Robust Digital Signature to Secure IP Core against Fraudulent Ownership and Cloning

Anirban Sengupta, E. Ranjith Kumar, N. Prajwal Chandra "Embedding Digital Signature using Encrypted-Hashing for Protection of DSP cores in CE", **IEEE Transactions on Consumer Electronics (TCE)**, Volume: 65, Issue:3, Aug 2019, pp. 398 - 407

Presented in IEEE ICCE-Berlin 2019, Germany

Dr. Anirban Sengupta, Assoc. Professor, CSE

Indian Institute of Technology Indore

FIET, FBCS, IEEE Distinguished Visitor and IEEE Distinguished Lecturer, IEEE Senior Member

IEEE

IEEE COMPUTER SOCIETY

IEEE CONSUMER ELECTRONICS SOCIETY

Outline

- Introduction
- Existing Approach
- Flow of Proposed Approach
- Motivational Example
- Experimental Results
- Conclusions

Introduction

- Digital signal processing (DSP) and multimedia based reusable Intellectual property (IP) cores form key components of system-on-chips (SoC) used in consumer electronic devices.
- The global semiconductor supply chain for SoC design is highly vulnerable to **security threats such as IP/IC cloning and false claim of ownership**.
- A novel **crypto digital signature approach** is presented here to secure IP/ICs against aforementioned threats.

Existing Approaches

- Existing approaches [1] [3] [4] employ watermark using two or multi-variable author signature.
- There is a designer's specified encoding rule for each signature variable.
- The security of these approaches is intact as long as the signature and encoding are not compromised/leaked.
- Once both are compromised, the vendor fails to prove his IP ownership or detect IP cloning/counterfeting.

Novelties of Proposed Approach

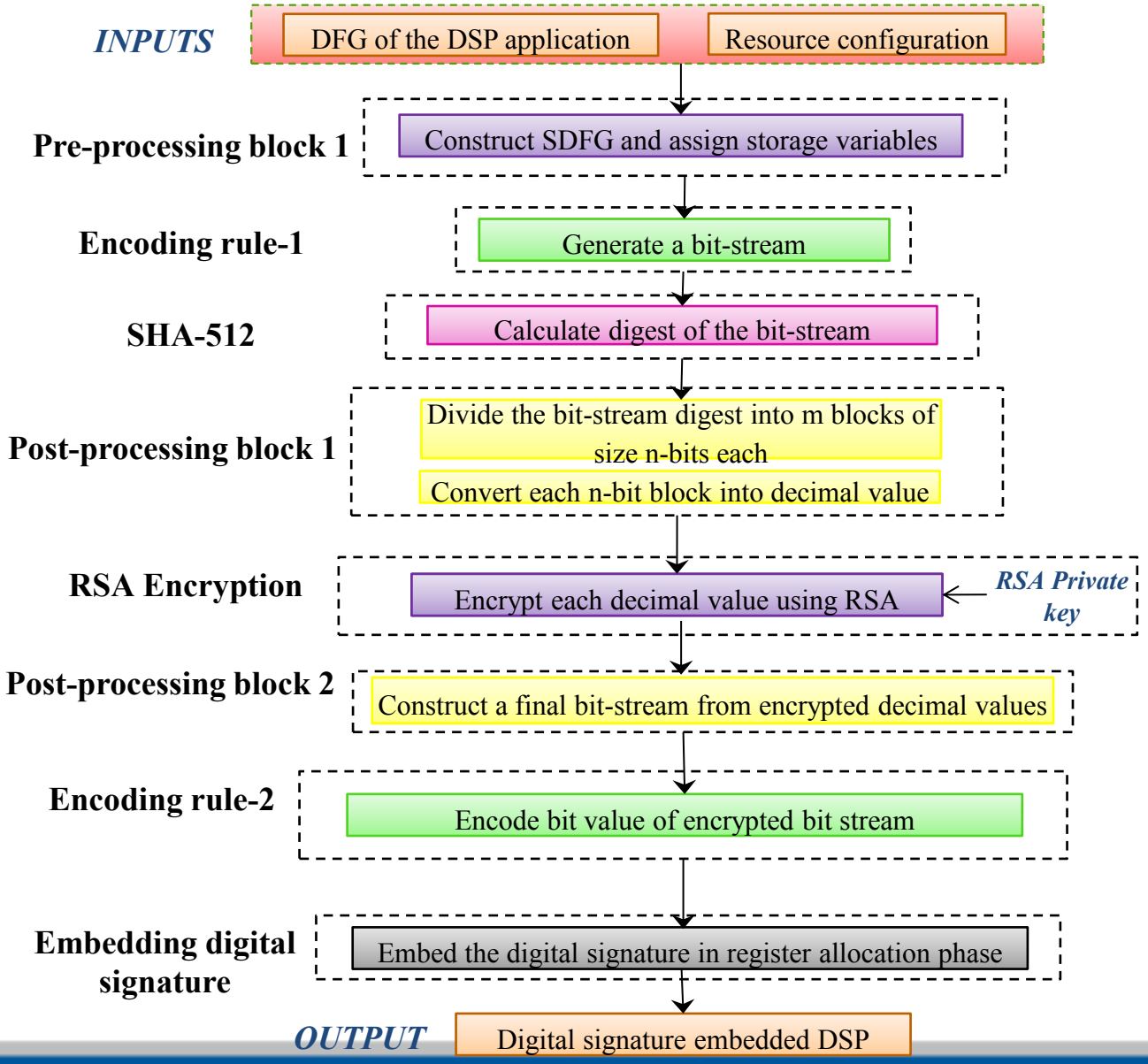
- Proposes a multi-level encoding encrypted-hash-based digital signature for protecting the DSP application.
- Proposes a novel methodology for encoding DSP application.
- The genuine designer (vendor) is able to prove his/her right over the digital signature in the design in a more meaningful, scientific and definite way.

