Security Vs Design Cost of Signature Driven Security Methodologies for Reusable Hardware IP Core

Authors: Rahul Chaurasia, Anirban Sengupta

Outline

- Introduction and Motivation
- Contemporary Approaches
- Overview of Proposed Approach
- Discussion on Proposed Approach
- Results and Analysis

Introduction and Motivation

- The digital signal processing (DSP) intellectual property (IP) cores are the integral part of consumer electronic systems, used to facilitate **applications such as image, audio and video processing** with higher efficacy and low cost [1].
- **Need of Security-design cost trade-off**:
- Rapid growth in modern technology
- Globalization process,
- Demand of hardware IP core designs that are secure and low-cost.
- Orthogonal issues: optimized design architecture yielding **lower design cost** as well as **enhanced security**.
- To ensure optimization and robust security in parallel.

Contemporary Approaches

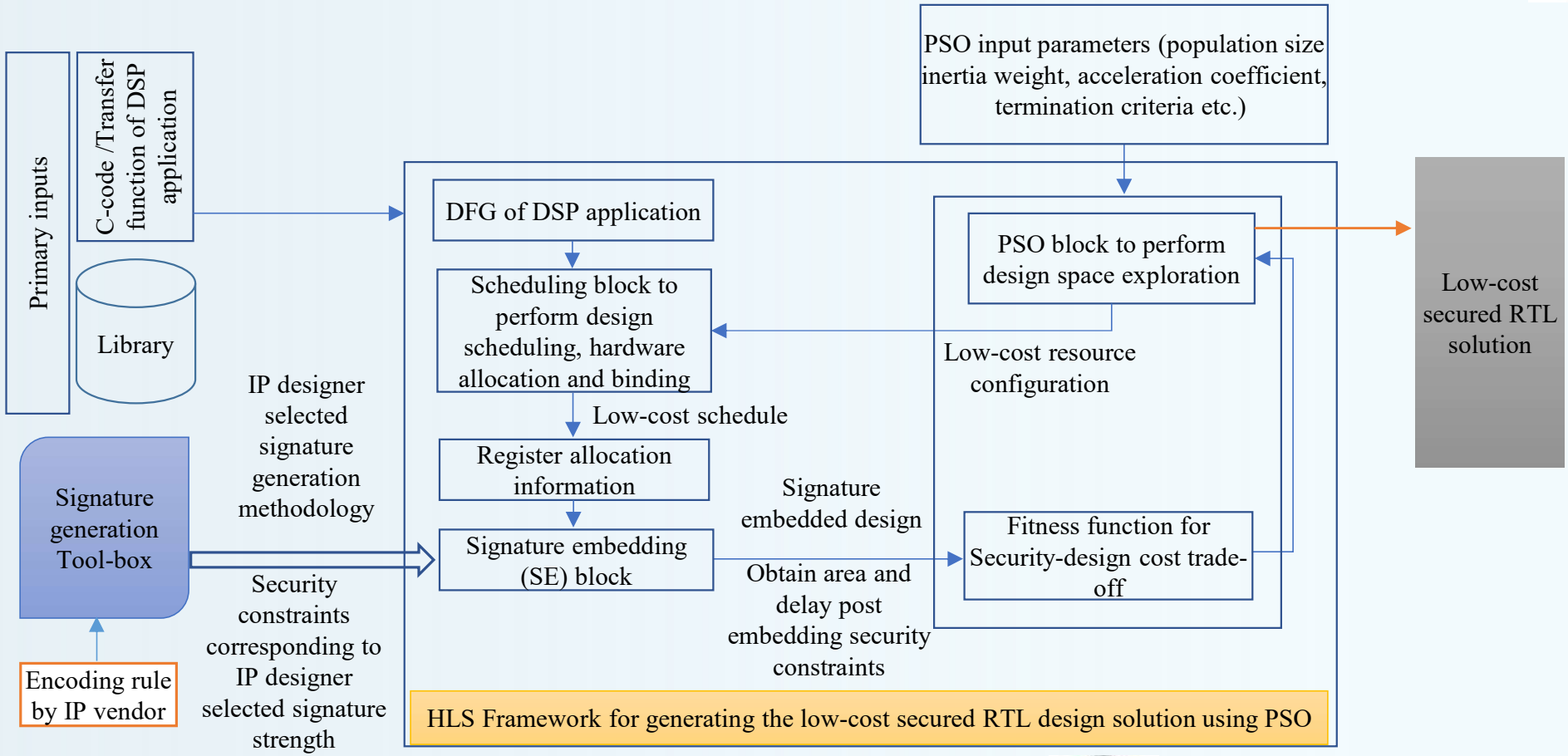
- The **watermarking approaches** [2], [3] insert security mark into the target design in the form of watermark, based on encoding of the auxiliary variable combinations.
- **Encrypted Hashing** [4], in this approach the generated digital signature is generated through encoding, secure hashing algorithm (SHA-512) and RSA encryption. Further, it involves complex computation during signature generation for hindering an adversary from regenerating the digital signature and also results into higher design cost .
- **Facial biometric** [5], based hardware security approach embeds IP vendor's authentic facial biometric constraints into the design. The facial biometric based digital template is generated by exploiting the nodal feature points of facial image.
- **Fingerprint biometric** [6], based hardware security approach embeds IP vendor's authentic fingerprint biometric constraints into the design. The fingerprint signature is generated based on the minutiae points of fingerprint.

