Ph.D. Thesis

Alternative Paradigms of Hardware Security for Addressing Threats of IP Piracy and Trojan during High Level Synthesis

Presented by:

Aditya Anshul (2101101007)

Under the supervision of:

Prof. Anirban Sengupta
Computer Science and Engineering
Indian Institute of Technology Indore

Sr. No.	Proposed Solutions of Research Problems	Journal Publication	Conference publication
1.	**Robust security of hardware accelerators using protein molecular biometric signature and facial biometric encryption key**	IEEE Transactions on Very Large Scale Integration Systems (TVLSI)	Proceedings of 8th IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST), China
2.	Securing Reusable IP Cores using Voice Biometric based Watermark	IEEE Transactions on Dependable and Secure Computing (TDSC)	--
3.	Exploring handwritten signature image features for hardware security	IEEE Transactions on Dependable and Secure Computing (TDSC)	--
4.	Bio-mimicking DNA fingerprint profiling for HLS watermarking to counter hardware IP piracy	Nature Scientific Reports	--
5.	**Secure hardware IP of GLRT cascade using color interval graph based embedded fingerprint for ECG detector**	Nature Scientific Reports	Pending
6.	M-HLS: Malevolent High-Level Synthesis for Watermarked Hardware IPs	IEEE Embedded Systems Letters (ESL)	--
7.	**Watermarking Hardware IPs Using Design Parameter Driven Encrypted Dispersion Matrix With Eigen Decomposition Based Security Framework**	IEEE Access	Pending
8.	A Survey of High Level Synthesis based Hardware Security Approaches for Reusable IP Cores	IEEE Circuits and Systems Magazine (CASM)	--
9.	A Survey of High Level Synthesis based Hardware (IP) Watermarking Approaches	IEEE Design & Test (DAT)	--
10.	Palmprint Biometric vs Encrypted Hash based Digital Signature for Securing DSP Cores Used in CE systems	IEEE Consumer Electronics (CEM)	--
11.	PSO based exploration of multi-phase encryption based secured image processing filter hardware IP core datapath during high level synthesis	Elsevier Journal on Expert Systems with Applications	Proceedings of 9th IEEE International Symposium on Smart Electronic Systems (IEEE – iSES), India
12.	Exploration of optimal functional Trojan-resistant hardware intellectual property (IP) core designs during high level synthesis	Elsevier Journal on Microprocessors and Microsystems	Pending
13.	**Exploration of optimal crypto-chain signature embedded secure JPEG-CODEC hardware IP during high level synthesis**	Elsevier Journal on Microprocessors and Microsystems	Proceedings of 35th IEEE International Conference on Microelectronics (ICM), Abu Dhabi
14.	Quadruple phase watermarking during high level synthesis for securing reusable hardware intellectual property cores	Elsevier Journal on Computers and Electrical Engineering	--
	Total	**14 Journals**	**3 Conferences**

Hardware intellectual property (IP) core (Application specific systems)

- The rapid evolution of technology and the increasing complexity of computational tasks have underscored the growing need for specialized computing, also known as application-specific computing.
- This approach focuses on designing computing systems tailored to perform specific tasks more efficiently than general-purpose systems. Some of the factors leading to the rise in the need for specialized computing are (a) *Performance Optimization*, (b) *Energy Efficiency*, (c) *Cost Efficiency*, (d) *Industry-Specific Applications*, (e) *Customization and Flexibility*, etc.
- Some crucial examples of application-specific computing that includes data and computation-intensive operations are (a) *image processing applications/filters*, (b) *machine learning/deep learning-based applications*, (c) *JPEG compression-decompression*, (d) *DCT*, (E) *FIR filter*, etc.
- These computation-intensive applications are designed as dedicated reusable hardware *Intellectual Property (IP) core* of *Hardware Accelerator* using the High Level Synthesis (HLS) process [1].

Hardware design process

- Due to the globalization of the design supply chain, the design process of these application-specific hardware systems involves various hardware threats [1], [2].

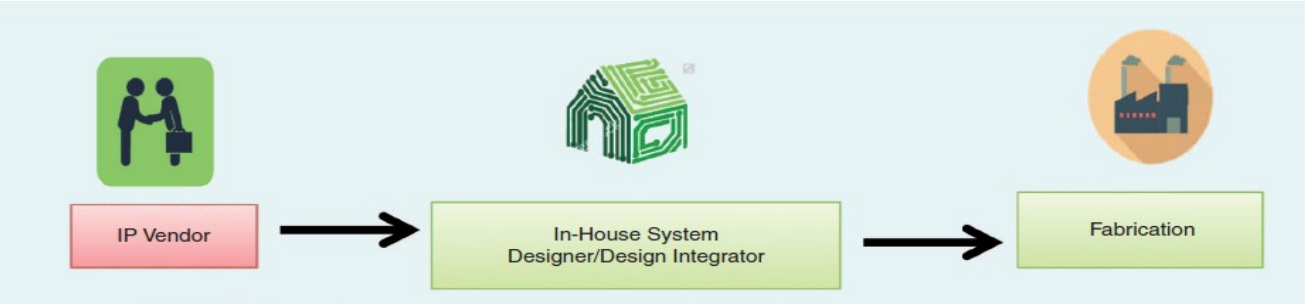
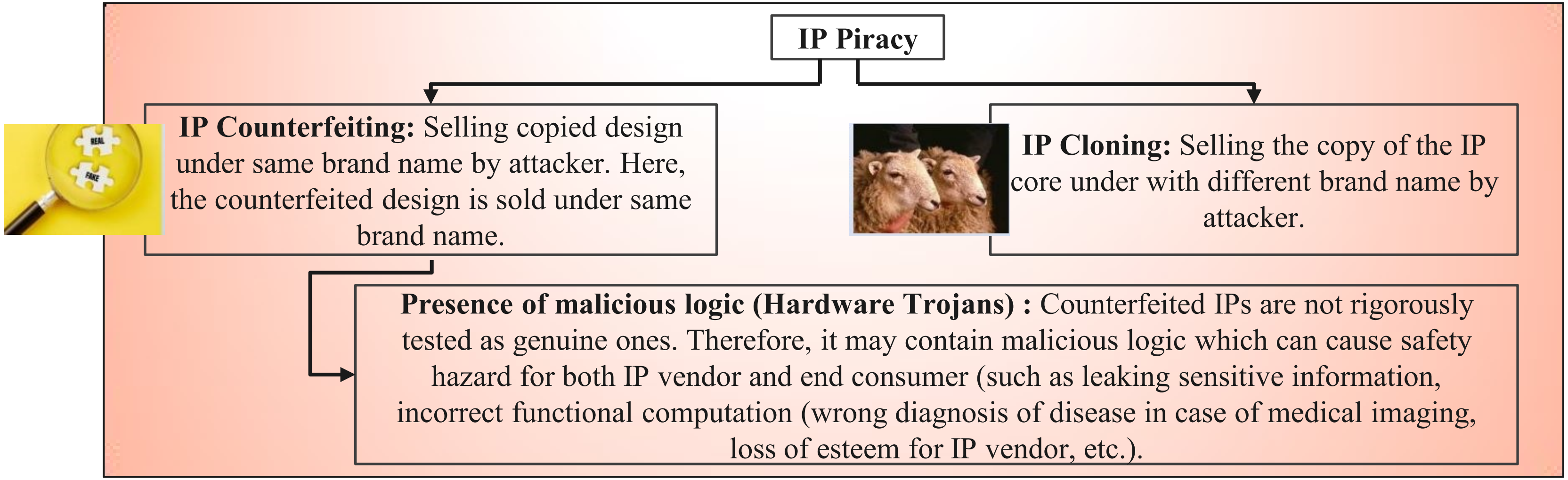


Figure 1: Hardware IC design process

Security Issues associated with hardware IP Cores [1], [2]

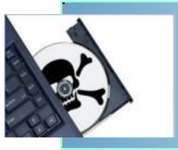


IP Piracy

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.

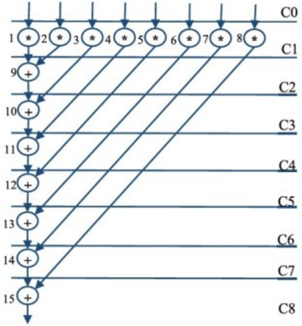
Therefore, it is essential to secure these hardware IP cores from these hardware threats.

Security Issues associated with hardware IP Cores [1], [19]

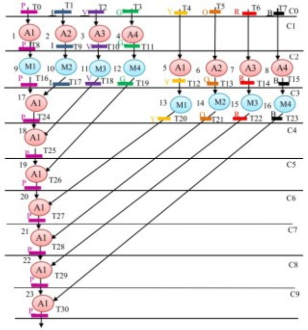
Hardware Trojan Attack- Malicious circuitry that damages the function and trustworthiness. Hardware Trojans are covertly inserted at safe places such that it goes undetected during testing process and they activate only under specific triggering condition.

Functional hardware Trojans are present in 3rd party IP module library (such as adder, and multiplier library), which on triggering disrupt the original functionality of the hardware system.

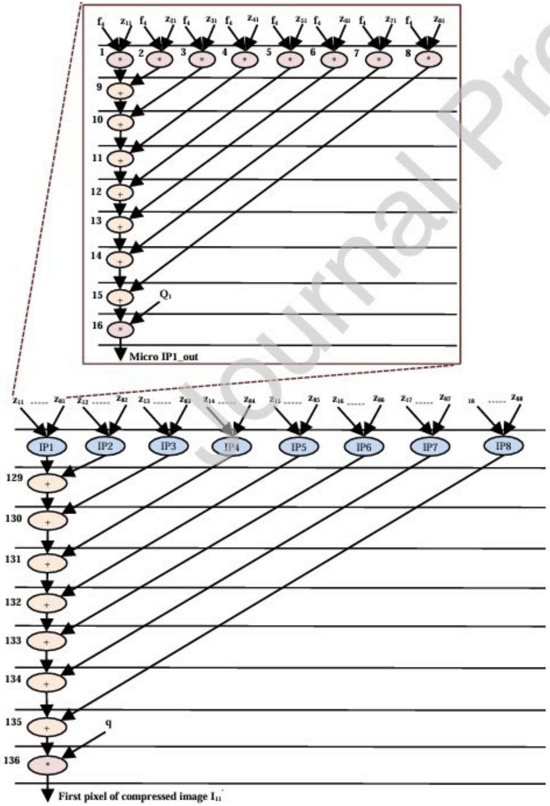
Benchmarks



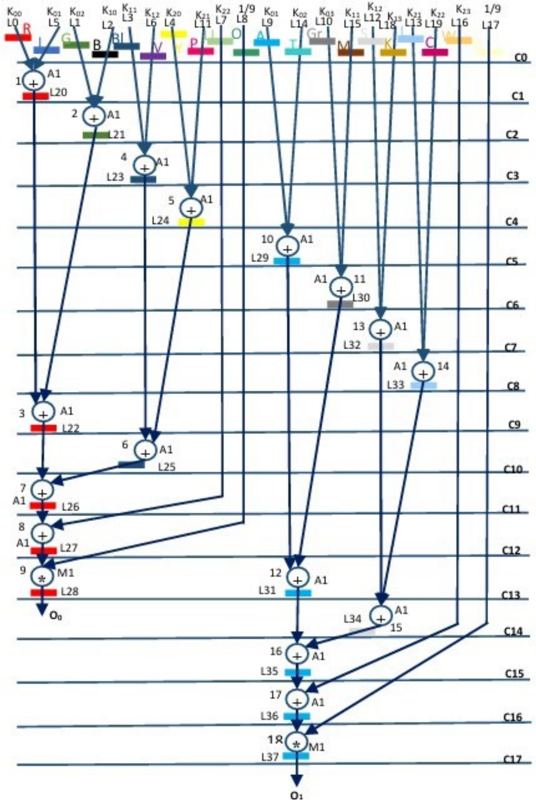
Data flow graph of 8-point DCT



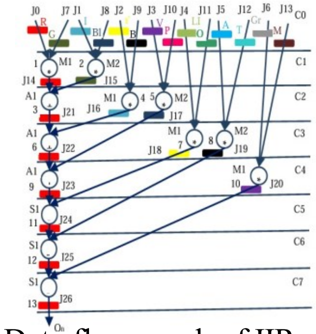
Data flow graph of FIR filter



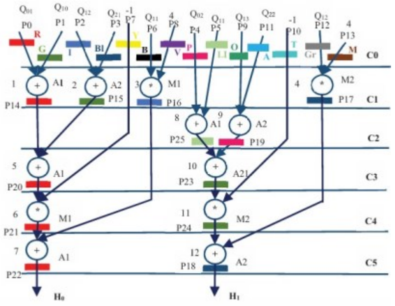
Data flow graph of JPEG-CODEC



Data flow graph of blur filter



Data flow graph of IIR



Data flow graph of Laplacian filter

Related work on hardware watermarking

Sr. No.	Existing Work	Technique Used	Remarks
1.	a). F. Koushanfar, I. Hong, and M. Potkonjak [3] (2005) b). A. Sengupta and S. Bhadauria [4] (2016)	IP seller's signature encoding-based hardware watermarking.	Weak watermarking mechanism due to involvement of only two and four variable signature encoding process. Not robust and future proof. The watermark inserted by watermarking technique becomes vulnerable if relevant information (like signature size, digit encoding, and combination) gets leaked.
2.	a) A. Sengupta and M. Rathor, [5] (2019) b). E. Castillo, et. al., [6] (2008) c). A. Sengupta, et. al., [7] (2019)	Steganography, encryption and digital signature-based hardware watermarking.	Provides weaker security due to the generation of limited security constraints. Additionally, they become weak in case of a compromised stego-threshold and RSA key value.
3.	a). A. Sengupta and M. Rathor, [8] (2020) b). A. Sengupta, et. al., [9] (2021)	IP seller's biometrics (such as facial and palmprint biometrics) based hardware watermarking.	Although [8] and [9] integrate the natural identity of IP sellers with the hardware design, they provide weaker security due to the generation of limited watermarking (security) constraints.

Related work Trojan detection approaches

Sr. No.	Existing Work	Technique Used	Remarks
1.	Martin *et. al.,* [16] (2018) and Gunti *et. al.,* [17] (2017)	[16] uses approximate circuits to prevent hardware Trojan insertion and [17] demonstrates neutralizing hardware Trojans in SCADA systems by employing a TMR scheme on selected paths.	Neither [16] nor [17] addresses functional hardware Trojan isolation in digital image filter IP cores, particularly within the context of 3PIP cores. Moreover, they do not integrate particle swarm optimization based design space exploration to optimize the architecture for Trojan resistance.
2.	Li *et. al.,* [18] (2021)	Efforts have been made to create adversarial hardware with functional camouflage, exploring ways to covertly insert Trojans at locations with low centrality values.	[18] does not focus on designing low-cost optimized Trojan-resistant digital image filter circuits.
3.	Sengupta et. al., [19] (2017)	Dual Modular Redundancy (DMR) design methodology for providing Trojan detection.	[19] falls short in providing Trojan isolation and resistance.

