Securing IP Cores for DSP Applications Using Structural Obfuscation and Chromosomal DNA Impression

ANIRBAN SENGUPTA, (Senior Member, IEEE), AND RAHUL CHAURASIA, (Member, IEEE)

Discipline of Computer Science and Engineering, Indian Institute of Technology Indore, Indore 453552, India
Corresponding author: Anirban Sengupta (asengupt@iiti.ac.in)

This work was supported by the Indian Institute of Technology Indore, India.

ABSTRACT This paper presents a novel hybrid methodology with structural obfuscation and encrypted chromosomal DNA impression to secure intellectual property (IP) cores of digital signal processing (DSP) applications. The proposed work offers security against altering register transfer level (RTL) description using multilevel structural obfuscation as well as security against IP piracy using secret chromosomal DNA impression. In this approach, an invisible DNA impression is covertly implanted into the structurally obfuscated DSP design using robust encoding and encryption using multi-iteration Feistel cipher. Our work is more robust than recent facial biometric and steganography-based hardware IP security techniques, in terms of stronger proof of digital evidence as well as tamper tolerance ability. The results report following qualitative and quantitative analysis of the proposed structural obfuscation with encrypted chromosomal DNA impression based framework: (a) very low probability of coincidence (Pc) (indicating strength of digital evidence) for different DSP IP cores in the range of 7.59E-5 to 1.2E-1; (b) stronger tamper tolerance for different DSP IP cores in the range of 5.62E+14 to 3.40E+38; (c) negligible design cost overhead of 0.00% for different DSP IP cores; (d) strength of obfuscation in terms of number of gates obfuscated.

INDEX TERMS IP core, obfuscation, DNA impression, security.

I. INTRODUCTION

DSP IP core(s) integrated in consumer electronic (CE) systems are capable to achieve high performance at lower cost [1]. Due to this efficacy, they have become an important part of portable electronic devices such as smart watches, mobile phones, tablets and digital camera. Digital signal processing cores such as discrete Fourier transform (DFT), discrete cosine transform (DCT) and finite impulse response (FIR) filter core etc. are such reusable IP cores that are used in executing several image/audio/video processing applications [2], [3]. In general, since DSP algorithms require complex computations and data intensiveness, therefore, for an IP designer it is not easy to design it from the lower abstraction level of system design. Therefore, to design an IP core, DSP algorithms are important to be synthesized into hardware level using high level synthesis (HLS) framework [4].

Further, an IP designed in a fabless center is either transferred to a system-on-chip (SoC) integrator for system integration or sent to a foundry for standalone IC fabrication [5], [6]. Since the modern design supply chain involves offshore design houses, hence they cannot be completely trustworthy [7]–[9]. An adversary in these offshore design houses may perform the following: (i) alteration of original register transfer level description (ii) counterfeiting the IP [10]–[12], both of which may cause safety hazard to end consumer. Therefore, IPs or integrated circuits (IC) of a CE system needs to be secured against external hardware threats such as piracy, for the benefit of end consumer.

The rest of the paper is organized as follows: section II discusses the main advances and contributions of our work; section III highlights the related work; section IV presents an overview of proposed methodology; section V discusses the details of the proposed methodology; section VI provides the results and its analysis, while section VII concludes the paper.

II. MAIN ADVANCES AND CONTRIBUTIONS

This section discusses the novelties of this paper, followed by the advancement and advantages over the state-of-the-art techniques.
A. NOVELTIES OF THE PAPER
This paper offers the following novelties:

a) A methodology with encrypted chromosomal DNA impression to secure IP cores of digital signal processing applications against IP piracy.

b) The proposed work also offers secondary security layer against altering register transfer level (RTL) description using multilevel structural obfuscation.

c) In this hybrid methodology, an invisible DNA impression is covertly implanted into the structurally obfuscated DSP design using robust encoding and encryption using multi-iteration Feistel cipher.

d) Our technique is more robust than recent facial biometric and steganography-based hardware IP security techniques in terms of stronger proof of digital evidence as well as tamper tolerance ability.

e) Our framework incurs zero design cost overhead post implanting encrypted DNA impression and post structural obfuscation.

B. ADVANCEMENT OF THE STATE OF THE ART
Our framework offers the following advancements and advantages compared to state of the art:

1) In case of hardware watermarking [17], the signature variables, their combination/size and mapping rules can be compromised by an attacker without significant efforts; while, our security framework embeds unique encrypted chromosomal DNA impression comprising of large security constraints in the obfuscated design, for enhanced robustness against IP piracy.

