HLS Design Methodology of Optimized and Secured Hardware IPs

Aditya Anshul, Anirban Sengupta,
Computer Science and Engineering,
Indian Institute of Technology,Indore

Outline:

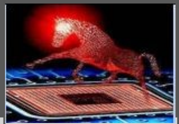
- Introduction about DSP IP cores
- Security issues with hardware (DSP)
- Abstraction level in hardware design
- State of the art approaches
- Discussion on some state of the art approaches
- Security metrics
- Limitations of current state of the arts

Intellectual Property (DSP IP cores):

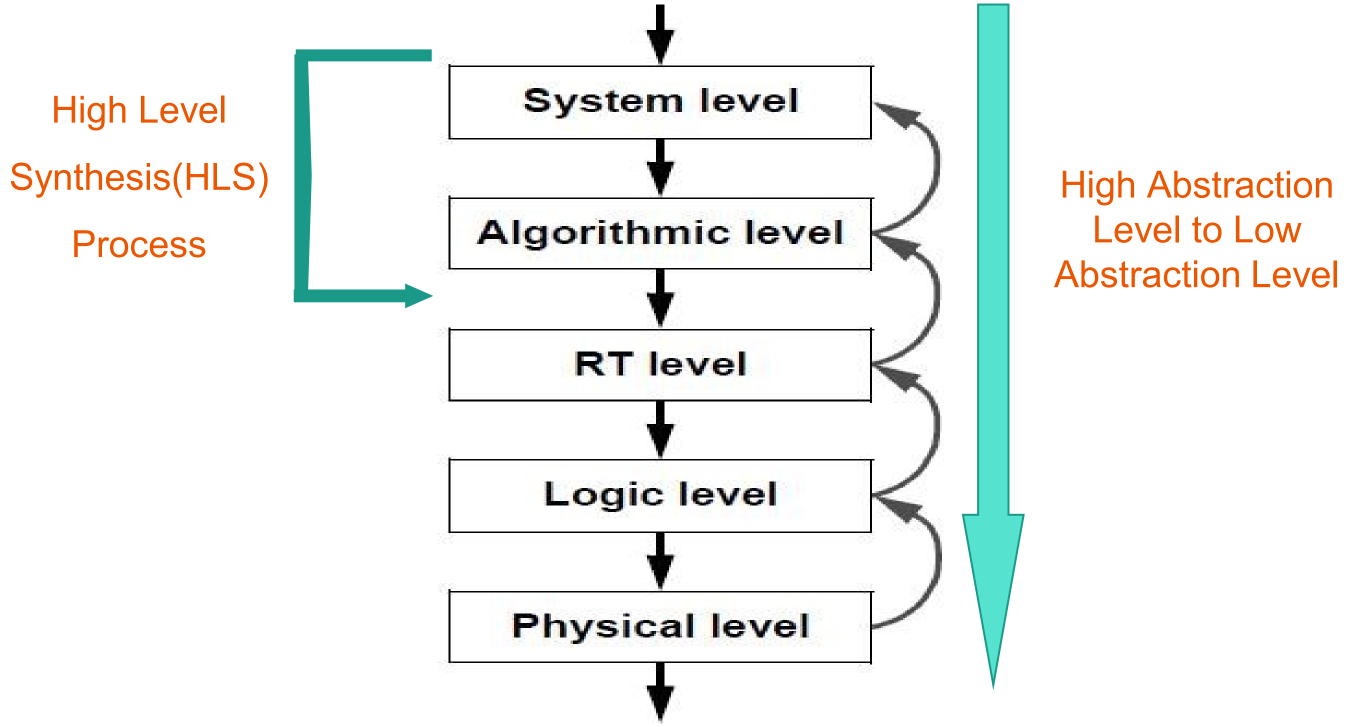
- Chips, Integrated circuits, and other designs owned by a company, designer, or manufacturer.
- Processors, Co- Processors(DSP) and other Consumer Electronics hardware.
- These co-processors performs various data-intensive and power-hungry applications involving massive computations like data compression-decompression, 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.**

Figure 1: IC design process

Security issues associated with IP Cores :

Sr. No.		Security Issues	
1.		Intellectual property(IP) Cloning-	Same product with different names.
2.		Intellectual property(IP) Counterfeiting-	Different product having same name.
3.		Hardware Trojan Attack-	Malicious circuitry that affects the functionality and trustworthiness.
4.		Overproduction-	Exceeding the specified licensing limit (illegally) of manufactured IPs .
5.		False claim of ownership-	Claiming illegal authority of IP.