Secure hardware IP of GLRT cascade using color interval graph based embedded fingerprint for ECG detector

- The proposed approach presents a novel secure hardware IP of generalized likelihood ratio test (GLRT) cascade using color interval graph (CIG) based embedded fingerprint, for electrocardiogram (ECG) detector, for the first time in literature [10].
- The GLRT unit is the primary component of the ECG detector that executes computation-intensive functions to estimate heart rate using (*Q wave*, *R wave* and *S wave*) *QRS wave complex* from incoming filter signals.
- The proposed approach uses the IP seller's fingerprint biometric sample to generate and embed the watermark signature (watermarking constraints) into the final hardware IP design.
- The embedded IP seller's watermark helps in the demarcation and isolation of pirated IPs from the authentic ones by system-on-chip (SoC) integrator before integration into the final hardware system.

[10] A. Sengupta, A. Anshul, Secure hardware IP of GLRT cascade using color interval graph based embedded fingerprint for ECG detector. Nature *Scientific Reports* 14, 13250 (2024).

Motivation

- From the perspective of the end user (patient), the safe and reliable functioning of the GLRT unit in the ECG detector is critical as it is responsible for the generation of important ECG parametric data such as *Heart Rate (HR)*, *PR Interval (PRI)*, *QRS Interval (QRSI)*, *QT Interval (QTI)*, *QTC Interval (QTCI)*.
- Therefore, it is essential to design the GLRT unit of the ECG detector as a reusable hardware IP core because of its wide usability and computation-intensive nature.
- A pirated (*i.e.,* counterfeited) GLRT hardware IP core is unreliable and may contain malicious logic that could result into inaccurate detection of vital ECG parametric data, erratic behavior or functionality of the ECG detector, mistimed pulse from ECG detector for cardiac pacemaker devices. Therefore, it is necessary to secure the hardware IP so that it can be verified before integration into the final system.

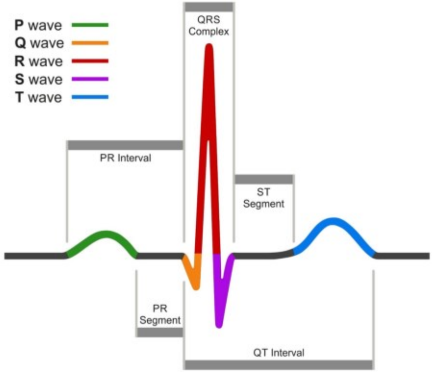


Figure 2: Sample ECG waveform

Detailed of the proposed approach

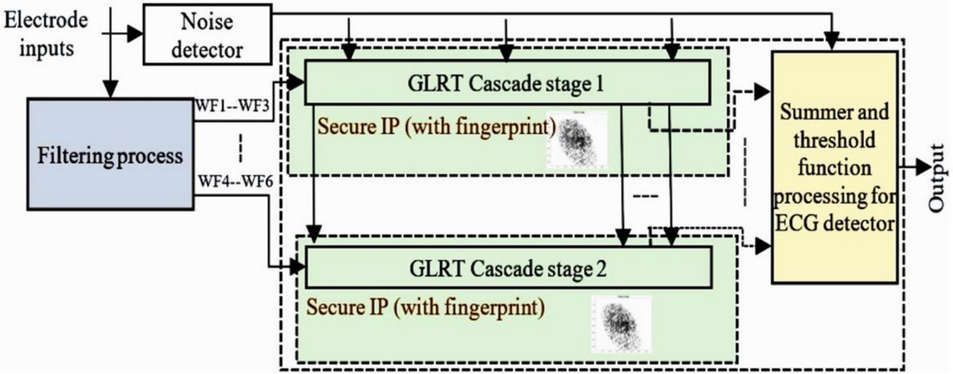
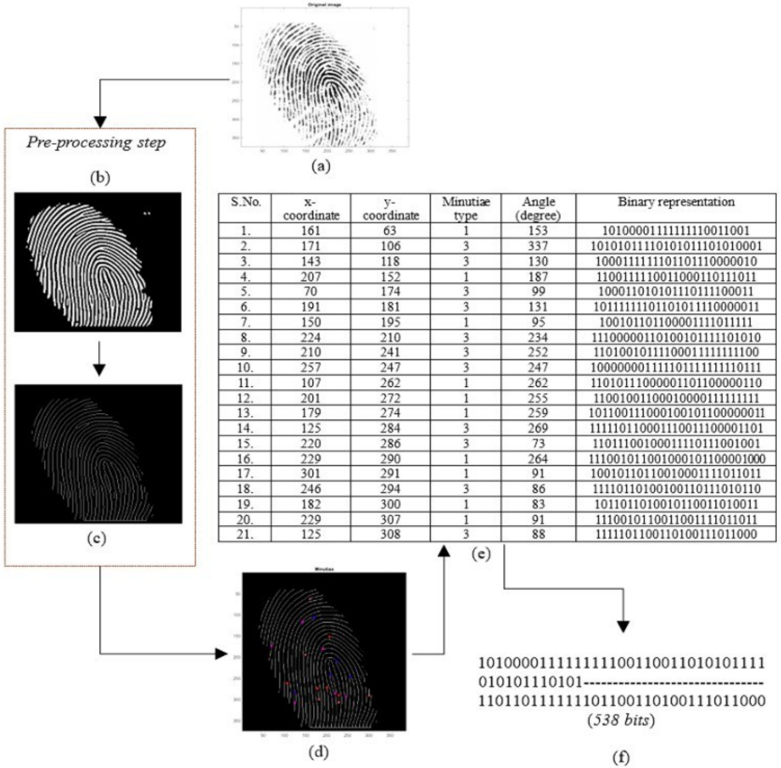

Electrode inputs
Noise detector
Filtering process
WF1--WF3
WF4--WF6
GLRT Cascade stage 1
Secure IP (with fingerprint)
GLRT Cascade stage 2
Secure IP (with fingerprint)
Summer and threshold function processing for ECG detector
Output

Figure 3: Proposed secure hardware IP of GLRT cascade for ECG detector

- At first, GLRT's mathematical/transfer function is taken as input, which is converted into its respective control data flow graph (CDFG).
- Next, the obtained CDFG is scheduled using input resource constraints (*i.e.,* number of adders and multipliers) to generate its corresponding scheduled data flow graph (SDFG).
- Transfer function: $Z(a) = s^T(n)H(H^TH)^{-1}H^Ts(n)$, where $s(n)$ is the input to the filtering unit and H is the linear combination matrix of the representative function. Here, $s^T(n)$ is a 6-by-1 matrix, H is a 1-by-6 matrix, $s(n)$ is a 1-by-6 matrix and (H^TH) is a 6-by-6 matrix.

Details of fingerprint watermark signature generation process



S.No.	x-coordinate	y-coordinate	Minutiae type	Angle (degree)	Binary representation
1.	161	63	1	153	10100001111111110011001
2.	171	106	3	337	10101011110101011101010001
3.	143	118	3	130	1000111111011011100000010
4.	207	152	1	187	1100111110011000110111011
5.	70	174	3	99	10001101010111011110001 1
6.	191	181	3	131	10111111101101011110000011
7.	150	195	1	95	1001011011000011110111111
8.	224	210	3	234	11100000110100101111101010
9.	210	241	3	252	1101001011110001111111100
10.	257	247	3	247	10000000111110111111110111
11.	107	262	1	262	11010111000001101100000110
12.	201	272	1	255	1100100110001000011111111
13.	179	274	1	259	101100111000100101100000011
14.	125	284	3	269	11111011000111001110000110 1
15.	220	286	3	73	1101110010001111011100100 1
16.	229	290	1	264	111001011001000101100001000
17.	301	291	1	91	10010110110010001111011011
18.	246	294	3	86	11110110100100110111010110
19.	182	300	1	83	1011011010010110011010011
20.	229	307	1	91	1110010110011001111011011
21.	125	308	3	88	1111101100110100111011000

1010000111111111001100110101011110
010101110101--------------------------------
110110111111110110011010011101 1000
(538 bits)

Figure 4: Proposed fingerprint digital template generation process extracted from captured IP vendor's fingerprint, (a) input IP sellers fingerprint image, (b) binarized fingerprint image, (c) thinned fingerprint image, (d) minutiae points generation on fingerprint image, (e) details of generated minutiae points parameters, (f) generated fingerprint biometric based digital template. The biometric captured is of a real IP vendor entity that is used for further processing of template generation

Final watermark constraints embedded SDFG of GRLT

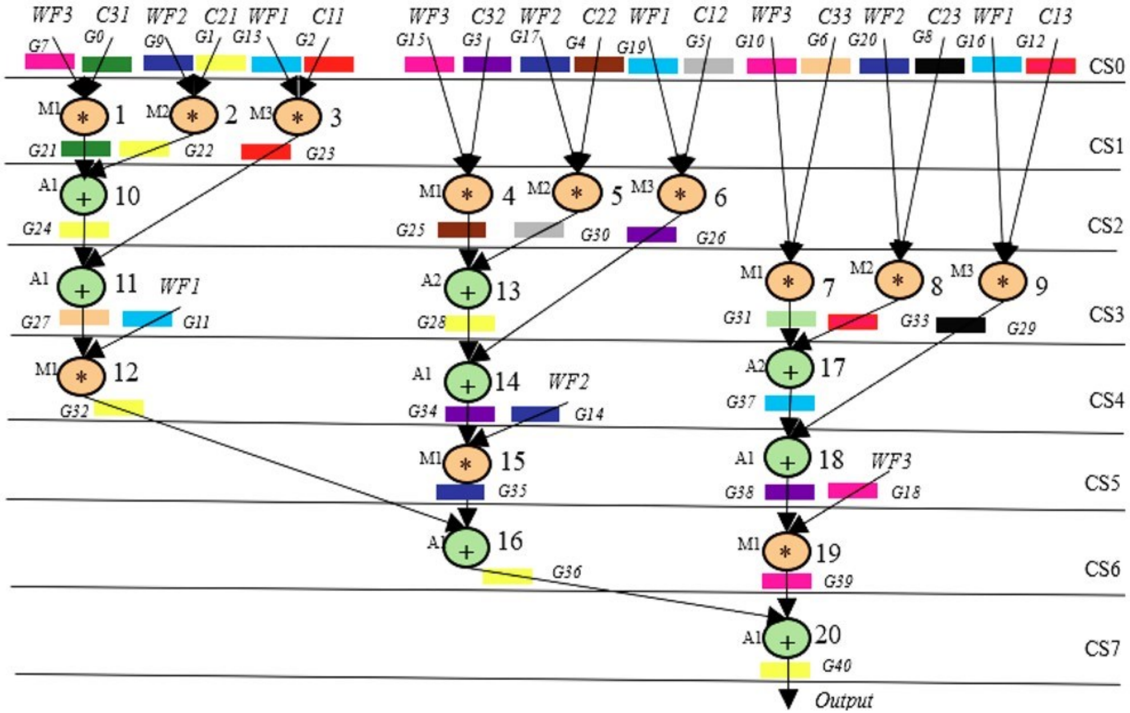


Figure 5: SDFG of GLRT cascade macro IP scheduled using three multipliers and two adders post embedding fingerprint

Final watermark constraints embedded RTL

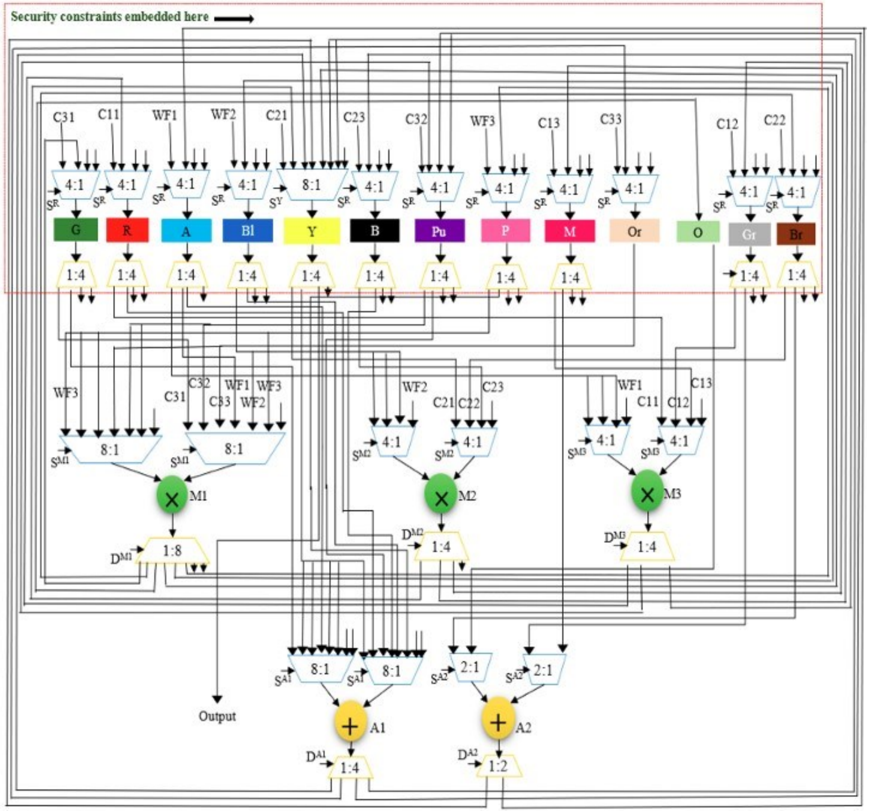


Figure 6: Secure RTL design of GLRT cascade macro IP core with CIG based embedded fingerprint

Evaluation parameters

- **Evaluation of Robustness Using Probability of Coincidence (*Pc/C$_i$*):**

$$P_c = \left(1 - \frac{1}{c}\right)^f$$

'*c*' denotes the number of registers used in the RAT, and '*f*' denotes the number of hardware constraints added.

