Designing Low Cost Secured DSP Core using Steganography and PSO for CE systems

Paper ID: 1570845186

Track: Hardware for Secure Information Processing (SIP) - 1

Authors: Aditya Anshul, K Bharath, Anirban Sengupta

Speaker Name: Aditya Anshul

Introduction

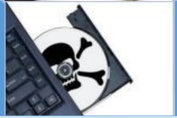
Intellectual Property (DSP IP cores)

- Chips, Integrated circuits, and other designs owned by a company, designer, or manufacturer.
- Processors, Co- Processors(DSP) and other Consumer Electronics hardware.
- These co-processors performs various data-intensive and power-hungry applications involving massive computations like data compression-decompression, digital data filtering, and different complex mathematical calculations.
- Due to globalization of design supply chain, the reusable IP cores or ICs are prone to various hardware threats [1], [2].

Figure 1: IC design process

Hardware Threats

Security Issues associated with hardware IP Cores

Sr. No.		Security Issues	Descriptions
1.		Intellectual property(IP) Cloning:	Assigning different names to the same cloned product.
2.		IP Counterfeiting:	Using different products under the same brand name.
3.		Hardware Trojan Attack:	Malicious circuitry that damages the functionality and trustworthiness.
4.		Overproduction:	Production of IP Cores more than the specified IP vendor licensing limit.
5.		False claim of ownership:	An adversary can fraudulently claim the ownership of IP.

Previous works

Related Work

Sr. No.	Existing Work	Technique Used	Remarks
1.	F. Koushanfar, I. Hong, and M. Potkonjak [6] (2005)	Hardware watermarking using two-variable (0, 1) signature encoding process.	Weak watermarking mechanism due to involvement of only two variable signature encoding process. Not robust and future proof.
2.	A. Sengupta and S. Bhadauria [7] (2016)	Hardware watermarking using four variable (i, I, T, !) signature encoding process to implant additional security constraints in the colored interval graph (CIG) of respective DSP applications using the HLS framework.	The watermark (original signature) inserted by watermarking technique becomes vulnerable if relevant information (like signature size, digit encoding, and digit combination) gets leaked.
3.	J. Qiu, H. Li, J. Dong, and G. Feng [3] (2017)	A biometrics encryption methodology is proposed using palmprint biometric and convolutional code for user authentication.	This approach is based on palmprint biometric for user authentication, however does not demonstrates the security of hardware IP core.

Proposed work

- The proposed approach based on a low-cost steganography technique for protection of complex reusable IP Cores used in CE Systems.
- The proposed approach is signature-free and capable of generating hardware security constraints for securing a DSP Kernel application.
- It makes use of the register allocation table of DSP kernel application itself to generate hardware security constraints.
- The generated hardware security constraints then embedded in the IP Cores design to authenticate genuine IP Maker.
- Threshold entropy option in the approach provides more control to designer as compared to signature based approach.
- Particle swarm optimization based design space exploration (PSO-DSE) is used to in the proposed approach to generate a low-cost optimized solution corresponding to secured DSP IP core.

PSO-DSE module

PSO-DSE module

- The integration of the PSO-DSE block with the steganography based security methodology serves the objective of determining an optimized architectural solution.
- PSO prunes the design search space based on IP vendor specified high level specification such as area, delay, energy, power, etc. corresponding to secured DSP design to generate an optimized low-cost design.

Advantage of PSO-DSE [8] over others such as genetic algorithm [4] and bacterial foraging [5] based DSE:

- PSO-DSE considers the magnitude of the previously computed velocity with the help of a parameter called inertia weight, while [4] and [5] do not consider the momentum of prior iterations, which increases the probability of getting stuck in the local minima during architecture exploration.
- PSO-DSE creates a balance between exploitation and exploration time with the help of linearly decreasing the value of inertia from 0.9 to 0.1. The algorithm takes more significant steps at the beginning and smaller steps on reaching higher fitness solutions, which is missing in [4]and [5]. This also enhances the chance of reaching global optimal solution.
- The inclusion of various other factors (hyperparameters), such as social and cognitive factors in PSO-DSE, helps achieve higher fitness solution within a very low exploration time.

