Hardware Security of Digital Image Filter IP Cores against Piracy using IP Seller's Fingerprint Encrypted Amino Acid Biometric Sample

Anirban Sengupta, Rahul Chaurasia, Aditya Anshul, "Hardware Security of Digital Image Filter IP Cores against Piracy using IP Seller's Fingerprint Encrypted Amino Acid Biometric Sample", Proceedings of 8th IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST) , China, 2023, pp. 1-6

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].**

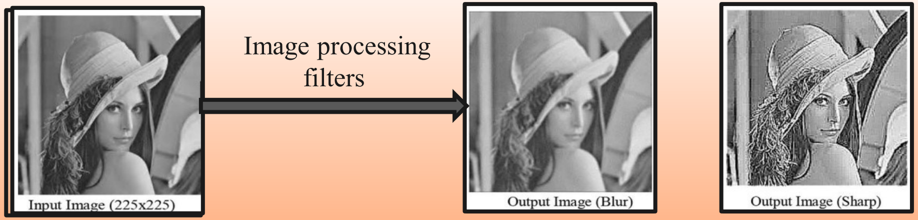


Figure 1: Image processing operations

Security Issues associated with image processing filter IP Cores [3]- [6], [8]

IP Piracy

IP Counterfeiting: Selling copied design under same brand name by attacker. Here, the counterfeited design is sold under same brand name.

IP Cloning: Selling the copy of the IP core under with different brand name by 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 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.,* [9] (2008)	The paper [9] 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 et. al., [10] (2019) (b) Sengupta and Rathor [11] (2021)	(a) Digital signature [10] and (b) Facial biometric [11] based hardware security approach.	[10] provides more robust security however becomes fragile in case of compromised RSA key value. Further, [11] provides inferior security due to the generation of lesser security constraints than proposed work.

Proposed Work

- The proposed hardware security methodology harnesses the combined power of fingerprint and amino acid chain based biometric to generate a fingerprint biometric encrypted IP seller's amino acid signature.
- The generation of encrypted amino acid signature associates unique natural identities of IP seller body samples due to the involvement of fingerprint and amino acid chain based biometric.
- Further, the secret hardware security constraints are determined using obtained encrypted 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 encrypted amino acid based 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

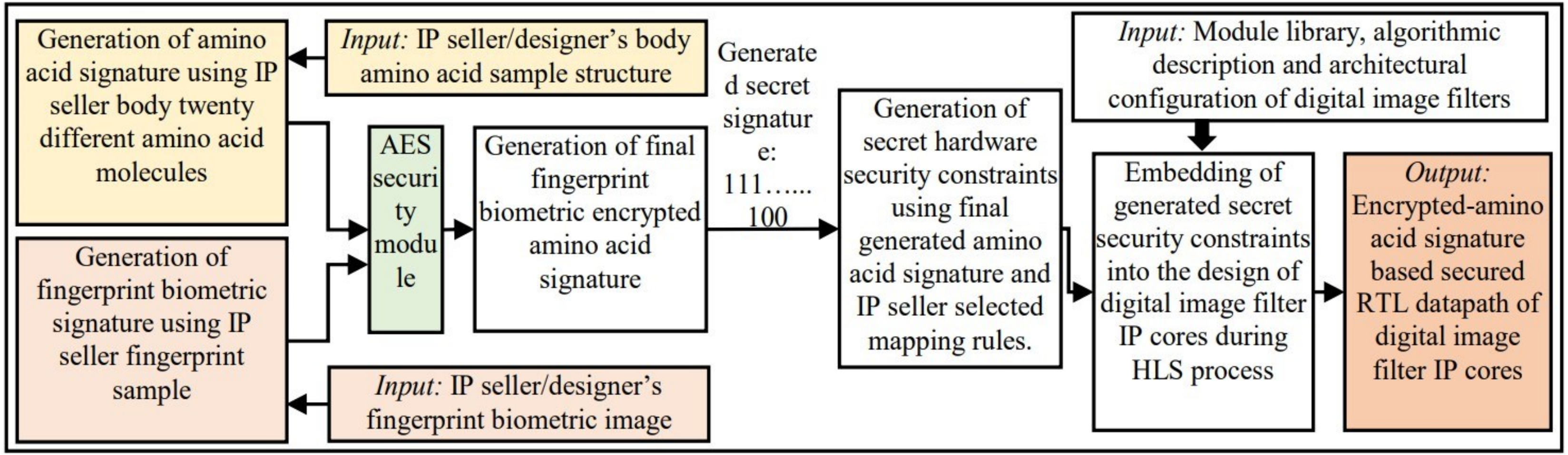


Figure 2: Details of the proposed security approach

Generation of pre-encrypted amino-acid digital template from IP vendor’s body insulin sample using protein sequencing [7]