- **Evaluation of tamper tolerance (*TT/T$_i$*):**

$$TT = (\mathrm{w})^f$$

'*w*' is the number of types of digits in the signature, and '*f*' is the signature size (or the number of corresponding hardware security constraints)

- **Design cost:**

$$Design\ cost = q1 * \left(\frac{Area(A)}{Amax}\right) + q2 * \left(\frac{Latency\ (L)}{Lmax}\right)$$

where q1=0.5 and q2=0.5 are designer-defined weighing factors used to provide equal weightage to design *area (A)* and execution time (*Latency (L)*) during design cost function evaluation. Further, A_{max} and L_{max} represents maximum design area (determined with available maximum functional resources) and time (delay) (determined with available minimum functional resources)

Results

Table 1: Comparison of tamper tolerance (TT) between the proposed fingerprint embedded secure GLRT cascade IP with facial biometric [8] embedded IP design and digital signature embedded IP design [7]

Proposed secure GLRT IP with fingerprint		**Design with facial constraints [25]**		**Design with digital signature [16]**	
Security constraints	T_i	Security constraints	T_i	Security constraints	T_i
250	1.80E+75	16	6.55E+04	16	6.55E+04
275	6.07E+82	32	4.29E+09	32	4.29E+09
300	2.03E+90	64	1.84E+19	64	1.84E+19
346	1.43E+104	81	2.41E+24	128	3.40E+38

Table 2: Comparison of tamper tolerance (TT) between the proposed fingerprint embedded secure GLRT cascade IP with encrypted signature embedded IP design [6] and hardware watermarking embedded IP design [3]

Proposed secure GLRT IP with fingerprint		**Design with encrypted signature [17]**		**Design with watermark [12]**	
Security constraints	T_i	Security constraints	T_i	Security constraints	T_i
250	1.80E+75	32	4.29E+09	32	4.29E+09
275	6.07E+82	64	1.84E+19	64	1.84E+19
300	2.03E+90	128	3.40E+38	128	3.40E+38
346	1.43E+104	160	1.46E+48	240	1.76E+72

Table 3: Comparison of probability of coincidence between the proposed fingerprint embedded secure GLRT cascade IP with facial biometric [8] embedded IP design and digital signature embedded IP design [7]

Proposed secure GLRT IP with fingerprint		**Design with facial constraints [25]**		**Design with digital signature [16]**	
Security constraints	C_i	Security constraints	C_i	Security constraints	C_i
250	3.57E-10	16	2.48E-01	16	2.48E-01
275	4.05E-11	32	6.17E-02	32	7.71E-02
300	4.60E-12	64	3.81E-03	64	3.81E-03
346	8.41E-14	81	8.69E-04	128	1.45E-05

Table 4: Comparison of probability of coincidence between the proposed fingerprint embedded secure GLRT cascade IP with facial biometric [8] embedded IP design and digital signature embedded IP design [7]

Proposed secure GLRT IP with fingerprint		**Design with encrypted signature [17]**		**Design with watermark [12]**	
Security constraints	C_i	Security constraints	C_i	Security constraints	C_i
250	3.57E-10	32	6.17E-02	32	6.17E-02
275	4.05E-11	64	3.81E-03	64	3.81E-03
300	4.60E-12	128	1.45E-05	128	1.45E-05
346	8.41E-14	160	8.99E-07	240	8.52E-10

Results (Design cost)

Table 5: Design latency, area, and resource configuration of proposed secure GLRT IP before and after embedding fingerprint signature

Application	Resource configuration	Unsecured design (before fingerprint embedding)		Proposed fingerprint embedded secure design	
GLRT cascade hardware IP core	2(+), 3(*)	Design area (um^2)	Design latency (ps)	Design area (um^2)	Design latency (ps)
		273.67	1656.07	273.67	1656.07

Table 6: Design cost, leakage power, register count and resource configuration of proposed secure GLRT hardware IP before and after embedding fingerprint signature

Application	Resource configuration	Unsecured design (before fingerprint embedding)		Proposed fingerprint embedded secure design	
GLRT cascade hardware IP core	2(+), 3(*) and 13 registers	Design cost	Leakage power	Design cost	Leakage power
		0.43	8.57 μw	0.43	8.57 μw

Robust security of hardware accelerators using protein molecular biometric signature and facial biometric encryption key

- This proposed approach presents a novel molecular biometric-based hardware security approach based on IP seller's protein molecule sequence, for the first time to secure hardware IP cores [11].
- Here, an IP seller/vendor-selected protein sequence comprising 20 unique amino acid combinations is used for molecular signature generation.
- The generated signature is then encrypted through AES using an encryption key generated with the facial biometric of an authentic IP vendor. Thus, the proposed approach incorporates two classes of biometrics of IP seller to ensure highly robust and unique authentication.
- The encrypted molecular signature is then converted into watermarking constraints using the IP seller's mapping rule and is further embedded in the hardware design during the register allocation phase of the HLS process.
- The embedded IP seller's watermark helps in the demarcation and isolation of pirated IPs from the authentic ones and protects IP seller from false IP ownership assertions.

[11] 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, pp. 826-839, June 2023.

Detailed of the proposed approach

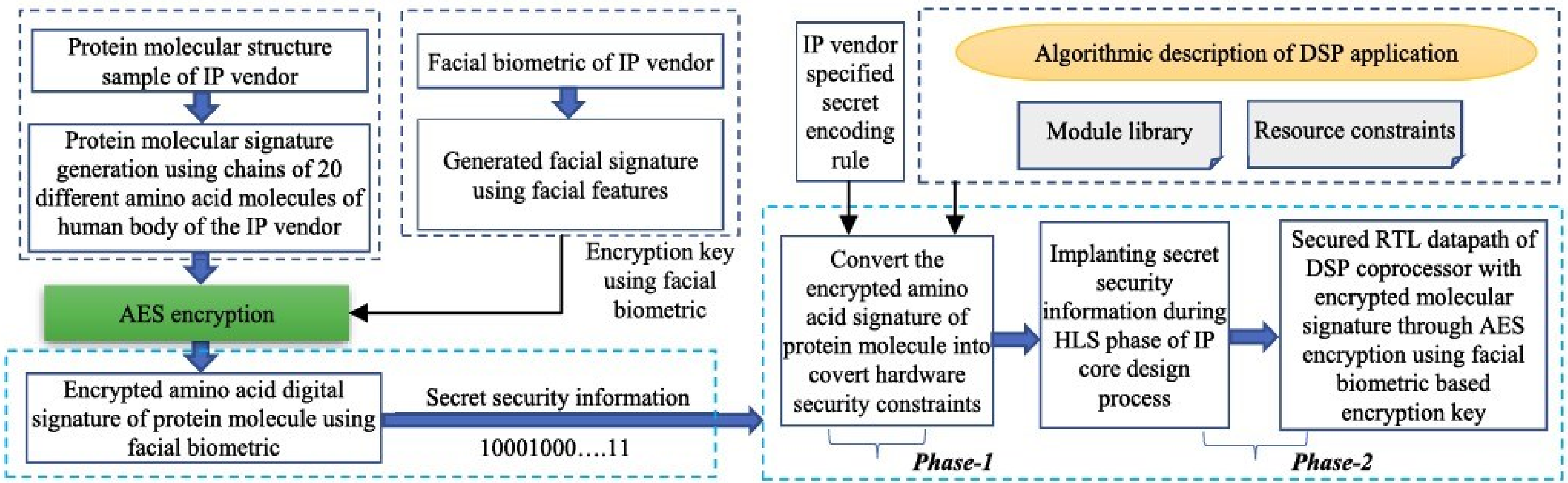
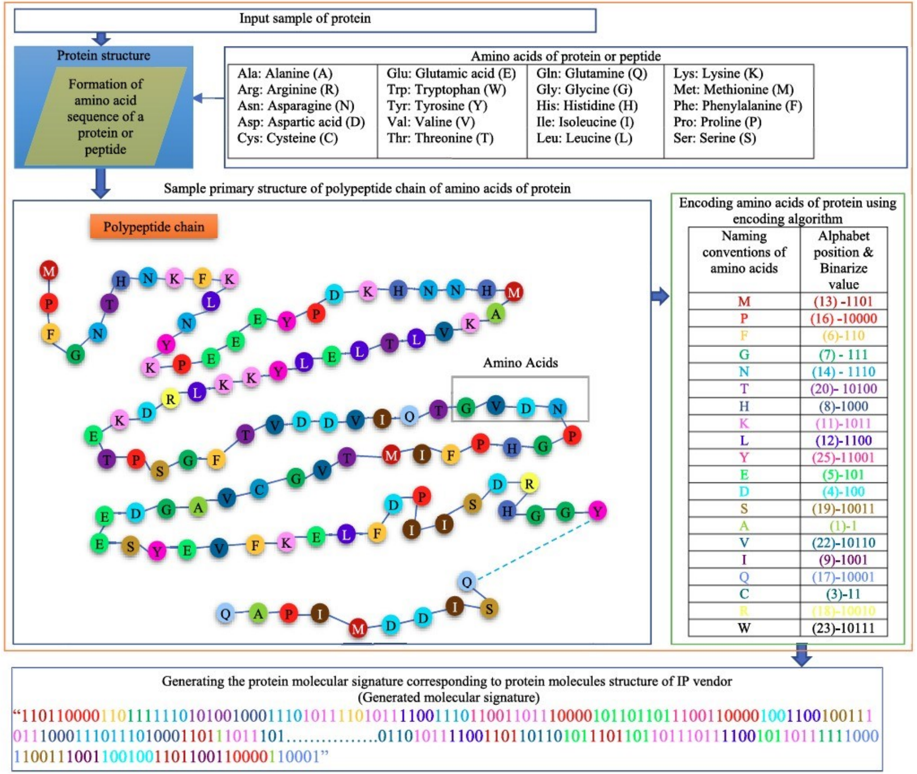

Protein molecular structure sample of IP vendor
Protein molecular signature generation using chains of 20 different amino acid molecules of human body of the IP vendor
Facial biometric of IP vendor
Generated facial signature using facial features
Encryption key using facial biometric
AES encryption
Encrypted amino acid digital signature of protein molecule using facial biometric
Secret security information
10001000….11
IP vendor specified secret encoding rule
Algorithmic description of DSP application
Module library
Resource constraints
Convert the encrypted amino acid signature of protein molecule into covert hardware security constraints
Implanting secret security information during HLS phase of IP core design process
Secured RTL datapath of DSP coprocessor with encrypted molecular signature through AES encryption using facial biometric based encryption key
Phase-1
Phase-2

Figure 7: Overview of the proposed methodology

Details of protein molecular signature generation process



Input sample of protein

Protein structure

Formation of amino acid sequence of a protein or peptide

Amino acids of protein or peptide

Ala: Alanine (A)	Glu: Glutamic acid (E)	Gln: Glutamine (Q)	Lys: Lysine (K)
Arg: Arginine (R)	Trp: Tryptophan (W)	Gly: Glycine (G)	Met: Methionine (M)
Asn: Asparagine (N)	Tyr: Tyrosine (Y)	His: Histidine (H)	Phe: Phenylalanine (F)
Asp: Aspartic acid (D)	Val: Valine (V)	Ile: Isoleucine (I)	Pro: Proline (P)
Cys: Cysteine (C)	Thr: Threonine (T)	Leu: Leucine (L)	Ser: Serine (S)

Sample primary structure of polypeptide chain of amino acids of protein

Encoding amino acids of protein using encoding algorithm

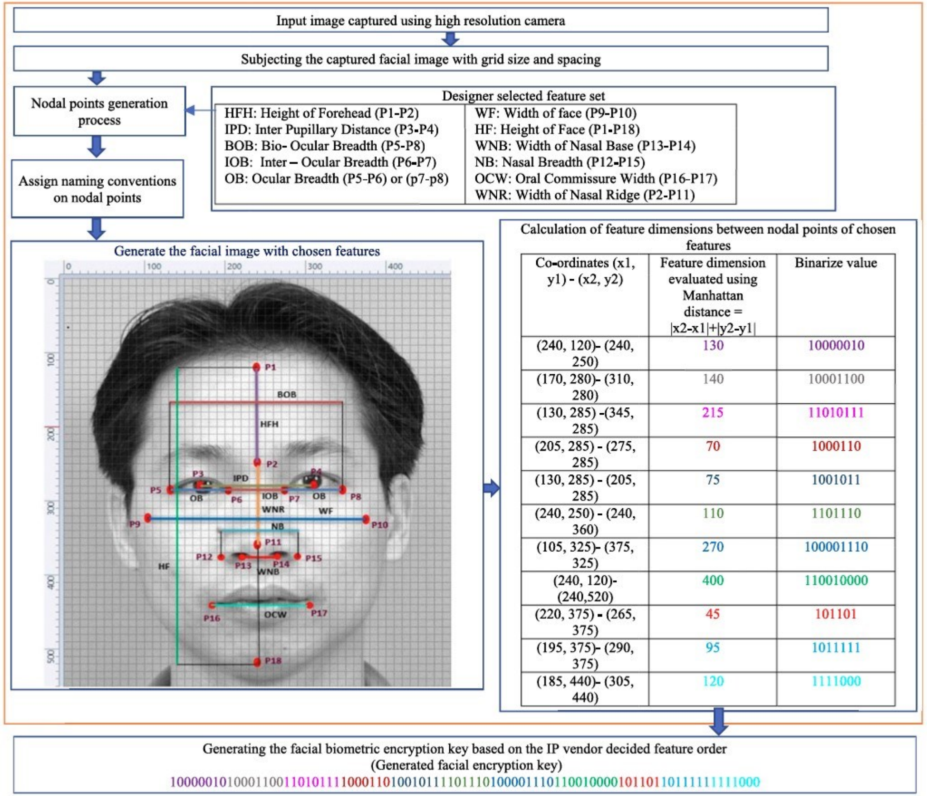
Naming conventions of amino acids	Alphabet position & Binarize value
M	(13) -1101
P	(16) -10000
F	(6)-110
G	(7) - 111
N	(14) - 1110
T	(20)- 10100
H	(8)-1000
K	(11)-1011
L	(12)-1100
Y	(25)-11001
E	(5)-101
D	(4)-100
S	(19)-10011
A	(1)-1
V	(22)-10110
I	(9)-1001
Q	(17)-10001
C	(3)-11
R	(18)-10010
W	(23)-10111

Generating the protein molecular signature corresponding to protein molecules structure of IP vendor
(Generated molecular signature)

“11011000011011111101010010001110101111010111100111011001101110000101101101110011000010011001001111
0111000111011101000110111011101……………0110101111001101101101011101101101110111100101101111111000
11001110011001001101100110000110001”

Figure 8: Generating the protein molecular signature corresponding to the amino acid sequence of sample protein

Details of IP seller’s facial biometric template generation process



Input image captured using high resolution camera

Subjecting the captured facial image with grid size and spacing

Nodal points generation process

Assign naming conventions on nodal points

Designer selected feature set

HFH: Height of Forehead (P1-P2)
IPD: Inter Pupillary Distance (P3-P4)
BOB: Bio- Ocular Breadth (P5-P8)
IOB: Inter – Ocular Breadth (P6-P7)
OB: Ocular Breadth (P5-P6) or (p7-p8)

WF: Width of face (P9-P10)
HF: Height of Face (P1-P18)
WNB: Width of Nasal Base (P13-P14)
NB: Nasal Breadth (P12-P15)
OCW: Oral Commissure Width (P16-P17)
WNR: Width of Nasal Ridge (P2-P11)

Generate the facial image with chosen features

Calculation of feature dimensions between nodal points of chosen features

Co-ordinates (x1, y1) - (x2, y2)	Feature dimension evaluated using Manhattan distance = |x2-x1|+|y2-y1|	Binarize value
(240, 120)- (240, 250)	130	10000010
(170, 280)- (310, 280)	140	10001100
(130, 285) -(345, 285)	215	11010111
(205, 285) - (275, 285)	70	1000110
(130, 285) - (205, 285)	75	1001011
(240, 250) - (240, 360)	110	1101110
(105, 325)- (375, 325)	270	100001110
(240, 120)- (240,520)	400	110010000
(220, 375) - (265, 375)	45	101101
(195, 375)- (290, 375)	95	1011111
(185, 440)- (305, 440)	120	1111000

Generating the facial biometric encryption key based on the IP vendor decided feature order
(Generated facial encryption key)
100000101000110011010111100011010010111101110100001110110010000101101101111111111000

Figure 9: Demonstration of facial biometric key generation used for encrypting the protein molecular signature