2) In case of hardware steganography [4], [18], the generated stego-constraints (stego-keys) are usually not as big and strong as proposed hybrid methodology based on structural obfuscation and encrypted chromosomal DNA impression. Additionally, the steganography technique depends only on secret design data, stego-encoder and mapping rules which are prone to susceptibility. On the contrary, rather than depending on such external secret information, our methodology scientifically produces encrypted digital DNA impression using big secret key, circularly shift functions, iterations of Feistel cipher, number of round functions, type of DNA base pair sequencing, chromosomal sequence and size, count/ordering of the polynucleotide inserted, dual encoding rule and S-Box type for DSP IP core applications.

3) In case of biometric based hardware security, although, the facial biometric [9] is stronger than hardware watermarking [14]–[17] and hardware steganography [18], in terms of hardware security constraints (resulting into greater robustness in the security of RTL circuit), however it is not as robust as the framework presented in this paper for DSP IP core(s). This is because ours is capable of generating several times larger security constraints than steganography [18] and facial biometric signature [9]. Therefore, it reports lower probability of co-incidence (indicating stronger digital evidence) and larger tamper tolerance ability. Furthermore, it hinders regeneration of the digital DNA impression implanted multi-level structurally obfuscated design due to multiphase high-level transformations involved in our work.

4) Moreover, the methodology we presented offers higher security in terms of stronger digital evidence, as evident through lower probability of coincidence and larger tamper tolerance ability than related works [9], [18] (details provided in experimental results). Stronger digital evidence enables robust differentiation between an IP vendor’s original and its counterfeited version. Additionally, the experimental results also validate the efficacy of our methodology in terms of strength of obfuscation. This security feature is non-existent in [9], [18].

III. PRIOR WORKS
In the literature, IP watermarking [17], IP steganography [4], [18], physically unclonable functions (PUF) based techniques for hardware IP authentication [20]–[22], facial biometric signature [9] based hardware security techniques and machine learning techniques, to detect Trojan and counterfeited chips [13]–[16], have been proposed to secure reusable IP core(s) used in CE systems against IP piracy. IP steganography [4], [18] techniques are responsible for generating stego-constraints using stego-key, followed by embedding them in the form of authentic covert information into the DSP IP core. The stego-constraints in these works are generated using entropy thresholding or key-triggered hash chaining mechanisms. These variables provide the designer, the flexibility of controlling the amount of digital evidence to be implanted into the DSP core design. In these works, if the entropy thresholding parameter or stego-key is compromised (leaked) by an adversary, it can affect the IP piracy detection process. Hardware watermarking [17] technique is capable of generating the embedded signature using signature variables, their combination/size and mapping rules. However, [17] suffers from incapability of providing sufficient digital evidence for robust IP piracy detection. Further, if the signature variable details and mapping rules are leaked by an adversary, then the hardware watermarking can be easily compromised. These limitations do not exist in our proposed work, as our framework employs strong encrypted DNA signature using multi-round Feistel cipher, with strong secret keys and security properties. Further, the proposed technique offers structural obfuscation as secondary defense against alteration of RTL description, which related works are unable to provide. Additionally, biometric techniques such as facial biometric [9] has been proposed to secure DSP based IP cores against IP piracy/counterfeiting. Though biometric techniques are effective against IP piracy threat, however it has dependency on external factors such as requirement of high-resolution camera, possibility of variation in facial signature due to aging and careful selection of facial features to generate a robust signature. Further, the implementation complexity of facial biometric technique [9] is higher. The proposed technique on the contrary, does not have dependency on above external factors. Rather it integrates
structural obfuscation (as a second line of defense) with digital DNA impression mechanism to hinder covert signature regeneration process, thus thwarting alteration of RTL description and IP counterfeiting. Further, machine learning techniques [13]–[16] have also been proposed for hardware Trojan detection process. These techniques employ Artificial Neural Network (ANN) and Support Vector Machine (SVM) learning models for hardware security. It employs classifier-based identification of Trojans in pipelined microprocessors. These works provide a classification of all possible hardware Trojan attacks and also provides discussion from four perspectives, i.e., detection, design-for-security, bus security, and secure architecture. However, these techniques are not capable of detecting IP piracy and hindering alteration of RTL description, unlike the proposed technique. Furthermore, PUF based techniques [20]–[22] have been proposed for IP authentication process. Further, they offer suitable lightweight security primitive for field programmable gate array (FPGA)/system-on-chips bitstream encryption and device authentication. These works have proved effective against such devices; however, they do not target security of DSP cores against IP piracy, unlike proposed technique. Further, they do not provide defense by hindering alteration of RTL description using structural obfuscation, unlike proposed approach. Further, [23], [24] have proposed machine learning techniques for hardware Trojan insertion using frameworks such as reinforcement learning. [23], [24] do not aim to secure IP cores against piracy and RTL design alteration, unlike presented paper. Therefore, prior works [4], [9], [13]–[18], [20]–[22] target the security against IP piracy/counterfeiting-based hardware threats, however do not provide obfuscation simultaneously for hindering alteration of RTL description, with respect to DSP hardware IPs. Further, these prior works do not embed robust chromosomal DNA impression using cipher and multi-level encodings for enhanced security against IP piracy attack, unlike proposed methodology. Our methodology further employs a robust structural obfuscation that uses high level transformations such as tree height transformation (THT) and loop unrolling (LU) to provide robust security. Therefore, addressing potential threat of alteration of RTL description along with IP piracy is imperative.

