Fusing IP Vendor Palmprint Biometric with Encoded Hash for Hardware IP Core Protection of Image Processing Filters

Anirban Sengupta, Aditya Anshul, Sumer Thakur, Chirag Kothari "Fusing IP Vendor Palmprint Biometric with Encoded Hash for Hardware IP Core Protection of Image Processing Filters", Proceedings of 35th IEEE International Conference on Microelectronics (ICM), Abu Dhabi, Dec 2023, pp. 218-221

Image processing filters:

- Image processing filters are mainly used to suppress either the high frequencies in the image, *i.e.,* smoothing the image, or the low frequencies, and enhancing or detecting edges in the image.
- The main objective of image processing is to extract some useful information from an image.
- From detection and recognition of license plates of vehicles on tolls (character recognition), advanced medical imagery (image analysis), biometric fingerprinting, robotics vision, and military operations to car driving automation, image processing plays a crucial role everywhere.
- Due to globalization of design supply chain, the design process of these image processing filters as a dedicated intellectual property (IP) core involves various **hardware threats [1], [2].**

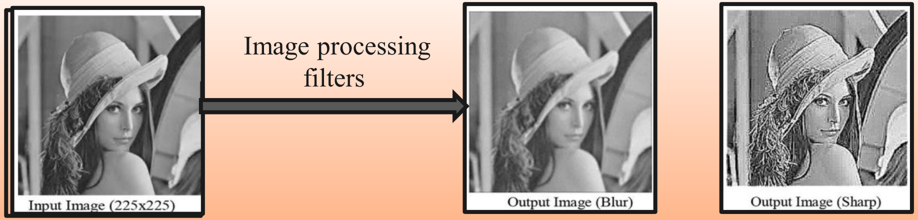


Figure 1: Image processing operations

Security Issues associated with image processing filter IP Cores [3]-[6]

IP Piracy

IP Counterfeiting: Selling different product under same brand name. Here, the counterfeited design (containing malicious logic) is sold under same brand name.

IP Cloning: Selling the cloned copy of the IP core under with different brand name.

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 hazard for both IP vendor and end consumer (such as leaking sensitive information, incorrect functional computation , wrong diagnosis of disease in case of medical imaging, loss of esteem for IP vendor, etc.

Fraudulent claim of IP ownership: An adversary tries to fraudulently claim the ownership of the IP.

Therefore, it is essential to secure these image processing filter IP cores from these hardware threats.

Related Work :

Sr. No.	Existing Work	Technique Used	Remarks
1.	Castillo *et. al.*, [5] (2008)	The paper [5] harnesses the power of MD5 and SHA1 to generate several blocks of signatures.	Fails to integrate a unique natural identity as a security parameter and leads to generation limited security constraints.
2.	F. Koushanfar, I. Hong, and M. Potkonjak [4] (2005)	Hardware watermarking using two-variable (0, 1) signature encoding process.	Weak watermarking mechanism due to involvement of only two variable signature encoding process. The watermark (original signature) inserted becomes vulnerable if relevant information (like signature size, digit encoding, and digit combination) gets leaked.
3.	(a) Sengupta and Rathor [2] (2021) (b) Sengupta and Chaurasia [3] (2021)	(a) Facial biometric [2] and (b) DNA biometric [3] based hardware security approach.	[2] provides inferior security due to the generation of lesser security constraints than proposed work. Further, [3] incurs greater computational complexity in signature generation process due to involvement of DNA sequencing apart from generation of lesser security constraints than the proposed approach.

Proposed Work

- This proposed work presents a novel hardware IP protection (IPP) approach as a detective countermeasure for nullifying an adversary's false claim of IP ownership, using the fusion of IP vendor's palmprint biometric and encoded hash.
- The proposed work presents the generation and embedding of secret security constraints (digital evidence) using an amalgamation of IP vendor's palmprint biometric and encoded hash.
- Further, the secret hardware security constraints are determined using obtained fused signature, which are embedded into the design of digital image filters IP cores using the register allocation table (RAT) framework of HLS process.
- The embedding of the IP seller's/Vendor's authentic fused signature into the design of digital image filters protects it from hardware security threats such as false claim of IP ownership and IP piracy.