➢ These approaches are incapable of generating solution for DSP architectures that satisfies both the objective of robust security and lower design cost.

Overview of Propose Approach

- Explores the **security-design cost tradeoff** for **signature-based security methodologies** used for IP piracy detection of DSP IP cores.
- It offers low-cost hardware design architectural solutions using particle swarm optimization (**PSO**).
- Three different hardware security methodologies such as **IP facial biometrics**, **encrypted-hashing** and **IP watermarking** have been integrated with the PSO framework for exploring the low-cost hardware architecture.
- The optimal DSP RTL hardware solution is optimized in terms of robust security and lower design cost (design area, delay).

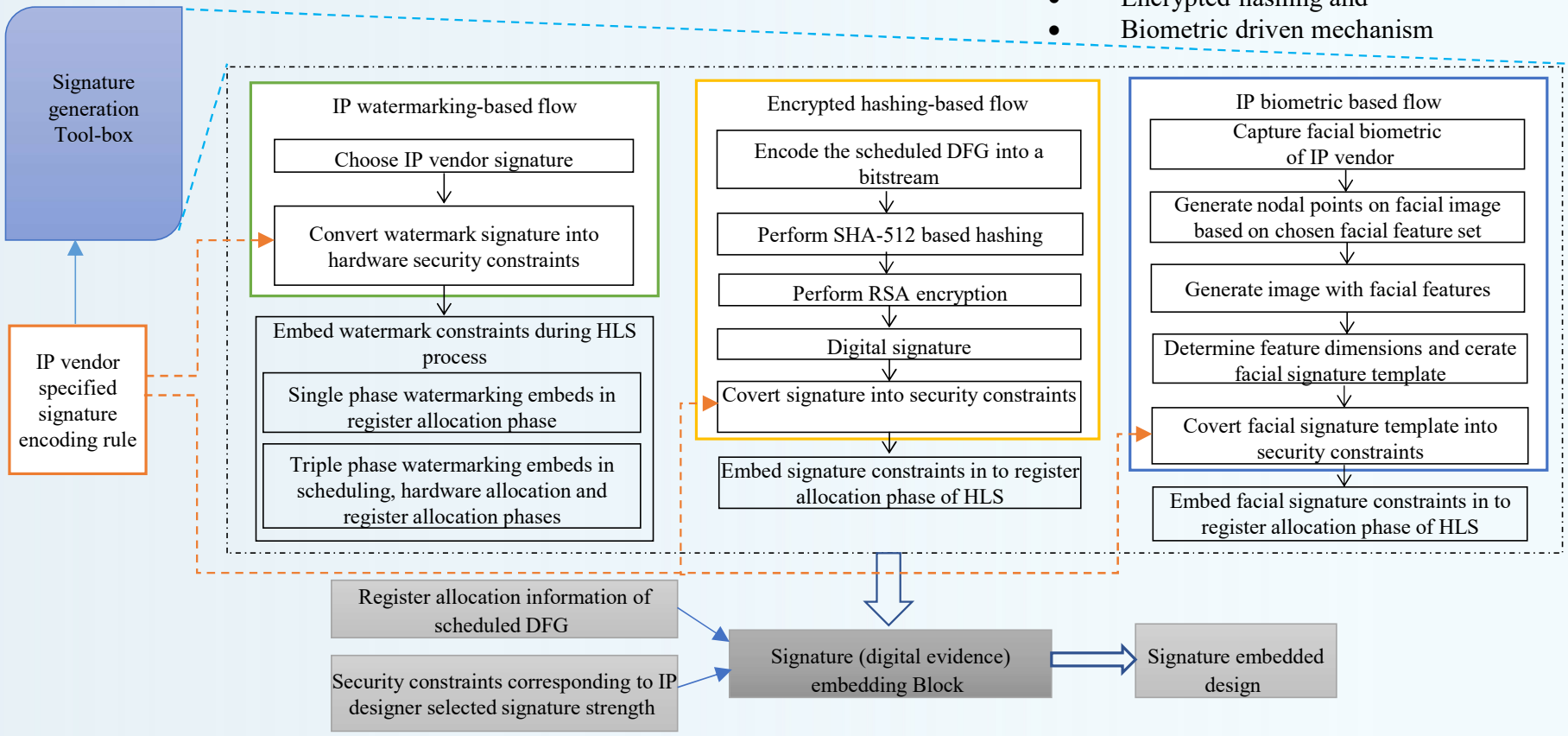
Design Flow of Proposed Work



Process flow of Security Approaches for Signature Generation

Signature generation methodology

- IP watermarking,
- Encrypted hashing and
- Biometric driven mechanism



Details of Signature Embedding Block:

Watermarking based hardware security:

- For the sake of brevity, assuming that watermark signature chosen by IP designer is: !,i,I,i,!,T,i,!,i,!,I,i,!,i,I,I.

Encoding rule for generating secret hardware security constraints

'!'- embed security constraints between Sv pairs of (zero-any integer).