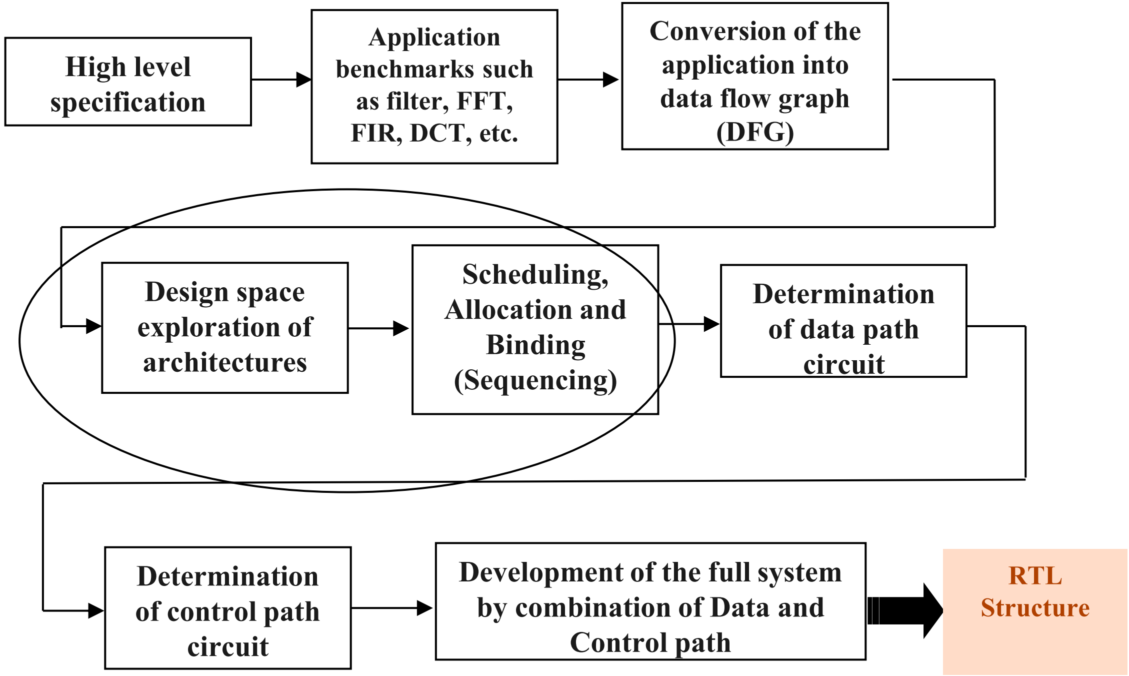
Abstraction levels in IP core(H/W) design:



Abstraction levels:

- ❖ **System level**
  - ➢ Represent the design at the highest level of abstraction
  - ➢ design (or application) is in the form of system specifications/input-output
  - ➢ At this level, functionality, space, speed and power requirement are considered
- ❖ **Algorithmic level**
  - ➢ Design description in terms of behavior
  - ➢ Control data flow graph is a popular intermediate representation of the design at the this level
  - ➢ Also known as electronic system level (ESL) or behavioural level
- ❖ **Register transfer level**
  - ➢ Interconnection between different units such as arithmetic and logic unit (ALU), control unit, storage hardware
- ❖ **Logic level**
  - ➢ Represents the design in terms of logic gates
- ❖ **Physical level**
  - ➢ Physical/Layout representation of the design

High Level Synthesis procedure and its importance:



- **Importance of HLS:**
  - Shorter design cycle. Reduces the design cycle due to automation of design process.
  - Easy error handling.
  - Ability to search the design space (optimal resource constraints).
  - Decisions made at higher levels has a great impact on lower levels.