Detailed flow diagram of the proposed approach

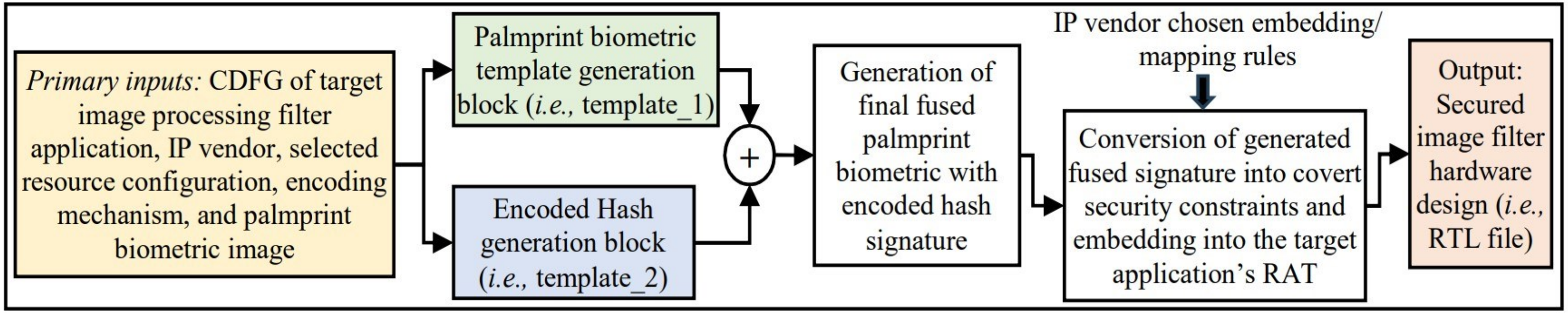
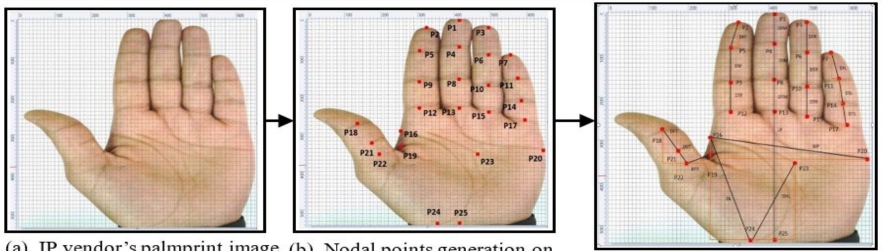


Figure 2: Flow diagram of the proposed hardware IP Protection (IPP) methodology

Details of Plamprint Biometric based hardware security approach for generating template_1



(a). IP vendor's palmprint image with grid size and spacing (b). Nodal points generation on palmprint image (c). Feature generation on palmprint image

Feature #	Feature name	Feature dimension	Binary representation
F1	DFT	64.03	1000000.000001111010111100001
F2	DSF	80	1010000
F3	DST	36.05	100100.00001100110011001101
F4	DSL	60.82	111100.11010001111010111
F5	DFR	70	1000110
F6	DL	260	100000100
F7	DTR	70	1000110
F8	DTF	70	1000110
F9	DSR	80	1010000
F10	DTL	50.99	110010.11111101011110000101
F11	DTT	63.24	111111.00111101011110000101
F12	DHL	210.95	11010010.1111001100110011
F13	DFM	70	1000110
F14	DFF	63.24	111111.00111101011110000101
F15	LP	300	100101100
F16	DFL	63.24	111111.00111101011110000101
F17	DSM	80	1010000
F18	DTM	80	1010000
F19	WP	393.19	110001001.00110000101000111101

(d). Features dimensions (magnitude) computation and its corresponding binary representation

(e). Generation of final palmprint biometric template post concatenation of all generated features as per IP vendor's chosen concatenation order (*i.e.*, template_1)

Figure 3: Generation of palmprint biometric template using IP vendor's palmprint biometric image

Advantage of palmprint biometric approach over other hardware security approaches

Advantages:

- The template generated using the original IP vendor palmprint is inherently unique, serving as a secret mark for the target hardware IP.
- Extracting palmprint signature is simpler compared to facial biometrics [2].
- Unlike facial biometrics [2], the palmprint biometric method exhibits more substantial feature variation, resulting in enhanced tamper tolerance.
- Furthermore, the palmprint-based approach boasts several advantages over contemporary techniques: it's contactless, secure from vulnerabilities, non-replicable (unlike stego-constraints and watermarking [4]), and doesn't rely on a secret key.
- Additionally, palmprint biometric depicts lesser complexity than DNA biometric [3].