Introduction to Proposed Approach

- **A novel crypto digital signature approach is presented which incorporates following security modules**
  - Crypto hash function- SHA-512
  - Crypto encryption function- RSA
  - Encoding

- **The generic steps of generating digital signature:**
  - Generate a Bit-stream representation of DSP Core.
  - Performing SHA-512
  - Post-processing Step1
  - RSA Encryption
  - Post-processing Step 2

Flow of the Proposed approach



Bit stream Generation

- Based on encoding rule-1

Operation number (OPN)	Corresponding control step (CS) number	Encoded bit
Even	Even	0
Odd	Even	1
Even	Odd	1
Odd	Odd	0

Performing SHA-512 and Post Processing-1

➢ **Performing SHA-512**

- Generates decimal digest of DSP core
- The collision resistance and deterministic properties of SHA-512 ensures that the generated hash digest carrying vendor secret mark is unique for an IP core design.

➢ **Post-Processing-1**

- Divide the bitstream digest into m blocks of size n bits each
- Convert each n-bit block into decimal value

RSA Encryption

- RSA is an asymmetric key encryption algorithm in which two distinct keys (private key and public key) are involved in the cryptography.
- It is used to sign the hash digest of vendor secret mark information to ensure authentication of the genuine owner.

Inputs (128 bits) and outputs of RSA module

RSA Decimal Input	Encrypted Decimal Output	Encrypted Binary Equivalent
328629211327023509667307560016780722176	259269232367594955022606516388222677830	110000110000110……01 1001101000110
338967726051337675217876235804913696768	1033044222147219398283219 19365106451481	100110110110111……10 0010000011001
7450807172495041329695951 9603599240546	2468224786302243196551204 2630223003075	100101001000110……11 1110111000011
1404762928918675873413822 5185020455483	2894117968894796223870676 77582110256178	110110011011101……11 0110000110010

Post-processing Block 2

- The encrypted decimal values— output of RSA module— are provided as input to the post-processing block 2.
- Each decimal value is converted to binary and these individual binary streams are concatenated to form a single bit-stream.
- This encrypted-hashed bit-stream is referred to as **Digital Signature**. The digital signature size can be selected based on vendor's choice from the continuous bit-stream.
- For instance, if the vendor selects digital signature size as 15, then the first 15 bits of the bit-stream is the digital signature.

Embedding Digital Signature

Having created the digital signature, the next step is to embed it in the design. The steps to implant the digital signature are stated below:

- **Mapping the digital signature bits to watermarking constraints**
  - Using the following encoding rule:
    - If bit = '0', then additional edge is added between node pair (prime, prime) in a colored interval graph.
    - If bit = '1', then additional edge is added between node pair (even, even) in a colored interval graph.
- **Embedding the watermarking constraints**.
  - Watermark constraints are embedded in register allocation step during HLS (And it is performed through colored interval graph framework).
  - These hidden constraints act as additional constraints to be imposed besides the regular design constraints of the design