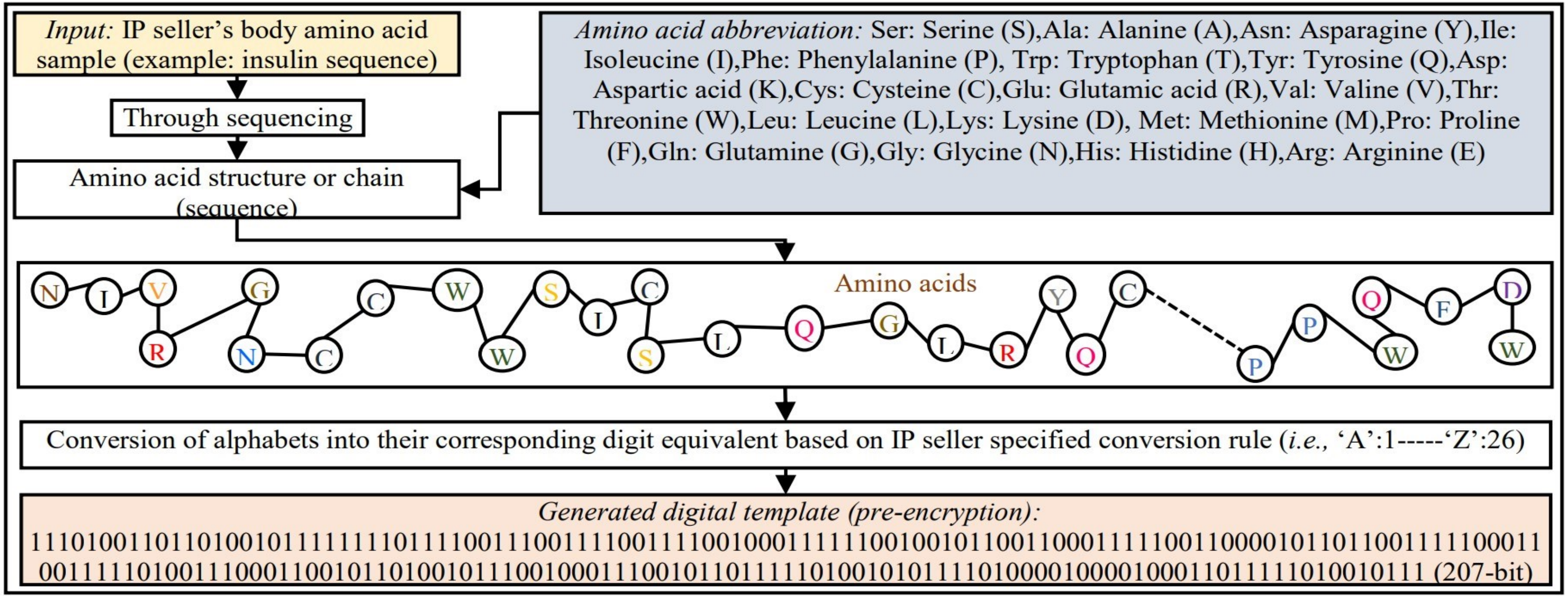
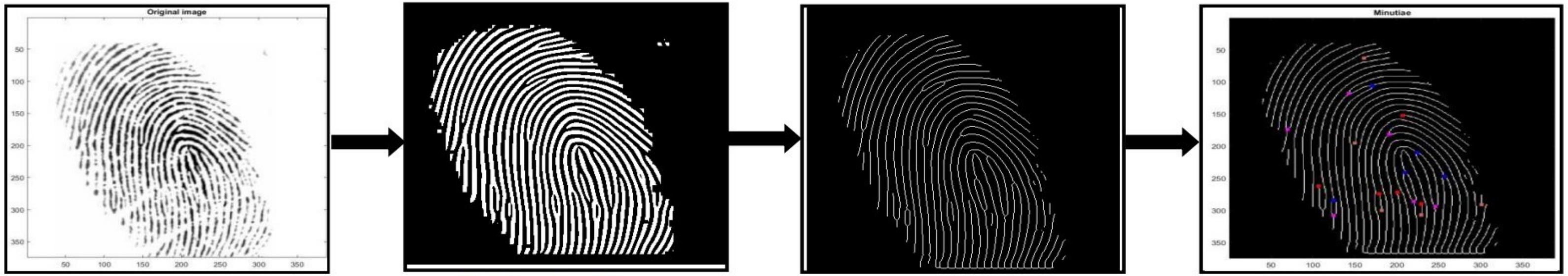