'i'-embed a security constraints between 'Sv' pairs of (prime-prime),

'I'- embed a security constraints between Sv pairs of (even-even),

'T'- embed security constraints between Sv pairs of (odd-even) and

Therefore, the derived security constraints are:

for signature bit '!' → (S_V0-S_V1), (S_V0- S_V2), (S_V0- S_V3), (S_V0- S_V4), (S_V0- S_V5),

for 'i→ (S_V2, S_V3), (S_V2, S_V5), (S_V2, S_V7), (S_V2, S_V11), (S_V2, S_V13), (S_V2, S_V17),

for 'I'→ (S_V2, S_V4), (S_V2, S_V6), (S_V2, S_V8), (S_V2, S_V10) and

for 'T'→ (S_V1, S_V2).

Cont.

***Encrypted hash-based hardware security*:**

- ❑ It encodes the scheduled DFG of the DSP application into a bit stream based on the following encoding rule:
- ➢ Bit=’0’, if opn number and the CS number assigned to the operation are of same parity
- ➢ Bit=’1’, if opn number and the CS number assigned to the operation are of different parity.
- ✓ Then, perform hashing based on **SHA-512** algorithm and **RSA encryption.**
- ➢ Assuming that IP designer selected 16-bit binarized encrypted signature is: 1,1,0,1,0,1,0,1,0,1,0,1,1,0,0,1.
- ✓ The generated constraints based on encoding algorithm are:

(S_V0, S_V2), (S_V0, S_VV4), (S_V2, S_V3), (S_V0, S_V6), (S_V2, S_V5), (S_V0, S_V8), (S_V2, S_V7), (S_V0, S_V10), (S_V2, S_V11), (S_V0, S_V12), (S_V2, S_V13), ……, (S_V0, S_V18).