Digital Signature Detection

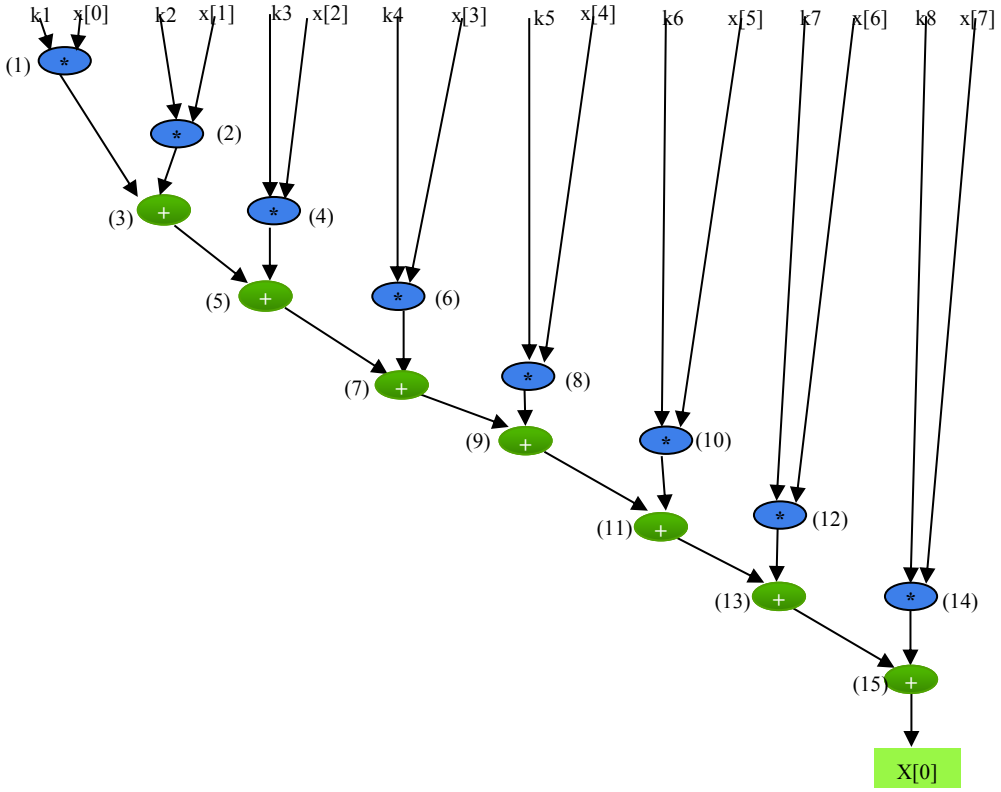
- ***Inspection:*** The RTL datapath of the IP core design under test is inspected to collect the information of storage variables. To do so, inputs of all muxes associated to each register are inspected. This inspection provides the information of register allocation of all storage variables.

- ***Signature Verification:*** The objective of this step is to verify the presence of digital signature (watermark) in the collected information from the preceding step. This is done by verifying the register multiplexer inputs of the Data path to check the presence of "*register allocation"* table information.

Motivational Example- 8-point DCT Core

Every camera system uses JPEG CODEC process that comprises of DCT core underneath. A 2D-DCT is useful in JPEG compression process in handling an 8x8 image block of pixels at a time.

Generic equation of 8-Point DCT to compute 1st sample is:
X[0]=k1*x[0]+ k2*x[1]+ k3*x[2]+ k4*x[3]+ k5*x[4]+ k6*x[5]+ k7*x[6]+ k8*x[7]