DSP IP security classification tree:

Security of Data Intensive DSP and Multimedia IP Core

- Security based on detective control
  - Signature based approach
    - Watermark based approaches
      - Multi-variable watermarking [1]
      - Multi-phase watermarking [2]
      - Multilevel Watermark[3]
    - Digital signature based authentication [5]
    - Biometric based approaches
      - Facial biometric [6]
      - Fingerprint biometric [7]
      - Palmprint biometric [20]
  - Non-signature based approach
    - Steganography based authentication[4]
- Security based on preventive control
  - Security using structural obfuscation
    - Folding based [8]
    - Multiple high level transformations based [9] [10]
    - Structural obfuscation on JPEG CODEC [11]
  - Security using functional obfuscation
    - Functional obfuscation using xor-xnor pair [12]
    - Functional obfuscation using Mux based obfuscation cells [13]
    - Functional obfuscation using robust ILBS [14]

Security need:

- **Protection against threat of IP ownership** is to authenticate genuine IP vendor/ designer in case of soc integrator falsely claiming the ownership of the IP core.

- **Protection against IP piracy** is to authenticate SoC integrator/ user from dishonest IP vendor selling extra copies of IPs and blaming the user.

- **Trojan** can be inserted at any stage of IP design and is not easily detectable during testing phase of IP design or remains dormant until the happening of some specific triggering/ timing event.

- **Counterfeited IPs** may cause leakage of credential information/ passwords, drowning energy resources, excessive heat dissipation of the IC components, and abnormal functioning or denial of service of the underlying computing device.

➢ Therefore, detective and preventive control of IP core from the SoC integrator's perspective must be mandatory.

Related Work :

Sr. No.	Existing Work	Technique Used	Remarks
1.	Bushnell and Agrawal [15] (2001)	Equivalence analysis by reducing number of suspicious signals.	It adds runtime overhead and neither all suspicious signals are Trojans.
2.	Rajendran and Zhang [16] (2013)	Concurrent error detection (CED) approach using multiple 3rd-party IP (3PIP) vendors for Trojan detection.	Making DSP design Trojan detectable not Trojan resistant. Further, it does not considers optimization.
3.	A. Sengupta and M. Rathor [4] (2019)	Hardware steganography based security approach to address the IP counterfeiting threat.	Signature free, becomes weak if secret value of chosen entropy threshold are leaked.
4.	A. Sengupta and M. Rathor [7] (2020)	Fingerprint biometric based hardware security approach.	Not contact-less and prone to external environmental factors such as dirt and grease etc.

IP core steganography used for protecting DSP kernels used in CE systems [4]:

- A Novel approach based on steganograpgy technique has been used for protection of complex reusable IP Cores used in CE Systems.
- The proposed approch 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 degine to authenticate genuine IP Maker.
- Threshold entropy option in the approach provides more control to designer as compared to signature based approach.

[4]. 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, doi: 10.1109/TCE.2019.2944882.

Steganography-based security approach ([4]) :