Flow Diagram

Flow Diagram

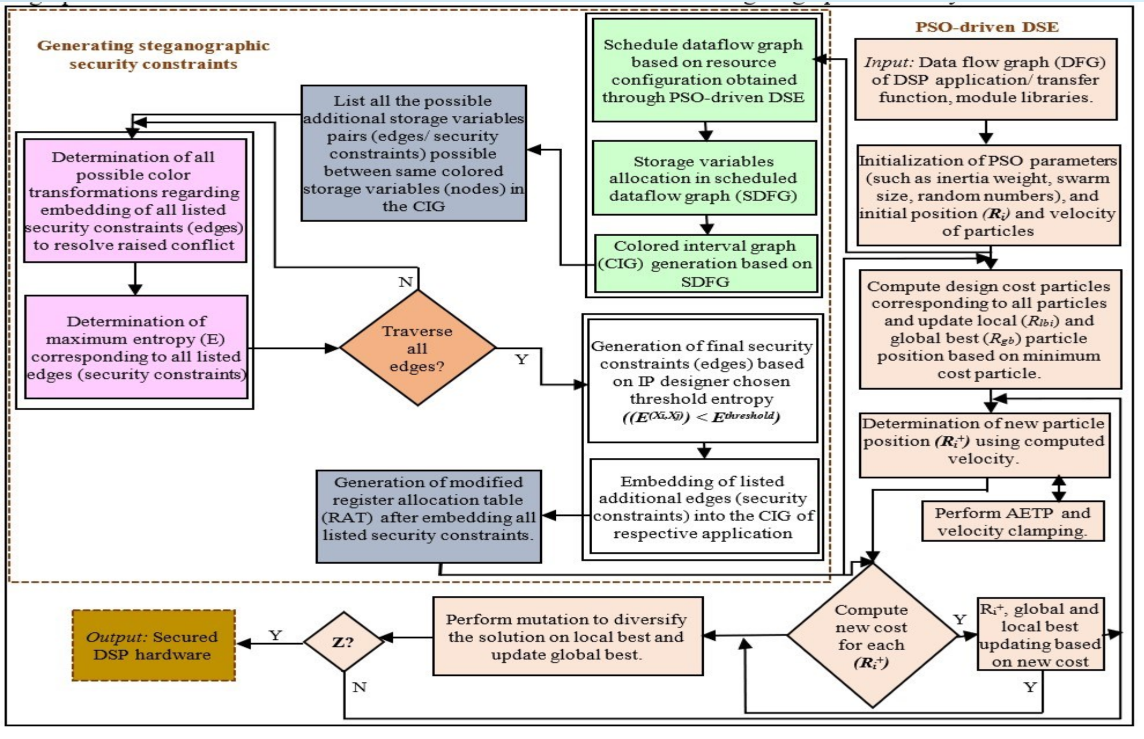


Fig. 2. Flow-chart of the proposed a low-cost PSO-driven DSE steganography approach

Proposed Work : Extraction of security constraints from SDFG of DSP application

Determination of hardware security constraints and their corresponding entropy value based on scheduled data flow graph of DSP application

TABLE I
REGISTER ALLOCATION TABLE (BEFORE AND AFTER EMBEDDING SECURITY CONSTARINTS)

CS	Red(R)	Teal (T)	Pink (P)	Yellow (Y)	Green (G)	Indigo (I)	Blue (BL)	Violet (V)	Lime (LI)
0	X0	X1	X2	X3	X4	X5	X6	X7	-
1	X8/X9	X9/X8	X2	X3	X4	X5	X6	X7	-
2	X16/X10	X11	X10/X16	X11	X4	X5	X6	X7	-
3	X17/X12	X11	X13	X11/X17	X12	X13	X6	X7	-
4	X18/X12	X14	X13	X15	X12/X18	X13	X14	X15	-
5	X19	X14	X13	X15	-	X13/X19	X14	X15	-
6	X20	X14	-	X15	-	-	X14/X20	X15	-
7	X21	-	-	X15	-	-	-	X15/X21	-
8	X22	-	-	-	-	-	-	-	X22

- Some examples of possible edges between same-colored storage variables for 8-point DCT are <X6, X14>, <X7, X15>, <X3, X11>, -------, <X5, X13>, <X2, X10>, <X0, X8>, <X0, X16>, <X0, X17>, <X0, X18>, <X0, X19>, <X0, X20>, <X0, X21>, <X0, X22>, <X21, X22> (generated from SDFG).
- For example, let's take the edge <X6, X14>: (([CS:0,1,2,3] (X6 ⇔ X0, X8, X16, X17), E (entropy)=5, (BL ⇔ R)), ([CS:4,5,6] (X14 ⇔ X18, X19, X20), E (entropy)=4, (BL ⇔ R))). So, the maximum entropy for embedding edge <X6, X14> is 5.
- Similarly, entropy for all possible edges are computed and final hardware security constraints are generated based on IP vendor selected value of threshold entropy.