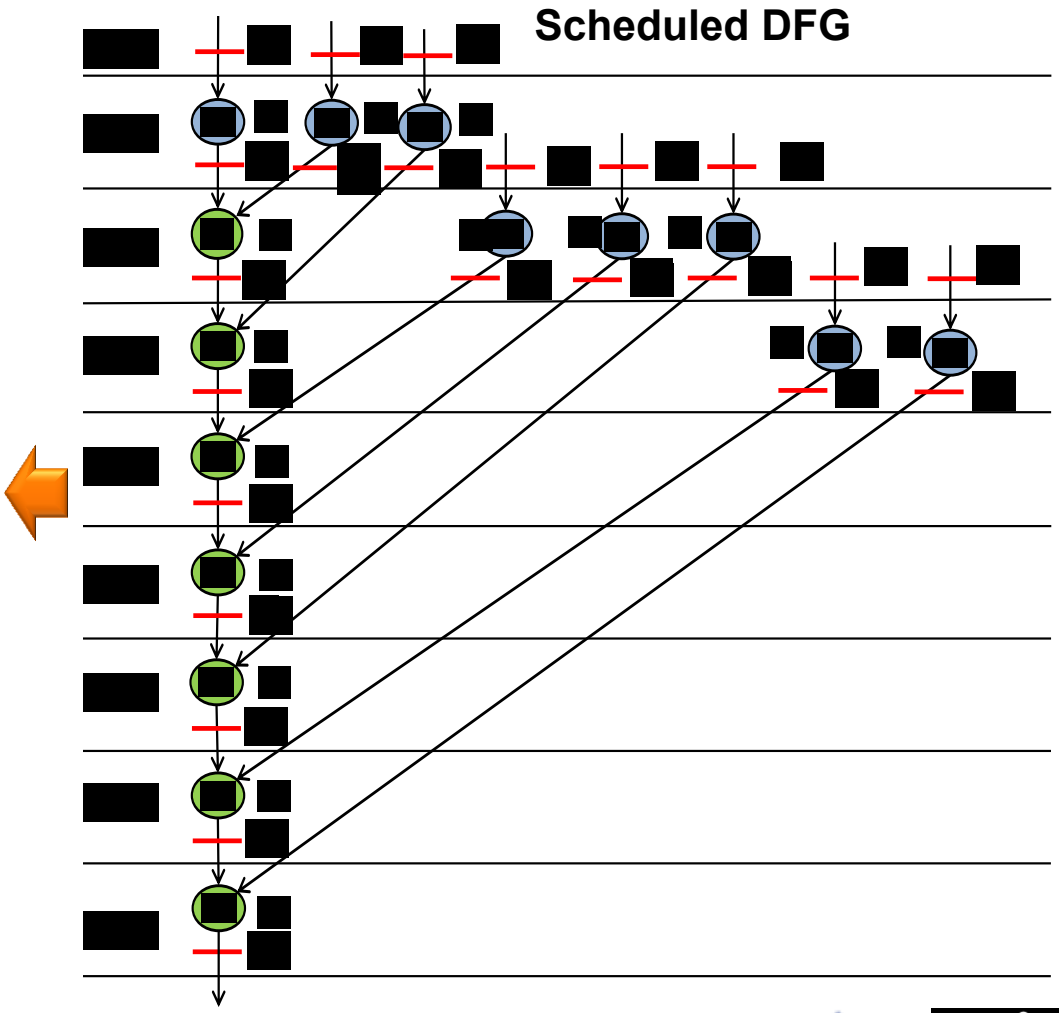


Inputs to the Proposed Approach:

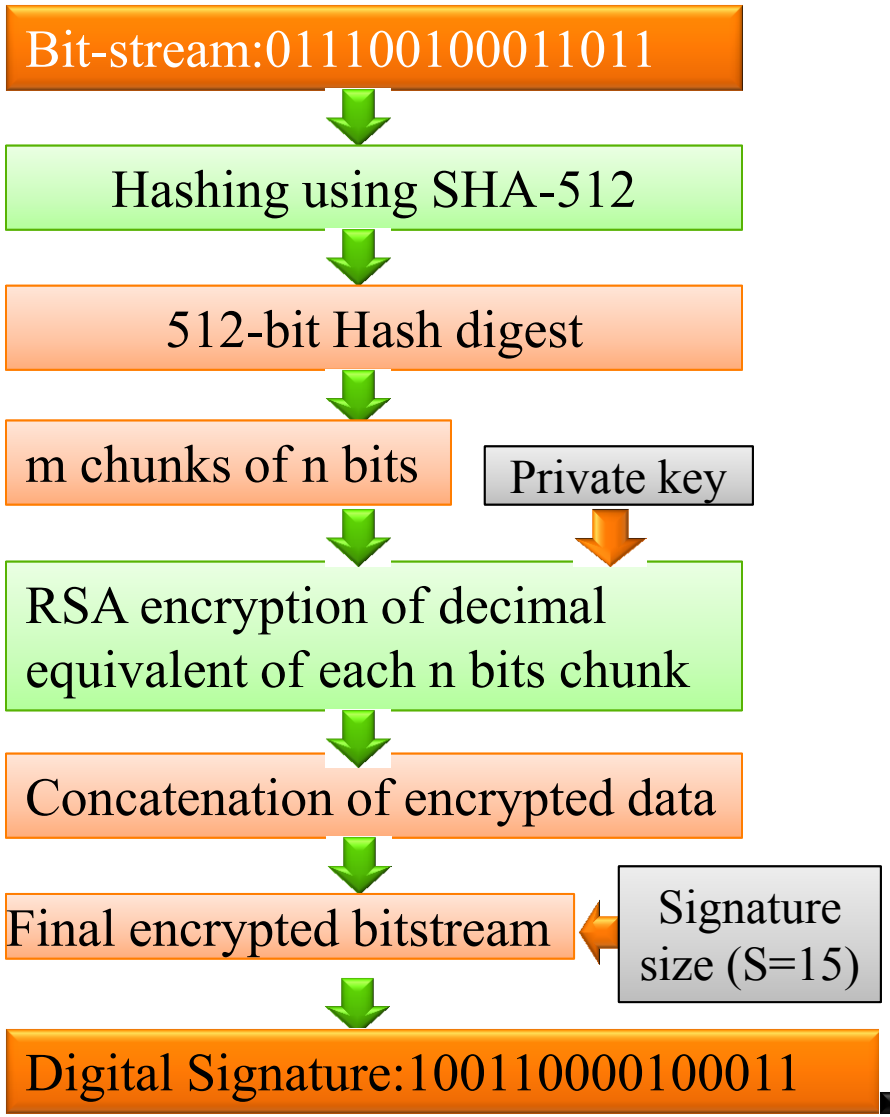
- The DFG of 8 point-DCT
- Hardware resource configuration as follows:
- Multipliers-3
- Adder-1