Cont.

***Facial biometric based hardware security*:**

- ✓ Capture facial biometric of IP vendor.
- ✓ Designate nodal points on captured facial image based on the chosen facial feature set (by IP vendor).
- ✓ Then, produce image with the facial features and determine feature dimensions.
- ✓ Thus, facial signature template has been generated.
- ✓ Assuming that the IP designer selected 16 bit facial biometric signature is (post truncating the biometric signature size) :
- ➢ 1,0,1,1,1,1,1,1,0,0,0,0,0,1,0,1.
- ✓ Generate hardware security constraints based on encoding rule: (S_V1,S_V3),(S_V0,S_V2),(S_V1,S_V5),(S_V1,S_V7),(S_V1,S_V9),(S_V1,S_V11),(S_V1,S_V13),(S_V1,S_V15),……,(S_V1,S_V19)

Signature Embedding Design:

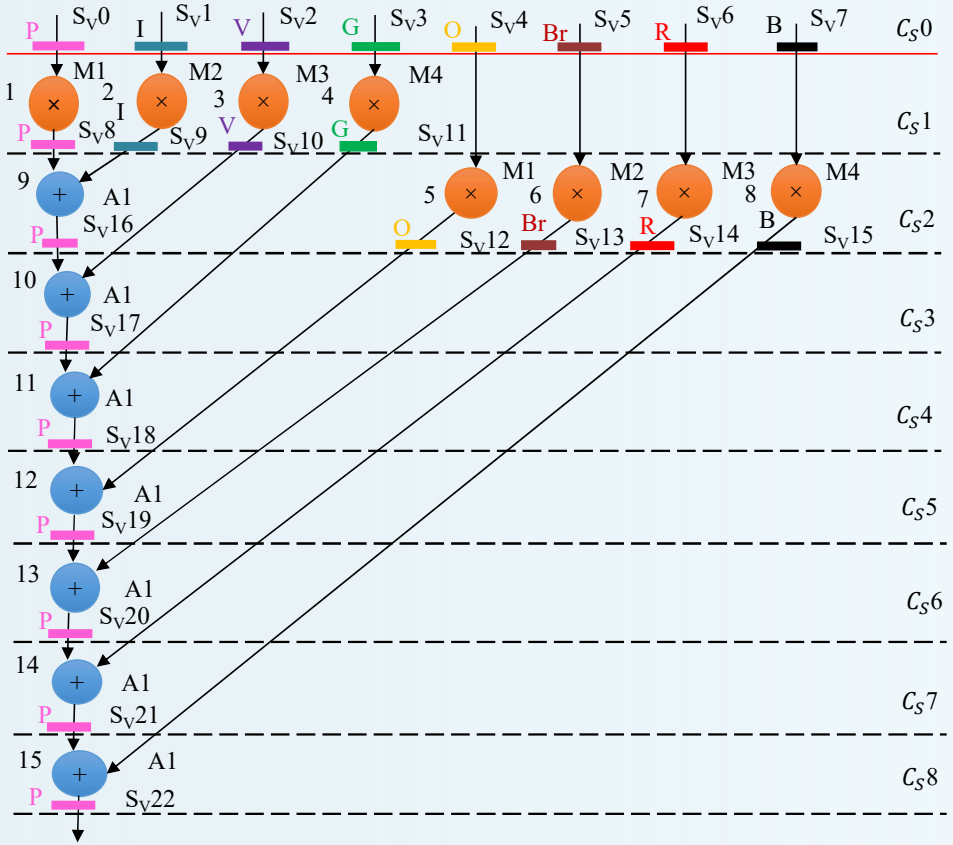


Fig. Scheduled DFG of 8-point DCT core using one adder (A) and four multipliers (M)

Register Allocation of 8-Point DCT (Pre-Embedding)