Details of IP seller’s facial biometric template generation process

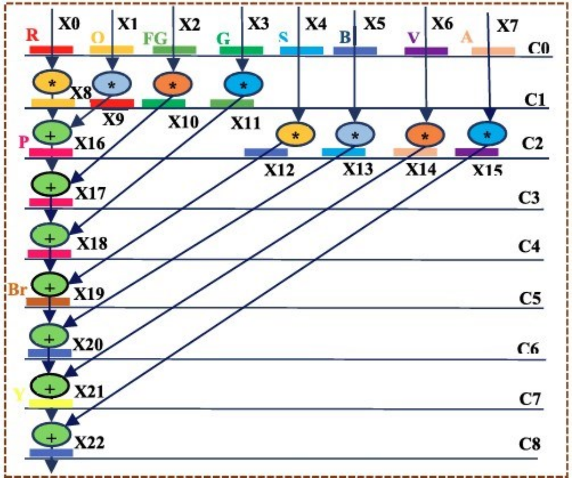
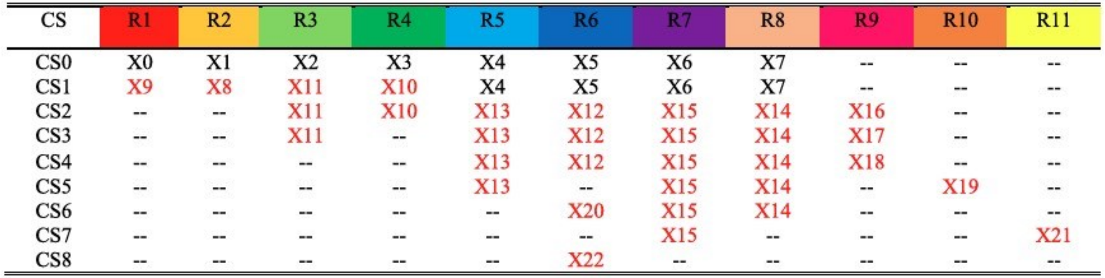


Figure 10: Scheduled DFG of DCT-8 with 1(+) and 4(∗) post embedding secret constraints

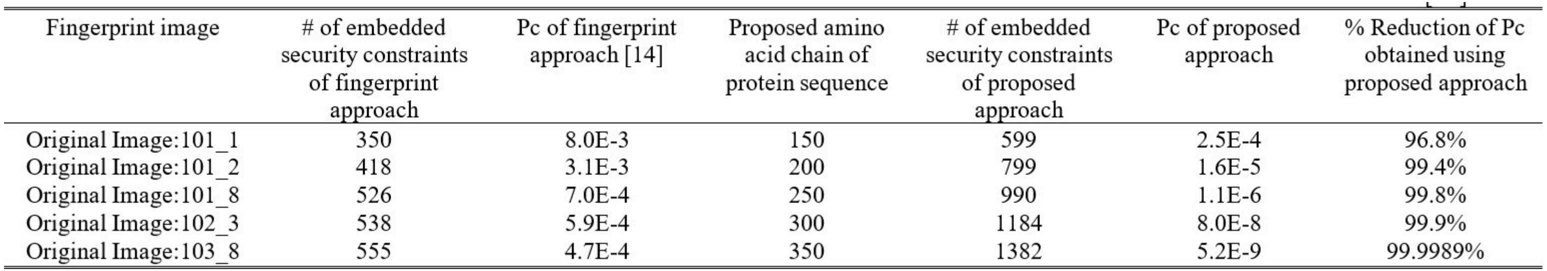
Table 7: Register allocation table (RAT) corresponding to 8-point DCT application after embedding watermarking constraints



CS	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11
CS0	X0	X1	X2	X3	X4	X5	X6	X7	--	--	--
CS1	X9	X8	X11	X10	X4	X5	X6	X7	--	--	--
CS2	--	--	X11	X10	X13	X12	X15	X14	X16	--	--
CS3	--	--	X11	--	X13	X12	X15	X14	X17	--	--
CS4	--	--	--	--	X13	X12	X15	X14	X18	--	--
CS5	--	--	--	--	X13	--	X15	X14	--	X19	--
CS6	--	--	--	--	--	X20	X15	X14	--	--	--
CS7	--	--	--	--	--	--	X15	--	--	--	X21
CS8	--	--	--	--	--	X22	--	--	--	--	--

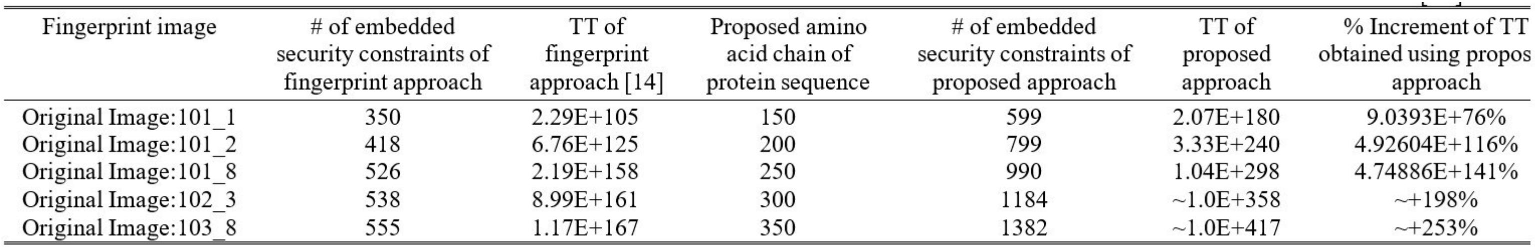
Results

Table 8: comparison of security in terms of Pc for JPEG-CODEC IP core between proposed approach and IP fingerprinting [14]



Fingerprint image	# of embedded security constraints of fingerprint approach	Pc of fingerprint approach [14]	Proposed amino acid chain of protein sequence	# of embedded security constraints of proposed approach	Pc of proposed approach	% Reduction of Pc obtained using proposed approach
Original Image:101_1	350	8.0E-3	150	599	2.5E-4	96.8%
Original Image:101_2	418	3.1E-3	200	799	1.6E-5	99.4%
Original Image:101_8	526	7.0E-4	250	990	1.1E-6	99.8%
Original Image:102_3	538	5.9E-4	300	1184	8.0E-8	99.9%
Original Image:103_8	555	4.7E-4	350	1382	5.2E-9	99.9989%

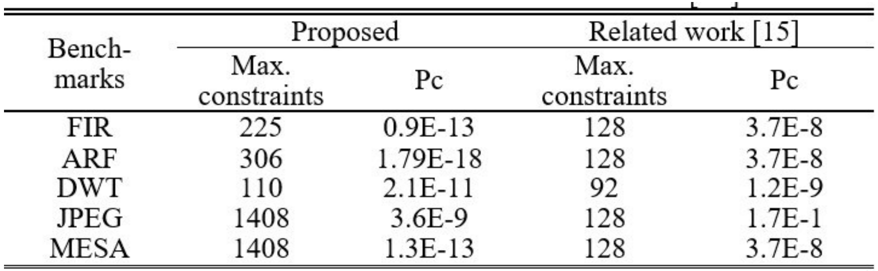
Table 9: Comparison of security in terms of TT for JPEG-CODEC IP core between proposed approach and IP fingerprinting [14]



Fingerprint image	# of embedded security constraints of fingerprint approach	TT of fingerprint approach [14]	Proposed amino acid chain of protein sequence	# of embedded security constraints of proposed approach	TT of proposed approach	% Increment of TT obtained using propos approach
Original Image:101_1	350	2.29E+105	150	599	2.07E+180	9.0393E+76%
Original Image:101_2	418	6.76E+125	200	799	3.33E+240	4.92604E+116%
Original Image:101_8	526	2.19E+158	250	990	1.04E+298	4.74886E+141%
Original Image:102_3	538	8.99E+161	300	1184	~1.0E+358	~+198%
Original Image:103_8	555	1.17E+167	350	1382	~1.0E+417	~+253%

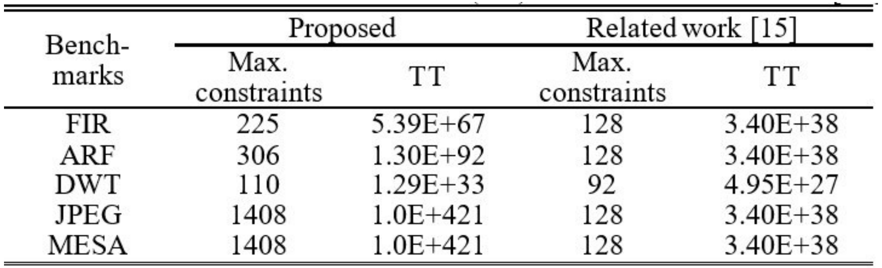
Results

Table 10: Comparison of Pc w.r.t. related work [15]



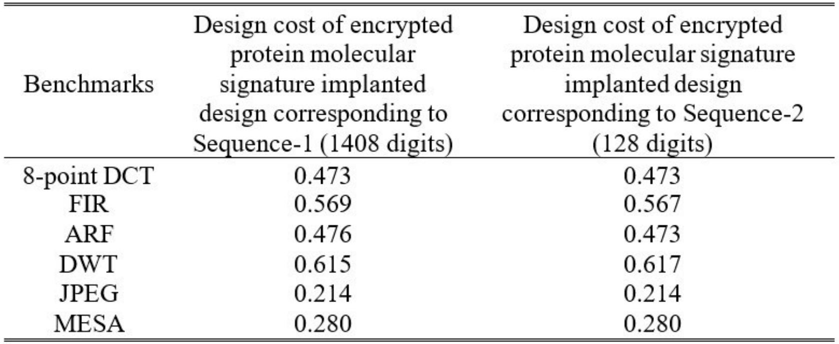
Bench-marks	Proposed		Related work [15]	
	Max. constraints	Pc	Max. constraints	Pc
FIR	225	0.9E-13	128	3.7E-8
ARF	306	1.79E-18	128	3.7E-8
DWT	110	2.1E-11	92	1.2E-9
JPEG	1408	3.6E-9	128	1.7E-1
MESA	1408	1.3E-13	128	3.7E-8

Table 11: Comparison of tamper tolerance (TT) w.r.t. related work [15]



Bench-marks	Proposed		Related work [15]	
	Max. constraints	TT	Max. constraints	TT
FIR	225	5.39E+67	128	3.40E+38
ARF	306	1.30E+92	128	3.40E+38
DWT	110	1.29E+33	92	4.95E+27
JPEG	1408	1.0E+421	128	3.40E+38
MESA	1408	1.0E+421	128	3.40E+38

Table 12: Design cost of embedding encrypted protein molecular signature



Benchmarks	Design cost of encrypted protein molecular signature implanted design corresponding to Sequence-1 (1408 digits)	Design cost of encrypted protein molecular signature implanted design corresponding to Sequence-2 (128 digits)
8-point DCT	0.473	0.473
FIR	0.569	0.567
ARF	0.476	0.473
DWT	0.615	0.617
JPEG	0.214	0.214
MESA	0.280	0.280

Proposed work (3)

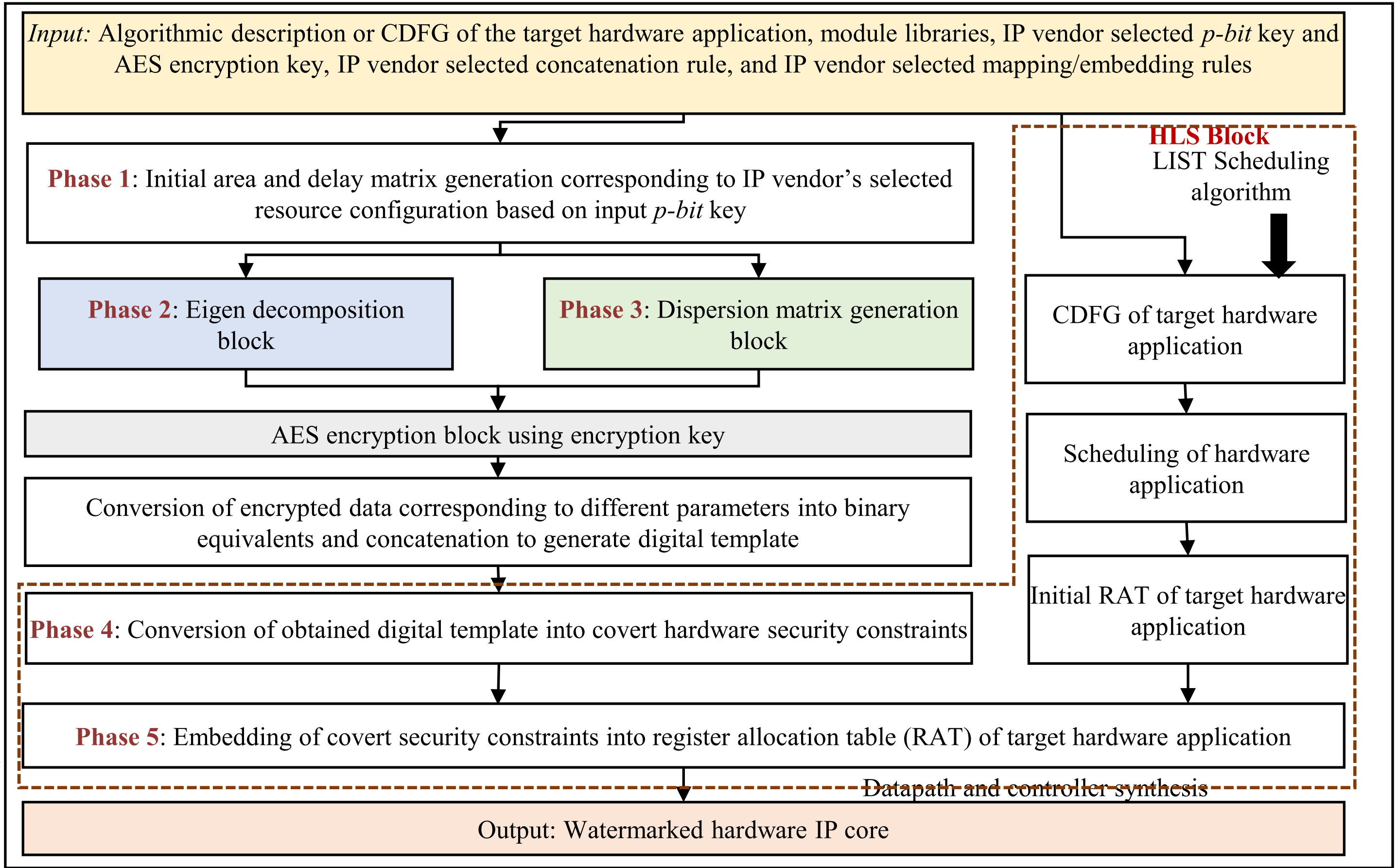
Watermarking Hardware IPs Using Design Parameter Driven Encrypted Dispersion Matrix With Eigen Decomposition Based Security Framework

- This paper presents a mathematical watermarking methodology using a design parameter-driven encrypted dispersion matrix (*characteristics of the IP vendor selected design space parameters*) with an eigen decomposition-based security framework (*design space's characteristics in terms of IP vendor chosen resource configuration*) for protecting hardware IP cores [12].
- An encrypted mathematical watermark is generated using dispersion matrix, eigen decomposition, and AES encryption.
- The encrypted watermark is then converted into watermarking constraints using the IP vendor's mapping rule and is further embedded in the hardware design during the register allocation phase of the HLS process.
- The embedded IP seller's watermark provides a detective countermeasure against potential IP piracy and false IP ownership claim by an adversary in SoC and fabrication house.

[12] A. Sengupta and A. Anshul, "Watermarking Hardware IPs Using Design Parameter Driven Encrypted Dispersion Matrix With Eigen Decomposition Based Security Framework," *IEEE Access*, vol. 12, pp. 47494-47507, 2024.