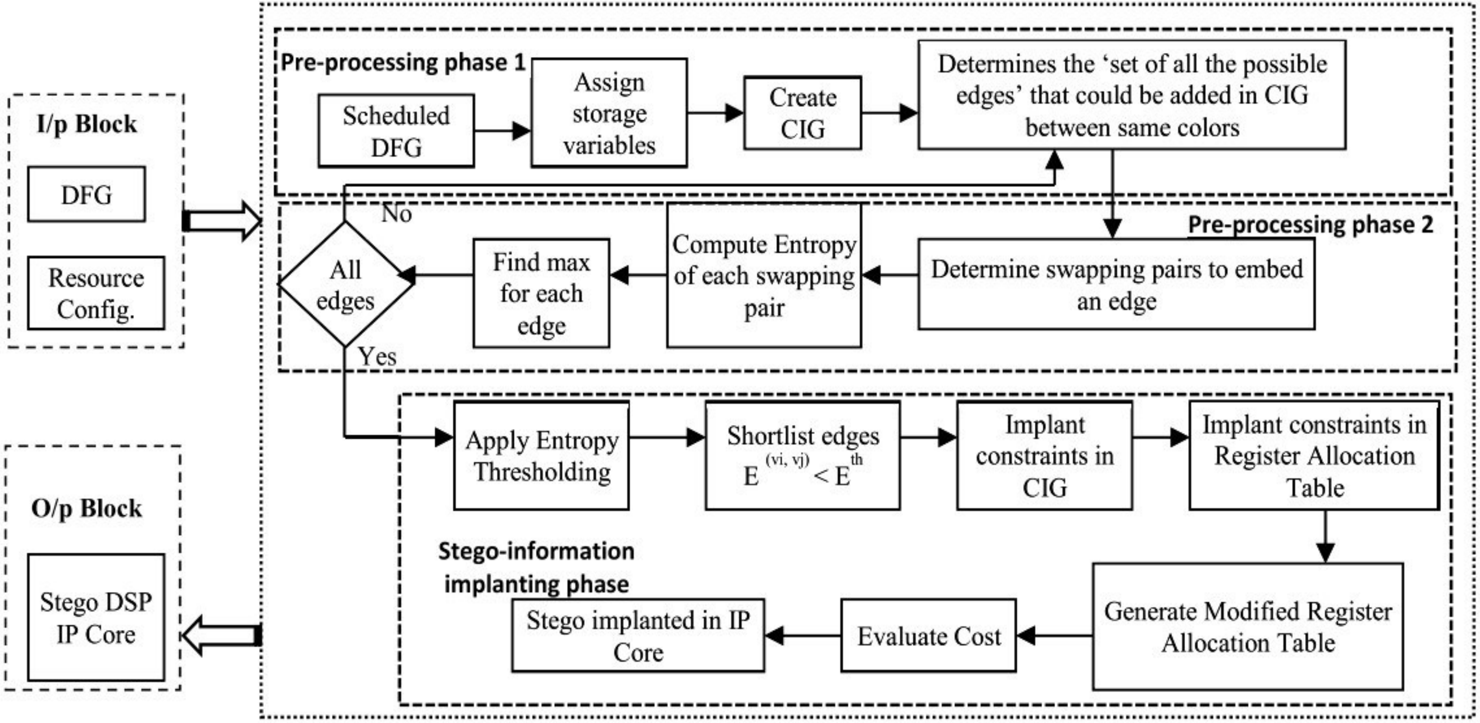


Figure 2: Flow-chart of steganography based approach

Generation of hardware security constraints from register allocation table [4]:

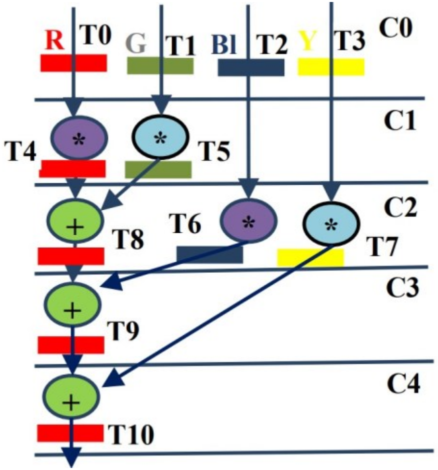


Figure 3: Scheduled data flow graph of 4-point DCT with 1(+) and 2(*) before secret constraint embedding.

	R	G	Bl	Y
C0	T0	T1	T2	T3
C1	T4	T5	T2	T3
C2	T8	-	T6	T7
C3	T9	-	-	T7
C4	T10	-	-	-

Table 1: Register allocation table of storage variables (T0-T10) of DCT-4.

	R	G	Bl	Y	O	V
C0	T0	T1	T2	T3	-	-
C1	T5	T4	T2	T3	-	-
C2	-	-	T7	T6	T8	-
C3	-	-	-	T6	T9	-
C4	-	-	-		-	T10

Table 2: Register allocation table of storage variables (T0-T10) of DCT-4 post signature embedding.