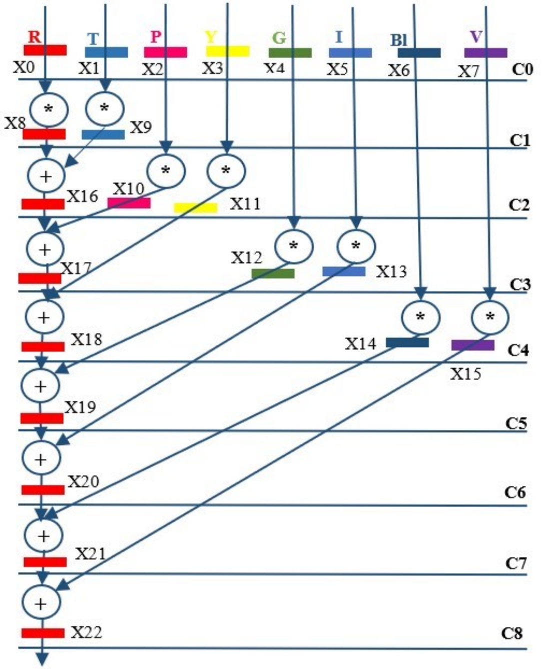


Fig 3: Scheduled Data flow graph of 8-point DCT with 1(+) and 2(*) obtained through PSO-driven DSE

Proposed Work : Embedding of generated security constraints

Embedding of generated security constraints using colored interval graph framework (Extra embedded security constraints are in red colored edges)

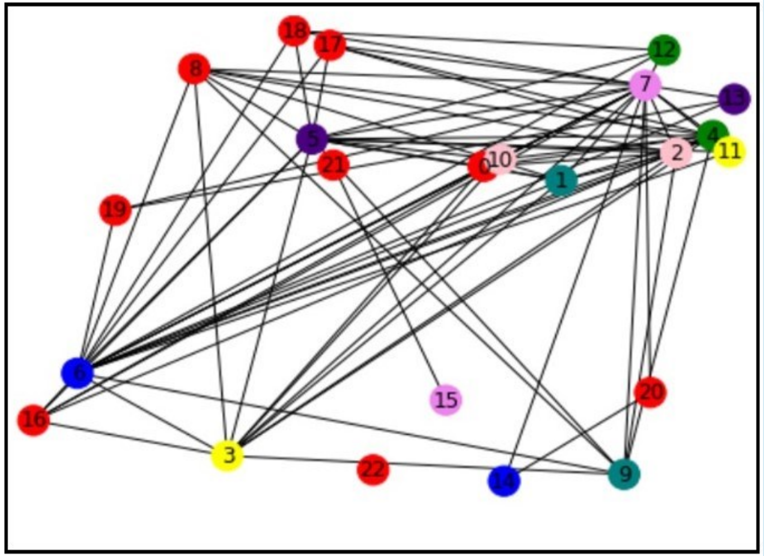


Fig.4. CIG of 8-point DCT before embedding steganographic hardware security constraints