IV. PROPOSED METHODOLOGY

The framework we proposed in this work, advances CE systems security and covers consumers’ safety in terms of their safe usage, by protecting the underlying DSP hardware cores against the threats of counterfeiting. Furthermore, our work also offers benefits from a SoC integrator’s or product designer’s perspective. Therefore, the proposed methodology is a mechanism to hinder register transfer level (RTL) description alteration using structural obfuscation and a detective measure against piracy/counterfeiting threat. By detecting a designer’s authentic mark in the IP cores, the SoC integrator can refrain from using fake IP components in the CE products and make sure of using only authentic designs.

We therefore, propose a structural obfuscation methodology integrated with Feistel cipher based encrypted chromosomal DNA impression has been proposed for securing the IP cores for DSP applications. The overview of our methodology, as shown in Fig. 1, has been explained using four major steps:

(a) The first step is responsible for generating the security constraints using the chromosomal DNA impression for the structurally obfuscated hardware design. The first step considers a DSP application as its input. In this phase, initially, structural obfuscation using high-level transformation has been performed.

(b) In the next step, subsequently two DNA base pairs have been formed on the basis of four chemical elements. The two DNA base pairs which then form the chromosomal DNA sequence by taking alternative base pairs of the same as well as of distinct type as part of digital DNA impression generation process. In this phase, hardware security constraints are finally produced as an output based on the IP core designer selected impression strength size) of the encrypted impression.

(c) In the third step, embedding of these hardware security constraints into obfuscated colored interval graph (CIG) of DSP hardware is performed.

(d) In the fourth step, post embedding the obfuscated DSP hardware register transfer level (RTL) with encrypted DNA impression as digital evidence, is generated.

V. DETAILS OF THE PROPOSED METHODOLOGY

The input block of our methodology (as shown in Fig. 1) consists of the DSP application (in the form of control data flow graph (CDFG)), resource constraints for the structurally obfuscated design, library, secret keys for the IP designer selected rounds and DNA base pairs. The output block consists of the RTL circuit of the obfuscated DSP hardware post embedding the encrypted DNA impression as digital evidence.

- The first block is responsible for structural obfuscation of the DSP application using loop based high level transformation i.e., loop unrolling.
- The second block, then performs the non-loop based high level transformation i.e., tree height transformation on the design architecture produced by the first block.
- The third block is responsible for generating the register allocation table of the structurally obfuscated design produced by second block.
- The fourth block is responsible for forming the DNA base pairs of same as well as of distinct type based on the chemical elements.
- Subsequently, the next block is responsible for generating the chromosomal DNA sequence based on the strength (size) selected by the IP designer.
- The next block, then generates the binary encoded chromosomal DNA sequence for the sequence produced by the previous block, based on an encoding rule-1.
The next block is responsible for performing the encryption using Luby–Rackoff Cipher on the binary encoded chromosomal DNA sequence (produced by the previous block). The encryption process accepts the keys, generated by the proposed key generation algorithm based on the number of rounds (Z) selected by the IP designer.

Subsequently, the next block is responsible for performing the truncation on the digital DNA impression, depending upon the final digital impression strength selected by IP designer.

The final block of the first phase, then converts the encrypted chromosomal DNA impression (selected by the IP designer as output of the previous block) into covert hardware security constraints based upon an encoding rule-2. These obtained hardware security constraints (based on the structural obfuscation of the hardware design) is given as input to the RTL generation phase, responsible for embedding the hardware security constraints into the obfuscated CIG of DSP application. Then, RTL circuit of the obfuscated DSP hardware with encrypted chromosomal DNA impression is generated as digital evidence.

A. PROPOSED STRUCTURAL OBFUSCATION

Hardware structural obfuscation obscures the actual hardware design architecture of the DSP IP core, to protect it from an adversary attempting to alter the RTL description. Structural obfuscation is performed through several loop based and non-loop based high level transformations. Structural obfuscation transforms the generic hardware design architecture into obfuscated design architecture without compromising its actual functionality. It makes it almost impossible and challenging for an adversary to alter the original RTL description, in order to correctly interpret the functionality and hardware interconnection from the structurally obfuscated design.

