}	-	-	f^{8}	f^{26}	-									f^{19}	f^{37}	-
--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
t17	-	-	-	-	-	-	-	-	-	-	-	f^{41}	-	-	-	--	-	-	-	-	-	-

RESULT AND ANALYSIS

Evaluation parameters :

- **Tamper Tolerance :**

$$TT = (\psi)^{W_C}$$

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

- Design Cost :

$$C(R_D) = \theta 1 * \frac{Y_D}{Y_{max}} + \theta 2 * \frac{\mu_D}{\mu_{Max}}$$

Where, '*Rd*' denotes the resource constraints utilized during the scheduling of the design. λd and µd are representing the area and latency of the watermarked design, respectively, while λmax and µmax indicate the maximum area and latency. Additionally, ɵ1 and ɵ2 serve as weighing factors used to normalize both parameters in the cost function.

RESULT AND ANALYSIS

TABLE 2. VARIATION IN TT FOR THE PROPOSED APPROACH (OCULAR IMAGE_1)

#IP vendor selected features	Ocular signature strength	Digital Signature size(digits)	#constraints	TT
33	922	128	1050	9.4E+500
32	896	128	1024	3.7E+488
31	870	128	998	1.4E+476
30	844	128	972	5.7E+463

TABLE 3. VARIATION IN Zp FOR DIFFERENT OCULAR IMAGES CORRESPONDING TO DIFFERENT DIGITAL FILTERS

#IP vendor selected features	Ocular signature strength	Digital Signature size(digits)	#constraints	Z_P				TT
				Blur Filter	Vertical embossment filter	Horizontal embossment filter	Sharpening filter	
Ocular Image_1	922	128	1050	4.07E-24	7.23E-84	7.23E-84	6.11E-22	9.4E+500
Ocular Image_2	953	128	1081	8.30E-25	2.54E-86	2.54E-86	1.14E-22	5.8E+515
Ocular Image_3	958	128	1086	6.42E-25	1.02E-86	1.02E-86	1.14E-22	1.4E+518
Ocular Image_4	1141	128	1269	5.38E-29	3.30E-101	3.30E-101	2.30E-26	2.93E+605

RESULT AND ANALYSIS

TABLE 4:COMPARISON OF TT ACHIEVED USING PROPOSED APPROACH WITH RELATED APPROACHES [1]-[8]

Security Technique	TT
Proposed Approach	2.9E+605
[1]	2.3E+21
[2]	8.9E+161
[3]	1.9E+25
[4]	1.7E+72
[5]	1.4E+48
[6]	3.4E+38
[7]	1.6E+110
[8]	4.4E+248

RESULT AND ANALYSIS

TABLE 5. VARIATION IN Zp **FO**R DIFFERENT OCULAR IMAGES CORRESPONDING TO DIFFERENT DIGITAL FILTERS

#IP vendor selected features	Ocular signature strength	Digital Signature size(digits)	#const-raints	Z_P			
				Blur filter	Vertical embossment filter	Horizontal embossment filter	Sharpening filter
33	922	128	1050	4.07E-24	7.23E-84	7.23E-84	6.11E-22
32	896	128	1024	1.54E-23	8.18E-82	8.18E-82	2.04E-22
31	870	128	998	5.86E-23	9.48E-80	9.48E-80	6.87E-21
30	844	128	972	2.22E-22	1.08E-77	1.08E-77	2.30E-20

RESULT AND ANALYSIS

TABLE 6: COMPARISON OF *Zp* OF PROPOSED APPROACH WITH RELATED WORKS [1]-[8]

Framework	Proposed	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
	Z_P	Z_P	Z_P	Z_P	Z_P	Z_P	Z_P	Z_P	Z_P
Blur filter	5.38E-29	2.6E-2	1.0E-12	1.3E-2	4.5E-6	2.7E-4	1.4E-3	7.13E-3	3.9E-19
Vertical embossment filter	3.30E-101	2.3E-6	2.5E-43	2.2E-7	9.9E-20	2.1E-13	7.3E-11	5.1E-19	3.9E-66
Horizontal embossment filter	3.30E-101	2.3E-6	2.5E-43	2.2E-7	9.9E-20	2.1E-13	7.3E-11	5.1E-19	3.9E-66
Sharpening filter	2.30E-26	3.6E-2	1.3E-11	2.0E-2	1.4E-5	5.8E-5	2.5E-3	2.1E-5	2.0E-17

TABLE 7: DESIGN COST COMPARISON FOR THE PROPOSED METHODOLOGY (PRE AND POST EMBEDDING FUSED WATERMARK)

Filter Design	Pre-Embedding Design cost	Post-embedding Design Cost	% Overhead
Blur filter	0.682	0.62	0%
Vertical embossment filter	0.75	0.75	0%
Horizontal embossment filter	0.75	0.75	0%
Sharpening filter	0.685	0.685	0%

REFERENCE

[1] 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.
[2] R. Chaurasia and A. Sengupta, “Multi-cut based architectural obfuscation and handprint biometric signature for securing transient fault detectable IP cores during HLS,” *Integr. VLSI J*, Vol. 95, 2023.
[3] A. Sengupta and R. Chaurasia, “Secured Convolutional Layer IP Core in Convolutional Neural Network Using Facial Biometric,” *IEEE Trans. Consum. Electron*., vol. 68, no. 3, pp. 291-306, Aug. 2022.
[4] F. Koushanfar, I. Hong, and M. Potkonjak, “Behavioral synthesis techniques for intellectual property protection,” *ACM Trans. Design Autom. Electron. Syst*., vol. 10, no. 3, pp. 523–545, Jul. 2005.
[5] E. Castillo, L. Parrilla, A. Garcia, U. Meyer-Baese, G. Botella and A. Lloris, “Automated Signature Insertion in Combinational Logic Patterns for HDL IP Core Protection,” *2008 4th Southern Conference on Programmable Logic*, Bariloche, Argentina, 2008, pp. 183-186.
[6] R. Karmakar, S. S. Jana and S. Chattopadhyay, “A Cellular Automata Guided Finite-State-Machine Watermarking Strategy for IP Protection of Sequential Circuits,” *IEEE Trans. Emerg. Topics Comput*., vol. 10, no. 2, pp. 806-823, 1 April-June 2022.
[7] A. Sengupta, R. Chaurasia and T. Reddy, “Contact-Less Palmprint Biometric for Securing DSP Coprocessors Used in CE Systems,” *IEEE Trans. Consum. Electron*., vol. 67, no. 3, pp. 202-213, Aug. 2021. [8] M. Rathor and G. P. Rathor, "Hard-Sign: A Hardware Watermarking Scheme Using Dated Handwritten Signature," *IEEE Des. Test*, vol. 41, no. 2, pp. 75-83, April 2024.
[9] Anirban Sengupta, Prajwal Chandra, Ranjith Kumar, “Robust Digital Signature to Protect IP Core against Fraudulent Ownership and Cloning”, *Proc. of 9th IEEE International Conference on Consumer Electronics (ICCE)- Berlin*, 2019, pp. 122-124.
[10] Anirban Sengupta, Mahendra Rathor "Obfuscated Hardware Accelerators for Image Processing Filters - Application Specific and Functionally Reconfigurable Processors", *IEEE Trans. Consum. Electron.*, Volume: 66, Issue: 4, 2020, pp. 386-395.
[11] 15 nm open cell library. [Online], Available: https://si2.org/open-cell-library/, last accessed on Aug. 2023.

Thank You!