Details of Encoded Hash based hardware security approach for generating template_2

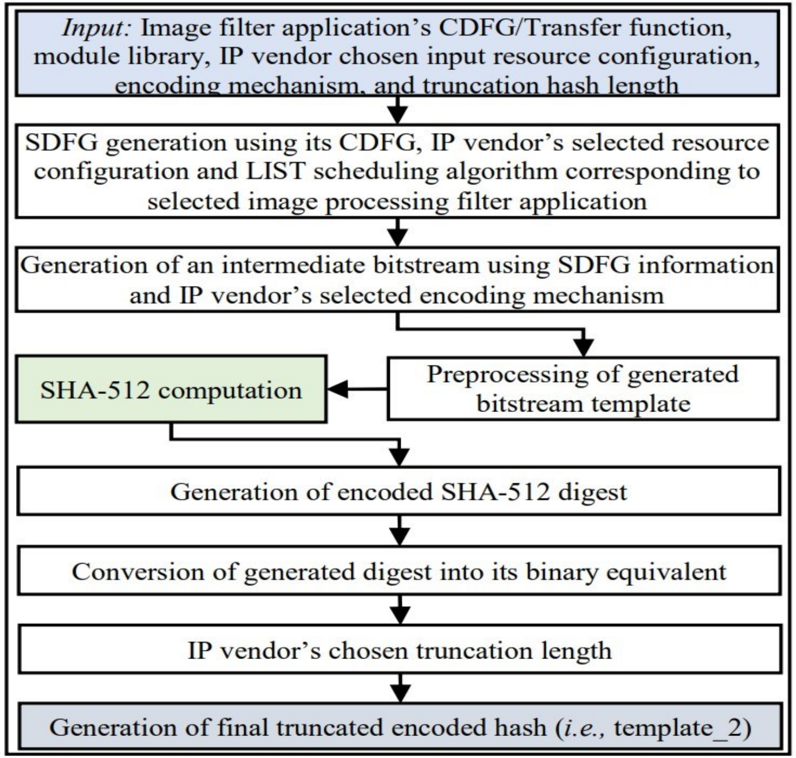


Figure 4: Generation of encoded hash

Generation of scheduled dataflow graph (SDFG) using mathematical function of Laplace Edge Detection (LED) image filter

$$Kernel_{Blur} = \left(\frac{1}{9}\right) * \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad Kernel_{laplace} = \begin{bmatrix} 0 & -1 & 0 \\ -1 & 4 & -1 \\ 0 & -1 & 0 \end{bmatrix} \quad Kernel_{Sharpening} = \begin{bmatrix} -1 & -1 & -1 \\ -1 & 9 & -1 \\ -1 & -1 & -1 \end{bmatrix}$$

$$H_0 = [(Q_{01}*(-1))] + [(Q_{10}*(-1)) + (Q_{11}*(4)) + (Q_{12}*(-1))] + [(Q_{21}*(-1))] \quad (1)$$

$$H_1 = [((Q_{02}*(-1))] + [(Q_{11}*(-1)) + (Q_{12}*(4)) + (Q_{13}*(-1))] + [(Q_{22}*(-1))] \quad (2)$$