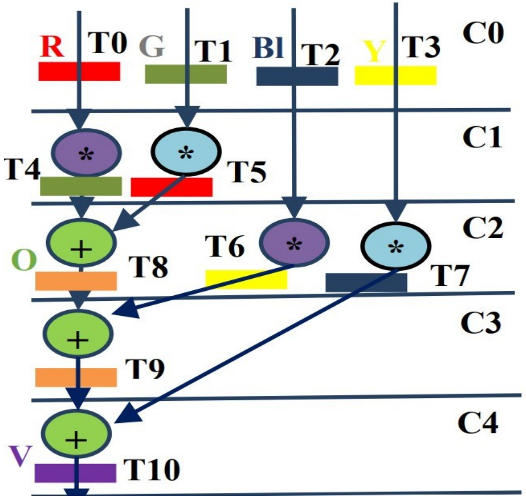


Figure 4: Scheduled data flow graph of 4-point DCT with 1(+) and 2(*) after secret constraint embedding.

Possible edge	Maximum entropy	Possible edge	Maximum entropy	Possible edge	Maximum entropy
<T1, T5>	2	<T0, T9>	3	<T4, T10>	3
<T2, T6>	3	<T0, T10>	3	<T8, T9>	2
<T3, T7>	3	<T4, T8>	3	<T8, T10>	3
<T0, T4>	2	<T4, T9>	3	<T9, T10>	3
<T0, T8>	3	-	-	-	-

Table 3: Additional edges (hardware security constraints) generated for DCT-4.

Embedding Digital Signature Using Encrypted-Hashing for protection of DSP cores in CE [5]:

- A novel approach named multi-level encoding and encrypted-hash based digital signature for protection of complex reusable IP cores used in CE Systems.
- The proposed approch is capable of encoding a DSP Kernel application.
- Digital signature is generated using RSA with the help of messege digest of encoded application.
- The generated signature is then mapped to its corresponding hardware security constraints based on a mapping rule and then implanted in IP cores degine to authenticate genuine IP Maker.

[5]. A. Sengupta, E. R. Kumar and N. P. Chandra, “Embedding Digital Signature Using Encrypted-Hashing for Protection of DSP Cores in CE,” in IEEE Transactions on Consumer Electronics, vol. 65, no. 3, pp. 398-407, Aug. 2019, doi: 10.1109/TCE.2019.2924049.

Digital-signature based security approach ([5]) :