Proposed work (3): Flow diagram

Detailed of the proposed approach



Input: Algorithmic description or CDFG of the target hardware application, module libraries, IP vendor selected *p-bit* key and AES encryption key, IP vendor selected concatenation rule, and IP vendor selected mapping/embedding rules

Phase 1: Initial area and delay matrix generation corresponding to IP vendor's selected resource configuration based on input *p-bit* key

Phase 2: Eigen decomposition block

Phase 3: Dispersion matrix generation block

AES encryption block using encryption key

Conversion of encrypted data corresponding to different parameters into binary equivalents and concatenation to generate digital template

Phase 4: Conversion of obtained digital template into covert hardware security constraints

HLS Block

LIST Scheduling algorithm

CDFG of target hardware application

Scheduling of hardware application

Initial RAT of target hardware application

Phase 5: Embedding of covert security constraints into register allocation table (RAT) of target hardware application

Datapath and controller synthesis

Output: Watermarked hardware IP core

Figure 11: Overview of the proposed methodology

Generation of initial data

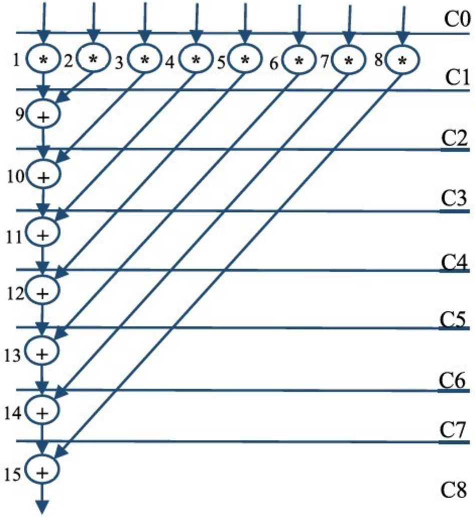
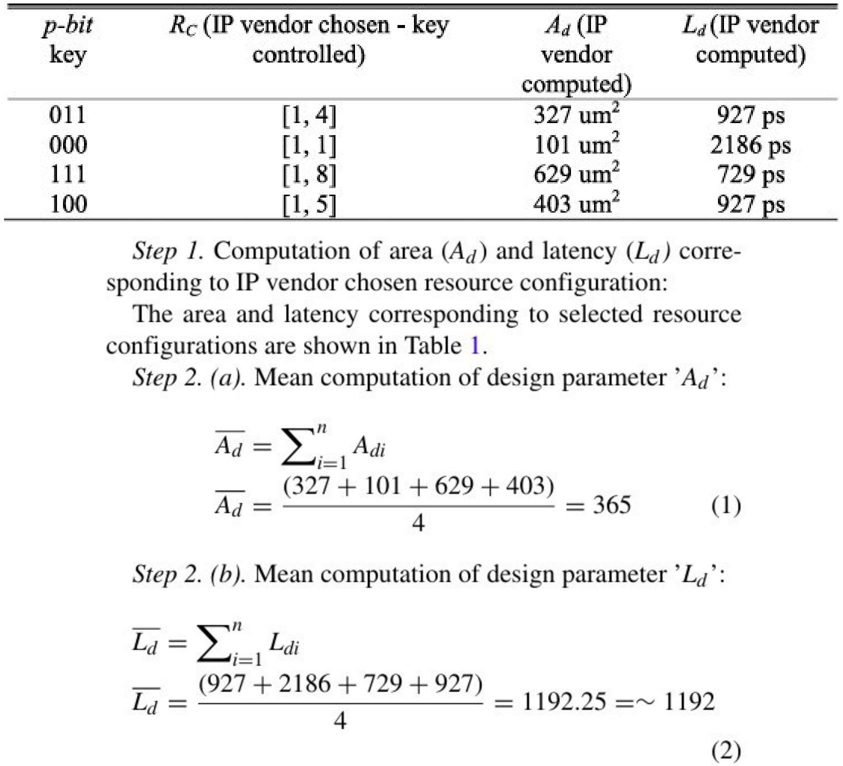


Figure 12: Control data flow graph of 8-point DCT



p-bit key	R_C (IP vendor chosen - key controlled)	A_d (IP vendor computed)	L_d (IP vendor computed)
011	[1, 4]	327 um^2	927 ps
000	[1, 1]	101 um^2	2186 ps
111	[1, 8]	629 um^2	729 ps
100	[1, 5]	403 um^2	927 ps

Step 1. Computation of area (A_d) and latency (L_d) corresponding to IP vendor chosen resource configuration:

The area and latency corresponding to selected resource configurations are shown in Table 1.

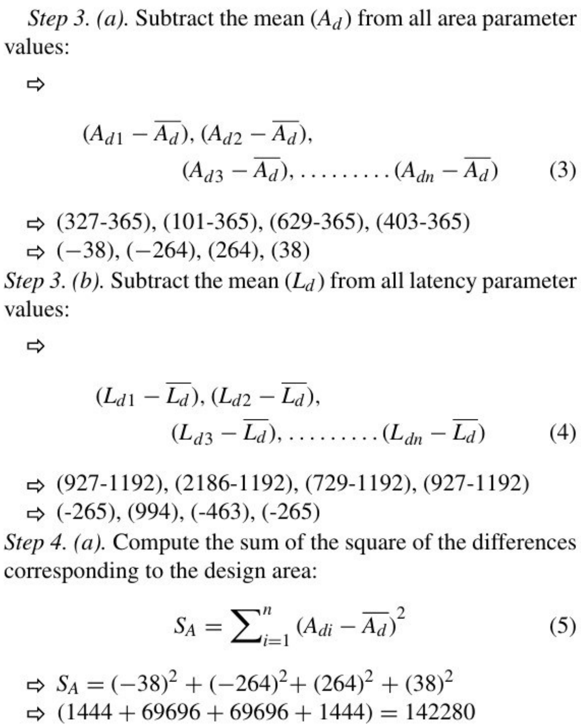
Step 2. (a). Mean computation of design parameter 'A_d':

$$\overline{A_d} = \sum\nolimits_{i=1}^{n} A_{di}$$
$$\overline{A_d} = \frac{(327 + 101 + 629 + 403)}{4} = 365 \qquad (1)$$

Step 2. (b). Mean computation of design parameter 'L_d':

$$\overline{L_d} = \sum\nolimits_{i=1}^{n} L_{di}$$
$$\overline{L_d} = \frac{(927 + 2186 + 729 + 927)}{4} = 1192.25 =\sim 1192 \qquad (2)$$

Estimation of dispersion matrix



Step 3. (a). Subtract the mean $(\overline{A_d})$ from all area parameter values:

⇨

$$(A_{d1}-\overline{A_d}),\ (A_{d2}-\overline{A_d}),\ (A_{d3}-\overline{A_d}), \ldots\ldots\ldots (A_{dn}-\overline{A_d}) \qquad (3)$$

⇨ (327-365), (101-365), (629-365), (403-365)

⇨ $(-38), (-264), (264), (38)$

Step 3. (b). Subtract the mean $(\overline{L_d})$ from all latency parameter values:

⇨

$$(L_{d1}-\overline{L_d}),\ (L_{d2}-\overline{L_d}),\ (L_{d3}-\overline{L_d}), \ldots\ldots\ldots (L_{dn}-\overline{L_d}) \qquad (4)$$

⇨ (927-1192), (2186-1192), (729-1192), (927-1192)

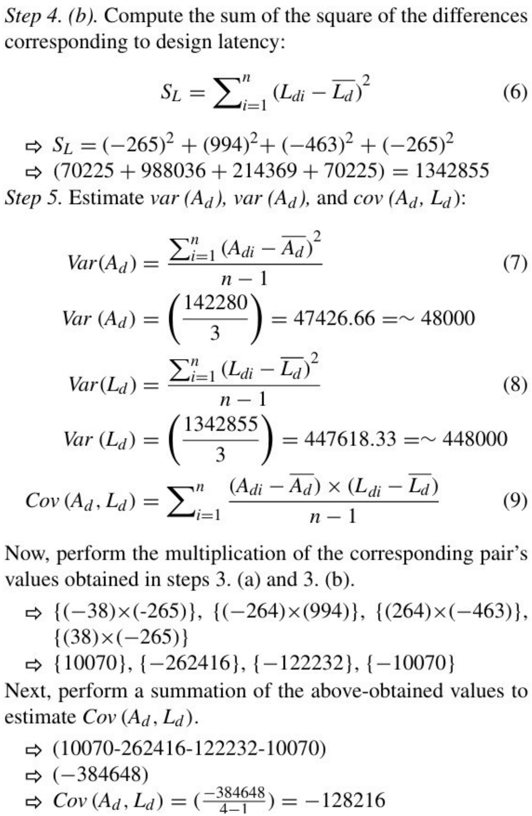
⇨ (-265), (994), (-463), (-265)

Step 4. (a). Compute the sum of the square of the differences corresponding to the design area:

$$S_A = \sum\nolimits_{i=1}^{n} (A_{di}-\overline{A_d})^2 \qquad (5)$$

⇨ $S_A = (-38)^2 + (-264)^2 + (264)^2 + (38)^2$

⇨ $(1444 + 69696 + 69696 + 1444) = 142280$



Step 4. (b). Compute the sum of the square of the differences corresponding to design latency:

$$S_L = \sum\nolimits_{i=1}^{n} (L_{di}-\overline{L_d})^2 \qquad (6)$$

⇨ $S_L = (-265)^2 + (994)^2 + (-463)^2 + (-265)^2$

⇨ $(70225 + 988036 + 214369 + 70225) = 1342855$

Step 5. Estimate *var* (A_d), *var* (A_d), and *cov* (A_d, L_d):

$$Var(A_d) = \frac{\sum_{i=1}^{n} (A_{di}-\overline{A_d})^2}{n-1} \qquad (7)$$

$$Var\ (A_d) = \left(\frac{142280}{3}\right) = 47426.66 =\sim 48000$$

$$Var(L_d) = \frac{\sum_{i=1}^{n} (L_{di}-\overline{L_d})^2}{n-1} \qquad (8)$$

$$Var\ (L_d) = \left(\frac{1342855}{3}\right) = 447618.33 =\sim 448000$$

$$Cov\ (A_d, L_d) = \sum\nolimits_{i=1}^{n} \frac{(A_{di}-\overline{A_d}) \times (L_{di}-\overline{L_d})}{n-1} \qquad (9)$$

Now, perform the multiplication of the corresponding pair's values obtained in steps 3. (a) and 3. (b).

⇨ $\{(-38)\times(-265)\}, \{(-264)\times(994)\}, \{(264)\times(-463)\}, \{(38)\times(-265)\}$

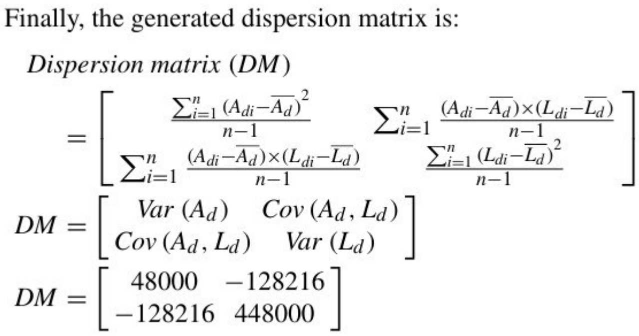
⇨ $\{10070\}, \{-262416\}, \{-122232\}, \{-10070\}$

Next, perform a summation of the above-obtained values to estimate *Cov* (A_d, L_d).

⇨ (10070-262416-122232-10070)

⇨ (-384648)

⇨ $Cov\ (A_d, L_d) = (\frac{-384648}{4-1}) = -128216$



Finally, the generated dispersion matrix is:

Dispersion matrix (DM)

$$= \begin{bmatrix} \frac{\sum_{i=1}^{n} (A_{di}-\overline{A_d})^2}{n-1} & \sum_{i=1}^{n} \frac{(A_{di}-\overline{A_d})\times(L_{di}-\overline{L_d})}{n-1} \\ \sum_{i=1}^{n} \frac{(A_{di}-\overline{A_d})\times(L_{di}-\overline{L_d})}{n-1} & \frac{\sum_{i=1}^{n} (L_{di}-\overline{L_d})^2}{n-1} \end{bmatrix}$$

$$DM = \begin{bmatrix} Var\ (A_d) & Cov\ (A_d, L_d) \\ Cov\ (A_d, L_d) & Var\ (L_d) \end{bmatrix}$$

$$DM = \begin{bmatrix} 48000 & -128216 \\ -128216 & 448000 \end{bmatrix}$$

Estimation of eigen roots

$$A = \begin{bmatrix} 1 & 4 \\ 1 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 8 \\ 1 & 5 \end{bmatrix}$$

$$\Rightarrow det\,(\lambda I - A) = 0$$

$$\Rightarrow det\left(\lambda \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 1 & 4 \\ 1 & 1 \end{bmatrix}\right) = 0$$

$$\Rightarrow det\left(\begin{bmatrix} \lambda - 1 & -4 \\ -1 & \lambda - 1 \end{bmatrix}\right) = 0$$

$$\Rightarrow \lambda^2 - 2\lambda - 3 = 0$$

$$\Rightarrow \lambda_1 = 3 and \lambda_2 = -1$$

Similarly,

$$\Rightarrow det\,(\lambda I - B) = 0$$

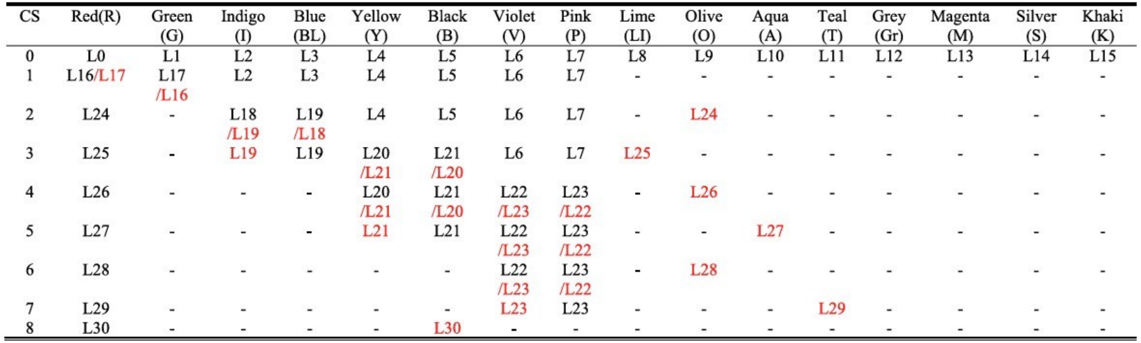
$$\Rightarrow det\left(\lambda \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 1 & 8 \\ 1 & 5 \end{bmatrix}\right) = 0$$

$$\Rightarrow det\left(\begin{bmatrix} \lambda - 1 & -8 \\ -1 & \lambda - 5 \end{bmatrix}\right) = 0$$

$$\Rightarrow \lambda^2 - 6\lambda - 3 = 0$$

$$\lambda_3 = 6.46 \; and \lambda_4 = -0.46$$

Table 13: Register allocation table (RAT) pre and post embedding generated signature



CS	Red(R)	Green (G)	Indigo (I)	Blue (BL)	Yellow (Y)	Black (B)	Violet (V)	Pink (P)	Lime (LI)	Olive (O)	Aqua (A)	Teal (T)	Grey (Gr)	Magenta (M)	Silver (S)	Khaki (K)
0	L0	L1	L2	L3	L4	L5	L6	L7	L8	L9	L10	L11	L12	L13	L14	L15
1	L16/L17	L17 /L16	L2	L3	L4	L5	L6	L7	-	-	-	-	-	-	-	-
2	L24	-	L18 /L19	L19 /L18	L4	L5	L6	L7	-	L24	-	-	-	-	-	-
3	L25	-	L19	L19	L20 /L21	L21 /L20	L6	L7	L25	-	-	-	-	-	-	-
4	L26	-	-	-	L20 /L21	L21 /L20	L22 /L23	L23 /L22	-	L26	-	-	-	-	-	-
5	L27	-	-	-	L21	L21	L22 /L23	L23 /L22	-	-	L27	-	-	-	-	-
6	L28	-	-	-	-	-	L22 /L23	L23 /L22	-	L28	-	-	-	-	-	-
7	L29	-	-	-	-	-	L23	L23	-	-	-	L29	-	-	-	-
8	L30	-	-	-	-	L30	-	-	-	-	-	-	-	-	-	-