Figure 3: Generation of pre-encrypted amino acid digital template from IP seller’s amino acid insulin sequence

Generation of IP vendor's Fingerprint biometric template



(a) Original fingerprint biometric image of IP seller

(b) Binarized image

(c) Thinned image

(d) Minutiae point generation

No.	x	y	Minutiae type number	Angle in degree	Binary representation	Total bits
1	161	63	1	153	1010 0001-11 1111-1-1001 1001	23
2	171	106	3	337	1010 1011-1101010-11-1 0101 0001	26
3	143	118	3	130	1000 1111-111 0110-11-1000 0010	25
4	207	152	1	187	1100 1111-1001 1000-1-1011 1011	25
-----	-----	-----	-----	-----	-----------	-----
21	125	308	3	88	111 1101-100110100-11-101 1000	25

Generated fingerprint biometric template:
1010 0001-11 1111-1-1001 1001 ------------

--------------111 1101-100110100-11-101 1000 (538-bits)

Figure 4: Template generation using IP seller's fingerprint biometric

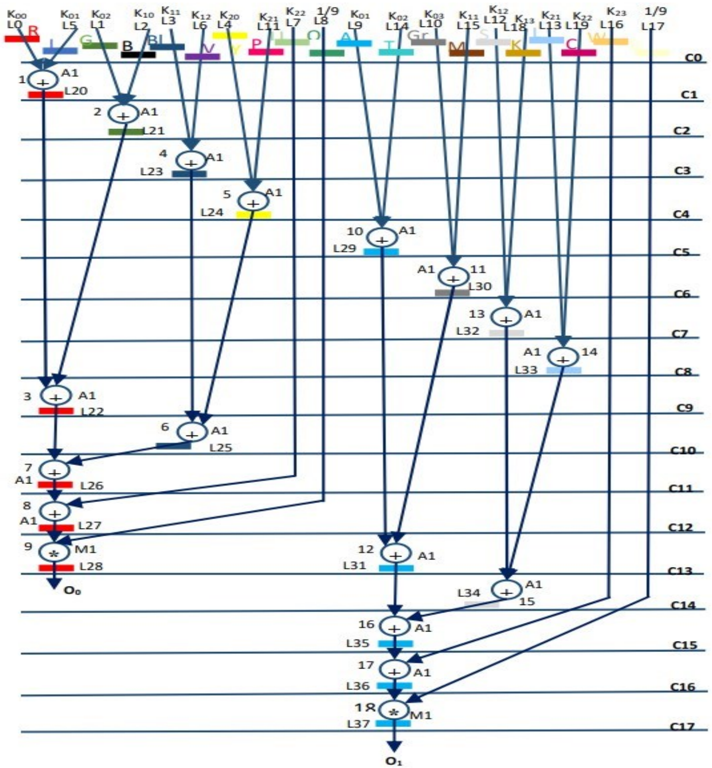
Demonstration of the proposed approach on Blur Filter

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

$$O_0 = [(K_{00}*(1/9)) + (K_{01}*(1/9)) + (K_{02}*(1/9))] + [(K_{10}*(1/9)) + (K_{11}*(1/9)) + (K_{12}*(1/9))] + [(K_{20}*(1/9)) + (K_{21}*(1/9)) + (K_{22}*(1/9))] \quad (1)$$

$$O_1 = [(K_{01}*(1/9)) + (K_{02}*(1/9)) + (K_{03}*(1/9))] + [(K_{11}*(1/9)) + (K_{12}*(1/9)) + (K_{13}*(1/9))] + [(K_{21}*(1/9)) + (K_{22}*(1/9)) + (K_{23}*(1/9))] \quad (2)$$

Generation of Scheduled Dataflow Graph (SDFG) from mathematical function and AES encryption



AES Encryption:

- The obtained amino acid template is divided into block size of 128-bits each.
- The obtained fingerprint template acts as AES-128 encryption key.
- The final generated encrypted template is as follows: "0101110…………………000000011"

Figure 5: SDFG of 3*3 blur filter with 1(+),and 1(*)

Generation of security constraints and security constraints embedded Register Allocation Table (RAT)

- Security constraints are derived from generated encrypted signature based on Ip vendor selected mapping/embedding rule: Implant an additional (*i.e.,* artificial) edge between (even, even) storage variables pair in the RAT framework in case of bit '0', otherwise embed an edge between (odd, odd) storage variables pair. The determined secret security constraints are as follows: *(L0,L2), (L0,L36),-----, (L6,L20), (L1,L3),--, (L9,L37)*.