Generating the Bit-stream of DCT Core

Operation Number	Control Step Number	Bit generated
1	1	0
2	1	1
3	2	1
4	1	1
5	3	0
6	2	0
7	4	1
8	2	0
9	5	0
10	2	0
11	6	1
12	3	1
13	7	0
14	3	1
15	8	1



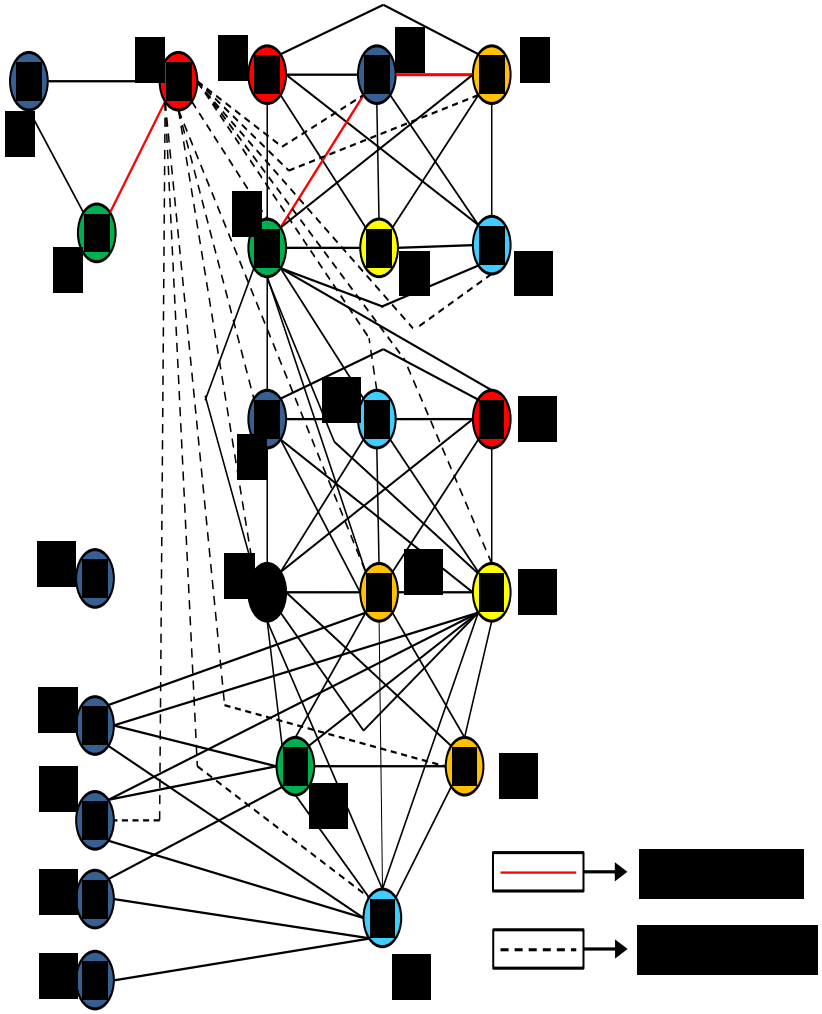
Digital Signature Generation



Bits in digital signature (S=15)	Corresponding additional edges
1	$<V_2,V_4>$
0	$<V_2,V_3>$
0	$<V_2,V_5>$
1	$<V_2,V_6>$
1	$<V_2,V_8>$
0	$<V_2,V_7>$
0	$<V_2,V_{11}>$
0	$<V_2,V_{13}>$
0	$<V_2,V_{17}>$
1	$<V_2,V_{10}>$
0	$<V_2,V_{19}>$
0	$<V_3,V_5>$
0	$<V_3,V_7>$
1	$<V_2,V_{12}>$
1	$<V_2,V_{14}>$

Encoded into constraints

Colored Interval Graph post Embedding Digital Signature (S=15)



Bits in digital signature (S=15)	Corresponding additional edges
1	$<V_2,V_4>$
0	$<V_2,V_3>$
0	$<V_2,V_5>$
1	$<V_2,V_6>$
1	$<V_2,V_8>$
0	$<V_2,V_7>$
0	$<V_2,V_{11}>$
0	$<V_2,V_{13}>$
0	$<V_2,V_{17}>$
1	$<V_2,V_{10}>$
0	$<V_2,V_{19}>$
0	$<V_3,V_5>$
0	$<V_3,V_7>$