CS	Pink	Indigo	Violet	Green	Orange	Brown	Red	Black
C_S0	S_V0	S_V1	S_V2	S_V3	S_V4	S_V5	S_V6	S_V7
C_S1	S_V8	S_V9	S_V10	S_V11	S_V4	S_V5	S_V6	S_V7
C_S2	S_V16	--	S_V10	S_V11	S_V12	S_V13	S_V14	S_V15
C_S3	S_V17	--	--	S_V11	S_V12	S_V13	S_V14	S_V15
C_S4	S_V18		--	--	S_V12	S_V13	S_V14	S_V15
C_S5	S_V19	--	--	--	--	S_V13	S_V14	S_V15
C_S6	S_V20	--	--	--	--	--	S_V14	S_V15
C_S7	S_V21	--	--	--	--	--	--	S_V15
C_S8	S_V22	--	--	--	--	--	--	--

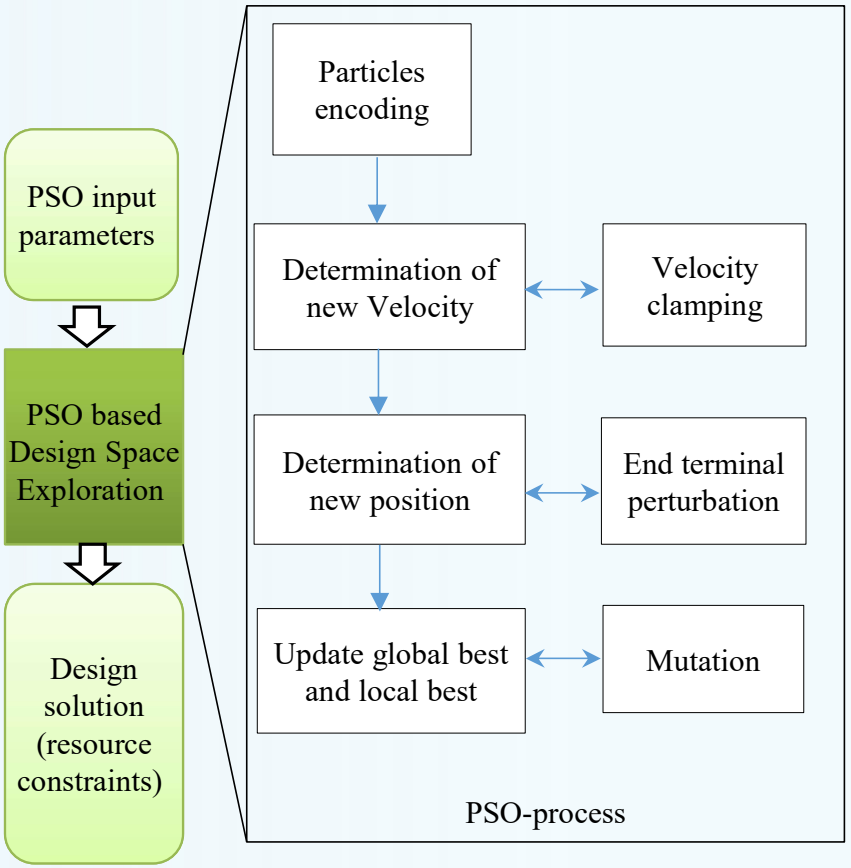
Register Allocation of 8-Point DCT (Post-Embedding in IP watermarking approach)

CS	pink	Indigo	violet	green	orange	brown	Red	Black
C_S0	S_V 0	S_V1	S_V2	S_V3	S_V4	S_V5	S_V6	S_V7
C_S1	S_V8	S_V9	S_V11	S_V10	S_V4	S_V5	S_V6	S_V7
C_S2	S_V16	--	S_V11	S_V10	S_V12	S_V13	S_V14	S_V15
C_S3	S_V17	--	S_V11	--	S_V12	S_V13	S_V14	S_V15
C_S4	S_V18		--	--	S_V12	S_V13	S_V14	S_V15
C_S5	S_V19	--	--	--	--	S_V13	S_V14	S_V15
C_S6	S_V20	--	--	--	--	--	S_V14	S_V15
C_S7	S_V21	--	--	--	--	--	--	S_V15
C_S8	S_V22	--	--	--	--	--	--	--