Table I

Register allocation table of 3*3 blur filter depicted in Fig. 3

CS	Red(R)	Green (G)	Indigo (I)	Blue (BL)	Yellow (Y)	Black (B)	Violet (V)	Pink (P)	Lime (LI)	Olive (O)	Aqua (A)	(T)	G)	(M)	(S)	(K)	(L)	(C)	(W)	(B)
0	L0	L1	L5	L3	L4	L2	L6	L11	L7	L8	L9	L14	L10	L15	L12	L18	L13	L19	L16	L17
1	L20/L21	L1	L20	L3	L4	-	-	-	L7	L8	L9	-	L10	-	L12	-	L13	-	L16	L17
2	L20/L21	L21	L20	L3	L4	-	-	-	L7	L8	L9	-	L10	-	L12	-	L13	-	L16	L17
3	L20/L21	L21	L20	L23	L4	L23	-	-	L7	L8	L9	-	L10	-	L12	-	L13	-	L16	L17
4	L20/L21	L21	L20	L23L24	L24	L23	-	-	L7	L8	L9	-	L10	-	L12	-	L13	-	L16	L17
5	L20/L21	L21	L20	L23L24	L24/L29	L23	-	-	L7	L8	L29	-	L10	-	L12	-	L13	-	L16	L17
6	L20/L21	L21	L20	L23L24	L24/L29	L23	L30	-	L7	L8	L29	-	L30	-	L12	-	L13	-	L16	L17
7	L20/L21	L21	L20	L23L24	L24/L29	L23	L30	-	L7	L8	L29/L32	-	L30	-	L32	-	L13	-	L16	L17
8	L20/L21	L21	L20	L23L24	L24/L29	L23	L30	-	L7	L8	L29/L32	-	L30	-	L32	-	L33	-	L16	L17
9	L22	L21L22	-	L23L24	L24/L29	L23	L30	-	L7	L8	L29/L32	-	L30	-	L32	-	L33	-	L16	L17
10	L22/L25	L22	-	L25	L29	-	L30	-	L7	L8	L29/L32	-	L30	-	L32	-	L33	-	L16	L17
11	L26	L26	-	-	L29	-	L30	-	L7	L8	L29/L32	-	L30	-	L32	-	L33	-	L16	L17
12	L27	-	-	-	L29	-	L30	-	-	L8	L29/L32	-	L30	-	L32	-	L33	-	L16	L17
13	L28/L31	L28	-	-	-	-	-	-	-	-	L31L32	-	-	-	L32	-	L33	-	L16	L17
14	L31	L34	-	-	-	-	-	-	-	-	L31	-	-	-	L34	-	-	-	L16	L17
15	L35	-	-	-	-	-	-	-	-	-	L35	-	-	-	-	-	-	-	L16	L17
16	-	L36	-	-	-	-	-	-	-	-	L36	-	-	-	-	-	-	-	-	L17
17	37	-	-	-	-	-	-	-	-	-	L37	-	-	-	-	-	-	-	-	-

Evaluation parameters:

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

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

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

- **Tamper tolerance:**

$$Lo = q^t$$

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

- **Design cost:**

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

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.

Results

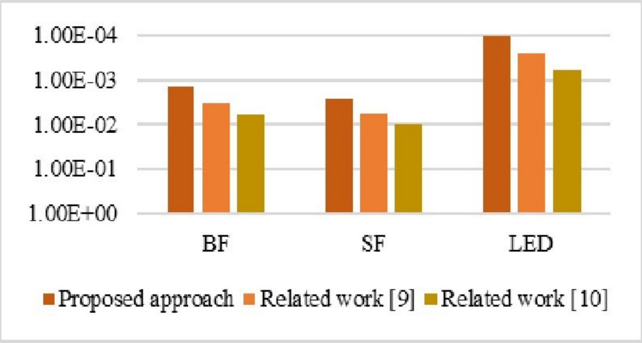


Figure 6: Probability of coincidence (*Ic*) comparison between proposed, [9], and [10]