In this work, DSP applications (such as FIR and DFT) are accepted as input and then structural obfuscation has been performed over them in order to make them secure against attacks from an adversary. In this work, structural obfuscation on DSP application has been performed using THT and LU algorithms. The un-obfuscated CDFG of FIR filter is shown in Fig. 2 and the corresponding obfuscated FIR filter using structural obfuscation based on THT and LU is shown in Fig. 3 respectively. THT divides the critical path computation into multiple sub computations and then executes them...
in parallel. THT based structural obfuscation results into change in interconnectivity of the RTL datapaths of the DSP hardware in terms of multiplexer size, demultiplexer size, storage element etc., without affecting the functionality. This therefore produces unobvious architecture of the respective DSP hardware and thwarts alteration of the original RTL design. On the other hand, the loop transformation unrolls the loop-based application depending on the unrolling factor. LU executes the same calculation present inside the loop multiple times. Loop unrolling based structural obfuscation also results into change in RTL datapath in terms of multiplexer size, demultiplexer size, storage element etc., without affecting the functionality. In the 4-point DFT application, tree height transformation (THT) has been performed to obfuscate the structure of the application. The respective non-obfuscated and obfuscated scheduled CDGF of 4-point DFT, is shown in Fig. 4 and Fig. 5 respectively.

B. PROPOSED ENCODED CHROMOSOMAL DNA FRAMEWORK

In the proposed chromosomal DNA model, two base pairs (BP) of chromosomal DNA have been taken. First base pair (BP-1) is formed with two chemical elements Thymine (T) and Adenine (A) whereas the second base pair (BP-2) is formed with two other chemical elements named Guanine (G) and Cytosine (C). Subsequently, from these two base pairs (BP-1 and BP-2) chromosomal DNA sequence can be formed in two ways, either by considering the alternative base pairs of same type or by considering alternative base pairs of distinct type, as presented in Fig. 6. The final chromosomal DNA sequence has been formed by adding the polynucleotide (Sugar phosphate backbone) represented as ‘S.’ Polynucleotide has been added as leading and lagging strand in the DNA sequence. An example of IP designer created possible chromosomal DNA sequence with alternative base pairing comprising of same type of base pairs, is shown in Fig. 7. Similarly, chromosomal DNA sequence for alternative base pairs of distinct types can also be generated. Consequently, the chromosomal DNA sequence selected by IP designer (either with alternative base pairs of same type or distinct type) can be encoded into binary digits using IP designers specified encoding rule-1. The encoding rule-1 for all the chemical elements (A, T, G, C and S) used in formation of final chromosomal DNA sequence, is shown below:

Element ‘A’ (alphabet value = 1) is being encoded in binary as ‘1,’ ‘T’ (20) as ‘10100,’ element ‘G’ (7) as ‘111,’ ‘C’ (3) as ‘11’ and ‘S’ (19) as ‘10011.’ An example of a final chromosomal DNA sequence with alternative base pairing of same type (as shown in Fig. 7) is depicted below:

STAS-SATS-SGCS-SCGS-STAS-SATS-SGCS-SCGS-STAS-SATS-SGCS-SCGS-STAS-SATS-SGCS-SCGS—

The corresponding binary encoded DNA impression, (for e.g., 128 bit), formed using encoding rule-1, is shown below:

\[
\begin{align*}
\text{x[0]} & \quad x[1] \\
\text{x[2]} & \quad x[3] \\
\text{x[0]} & \quad x[1] \ e^{-j\pi/2} x[2] \ e^{-j\pi/4} x[3] \ e^{-j3\pi/4} \\
\end{align*}
\]

FIGURE 3. Scheduled DFG of FIR based on resource constraint (1M, 1A) after high level transformation.

FIGURE 4. DFG of 4-point DFT computing two samples at a time.

VOLUME 10, 2022
FIGURE 5. Scheduled DFG of obfuscated 4-point DFT based on resources constraints of 3M and 2A.

FIGURE 6. Proposed chromosomal DNA with distinct/same type base pairs.

FIGURE 7. Example of a possible chromosomal DNA sequence with base pairs and polynucleotide using proposed work.

Similarly, an example of a final chromosomal DNA sequence with alternative base pairing of distinct type can be created. The corresponding binary encoded digital DNA impression (for e.g. 128 bit), formed using encoding rule-1, is shown below. (Note: The 128-bit DNA impression is also expandable upto designer specified strength
FIGURE 8. Encryption process using Feistel cipher.

C. GENERATING PROPOSED ENCRYPTED ENCODED DIGITAL DNA IMPRESSION

The generated binary encoded chromosomal DNA impression with the alternative base pairs of the same or distinct type can be fed into the Feistel cipher for encryption purpose. For an instance encoded chromosomal DNA impression with alternative base pairs of distinct type has been fed into the multi round Feistel cipher process, as shown in Fig. 8 (Note: the right part of Fig. 8 is the continuation of the left part). The 128-bit binary encoded chromosomal DNA sequence having alternative base pair of distinct type is further divided into two segments (64 bit each) and fed into the cipher process iteratively. In the first round of Feistel cipher, the initial 64-bit binary encoded output (the first segment) of chromosomal DNA impression is bifurcated into two parts as left ‘L’ and right ‘R’ of 32 bit each. Subsequently the right part is supplied into the encryption function ‘F (K, Z)’ which is capable of performing diffusion (permutation) and confusion (substitution) on the input value. Diffusion is performed by expanded P-box, whereas confusion is performed by S-box mechanism. Expanded P-box proceeds with right part (R) by accepting it as its input and transforms it into 48-bit output, which then gets XORed with the 48-bit key (K1 for round-1) fed into the cipher process. Consequently the 64-bit encrypted chromosomal DNA impression is obtained after the first round. This process continues for the rounds ‘Z’ selected by the IP designer (where a separate key for each round is fed by the IP designer).