1	$<V_2,V_{12}>$
1	$<V_2,V_{14}>$

Pre-embedding

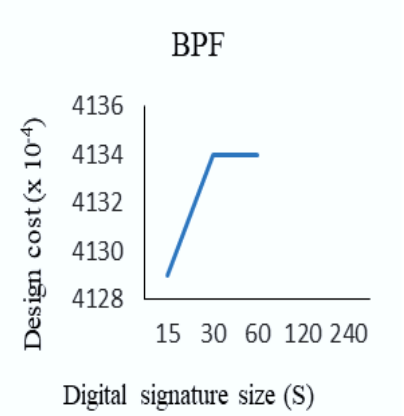
Control Step	B	R	G	O	Y	C	Bl
0	V_0	V_2	V_4	-	-	-	-
1	V_1	V_3	V_5	V_7	V_9	V_{11}	-
2	V_6	V_8	V_5	V_{10}	V_{12}	V_{14}	V_{16}
3	V_{13}	V_8	V_{15}	V_{10}	V_{12}	V_{17}	-
4	V_{18}	-	V_{15}	V_{10}	V_{12}	V_{17}	-
5	V_{19}	-	V_{15}	-	V_{12}	V_{17}	-
6	V_{20}	-	V_{15}	-	-	V_{17}	-
7	V_{21}	-	-	-	-	V_{17}	-
8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

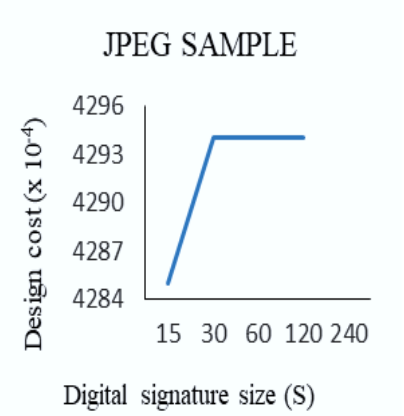
Post-embedding

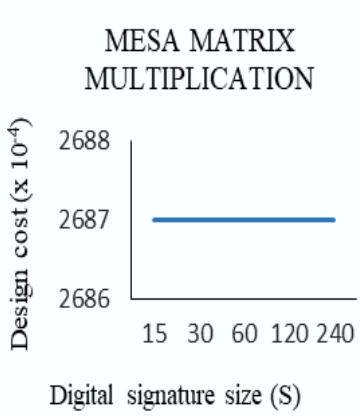
Control Step	B	R	G	O	Y	C	Bl
0	V_0	V_2	V_4	-	-	-	-
1	V_3	V_1	V_5	V_7	V_9	V_{11}	-
2	V_6	V_{16}	V_5	V_{10}	V_{12}	V_{14}	V_8
3	V_{13}	-	V_{15}	V_{10}	V_{12}	V_{17}	V_8
4	V_{18}	-	V_{15}	V_{10}	V_{12}	V_{17}	-
5	V_{19}	-	V_{15}	-	V_{12}	V_{17}	-
6	V_{20}	-	V_{15}	-	-	V_{17}	-
7	V_{21}	-	-	-	-	V_{17}	-
8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