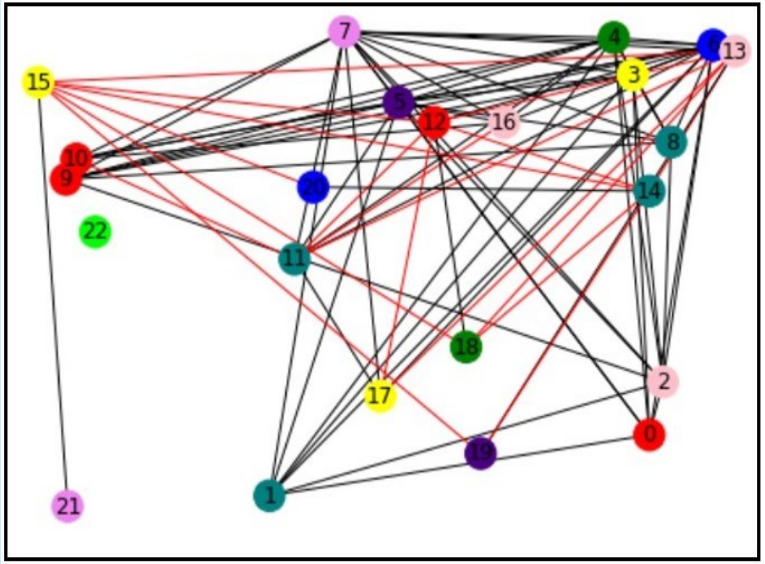


Fig.5. CIG of 8-point DCT post embedding steganographic hardware security constraints

Security metrics

Evaluation parameters

- **Evaluation of Robustness Using Probability of Coincidence (P):**

$$P = \left(1 - \frac{1}{l}\right)^{e}$$

'l' denotes the number of registers used in the CIG and 'e' denotes the number of hardware constraints added.

- **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)

Comparative Analysis

Comparison of Probability of coincidence (P) between proposed and [6] and [7]

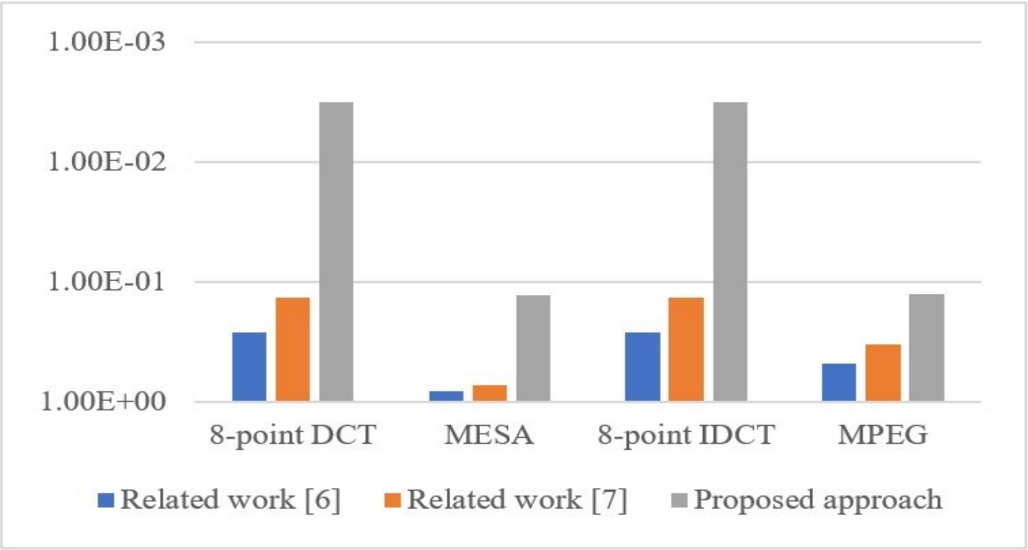


Fig.6. Comparison of probability of coincidence between the proposed approach and [6], [7]

Comparative Analysis : Design cost comparison

Design cost comparison (before and after embedding stego-security constraints)

TABLE II
Area, Latency, Cost, and Resource configuration of proposed low-cost steganography-based hardware security methodology

Benchmarks	Resource configuration	Baseline design (before signature embedding)			Signature embedded design			Design cost overhead %
		Design area (um^2)	Design latency (ps)	Design cost	Design area (um^2)	Design latency (ps)	Design cost	
8-point DCT	1(+), 2(*)	176.16	1324.856	0.443	176.947	1324.856	0.443	0
MESA	4(+), 4(*)	415.235	3113.412	0.216	416.808	3113.412	0.216	~0
8-point IDCT	1(+), 2(*)	176.16	1324.856	0.443	176.947	1324.856	0.443	0
MPEG	2(+), 2(*)	200.54	1987.284	0.418	200.54	1987.284	0.418	0