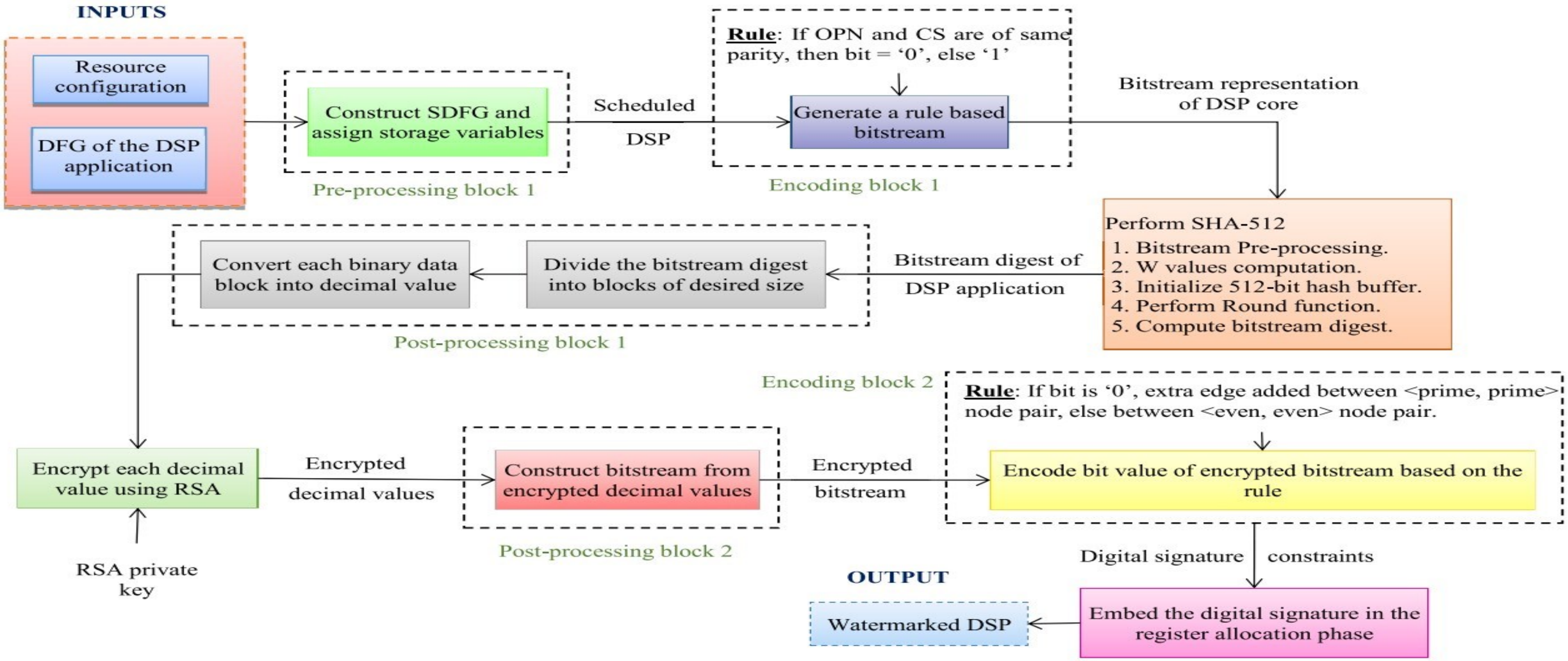


Figure 5: Details of the digital signature embedding approach.

SDFG of 8-point DCT and its corresponding RAT ([5]) :

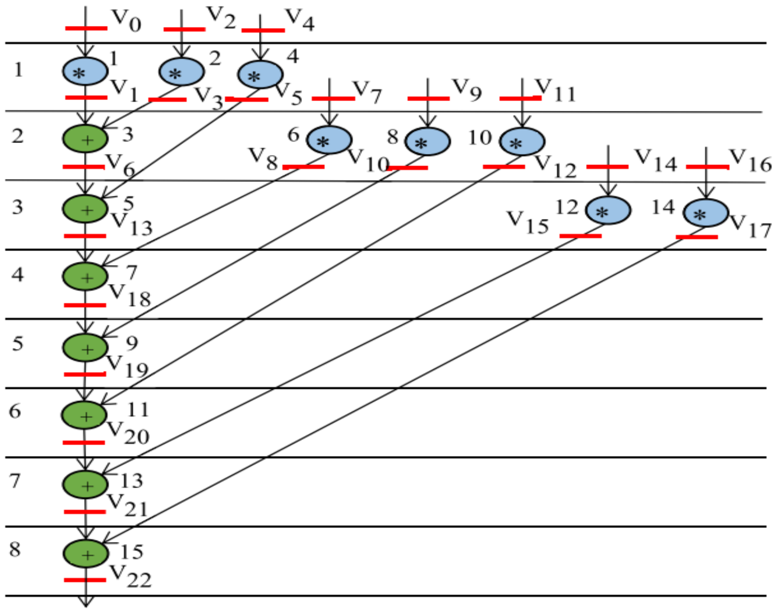


Figure 6: Scheduled DFG of 8-point DCT with storage variables.