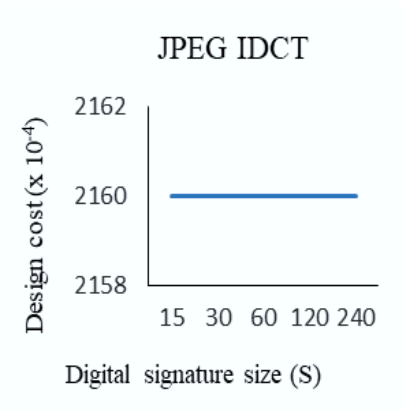
Experimental Results

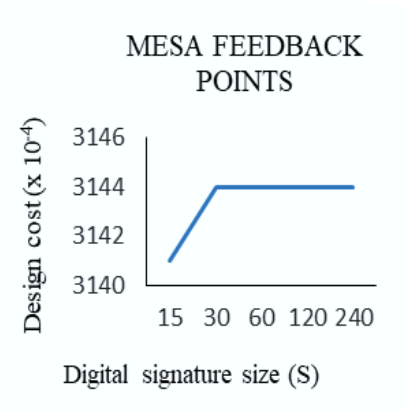
- **Graphical Representation of Design Cost for different benchmarks**

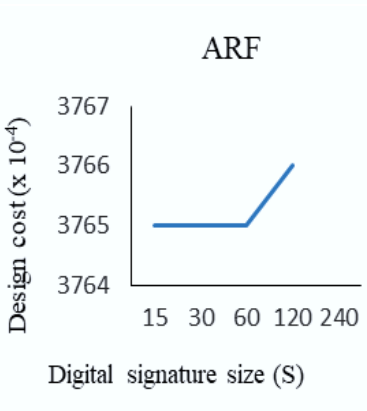












Design cost

$$C_f(X_i) = \phi_1 \frac{L_T}{L_{max}} + \phi_2 \frac{A_T}{A_{max}}$$

L_T =design latency
A_T =hardware area
L_{max}= maximum execution latency
A_{max} = maximum hardware area.

ϕ_1, ϕ_2 represent the user specified weights both fixed at 0.5 to assign equal preference

Experimental Results

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

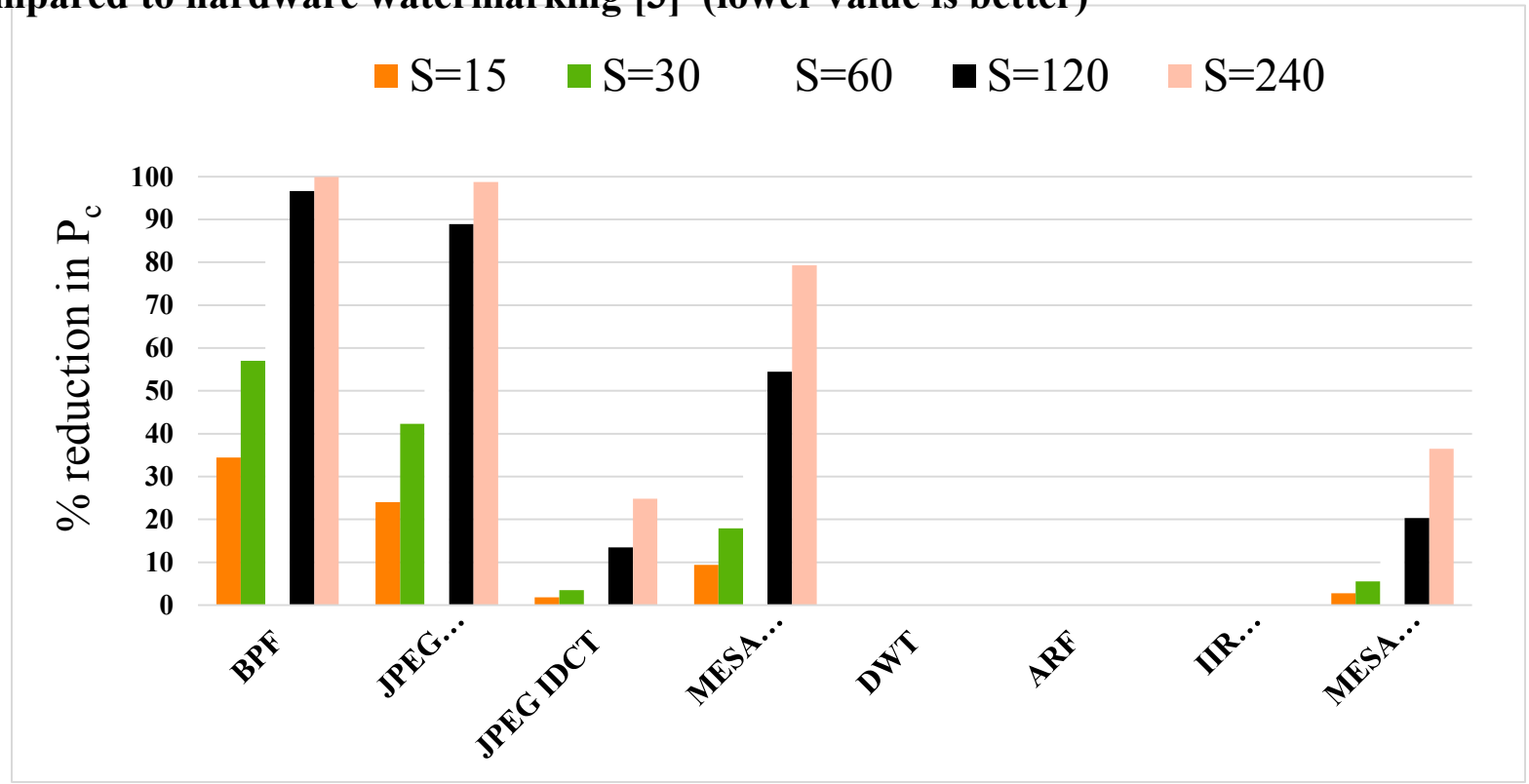
$$P_c = \left(1 - \frac{1}{c}\right)^S$$