The key generation process is shown in Fig. 9. As can be observed from Fig. 9, initial 48 bit key (K1 for round-1) is bifurcated into two parts, 24 bit each. The left 24 bit and right 24 bits are fed into circularly left shift and circularly right shift functions respectively. The output of both these functions is then XORed, which generates the 24-bit key value. Subsequently this 24-bit value is concatenated with a fresh 24-bit key value selected by the IP designer, which generates the key K2 for the next round. Thus, by operating the keys (K1, K2 … KZ) on each round of Feistel cipher process (selected by the IP designer) it produces the encrypted chromosomal DNA impression. Similarly for the
second segment of encoded chromosomal DNA impression, encrypted chromosomal DNA impression is also generated.

**D. IMPLANTING HARDWARE SECURITY CONSTRAINTS**

As observed in Fig. 1, truncation needs to be performed (using the IP designer selected value e.g., 32, 64, and 128 bit) on the final encrypted chromosomal DNA impression resulting from the Feistel cipher. Subsequently the encrypted impression based on IP designer selected strength is converted into its respective hardware security constraints for embedding into the DSP design using IP designer specified encoding rule-2. In the encoding rule-2, bit ‘0’ signifies embedding an artificial edge between storage variable node pair (even-even) of the obfuscated CIG of DSP application; while bit ‘1’ signifies embedding an artificial edge between storage variable node pair (odd-odd) of the obfuscated CIG of DSP application. The 128-bit encrypted chromosomal DNA impression, generated using Feistel cipher, corresponding to the genome/DNA binary encoded digital impression (shown in sequence (2) in section IV.B) is shown below:

```
“001001011011000001010111101011110110110110101
111010101000011100100011011110001011001001
010111001001010010101101101110100.”
```

For example, the hardware security constraints for the above 128-bit encrypted chromosomal DNA impression corresponding to 4-point DFT (comprising of storage variables (V1-V26)), using the encoding rule-2 are as follows:

{(V2, V4), (V2, V6), (V2, V8), (V2, V10), (V2, V12), (V2, V14), (V2, V16), (V2, V18), (V2, V20), (V2, V22), (V12, V18), (V12, V20), (V12, V22), (V12, V24), (V12, V26), (V14, V16), (V14, V18), (V14, V20), (V14, V22), (V14, V24), (V14, V26), (V16, V18), (V16, V20), (V16, V22), (V16, V24), (V16, V26), (V18, V20), (V1, V3), (V1, V5), (V1, V7), (V11, V17), (V11, V19), (V11, V21), (V11, V23), (V11, V25), (V13, V15), (V13, V17).}

Now the embedding of these covert hardware security constraints into obfuscated CIG of the 4-point DFT using HLS is performed. Register allocation tables representing the assignment of storage variables of the obfuscated 4-point DFT, before and after implantation of the constraints, is shown in Table 1 and Table 2 respectively. In Table 1, assignment of storage variables (V1-V26) to fourteen distinct registers (colors) and scheduling (timing steps) represented by C0, C1...C5 are shown. The register allocation of storage variables (as shown in Table 1) has been generated using scheduled graph based on designer selected resource constraints 2 adder and 3 multipliers. The variables marked in red in Table 2 indicate that local transformations have been made to accommodate the above hardware security constraints. It is to be noted that the register variables required at the same time step cannot share the same register, as it results into conflict in timing overlap. However, the variables required at different time steps can share the same register (color). It can be observed (from Table 2) that there is no requirement of any extra color (register) for embedding all the above hardware security constraints into the structurally obfuscated CIG of 4-point DFT.

**VI. RESULTS**

This section analyses results of the proposed structural obfuscation and chromosomal DNA impression-based technique for securing the IP cores corresponding to the DSP applications. Our technique is automated using C++ language and run-on intel(R) core (TM) i5-11235G7 processor with 2.40GHz frequency. The implementation run time of this methodology is 3.041s.