Results(3)

Results

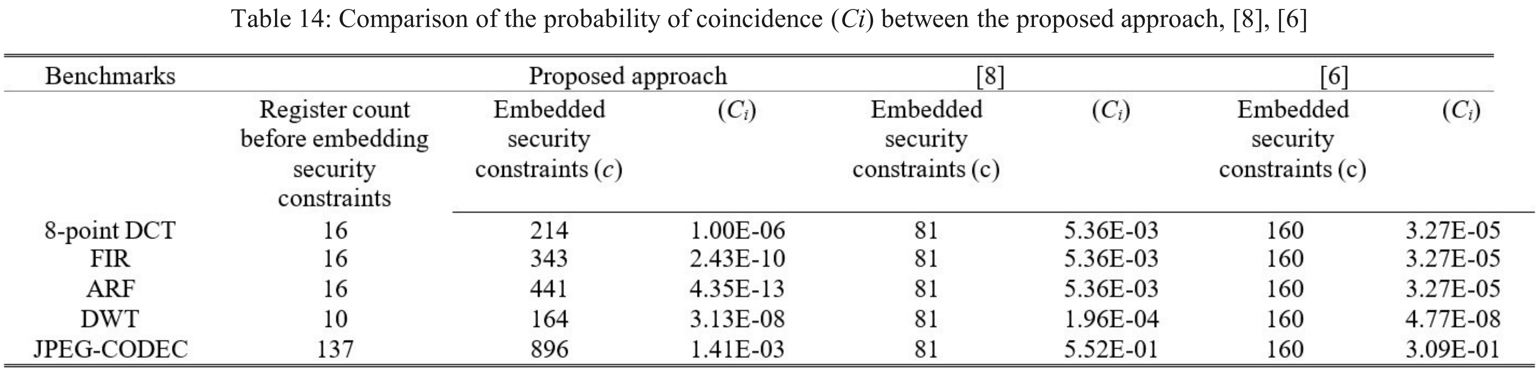


Table 14: Comparison of the probability of coincidence (*Ci*) between the proposed approach, [8], [6]

Benchmarks		Proposed approach		[8]		[6]	
	Register count before embedding security constraints	Embedded security constraints (*c*)	(C_i)	Embedded security constraints (c)	(C_i)	Embedded security constraints (c)	(C_i)
8-point DCT	16	214	1.00E-06	81	5.36E-03	160	3.27E-05
FIR	16	343	2.43E-10	81	5.36E-03	160	3.27E-05
ARF	16	441	4.35E-13	81	5.36E-03	160	3.27E-05
DWT	10	164	3.13E-08	81	1.96E-04	160	4.77E-08
JPEG-CODEC	137	896	1.41E-03	81	5.52E-01	160	3.09E-01

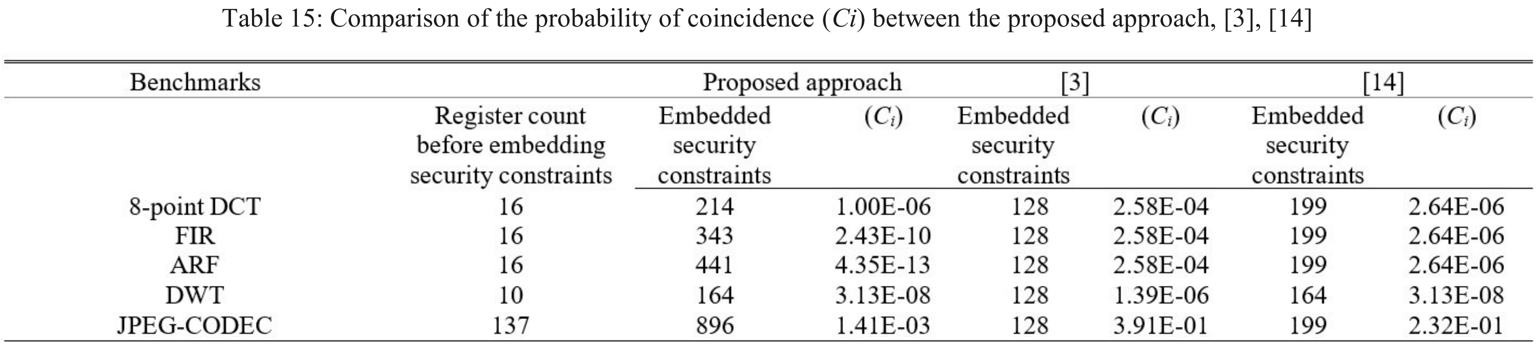


Table 15: Comparison of the probability of coincidence (*Ci*) between the proposed approach, [3], [14]

Benchmarks		Proposed approach		[3]		[14]	
	Register count before embedding security constraints	Embedded security constraints	(C_i)	Embedded security constraints	(C_i)	Embedded security constraints	(C_i)
8-point DCT	16	214	1.00E-06	128	2.58E-04	199	2.64E-06
FIR	16	343	2.43E-10	128	2.58E-04	199	2.64E-06
ARF	16	441	4.35E-13	128	2.58E-04	199	2.64E-06
DWT	10	164	3.13E-08	128	1.39E-06	164	3.13E-08
JPEG-CODEC	137	896	1.41E-03	128	3.91E-01	199	2.32E-01

Results

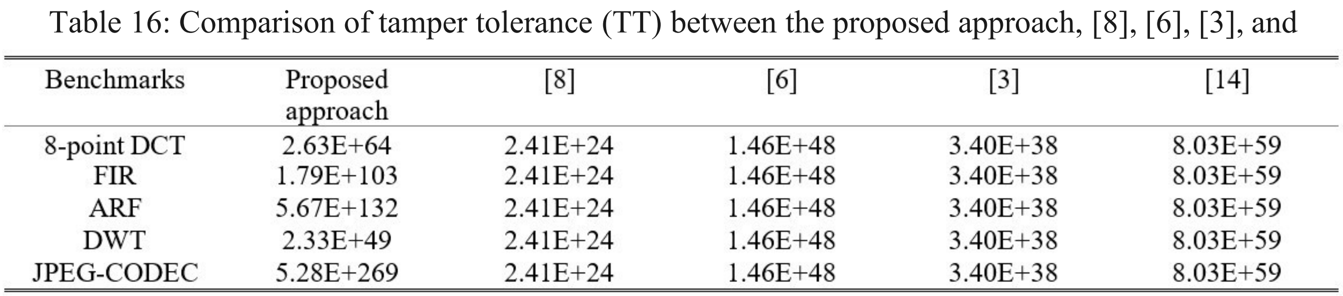


Table 16: Comparison of tamper tolerance (TT) between the proposed approach, [8], [6], [3], and

Benchmarks	Proposed approach	[8]	[6]	[3]	[14]
8-point DCT	2.63E+64	2.41E+24	1.46E+48	3.40E+38	8.03E+59
FIR	1.79E+103	2.41E+24	1.46E+48	3.40E+38	8.03E+59
ARF	5.67E+132	2.41E+24	1.46E+48	3.40E+38	8.03E+59
DWT	2.33E+49	2.41E+24	1.46E+48	3.40E+38	8.03E+59
JPEG-CODEC	5.28E+269	2.41E+24	1.46E+48	3.40E+38	8.03E+59

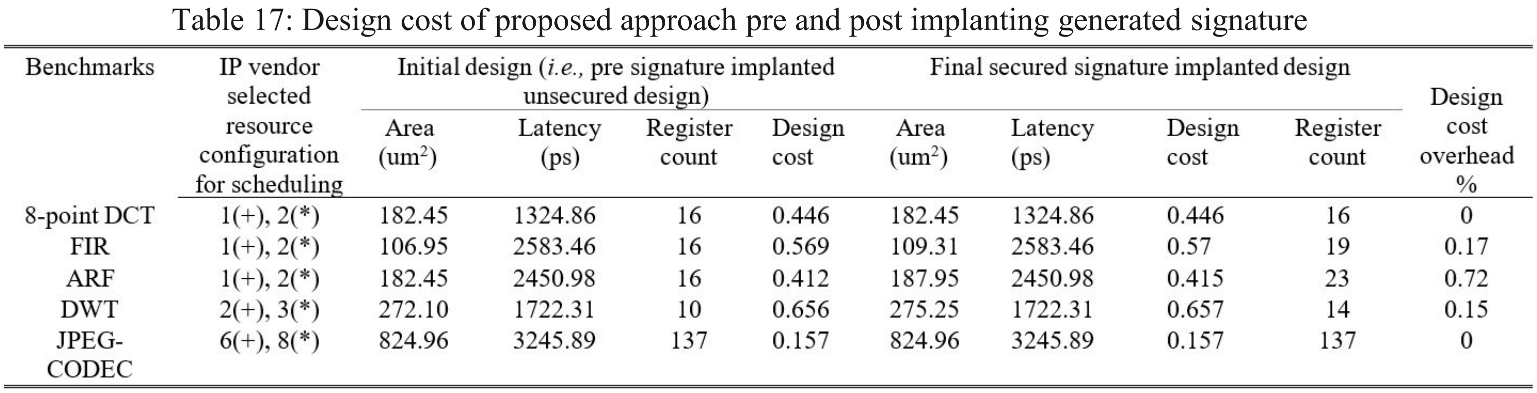


Table 17: Design cost of proposed approach pre and post implanting generated signature

Benchmarks	IP vendor selected resource configuration for scheduling	Initial design (*i.e.*, pre signature implanted unsecured design)				Final secured signature implanted design				Design cost overhead %
		Area (um^2)	Latency (ps)	Register count	Design cost	Area (um^2)	Latency (ps)	Design cost	Register count	
8-point DCT	1(+), 2(*)	182.45	1324.86	16	0.446	182.45	1324.86	0.446	16	0
FIR	1(+), 2(*)	106.95	2583.46	16	0.569	109.31	2583.46	0.57	19	0.17
ARF	1(+), 2(*)	182.45	2450.98	16	0.412	187.95	2450.98	0.415	23	0.72
DWT	2(+), 3(*)	272.10	1722.31	10	0.656	275.25	1722.31	0.657	14	0.15
JPEG-CODEC	6(+), 8(*)	824.96	3245.89	137	0.157	824.96	3245.89	0.157	137	0

Detection of embedded watermark for resolution of false IP ownership claim and IP piracy detection

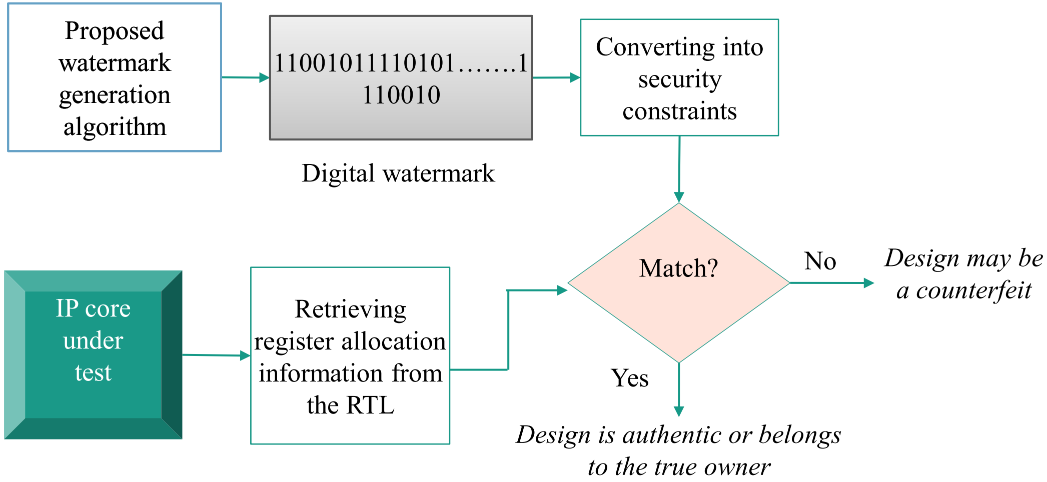

Proposed watermark generation algorithm
11001011110101…….1 110010
Digital watermark
Converting into security constraints
Match?
No
Design may be a counterfeit
Yes
Design is authentic or belongs to the true owner
IP core under test
Retrieving register allocation information from the RTL

Figure 13: Figure illustrating the signature/watermark detection for IP authentication/verification

Proposed work (4)

Exploration of Optimal Functional Trojan-Resistant Hardware Intellectual Property (IP) Core Designs during High Level Synthesis

- The proposed approach presents an exploration of optimized Trojan resistant (capable of detection and isolation both) hardware design architecture using the design space exploration framework of the HLS process [13].
- Presents a particle swarm optimization-driven design space exploration (PSO-DSE) to determine an optimal hardware IP core datapath after performing the design area-delay tradeoff.
- The proposed approach proposes a Trojan-resistant design flow for the reusable hardware IP core using TMR-based distinct multivendor allocation policy.
- This is the first work in the literature to present a complete Trojan resistant framework (from functional Trojans) for generation of low-cost hardware IP design, where Trojan unit computations are isolated in the final output value.

[13] A. Sengupta, A. Anshul, R. Chaurasia "Exploration of Optimal Functional Trojan-Resistant Hardware Intellectual Property (IP) Core Designs during High Level Synthesis", *Elsevier Journal on Microprocessors and Microsystems*, Volume 103, November 2023, 104973.

Motivation

● Hardware Trojan can be inserted by a rogue element or an adversary at any stage of the chip design cycle.

● The proposed approach addresses the threat model of functional hardware Trojans inserted covertly in third-party IP cores of hardware systems used in application-specific computing devices.

● Functional hardware Trojans have been investigated in the literature [20], [21], which shows that such Trojan logic could cause erroneous functional output, causing safety and reliability hazards to the end consumer.

● Such Trojans can create unreliable behavior if covertly inserted in real-time hardware systems of custom computing devices.

● Therefore, it is essential to detect and isolate these functional Trojan, such that the final computation of the hardware system should nor be disrupted.

● Some real world critical applications where these Trojans can cause safety hazard: (a) the presence of such Trojans in machine learning/ deep learning (CNN convolutional) coprocessor systems may alter the prediction of the model, (b) In image compression applications, such as JPEG-codec, a backdoor functional Trojan may induce incorrect computation of output pixel value, resulting in unwanted loss of important imaging/video data, etc.