PSO based Design Space Exploration

- Initialize position of particles by hardware resources: S_n= (P1, P2), where P1 and P2 are the hardware resource types, adder(s) and multiplier(s) respectively (available in the library).
- For example, in 8-point DCT, particle positions are, S_1= $(1,1)_{min}$, S_2= $(1,8)_{max}$, S_3= $(1,4)_{Avg}$.
- Determined new velocity of the particles (initial velocity=0):

$$v_{id}^{+} = \tau.v_{id} + t1x1(S_{lbi} - S_{id}) + t2x2(S_{Gb} - S_{id})$$



Details of Fitness function for Security Design-Cost Tradeoff

- Based on the embedded security constraints, **security metric** in terms of embedded constraints size of the corresponding signature 'S_m^1' can be determined as:

$$\text{Security metric } (S_m^1) = L/M$$

Where '*L*' represents number of embedded security constraints and '*M*' represents total possible security constraints (corresponding to security methodology).

- Furthermore, the **design cost (Z_c)** of a particular DSP application is determined using metric.

$$Z_c(S_{id}) = W_a.(K_d/K_m) + W_l.(T_d/T_m)$$

- Subsequently, the **security-design cost tradeoff fitness** value for each particle can be determined using the equation below:

$$f_{S-C} = W_s(S_m^1) + W_d(Z_c)$$

Results and Analysis

Proposed approach analyzes the security of the signature-based security methodologies for DSP applications.

➢ *Security Analysis:*

The security of the proposed approach is analyzed in terms of probability of coincidence (strength of ownership proof).

- The Pc metric is formulated as follows [5]:

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

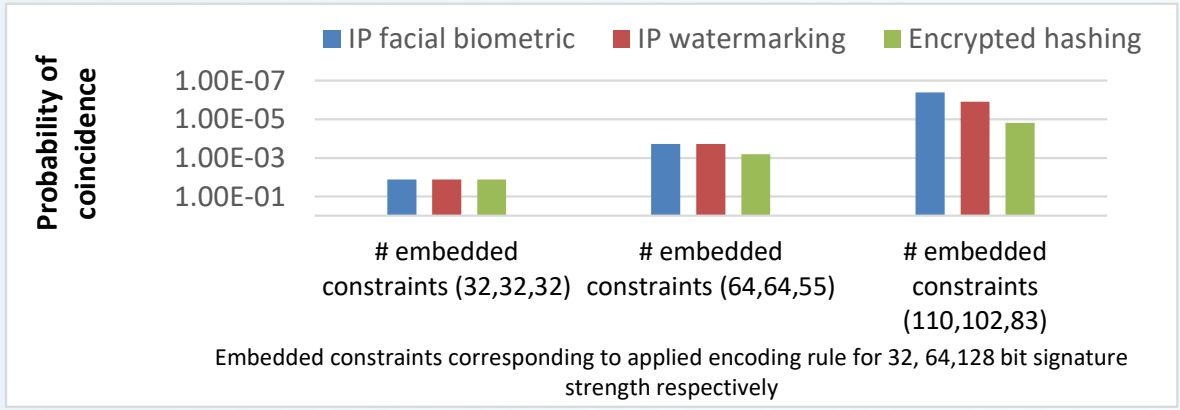


Fig. Pc comparison of security methodologies for 8-point DCT application

Results and Analysis

➢ *Analyzing the Security Methodologies in terms of Hardware Cost, Embedded Security Constraints and Exploration Time :*

Details of the IP Designer Selected Signature Strength, Embedded Security Constraints '*L*' Corresponding to the Encoding Rule of the Approach, Fitness Function, Design Area and Latency of the Proposed Approach for 8-Point DCT W.R.T. Various Security Methodologies.