**A. SECURITY ANALYSIS**

The obfuscation achieved is measured by strength of obfuscation in terms of number of gates modified in the datapath of the DSP design (as shown in Fig. 10). The more the number of gates affected, more is the strength of obfuscation and harder it is for an adversary to alter the RTL description of the DSP core. Fig. 8 shows the strength of obfuscation achieved using proposed method for different DSP applications. Further the proposed work embeds a robust chromosomal DNA impression on the obfuscated DSP design to provide detection against pirated IP core. It is very challenging for an attacker to regenerate the encrypted DNA digital impression for evading IP piracy detection process, because he/she needs to have the following secret information:

(a) **Secret key** (N): By considering the initial key size of 48 bit, the function for populating the size of the secret key in our technique is, \( 48 * Z * I \) bits; where ‘Z’ and ‘I’ (both variables are unknown to an adversary) signifies the number of encryption rounds used in a single Feistel cipher and the number of Feistel cipher iterations required, respectively (depending on the strength of the binaries chromosomal DNA impression). Additionally, binaries chromosomal DNA impression strength depends on the formed chromosomal DNA sequence, initially. For example, if the binaries chromosomal DNA impression is 128 bits, then \( I = 2 \), while if the binaries chromosomal DNA impression is 192 bits, then \( I = 3 \) and so forth. Therefore, for example, if \( Z = 16, C = 2, \)

**FIGURE 10. Strength of obfuscation of proposed approach.**
then \( N = 1536 \) bits then the key size space is 21536. Deriving an exact digital impression from this massive key space gets harder even through the brute force parser.

\[ b \] Secret key \((N)\) also depends on the shift variables \(('n' \text{ and } 'm')\): The derivation of the original digital impression implanted into the obfuscated design can be prevented from an adversary (due to the unknown behavior of circularly shift functions of the key generation process).

\[ c \] Chromosomal DNA sequence and size: The sequence and size of base pairs used in forming the chromosomal DNA sequence is highly challenging to precisely estimate for an adversary. Further, the order/counting of the inserted polynucleotide as well as the number of chemical elements \( (A, T, C, G, S) \) associated in a particular DNA sequence (formed with either distinct or same type of base pairs) is highly challenging for an attacker to precisely estimate.

\[ d \] Strength of encrypted chromosomal DNA impression: The strength of encrypted chromosomal DNA impression after performing the truncation is extremely difficult for an attacker to gauge.

\[ e \] Dual encoding rule: intricacies of both encoding rules (1 and 2) are very complex, thereby making it extremely difficult to decode.

\[ f \] S-Box Selection: The S-box type(s) used during substitution phase of encryption function is difficult to precisely estimate for an attacker. As a same S-box to convert all 6-bit to 4-bit or to convert each 6-bit to 4-bit, different S-boxes may be used.

Our technique exhibits the aforesaid security properties against brute-force attack and tamper tolerance. So, the attacker cannot extract the exact design without knowing the exact DNA impression and resource configuration (adders and multipliers used in CDFG of DSP application). Further, without the knowledge of (a) to (f), regeneration of embedded digital impression is impossible. An adversary’s extracted design cannot fully match with the original design (pre-embedding). Security against IP piracy is analyzed (in terms of strength of ownership proof) using following probability of coincidence \((P_c)\) metric \([15], [18]\):

\[
P_c = \left(1 - \frac{1}{r^c}\right)
\]

where, ‘r’ signifies the number of colors/registers, before implanting secret constraints in the CIG of the design and ‘c’ refers the number of covert constraint edges added to the CIG. The ‘\(P_c\)’ value specifies the probability of coincidently detecting security constraints in an unsecured design; hence it is desirable for it to be low as much as possible. The \(P_c\) value achieved using our method for FIR, 4-point DFT, 4-point DCT and 8-point DCT are reported in Table 3, for varying effective constraints size with respect to encrypted chromosomal DNA impression (corresponding to different number of base Pairs \((AT/GC)\) in chromosomal DNA and different number of polynucleotide). As shown in the Table 3, a low ‘\(P_c\)’ is achieved for all the variations of encrypted chromosomal DNA impression sizes implanted into the obfuscated DSP designs.

The proposed encrypted digital DNA impression methodology is also compared with a recent state-of-the art security work based on facial biometric \([9]\) and hardware steganography \([18]\). The comparisons of ‘\(P_c\)’ of presented work with \([9]\) and \([18]\) are reported in Fig. 11. As evident, our methodology
TABLE 4. Obfuscated design cost pre and post embedding encrypted chromosomal DNA impression constraints (32, 64, 128 bits).

| Benchmarks | # of registers in obfuscated design (pre embedding digital DNA impression) | # of registers in proposed obfuscated encrypted digital DNA impression implanted design | Design cost of baseline | Design cost of proposed obfuscated encrypted digital DNA impression implanted design | % Cost overhead in proposed obfuscated encrypted digital DNA impression implanted design |
|------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| 4-point DCT | 8                                                                       | 8                                                                                          | 0.5659                 | 0.5659                                                                           | 0.00%                                                                            |
| 4-point IDCT | 8                                                                      | 8                                                                                           | 0.5659                 | 0.5659                                                                           | 0.00%                                                                            |
| 8-point DCT | 16                                                                     | 16                                                                                          | 0.4771                 | 0.4771                                                                           | 0.00%                                                                            |
| 8-point IDCT | 16                                                                    | 16                                                                                         | 0.4771                 | 0.4771                                                                           | 0.00%                                                                            |

FIGURE 11. Comparison of probability of coincidence (Pc).