'c' denotes the number of colours used in the CIG and 'S' denotes the digital signature size

Benchmarks	c	Size of Digital signature (S)				
		S = 15	S = 30	S = 60	S = 120	S = 240
		P_c	P_c	P_c	P_c	P_c
BPF	6	0.0649	4.2127×10^{-3}	1.7747×10^{-5}	3.1496×10^{-10}	9.9198×10^{-20}
JPEG SAMPLE	10	0.2059	0.0424	1.7970×10^{-3}	3.2292×10^{-6}	1.0428×10^{-11}
JPEG IDCT	29	0.5907	0.3490	0.1218	0.0148	2.1999×10^{-4}
MESA FEEDBACK POINTS	17	0.4028	0.1622	0.0263	6.9267×10^{-4}	4.7979×10^{-7}
ARF	8	0.1349	0.0182	3.3150×10^{-4}	1.0989×10^{-7}	1.2076×10^{-14}
MESA MATRIX MULTIPLICATION	23	0.5134	0.2635	0.0695	4.8237×10^{-3}	2.3268×10^{-5}

Comparison with Existing Approach [3]

Percentage reduction in Pc values (stronger proof of IP ownership) of proposed approach compared to hardware watermarking [3] (lower value is better)



Conclusion

- A new cryptosystem based digital signature generation and embedding approach for protection of reusable IP cores is proposed.
- The digital signature generation process comprises of three security modules that makes the watermark robust and secure.
- For conclusion, proposed approach yields stronger protection through robust digital signature and it is reflected in **reduction of P_c value on an average by ~24.8%** compared to [3], while significantly **lowering the average design overhead** incurred in terms of register hardware **by ~13.73%.**

References

- F. Koushanfar, I. Hong, and M. Potkonjak, “Behavioral synthesis techniques for intellectual property protection”, in ACM Trans. Des. Autom. Electron. Syst., Vol. 10, No. 3, July 2005, pp. 523-545.
- Cryptography and Network Security: Principles and Practice – William Stallings.
- A. Sengupta and S. Bhadauria, “Exploring low cost optimal watermark for reusable ip cores during high level synthesis,” IEEE Access, vol. 4, no. 99, pp. 2198–2215, May 2016.
- Anirban Sengupta, Dipanjan Roy, "Anti-Piracy aware IP Chipset Design for CE Devices: Robust Watermarking Approach", in IEEE Consumer Electronics, Volume: 6, Issue: 2, April 2017, pp. 118 - 124.
- University of California Benchmark Suite, Express Benchmarks, https://www.ece.ucsb.edu/EXPRESS/benchmark/, 2018

Thank You