Control Step	B	R	G	O	Y	C	Bl
0	V_0	V_2	V_4	-	-	-	-
1	V_1	V_3	V_5	V_7	V_9	V_{11}	-
2	V_6	V_8	V_5	V_{10}	V_{12}	V_{14}	V_{16}
3	V_{13}	V_8	V_{15}	V_{10}	V_{12}	V_{17}	-
4	V_{18}	-	V_{15}	V_{10}	V_{12}	V_{17}	-
5	V_{19}	-	V_{15}	-	V_{12}	V_{17}	-
6	V_{20}	-	V_{15}	-	-	V_{17}	-
7	V_{21}	-	-	-	-	V_{17}	-
8	V_{22}	-	-	-	-	-	-

Table 4: Register allocation table of 8-point DCT before embedding digital security constraints

CIG of 8-point DCT and RAT after digital signature embedding [5]:

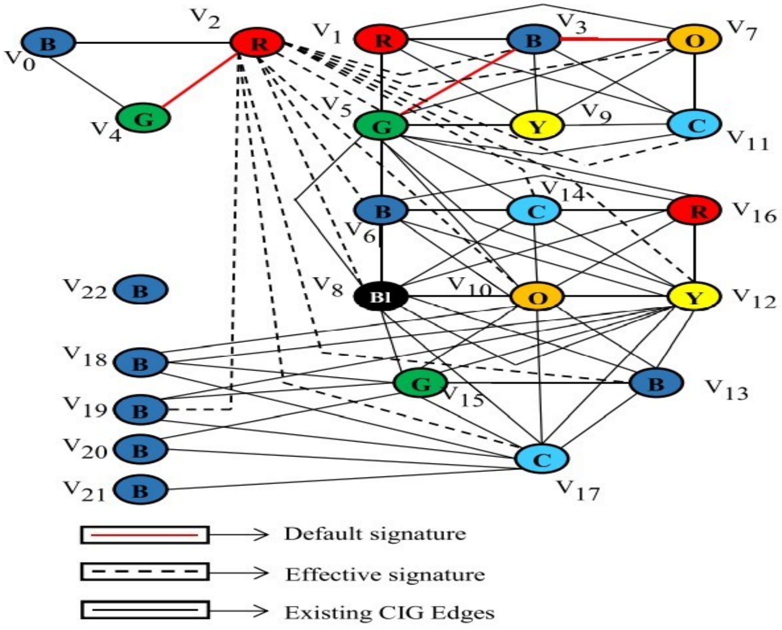


Figure 7: Colored interval graph of 8-point DCT after embedding digital signature constraints

Control Step	B	R	G	O	Y	C	Bl
0	V_0	V_2	V_4	-	-	-	-
1	V_3	V_1	V_5	V_7	V_9	V_{11}	-
2	V_6	V_{16}	V_5	V_{10}	V_{12}	V_{14}	V_8
3	V_{13}	-	V_{15}	V_{10}	V_{12}	V_{17}	V_8
4	V_{18}	-	V_{15}	V_{10}	V_{12}	V_{17}	-
5	V_{19}	-	V_{15}	-	V_{12}	V_{17}	-
6	V_{20}	-	V_{15}	-	-	V_{17}	-
7	V_{21}	-	-	-	-	V_{17}	-
8	V_{22}	-	-	-	-	-	-

Table 5: Register allocation table of 8-point DCT post embedding digital security constraints

Evaluation parameters:

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

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

'c' denotes the number of registers used in the CIG and 'f' denotes the number of hardware constraints added.

- **Evaluation of tamper tolerance (TT):**

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

'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)

Limitations of the state-of-art approches:

- **Limitations of non-signature based hardware security based approach (steganography-based approach)** – the approach becomes weak if the chosen threshold entropy value gets compromised. Further, it is incapable of handling backdoor trojan insertion.

- **Limitations of digital signature based hardware security approach-** the security of the digital signature secured hardware IP core gets compromised in case if adversary manages to access the following details such as encoding rule and signature size. Further, it is incapable of handling backdoor trojan insertion.

- **Limitations of biometric-based hardware security approach-** the biometric-based approaches enable the robust security against counterfeited detections of IP core. However they are incapable of handling the threats due to back-door trojan insertion and reverse engineering.