This achieves much lower ‘Pc’ compared to both [9] and [18]. This is because the number of security constraints generated using [9] and [18] are significantly lesser compared to the methodology presented in this paper. Security against tampering vulnerability is evaluated using the tamper tolerance ability. The larger key-space proportionately increases the resistance for an attacker to find the exact encrypted digital DNA impression implanted in the design. The tamper tolerance ability (TA) is measured using the following metric:

\[ \text{TA} = (\alpha)^\beta \]  

where, ‘\( \alpha \)’ signifies the number of variables used in the encrypted digital DNA impression (which is two for both proposed and [9] and [18]) and ‘\( \beta \)’ denotes the number of implanted hardware security constraints. Since the security constraints generated and embedded through our work is comparatively higher, thus the tamper tolerance ability of proposed method is far stronger than [9] and [18]. The comparisons of tamper tolerance ability of our work with [9] and [18] are shown in Fig. 12. As evident, the TA of the method that we presented is far robust than [9] and [18] due to generation of more security constraints.

B. ANALYSIS OF EMBEDDED DESIGN COST

The impact of our methodology on embedding design cost (\( C_f(H_i) \)) is analyzed using the following [9], [15]:

\[ C_f(H_i) = x_1 \frac{Td}{Tm} + x_2 \frac{Rd}{Rm} \]  

where, ‘\( H_i \)’ denotes the resource constraints, Rd and Td denote the design area and delay respectively, Rm and Tm denote the maximum area and delay of the design, x1 and x2 signifies weights of delay and area in the cost function. Design cost also known as implementation cost of a DSP design and it is a normalized function of area and latency. A 15nm open-cell library [19] is used to calculate both the delay and area of a hardware design. Table 4 reports the design cost of proposed obfuscated encrypted digital DNA impression implanted design and pre-embedded (baseline) obfuscated version. As evident, our methodology incurs design cost overhead of 0.00% corresponding to all DSP designs.

The implementation run time of the proposed security approach for different DSP benchmarks have been show in Table 5. As evident from the table, the proposed technique is capable of embedding robust encrypted DNA impression into the DSP designs at very less implementation complexity (in terms of embedding time).

VII. CONCLUSION

Ensuring security of DSP based IP cores against alteration of RTL description and counterfeiting threats is crucial for both SoC designer and end consumers, as these IP cores are integral part of CE systems. This paper has presented a novel methodology for securing DSP based IP cores against alteration of RTL description and IP piracy using hybrid structural
obfuscation and encrypted chromosomal DNA impression mechanism. The presented methodology was proven to be more robust security wise than recent similar works.

REFERENCES

[1] C. Pilato, S. Garg, K. Wu, R. Karri, and F. Regazzoni, “Security hardware accelerators: A new challenge for high-level synthesis,” IEEE Embedded Syst. Lett., vol. 10, no. 3, pp. 77–80, Sep. 2018, doi: 10.1109/LES.2017.2774800.

[2] K.-W. Chan, C.-C. Sun, and N.-J. Yang, “An improved LOMB algorithm for HRV analysis on a PPG sensor for low-cost DSP processor,” in Proc. IEEE Int. Conf. Consum. Electron. Taiwan (ICCE-TW), Jun. 2017, pp. 405–406, doi: 10.1109/ICCE-China.2017.7991167.

[3] N. Pezek, N. Kaprocki, and J. Kovacevic, “Firmware update procedure for audio systems based on CS4953xx DSP family,” in Proc. Int. Conf. Smart Syst. Technol. (SSST), Oct. 2018, pp. 29–34, doi: 10.1109/SSST.2018.8564683.

[4] M. Rathor and A. Sengupta, “IP core steganography using switch based key-driven hash-chaining and encoding for securing DSP kernels used in CE systems,” IEEE Trans. Consum. Electron., vol. 66, no. 3, pp. 251–260, Aug. 2020, doi: 10.1109/TCE.2020.3006050.

[5] G. He, C. Dong, Y. Liu, and X. Fan, “IPlock: An effective hybrid encryption for neomorphic systems IP core protection,” in Proc. IEEE 4th Inf. Technol., Netw., Electron. Automon. Control Conf. (ITNEC), Jun. 2020, pp. 612–616, doi: 10.1109/ITNEC48623.2020.9085144.