Security methodology	Signature size (in bits)	'*L*'	Fitness value (Security -Design cost)	Design area 'Ad' (um2)	Design latency 'Ld' (ms.)
IP watermarking	32	32	0.32	327.15	927.39
	64	64	0.42	328.72	927.39
	128	102	0.53	328.72	927.39
Encrypted hashing	32	32	0.40	327.94	927.39
	64	55	0.52	327.94	927.39
	128	83	0.67	327.94	927.39
IP facial biometric	32	32	0.36	327.15	927.39
	64	64	0.50	327.94	927.39
	128	110	0.69	329.51	927.39

Details of the IP Designer Selected Signature Strength, Embedded Security Constraints '*L*' Corresponding to the Encoding Rule of the Approach, Fitness Function, Design Area and Latency of the Proposed Approach for FIR W.R.T. Various Security Methodologies.

Security methodology	IP designer selected signature size (in bits)	'*L*'	Fitness value (Security-Design cost)	Design area 'Ad' (um2)	Design latency 'Ld' (ms.)
IP watermarking	32	32	0.27	384.56	993.64
	64	64	0.32	385.35	993.64
	128	122	0.42	386.13	993.64
Encrypted hashing	32	32	0.31	383.77	993.64
	64	64	0.41	384.56	993.64
	128	100	0.52	385.35	993.64
IP facial biometric	32	32	0.29	383.77	993.64
	64	64	0.36	383.77	993.64
	128	128	0.50	385.35	993.64

Note: there is no change in the area and latency as the register count remains constant post embedding the signature.

Results and Analysis

Details of DSP Hardware Units Obtained During Trade-Off Exploration (Security–Design Cost)

DSP Application	Security methodology	Post embedding register count based on signature size(bits)			#Adder unit(s)	#Multiplier unit(s)	#Multiplexer units	#Demultiplexer units
		32	64	128				
8-point DCT	IP watermarking	8	10	10	1	4	10	5
	Encrypted hashing	9	9	9	1	4	10	5
	IP facial biometric	8	9	11	1	4	10	5
FIR	IP watermarking	9	10	11	4	4	16	8
	Encrypted hashing	8	9	10	4	4	16	8
	IP facial biometric	8	8	10	4	4	16	8

Details of Explored Global Best Resource Configuration and Exploration Time for Security Methodologies and DSP Applications

DSP application	Security methodology	Sgb	Exploration time
8-point DCT	Watermarking	[1,4]	164.4
	Encrypted hashing	[1,4]	150
	IP facial biometric	[1,4]	173.7
FIR	Watermarking	[4,4]	163.6
	Encrypted hashing	[4,4]	161.8
	IP facial biometric	[4,4]	153.1

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 Syst. Lett.*, vol. 10, no. 3, pp. 77-80, Sept. 2018.
2. R. Karmakar and S. Chattopadhyay, “Hardware IP Protection Using Logic Encryption and Watermarking,” *2020 IEEE International Test Conference (ITC)*, 2020, pp. 1-10.
3. F. Koushanfar, I. Hong and M. Potkonjak, “Behavioral synthesis techniques for intellectual property protection,” *ACM Trans. Des. Autom. Electron. Syst.*, vol. 10, no. 3, pp. 523-545, 2005.
4. A. Sengupta, E. R. Kumar and N. P. Chandra, “Embedding Digital Signature Using Encrypted-Hashing for Protection of DSP Cores in CE,” *in IEEE Trans. Consum. Electron.*, vol. 65 (3), pp. 398-407, 2019.
5. A. Sengupta and R. Chaurasia, "Secured Convolutional Layer IP Core in Convolutional Neural Network Using Facial Biometric," *IEEE Trans. Consum. Electron.*, vol. 68, no. 3, pp. 291-306, Aug. 2022.
6. 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.
7. V. Mishra, A. Sengupta, “MO-PSE: Adaptive Multi Objective Particle Swarm Optimization Based Design Space Exploration in Architectural Synthesis for Application Specific Processor Design”, *Elsevier Journal on Adv. in Eng. Softw.*, Vol. 67, January 2014, pp. 111-124.
8. 15 nm open cell library. [Online], Available: https://si2.org/open-cell-library/, last accessed on Jan. 2020.