References

1. 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.
2. A. Sengupta and D. Roy, “Multi-phase watermark for IP core protection”, in *Proc. ICCE*, LV, 2018, pp. 1–3. DOI: 10.1109/ICCE.2018.8326058.
3. D. Roy and A. Sengupta, "Multilevel Watermark for Protecting DSP Kernel in CE Systems [Hardware Matters]," in IEEE Consumer Electronics Magazine, vol. 8, no. 2, pp. 100-102, March 2019, doi: 10.1109/MCE.2018.2880849.
4. 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, doi: 10.1109/TCE.2019.2944882.
5. A. Sengupta, E. R. Kumar and N. P. Chandra, “Embedding Digital Signature Using Encrypted-Hashing for Protection of DSP Cores in CE,” in IEEE Transactions on Consumer Electronics, vol. 65, no. 3, pp. 398-407, Aug. 2019, doi: 10.1109/TCE.2019.2924049.
6. A. Sengupta and M. Rathor, “Facial Biometric for Securing Hardware Accelerators,” in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 29, no. 1, pp. 112-123, Jan. 2021, doi: 10.1109/TVLSI.2020.3029245.
7. A. Sengupta and M. Rathor, “Securing Hardware Accelerators for CE Systems Using Biometric Fingerprinting,” in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 28, no. 9, pp. 1979-1992, Sept. 2020, doi: 10.1109/TVLSI.2020.2999514.

References

8. Y. Lao and K. K. Parhi, “Obfuscating DSP Circuits via High-Level Transformations,” *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 23, no. 5, pp. 819–830, May 2015.
9. A. Sengupta and D. Roy, “Protecting an intellectual property core during architectural synthesis using high-level transformation based obfuscation,” *IET Electronics Letters*, Vol: 53, Issue: 13, pp. 849 – 851, June 2017.
10. A. Sengupta, D. Roy, S.P. Mohanty, and P. Corcoran, “DSP Design Protection in CE through Algorithmic Transformation based Structural Obfuscation,” *IEEE Trans. Consum. Electron.,* Vol. 63, no. 4, pp. 467 – 476, Nov. 2017.
11. Sengupta A., Roy D., Mohanty S. P. and Corcoran P. 2018. Low-Cost Obfuscated JPEG CODEC IP Core for Secure CE Hardware. *IEEE Transactions on Consumer Electronics*, 64, 3, 365-374.
12. J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri, “Security analysis of logic obfuscation,” in *DAC, 2012*, San Francisco, June 2012, pp. 83–89.
13. J. Zhang, “A Practical Logic Obfuscation Technique for Hardware Security,” *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.,* vol. 24, no. 3, pp. 1193–1197, 2015.
14. A. Sengupta, D. Kachave, and D. Roy, “Low Cost Functional Obfuscation of Reusable IP cores used in CE Hardware through Robust Locking,” *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, 2019, DOI: 10.1109/TCAD.2018.2818720.

References

15. M. Bushnell and V. Agrawal, “Essentials of electronic testing for digital, memory, and mixed-signal VLSI circuits,” *in IEEE Circuits and Devices Mag.*, vol. 17, no. 4, pp. 39-40, July 2001, doi: 10.1109/MCD.2001.950085.

16. J. Rajendran, H. Zhang, O. Sinanoglu and R. Karri, “High-level synthesis for security and trust,” *s IEEE 19th International On-Line Testing Symposium (IOLTS)*, 2013, pp. 232-233, doi: 10.1109/IOLTS.2013.6604087.

17. 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,” *in IEEE Trans. on Comput.-Aided Design of Integr. Circuits and Syst.*, vol. 36, no. 4, pp. 655-668, April 2017, doi: 10.1109/TCAD.2016.2597232.

18. 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, doi: 10.1109/TEVC.2005.860764.

19. 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, doi: 10.1109/CCECE.2014.6900920.

20. A. Sengupta, R. Chaurasia and T. Reddy, "Contact-Less Palmprint Biometric for Securing DSP Coprocessors Used in CE Systems," in IEEE Transactions on Consumer Electronics, vol. 67, no. 3, pp. 202-213, Aug. 2021, doi: 10.1109/TCE.2021.3105113.

Thank You!