TABLE III.
CONVERGENCE AND EXPLORATION TIME IN PSO-DSE AFTER SECURITY CONSTRAINTS EMBEDDING (PARTICLE SIZE = 3)

Benchmark	Resource configuration	Convergence time(ms)	Exploration time(ms)
8-point DCT	1(+), 2(*)	41	329
MESA	4(+), 4(*)	3646	15178
8-point IDCT	1(+), 2(*)	642	436
MPEG	2(+), 2(*)	1283	2349

Comparative Analysis

Design cost and area reduction for the proposed approach compared to [7]

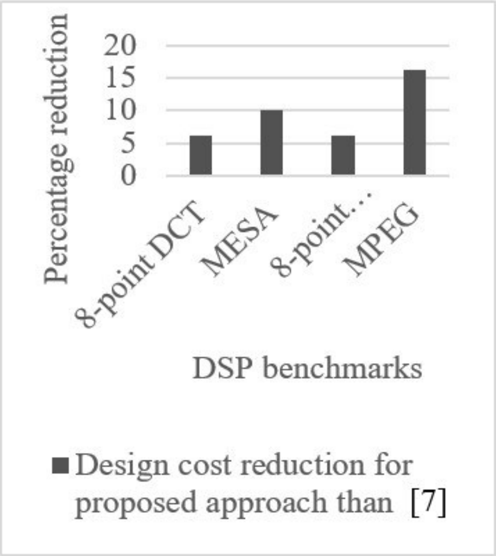


Fig.7. Reduction in design cost for the proposed approach than [7]

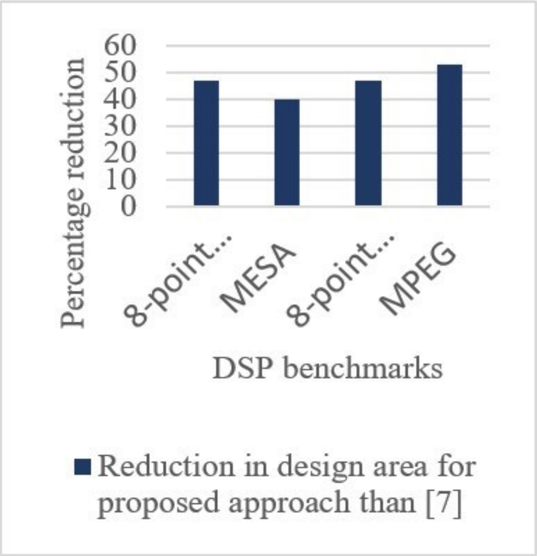


Fig.8. Reduction in design area for the proposed approach than [7]

References

1. C. Pilato, S. Garg, K. Wu, R. Karri and F. Regazzoni, "Securing Hardware Accelerators: A New Challenge for High-Level Synthesis," in *IEEE Embedded Systems Letters*, vol. 10, no. 3, pp. 77-80, Sept. 2018.
2. M. Pudzs, R. Fuksis, R. Ruskuls, T. Eglitis, A. Kadikis, and M. Greitans, “FPGA based palmprint and palm vein biometric system,” in Proc. *BIOSIG*, 2013.
3. J. Qiu, H. Li, J. Dong, and G. Feng, "Biometrics encryption based on palmprint and convolutional code," in Proc. *IEEE Int. Conf. Multimedia Image Process. (ICMIP)*, 2017, pp. 187–190.
4. V. Krishnan and S. Katkoori, "A genetic algorithm for the design space exploration of datapaths during high-level synthesis," *IEEE Transactions on Evolutionary Computation*, vol. 10, no. 3, pp. 213-229, June 2006.
5. A. Sengupta and S. Bhadauria, "Automated exploration of datapath in high level synthesis using temperature dependent bacterial foraging optimization algorithm," 2014 *IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE),* 2014, pp. 1-5.
6. 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.
7. A. Sengupta and S. Bhadauria, "Exploring Low Cost Optimal Watermark for Reusable IP Cores During High Level Synthesis," in *IEEE Access*, vol. 4, pp. 2198-2215, 2016.
8. Vipul Kumar Mishra, Anirban Sengupta,MO-PSE: Adaptive multiobjective particle swarm optimization based design space exploration in architectural synthesis for application specific processor design,*Advances in Engineering Software*,Vol 67,2014,pp. 111- 124.

Thank You