Detailed flow diagram of the proposed approach

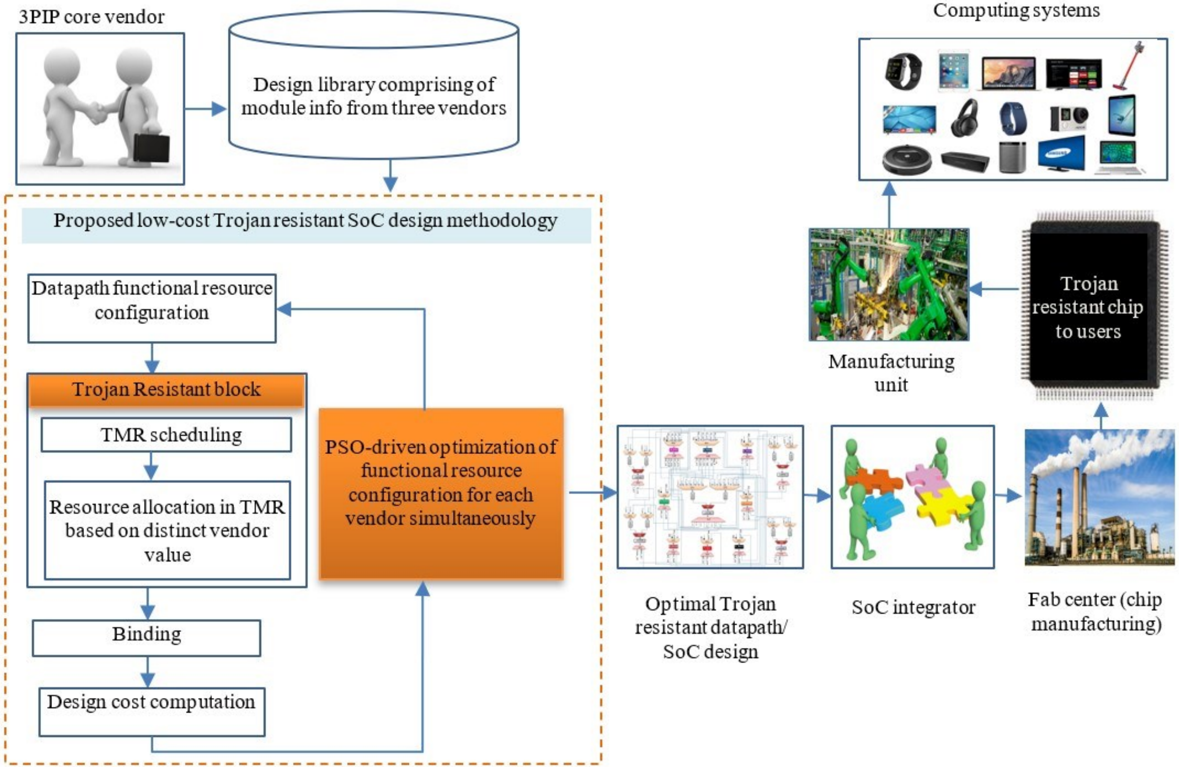

3PIP core vendor
Design library comprising of module info from three vendors
Proposed low-cost Trojan resistant SoC design methodology
Datapath functional resource configuration
Trojan Resistant block
TMR scheduling
Resource allocation in TMR based on distinct vendor value
Binding
Design cost computation
PSO-driven optimization of functional resource configuration for each vendor simultaneously
Optimal Trojan resistant datapath/ SoC design
SoC integrator
Fab center (chip manufacturing)
Trojan resistant chip to users
Manufacturing unit
Computing systems

Figure 14: Figure illustrating the Overview of proposed optimal Trojan defense IP core/SoC design generation process for DSP applications

Details of the TMR (Triple Modular Redundant unit)

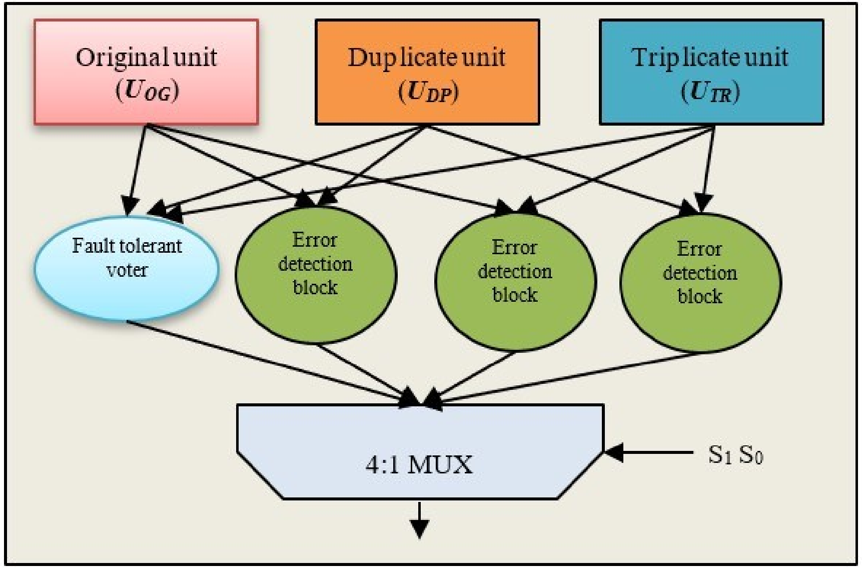


Figure 15: Illustration of the trojan resistance capability of the proposed approach with the help of voter and 4:1 multiplexer

Assumptions in the proposed approach:

1. The voter in the proposed approach is fault tolerant (adopted from [22]), which means it produces functionally correct output always.
2. We have considered an error detection block (EDB), which is a multi-stage setup (adopted from [22]) designed to protect the Trojan-resistant design from faulty comparators. The fault-tolerant voter and error detection block used in the proposed approach is considered to be Trojan-free (trustworthy). This is because these hardware modules are considered to be designed in-house (by a system integrator). In the proposed approach, the system integrator is considered to be trustworthy.
3. The information corresponding to multiple vendors is confidential and only known to the system integrator. The vendors are completely unaware of the information about their counterparts. As vendors in the proposed approach are unaware of their counterparts. Therefore, the chances of collusion between distinct unknown 3PIP vendors to achieve the same Trojan payload are very low. Henceforth, the proposed approach always, at minimum always, ensures Trojan detection [19].

Generation of low-cost Trojan resistant SDFG for FIR filter

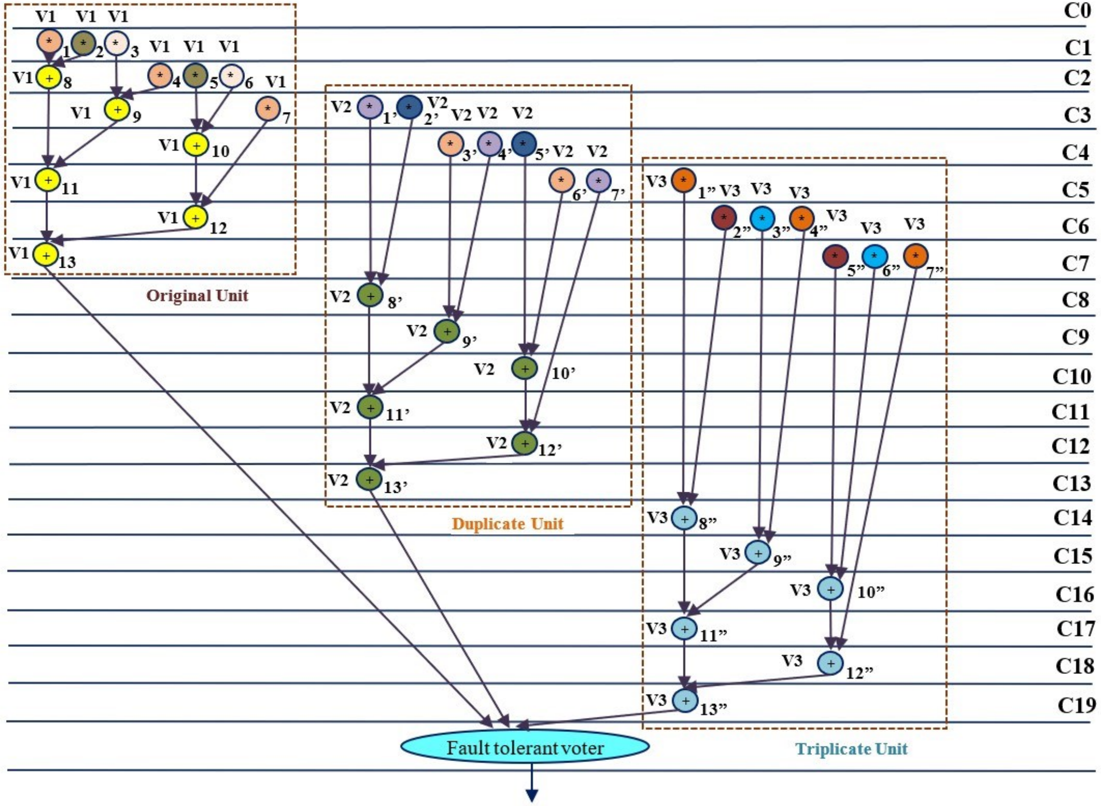


Figure 16: Scheduled data flow graph of FIR filter (TMR) with 9(*), 3(+).

Result

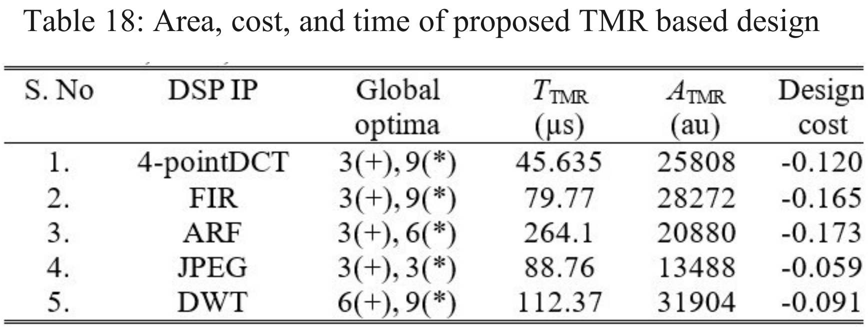
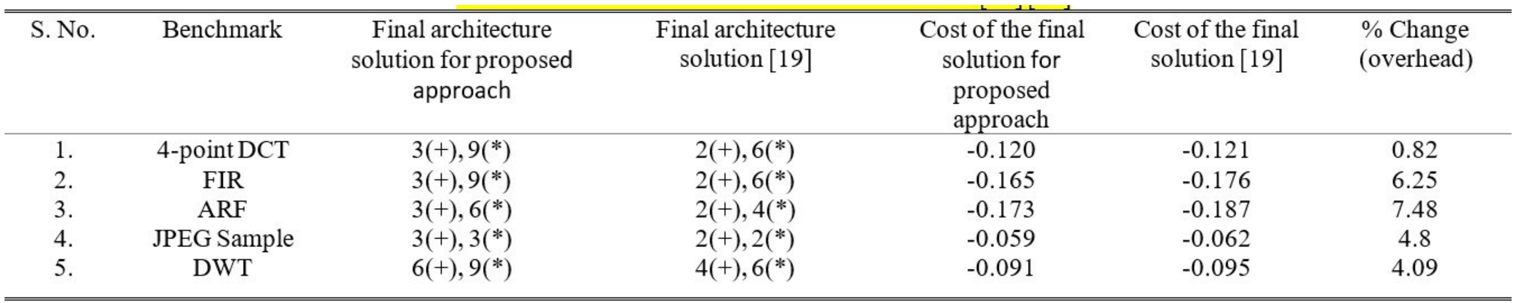


Table 18: Area, cost, and time of proposed TMR based design

S. No	DSP IP	Global optima	T_{TMR} (µs)	A_{TMR} (au)	Design cost
1.	4-pointDCT	3(+), 9(*)	45.635	25808	-0.120
2.	FIR	3(+), 9(*)	79.77	28272	-0.165
3.	ARF	3(+), 6(*)	264.1	20880	-0.173
4.	JPEG	3(+), 3(*)	88.76	13488	-0.059
5.	DWT	6(+), 9(*)	112.37	31904	-0.091

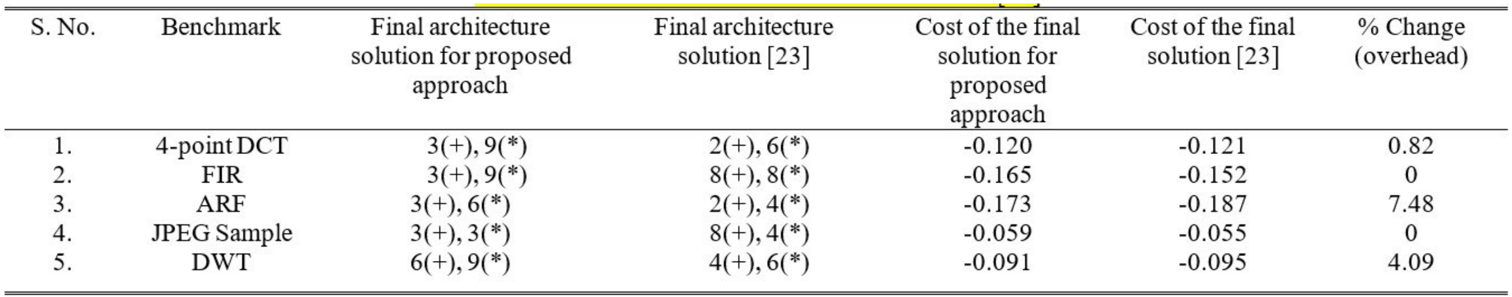
Results

Table 19: Comparison of the proposed approach with [19]



S. No.	Benchmark	Final architecture solution for proposed approach	Final architecture solution [19]	Cost of the final solution for proposed approach	Cost of the final solution [19]	% Change (overhead)
1.	4-point DCT	3(+), 9(*)	2(+), 6(*)	-0.120	-0.121	0.82
2.	FIR	3(+), 9(*)	2(+), 6(*)	-0.165	-0.176	6.25
3.	ARF	3(+), 6(*)	2(+), 4(*)	-0.173	-0.187	7.48
4.	JPEG Sample	3(+), 3(*)	2(+), 2(*)	-0.059	-0.062	4.8
5.	DWT	6(+), 9(*)	4(+), 6(*)	-0.091	-0.095	4.09

Table 20: Comparison of the proposed approach with [23]



S. No.	Benchmark	Final architecture solution for proposed approach	Final architecture solution [23]	Cost of the final solution for proposed approach	Cost of the final solution [23]	% Change (overhead)
1.	4-point DCT	3(+), 9(*)	2(+), 6(*)	-0.120	-0.121	0.82
2.	FIR	3(+), 9(*)	8(+), 8(*)	-0.165	-0.152	0
3.	ARF	3(+), 6(*)	2(+), 4(*)	-0.173	-0.187	7.48
4.	JPEG Sample	3(+), 3(*)	8(+), 4(*)	-0.059	-0.055	0
5.	DWT	6(+), 9(*)	4(+), 6(*)	-0.091	-0.095	4.09

Results:

Table 21: Comparison of convergence time (msec) for generating trojan resistant hardware designs *w.r.t* swarm size ‘*n*’

S. No.	Benchmark	n=3	n=5	n=7
1.	4-point DCT	16	24	27
2.	FIR	196	200	200
3.	ARF	32	57	96
4.	JPEG	44	48	93
5.	DWT	65	68	68

Table 22: Comparison of exploration time (msec) for generating trojan resistant hardware designs *w.r.t* swarm size ‘*n*’

S. No.	Benchmark	n=3	n=5	n=7
1.	4-point DCT	96	130	190
2.	FIR	674	867	973
3.	ARF	231	416	868
4.	JPEG	299	485	1048
5.	DWT	267	281	353

Publication list (Journals):

Journal publications (17 publications):

1. 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, pp. 826-839, June 2023, *Impact Factor: 2.8.*
2. M. Rathor, A. Sengupta, R. Chaurasia and A. Anshul, "Exploring Handwritten Signature Image Features for Hardware Security," **IEEE Transactions on Dependable and Secure Computing**, vol. 20, no. 5, pp. 3687-3698, 1 Sept.-Oct. 2023, *Impact Factor: 7.0.*
3. A. Sengupta, A. Anshul, Secure hardware IP of GLRT cascade using color interval graph based embedded fingerprint for ECG detector. **Nature Scientific Reports,** 14, 13250 (2024), *Impact factor: 3.8.*
4. M. Rathor, A. Anshul, Anirban Sengupta, "Securing Reusable IP Cores using Voice Biometric based Watermark", **IEEE Transactions on Dependable and Secure Computing**, Accepted, Sep 2023, *Impact factor: 7.0.*
5. A. Sengupta, A. Anshul, V. Chourasia and N. Kumar, "M-HLS: Malevolent High-Level Synthesis for Watermarked Hardware IPs," **IEEE Embedded Systems Letters**, Accepted, June 2024, *Impact factor: 1.7.*
6. A. Sengupta and A. Anshul, "Watermarking Hardware IPs Using Design Parameter Driven Encrypted Dispersion Matrix With Eigen Decomposition Based Security Framework," **IEEE Access**, vol. 12, pp. 47494-47507, 2024, *Impact Factor; 3.4.*
7. R. Chaurasia, A. Anshul, A. Sengupta and S. Gupta, "Palmprint Biometric Versus Encrypted Hash Based Digital Signature for Securing DSP Cores Used in CE Systems," **IEEE Consumer Electronics**, vol. 11, no. 5, pp. 73-80, 1 Sept. 2022, *Impact Factor: 3.7.*
8. A. Anshul and A. Sengupta, "A Survey of High Level Synthesis Based Hardware Security Approaches for Reusable IP Cores," **IEEE Circuits and Systems**, vol. 23, no. 4, pp. 44-62, Fourthquarter 2023, *Impact Factor: 5.6.*

Publication list (Journals):

Journal publications (Contd.):

9. 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, ISSN 0957-4174, *Impact Factor: 7.5*.