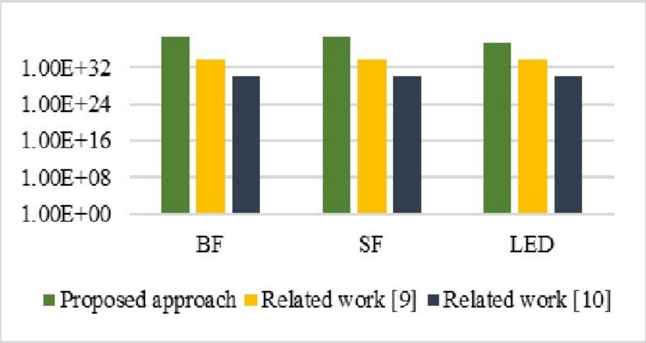


Figure 7: Tamper tolerance (*Lo*) comparison between proposed, [9], and [10]

Table II
Comparison of *Ic* For blur filter between proposed and facial biometric [11] based security approach

Facial biometric image	# of hardware security constraints generated using facial biometric	*Ic* of facial biometric [11]	Proposed chain length of amino-acid	# of hardware security constraints generated using proposed approach	*Ic* of proposed approach	% Reduction of Ic obtained using proposed approach
Facial image_1	81	1.56E-02	25	98	6.56E-03	57.95%
Facial image_2	84	1.34E-02	33	128	1.40E-03	89.55%
Facial image_3	83	1.41E-02	51	207	2.44E-05	99.82%

Results

Table III

Comparison of *Lo* corresponding to blur filter between proposed and facial biometric [11] based security approach

Facial biometric image	# of hardware security constraints generated using facial biometric	*Lo* of facial biometric [11]	Proposed chain length of amino-acid	# of hardware security constraints generated using proposed approach	*Lo* of proposed approach
Facial image_1	81	2.41E+24	25	98	3.16E+29
Facial image_2	84	1.93E+25	33	128	3.40E+38
Facial image_3	83	9.67E+24	51	207	2.05E+62

Table IV

Resource configuration, latency, area, and cost of proposed security methodology pre and post implanting hardware security constraints

Benchmarks	Baseline design (before signature embedding)			Amino acid signature implanted design			Design cost overhead %
	Design area (um^2)	Design latency (ps)	Design cost	Design area (um^2)	Design latency (ps)	Design cost	
Blur filter (BF)	110.10	1523.58	0.67	110.10	1523.58	0.67	0
Sharpening filter (SF)	111.67	1921.04	0.67	111.67	1921.04	0.67	0
Laplacian filter (LED)	105.38	1258.61	0.72	105.38	1258.61	0.72	0

References

1. R. Schneiderman, "DSPs Evolving in Consumer Electronics Applications," *IEEE Signal Processing Magazine*, vol. 27, no. 3, pp. 6-10, May 2010.
2. 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, pp. 77-80, Sept. 2018..
3. Rizzo, S., Bertini, F. & Montesi, D. Fine-grain watermarking for intellectual property protection. *EURASIP J. on Info. Security*, 10, 2019.
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. A. Anshul and A. Sengupta, "IP Core Protection of Image Processing Filters with Multi-Level Encryption and Covert Steganographic Security Constraints," *2022 IEEE International Symposium on Smart Electronic Systems (iSES)*, Warangal, India, 2022, pp. 83-88.
6. National Library of Medicine-National Institutes of Health,https://www . ncbi.nlm.nih.gov/books/NBK26830/#:~:text=Since%20each%20of%20the%2020,chains%20n%20amino%20acids%20long, April 2023.
7. K. Steendam, M. Ceuleneer, M. Dhaenens, et al. “Mass spectrometry-based proteomics as a tool to identify biological matrices in forensic science,” *Int J Legal Med* 127, 287–298 (2013).
8. A. Anshul, A. Sengupta, PSO based exploration of multi-phase encryption based secured image processing filter hardware IP core datapath during high level synthesis, *Elsevier*, *Expert Systems with Applications*, Volume 223, 2023, 119927.
9. 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.
10. A. Sengupta, E. R. Kumar, and N. P. Chandra, “Embedding digital signature using encrypted-hashing for protection of DSP cores in CE,” *IEEE Trans. Consum. Electron.,* vol. 65, no. 3, pp. 398–407, Aug. 2019.
11. A. Sengupta and M. Rathor, “Facial biometric for securing hardware accelerators,” *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 29, no. 1, pp. 112-123, Jan. 2021.

Thank You!