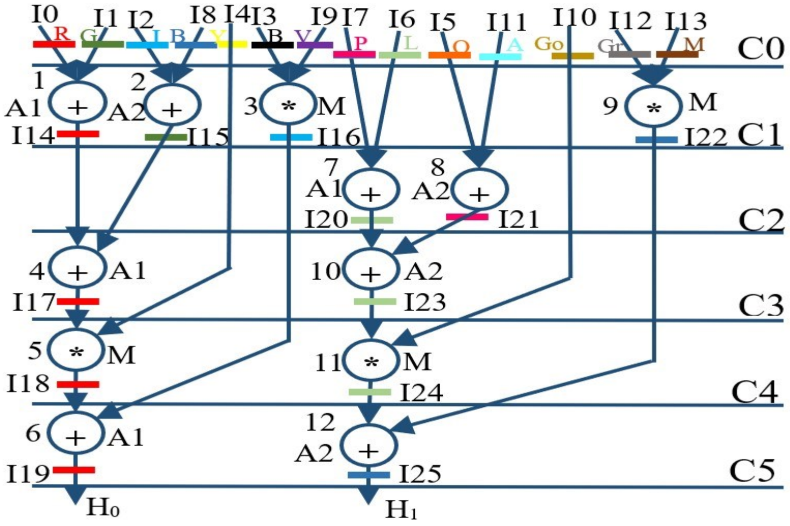


Figure 5: Scheduled data flow graph (SDFG) of LED filter

Generation and embedding of fused signature in the Register Allocation Table (RAT) corresponding to the SDFG of the image filter

- The generated templates (*i.e.,* template_1 and 2) are fused to generate final fused signature, which is further truncated and converted into covert hardware security constraints using IP vendor selected truncation length and mapping/embedding rule, respectively.
- ***Mapping/Embedding rule:*** Implant an additional artificial edge within (even, even) pairs of storage variables in the register allocation table (RAT) when the bit is '0'. Conversely, an edge is integrated between (odd, odd) storage variable pairs of the RAT when the bit is '1’. The generated security constraints are embedded into the RAT of the image filter.

Table I
RAT pre and post implanting security constraints corresponding to LED filter

	C0	C1	C2	C3	C4	C5
Red(R)	I0	I14/I15	I14	I17	I18	I19
Green (G)	I1	I15/I14	I15	-	-	-
Indigo (I)	I2	I16	I16	I16/I17	I16	-
Blue (BL)	I8	I22	I22	I22	I22	I25
Yellow (Y)	I4	I4	I4	I4	-	-/I19
Black (B)	I3	-/I16	-/I16	-/I16	-/I16	-
Violet (V)	I9	-/I22	-	-	-	-
Pink (I)	I7	I7	I21/I20	-	-/I18	-
Lime (LI)	I6	I6	I20/I21	I23	I24	-
Orange (O)	I5	I5	-	-	-/I18	-
Aqua (A)	I11	I11	-	-	-/I24	-
Gold (Go)	I10	I10	I10	I10	-	-
Gray (Gr)	I12	-	-	-	-	-
Maroon (M)	I13	-	-	-	-	-

Evaluation parameters [7]-[9]:

- **Evaluation of Robustness Using Probability of Coincidence:**

$$Pc = \left(1 - \frac{1}{x}\right)^z$$

Where ‘x’ denotes the number of registers used in the CIG and ‘z’ denotes the number of hardware constraints added.

- **Tamper tolerance:**

$$TT = q^t$$

Where ‘q’ and ‘t’ are types of encoding bits present in the mapping rule and strength (size) of generated security constraints respectively.

- **Design cost:**

$$Cost = t1 * \frac{Area}{Max\ area} + t2 * \frac{Latency}{Maximum\ latency}$$

Where ‘area’ and ‘latency’ represents the total area and latency (delay) of the proposed methodology-based secured IP core design; ‘max area and max latency’ depict the maximum area and latency of the proposed secured design of IP core using maximum resource constraints possible. ‘t1 and t2’ are the weighing factors (weightage given to are and delay), which in the proposed approach is 0.5 each.

- **Entropy :**

$$X_E = ((1/2^d * 1/m!) * ((1/2^k)*(1/R)*(1/2^{64})))$$

where '*d*' is the final generated palmprint template length and '*m*' is the total number of features selected on the palmprint, '*k*' is the length of truncated encoded hash, '*R*' is the round computation's maximum value, and $(1/2^{64})$ is the probability of finding the exact key hash buffer initialized value in SHA-512 cryptographic module (each hash buffer is initialized with pre-defined 64-bit value).