10. A. Anshul, A. Sengupta "Exploration of Optimal Crypto-Chain Signature Embedded Secure JPEG-CODEC Hardware IP during High Level Synthesis", **Elsevier Journal on Microprocessors and Microsystems**, Volume 102, October 2023, 104916, *Impact factor 1.9*.

11. A. Sengupta, A. Anshul, R. Chaurasia "Exploration of Optimal Functional Trojan-Resistant Hardware Intellectual Property (IP) Core Designs during High Level Synthesis", **Elsevier Journal on Microprocessors and Microsystems**, Volume 103, November 2023, 104973, *Impact Factor: 1.9*.

12. M. Rathor, A. Anshul, K Bharath, R. Chaurasia, A. Sengupta, Quadruple phase watermarking during high level synthesis for securing reusable hardware intellectual property cores, **Elsevier Computers and Electrical Engineering**, Volume 105, 2023, 108476, ISSN 0045-7906, *Impact factor: 4.0*.

13. A. Sengupta and A. Anshul, "A Survey of High Level Synthesis based Hardware (IP) Watermarking Approaches," ***IEEE Design & Test***, Accepted, 2024, doi: 10.1109/MDAT.2024.3435056, *Impact factor: 1.9*.

14. A. Sengupta, N. Bhui, A. Anshul, V. Chourasia "Bio-mimicking DNA Fingerprint Profiling for HLS Watermarking to Counter Hardware IP Piracy", **Nature Scientific Reports**, 14, Article number: 22413, 2024, DOI: https://doi.org/10.1038/s41598-024-73119-y, *Impact factor: 3.8*.

Publication list (Journals):

Journal publications (Contd.):

15. A. Sengupta, A. Anshul, V. Chourasia and N. Bhui, "Security Vulnerability (Backdoor Trojan) During Machine Learning Accelerator Design Phases," **IT Professional**, vol. 27, no. 1, pp. 65-72, Jan.-Feb. 2025, doi: 10.1109/MITP.2024.3519632, *Impact Factor: 2.2*.

16. A. Sengupta, A. Anshul, Exploring low overhead fingerprint biometric watermark for loop pipelined hardware IPs during behavioral synthesis, **Elsevier Journal of Information Security and Applications**, Volume 90, 2025, 104041, *Impact factor 3.8*.

17. A. Sengupta, A. Anshul, A. K. Singh, Hardware security against IP piracy using secure fingerprint encrypted fused amino-acid biometric with facial anthropometric signature, **Elsevier Journal on Microprocessors and Microsystems**, Volume 112, 2025, 105131, *Impact Factor: 1.9*.

Publication list (Conferences):

Conference publications (10 publications):

1. A. Sengupta, R. Chaurasia and A. 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)**, Tianjin, China, 2023, pp. 1-6.
2. A. Sengupta, A. Anshul, S. Thakur and C. 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, United Arab Emirates, 2023, pp. 218-221.
3. A. Sengupta, A. Anshul, C. Kothari and S. Thakur, "Secured and Optimized Hardware Accelerators using Key-Controlled Encoded Hash Slices and Firefly Algorithm based Exploration," **Proceedings of 35th IEEE International Conference on Microelectronics (ICM)**, Abu Dhabi, United Arab Emirates, 2023, pp. 149-152.
4. A. Anshul and A. Sengupta, "Low-Cost Hardware Security of Laplace Edge Detection and Embossment Filter Using HLS Based Encryption and PSO," **Proceedings of 9th IEEE International Symposium on Smart Electronic Systems (iSES)**, Ahmedabad, India, 2023, pp. 135-140.
5. A. Sengupta and A. Anshul, "Key-Driven Multi-Layered Structural Obfuscation of IP cores using Reconfigurable Obfuscator based Network Challenge and Switch Control Logic," **Proceedings of 9th IEEE International Symposium on Smart Electronic Systems (iSES)**, Ahmedabad, India, 2023, pp. 141-146.
6. A. Anshul, K. Bharath and A. Sengupta, "Designing Low Cost Secured DSP Core using Steganography and PSO for CE systems," **Proceedings of 8th IEEE International Symposium on Smart Electronic Systems (iSES)**, Warangal, India, 2022, pp. 95-100.

Publication list (Conferences):

Conference publications (Contd.):

7. A. Anshul and A. Sengupta, "IP Core Protection of Image Processing Filters with Multi-Level Encryption and Covert Steganographic Security Constraints," **Proceedings of 8th IEEE International Symposium on Smart Electronic Systems (iSES)**, Warangal, India, 2022, pp. 83-88.

8. A. Sengupta, V. Chourasia, A. Anshul "HLS Scheduling Driven Encoded Watermarking for Secure Convolutional Layer IP Design in CNN", **Proceedings of 11th IEEE International Conference on Consumer Electronics (ICCE-TW)**, Taichung, Taiwan, 2024, pp. 587-588, doi: 10.1109/ICCE-Taiwan62264.2024.10674266.

9. A. Sengupta, V. Chourasia, A. Anshul, N. Kumar "Robust Watermarking of Loop Unrolled Convolution Layer IP Design for CNN using 4-variable Encoded Register Allocation", **Proceedings of 11th IEEE International Conference on Consumer Electronics (ICCE-TW)**, Taichung, Taiwan, 2024, pp. 589-590, doi: 10.1109/ICCE-Taiwan62264.2024.10674385.

10. A. Sengupta, A. Anshul and V. Chourasia, "HLS Based Hardware Watermarking Using IP Seller's Superimposed Facial Anthropometric Features," **2024 IEEE International Symposium on Smart Electronic Systems (iSES)**, New Delhi, India, 2024, pp. 110-115, doi: 10.1109/iSES63344.2024.00032.

Publication list (Book chapters):

Book Chapters (10 publications):

1. A. Sengupta, A. Anshul "Palmprint Biometrics Vs. Fingerprint Biometrics Vs. Digital Signature using Encrypted Hash: Qualitative and Quantitative Comparison for Security of DSP coprocessors"**, IET Book "Physical Biometrics for Hardware Security of DSP and Machine Learning Coprocessors"**, 2023, Chapter DOI**:** 10.1049/PBCS080E_ch6.

2. A. Sengupta, A. Anshul "Secured Design Flow using Palmprint Biometrics, Steganography and PSO for DSP coprocessors"**, IET Book "Physical Biometrics for Hardware Security of DSP and Machine Learning Coprocessors"**, 2023, Chapter DOI: 10.1049/PBCS080E_ch7.

3. A. Sengupta, A. Anshul "Taxonomy of Hardware Security Methodologies: IP Core Protection and Obfuscation"**, IET Book "Physical Biometrics for Hardware Security of DSP and Machine Learning Coprocessors"**, 2023, Chapter DOI: 10.1049/PBCS080E_ch9.

4. A Anshul, R. Chaurasia, A. Sengupta "Securing Hardware Coprocessors against Piracy using Biometrics for Secured IoT systems"**, IET Book "Artificial Intelligence for Biometrics and Cybersecurity"**, 2023, Chapter DOI: 10.1049/PBSE020E_ch8.

5. A. Anshul, A. Sengupta "Role of Consumer Technology and Connected Electronic Devices on SCM: A Discussion on its Usages, Impact, and Challenges"**, UTHM Book "Evolution of Information, Communication and Computing System"**, 4(1), 1-11, 2023.

Publication list (Book chapters):

Book Chapters (Contd.):

5. A. Sengupta, A. Anshul "HLS Based Fingerprinting"**, IET Book "High-Level Synthesis based Methodologies for Hardware Security, Trust and IP Protection"**, 2024, Chapter DOI**:** 10.1049/PBCS084E_ch7.

6. A. Sengupta, A. Anshul "High Level Synthesis based Watermarking using Crypto-Chain Signature Framework"**, IET Book "High-Level Synthesis based Methodologies for Hardware Security, Trust and IP Protection"**, 2024, Chapter DOI**:** 10.1049/PBCS084E_ch6.

7. A. Sengupta, A. Anshul "High Level Synthesis based Watermarking using Multi-modal Biometric"**, IET Book "High-Level Synthesis based Methodologies for Hardware Security, Trust and IP Protection"**, 2024, Chapter DOI**:** 10.1049/PBCS084E_ch5.

8. A. Sengupta, A. Anshul "HLS based Mathematical Watermarks for Hardware Security and Trust"**, IET Book "High-Level Synthesis based Methodologies for Hardware Security, Trust and IP Protection"**, 2024, Chapter DOI**:** 10.1049/PBCS084E_ch4.

9. A. Sengupta, A. Anshul "High-Level Synthesis based Watermarking using Protein Molecular Biometric with Facial Biometric Encryption"**, IET Book "High-Level Synthesis based Methodologies for Hardware Security, Trust and IP Protection"**, 2024, Chapter DOI**:** 10.1049/PBCS084E_ch2.

References

1. A. Anshul and A. Sengupta, "A Survey of High Level Synthesis Based Hardware Security Approaches for Reusable IP Cores [Feature]," IEEE Circuits and Systems Magazine, vol. 23, no. 4, pp. 44-62, Fourthquarter 2023.
2. M. Rathor, A. Sengupta, R. Chaurasia and A. Anshul, "Exploring Handwritten Signature Image Features for Hardware Security," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 5, pp. 3687-3698, 1 Sept.-Oct. 2023.
3. 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.
4. 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.
5. A. Sengupta and M. Rathor, “IP Core Steganography for Protecting DSP Kernels Used in CE Systems,” in *IEEE Transactions on Consumer Electronics*, vol. 65, no. 4, pp. 506-515, Nov. 2019.
6. 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*, 183–186, 2008.
7. A. Sengupta, E. R. Kumar and N. P. Chandra, "Embedding Digital Signature Using Encrypted-Hashing for Protection of DSP Cores in CE," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 398-407, Aug. 2019.
8. 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.

References

9. A. Sengupta, R. Chaurasia and T. Reddy, "Contact-Less Palmprint Biometric for Securing DSP Coprocessors Used in CE Systems," *IEEE Transactions on Consumer Electronics*, vol. 67, no. 3, pp. 202-213, Aug. 2021.

10. A. Sengupta, A. Anshul, Secure hardware IP of GLRT cascade using color interval graph based embedded fingerprint for ECG detector. *Sci Rep* 14, 13250 (2024).

11. 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, pp. 826-839, June 2023.

12. A. Sengupta and A. Anshul, "Watermarking Hardware IPs Using Design Parameter Driven Encrypted Dispersion Matrix With Eigen Decomposition Based Security Framework," *IEEE Access*, vol. 12, pp. 47494-47507, 2024.

13. A. Sengupta, A. Anshul, R. Chaurasia "Exploration of Optimal Functional Trojan-Resistant Hardware Intellectual Property (IP) Core Designs during High Level Synthesis", *Elsevier Journal on Microprocessors and Microsystems*, Volume 103, November 2023, 104973.

14. A. Sengupta and M. Rathor, "Securing hardware accelerators for CE systems using biometric fingerprinting," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.,* vol. 28, no. 9, pp. 1979-1992, 2020.

15. A. Sengupta and R. Chaurasia, "Securing IP Cores for DSP Applications Using Structural Obfuscation and Chromosomal DNA Impression," in *IEEE Access*, vol. 10, pp. 50903-50913, 2022.

References

16. H. Martin, L. Entrena, S. Dupuis and G. Di Natale, "A Novel Use of Approximate Circuits to Thwart Hardware Trojan Insertion and Provide Obfuscation," *IEEE 24th International Symposium on On-Line Testing And Robust System Design (IOLTS)*, 2018, pp. 41-42.

17. N. B. Gunti and K. Lingasubramanian, "Neutralization of the Effect of Hardware Trojan in SCADA System Using Selectively Placed TMR," *2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, 2017, pp. 99-104.

18. H. Li, A. Abdelhadi, R. Shi, J. Zhang and Q. Liu, "Adversarial Hardware With Functional and Topological Camouflage," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 5, pp. 1685-1689, May 2021.

19. A. Sengupta, S. Bhadauria and S. P. Mohanty, "TL-HLS: Methodology for Low Cost Hardware Trojan Security Aware Scheduling With Optimal Loop Unrolling Factor During High Level Synthesis, " *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 36, no. 4,pp. 655-668, April 2017.

20. W. Hu, C. -H. Chang, A. Sengupta, S. Bhunia, R. Kastner and H. Li, “An Overview of Hardware Security and Trust: Threats, Countermeasures, and Design Tools,” *IEEE Trans. on Comput.-Aided Design of Integr. Circuits and Syst.*, vol. 40, no. 6, pp. 1010-1038, June 2021.

21. A. Nejat, Z. Kazemi, V. Beroulle, D. Hely and M. Fazeli, "Restricting Switching Activity Using Logic Locking to Improve Power Analysis-Based Trojan Detection," 2019 *IEEE 4th International Verification and Security Workshop (IVSW)*, 2019, pp. 49-54.

References

22. Deepak Kachave, Anirban Sengupta, “Integrating Physical Level Design and High Level Synthesis for Simultaneous Multi-Cycle Transient and Multiple Transient Fault Resiliency of Application Specific Datapath Processors”, *Elsevier Journal on Microelectronics Reliability*, Volume 60, Pages 141-152, May 2016.

23. J. J. Rajendran, O. Sinanoglu and R. Karri, "Building Trustworthy Systems Using Untrusted Components: A High-Level Synthesis Approach," in *IEEE Trans. Very Large Scale Integr. (VLSI) Syst*, vol. 24, no. 9, pp. 2946-2959, Sept. 2016.

Thank You!