[6] A. Sengupta and S. Bhaduria, “Exploring low cost watermark for reusable IP cores during high level synthesis,” IEEE Access, vol. 4, pp. 2198–2215, 2016, doi: 10.1109/ACCESS.2016.2552058.

[7] S. M. Plaza and I. L. Markov, “Solving the third-shift problem in cc piracy with test-aware logic locking,” IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 34, no. 6, pp. 961–971, Jun. 2015, doi: 10.1109/TCAD.2015.2404876.

[8] B. Colombier, U. Mureddu, M. Laban, O. Petura, L. Bossuet, and F. C. Plessas, “Machine learning for hardware trojan detection: A review,” IEEE Trans. Comput., vol. 69, no. 6, pp. 231–246, Nov. 2020, doi: 10.1109/TC.2019.2933331.

[9] M. Xue, C. Gu, W. Liu, S. Yu, and M. O’Neill, “Ten years of hardware trojans: A survey from the attacker’s perspective,” IET Comput. Digit. Techn., vol. 10, no. 1, pp. 112–123, Jan. 2021, doi: 10.1049/iet-cdt.2020.0041.

[10] X. Wang, Y. Zheng, A. Basak, and S. Bhunia, “IIPS: Infrastructure IP for secure SoC design,” IEEE Trans. Comput., vol. 64, no. 8, pp. 2226–2238, Aug. 2015, doi: 10.1109/TC.2014.2360535.

[11] S. S. Zalivaka, A. A. Ivaniuk, and C.-H. Chang, “Reliable and modeling attack resistant authentication of arbitrer PUF in FPGA implementation with trinary quadruple response,” IEEE Trans. Inf. Forensics Security, vol. 14, no. 4, pp. 1109–1123, Apr. 2019, doi: 10.1109/TIFS.2018.2870835.

[12] Y. Lao, B. Yuan, C. H. Kim, and K. K. Parhi, “Reliable PUF-based local authentication with self-correction,” IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 36, no. 2, pp. 201–213, Feb. 2017, doi: 10.1109/TCAD.2016.2569581.

[13] I. Cruz, P. Gaikwad, A. Nair, P. Chakraborty, and S. Bhunia, “Automatic hardware trojan insertion using machine learning,” 2022, arXiv:2204.08580.

[14] A. Sarihi, A. Patoobygh, P. Jamieson, and A.-H. A. Badawy, “Hardware trojan insertion using reinforcement learning,” 2022, arXiv:2204.04350.

ANIRBAN SENGUPTA (Senior Member, IEEE) received the Ph.D. degree in ECE from Ryerson University, Toronto, ON, Canada, in 2012. He is currently an Associate Professor of CSE at the Indian Institute of Technology Indore. He has around over 250 research contributions, which include more than 100 journals, patents, and invited book chapters from IET, Elsevier, the IEEE, Springer, and USPTO/CIP/PO. He is the owner 11 patents (granted/published/pending). His patents generated funding from the Ontario Center of Excellence, Canada. He had performed industry interactive research extensively for more than two years with Calypso, Bluespec, BEECube, and Huawei, Canada, during development of his Ryerson design space exploration tool arising from his patent. His research interests include optimization during design space exploration for hardware accelerators, high-level synthesis, fault secured high-level synthesis, hardware trust in high-level synthesis, digital watermarking, evolutionary computing, and physical design using CAD.

Dr. Sengupta is an Elected Fellow of the IET, IETE, and British Computer Society. He regularly serves as a member of the Technical Program Committee for the IEEE-CS ISVLSI, ACM GLVLSI, the IEEE CCECE, and the IEEE ICT. For his excellence in Ph.D. research, he has been awarded/nominated by the Ministry of Training, Colleges and Universities, Ontario for multiple years through OGS as well as by Ryerson University through GREA, RGA, and NSERC ICA for consecutive years. He also serves on the editorial board for four IEEE/IET journals. He is also serving as an Associate Editor for the IEEE Journal on Computer and Digital Techniques, an Associate Editor and a Columnist for the IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, an Associate Editor for the IEEE VLSI CIRCUITS AND SYSTEMS LETTER, and an Associate Editor for IEEE ACCESS journal. He further serves as a Guest Editor for special sessions in the IEEE TRANSACTIONS ON CONSUMER ELECTRONICS and IEEE ACCESS journal. He is a Regular Reviewer of the IEEE Journal on Computers and Digital Techniques, the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, the Journal on Swarm and Evolutionary Computation (Elsevier), the Journal on Applied Soft Computing (Elsevier), and the Journal on Expert Systems (Elsevier).

RAHUL CHAURASIA (Member, IEEE) received the M.Tech. degree in computer science engineering from RGPV, Bhopal, India, in 2018. He is currently pursuing the Ph.D. degree in CSE with the Indian Institute of Technology (IIT) Indore. He was awarded with the UGC-NET JRF Fellowship in January 2019.

VOLUME 10, 2022
50913