Results

Table II
Comparison of entropy and tamper tolerance between the proposed approach, [2], [3], [4], [5], and [6]

Security approach	Security parameters		
	Embedded constraints (q)	Entropy	Tamper tolerance
Proposed approach	400	8.27E-252	2.58E+120
Facial biometric [2]	83	1.03E-32	9.67E+24
Digital signature [5]	160	2.01E-87	1.46E+48
Watermarking [4]	240	1.66E-111	1.76E+72
DNA biometric [3]	128	2.9E-39	3.40E+38
HDL watermarking [6]	256	5.85E-99	1.15E+77

Table III
Comparison of probability of coincidence between the proposed approach, [2], [3], [4], [5], and [6]

Security approach	Benchmarks		
	Blur filter	Sharpening filter	LED filter
Proposed approach	6.05E-08	8.29E-09	2.49E-5
Facial biometric [2]	1.41E-02	2.10E-02	2.13E-03
Digital signature [5]	2.72E-04	5.85E-04	2.49E-5
Watermarking [4]	4.50E-06	1.41E-05	2.49E-5
DNA biometric [3]	1.40E-03	2.59E-03	7.59E-05
HDL watermarking [6]	1.98E-06	6.72E-06	2.49E-5

Results

Table IV
Design cost, area and latency of proposed technique

Benchmarks	Design cost	Design Area (um^2)	Design Latency (ps)
Blur filter	0.537	147.84	927.39
Sharpening filter	0.588	243.79	794.91
LED filter	0.71	199.75	728.67
Vertical embossment	0.756	99.09	596.18
Horizontal embossment	0.756	99.09	596.18

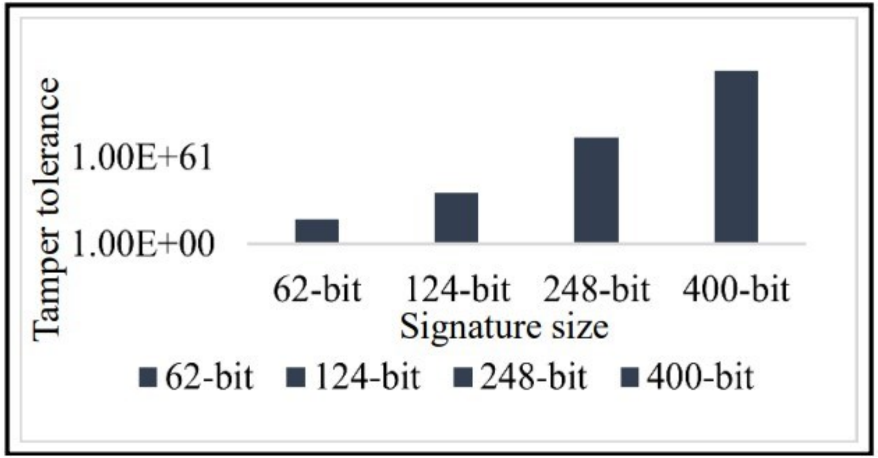


Figure 6: Security analysis of the proposed approach in terms of varying signature sizes and its impact on tamper tolerance

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 Systems Letters*, vol. 10, no. 3, (2018), 77-80, Sept.
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, R. Chaurasia, "Securing IP Cores for DSP Applications Using Structural Obfuscation and Chromosomal DNA Impression," *IEEE Access*, vol. 10, 2022, 50903-50913.
4. F. Koushanfar, I. Hong, M. Potkonjak, Behavioral synthesis techniques for intellectual property protection, *ACM Trans. Des. Autom. Electron. Syst*. 10, 3 (2005), 523–545, July.
5. E. Castillo, L. Parrilla, A. Garcia, U. Meyer-Baese, G. Botella, A. Lloris, "Automated Signature Insertion in Combinational Logic Patterns for HDL IP Core Protection," *2008 4th Southern Conference on Programmable Logic, Bariloche, Argentina*, (2008), 183-186.
6. T. Yu and Y. Zhu, "A new watermarking method for soft IP protection," 2011 International Conference on Consumer Electronics, *Communications and Networks (CECNet)*, China, 2011, 3839-3842.
7. Open Cell NanGate Library, 15 nm open cell library, Available: https://si2.org/open-cell-library/, last accessed on March 2023.
8. A. Sengupta, R. Chaurasia and A. Anshul, "Robust Security of Hardware Accelerators Using Protein Molecular Biometric Signature and Facial Biometric Encryption Key," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 31, no. 6, 826-839, 2023.
9. B. L. Gal and L, Bossuet, Automatic low-cost IP watermarking technique based on output mark insertions. *Des. Autom. Embedded Syst.* 16, 71–92, 2012..

Thank You!