A Sequential Circuit-Based IP Watermarking Algorithm for Multiple Scan Chains in Design-for-Test

Wei LIANG1,2,3, Xingming SUN1,3, Zhiqiang RUAN1,3, Jing LONG2, Chengtao WU3

1Jiangsu Engg. Center of Network Monitoring, Nanjing Univ. of Information Sci. & Technology, Nanjing, 210044, China
2School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, 411201, China
3School of Computer and Communication, Hunan University, Changsha, 410082, China

idlink@163.com, sunnudt@163.com, rzq_911@163.com, longjing0404@163.com, chengtao_wu@163.com

Abstract. In Very Large Scale Integrated Circuits (VLSI) design, the existing Design-for-Test(DFT) based watermarking techniques usually insert watermark through reordering scan cells, which causes large resource overhead, low security and coverage rate of watermark detection. A novel scheme was proposed to watermark multiple scan chains in DFT for solving the problems. The proposed scheme adopts DFT scan test model of VLSI design, and uses a Linear Feedback Shift Register (LFSR) for pseudo random test vector generation. All of the test vectors are shifted in scan input for the construction of multiple scan chains with minimum correlation. Specific registers in multiple scan chains will be changed by the watermark circuit for watermarking the design. The watermark can be effectively detected without interference with normal function of the circuit, even after the chip is packaged. The experimental results on several ISCAS benchmarks show that the proposed scheme has lower resource overhead, probability of coincidence $P_c$ and higher coverage rate of watermark detection $\Delta S$ by comparing with the existing methods.

Keywords
IP reuse, VLSI, DFT, LFSR, multiple scan chains.

1. Introduction

With the rapid development of deep sub-micron integrated circuit systems, SOC (System on Chip) has become the mainstream in IC (Integrated Circuit) design. IP (Intellectual Property) reuse used by more semiconductor companies is essential to shorten design time and reduce product risk [1-3]. The problem of effective IP protection has been widely concerned.

Digital watermarking applied in DFT design has been extensively concerned [4], [5]. For most of the DFT watermarking techniques, the authors can insert their copyright into IP core, thus enabling identification of these cores. DFT watermarking, typically "protection and detection", is an IP protection technique for embedding watermark at various design stage of SOC design by using testability.

Recently, a number of DFT watermarking techniques have been proposed [6-22]. In the methods proposed by Fan et al. [7-8], the watermark generation is integrated in the test module. Five possible methods for watermark hiding are presented. Since only the test circuit instead of the IP core is marked independently, it is vulnerable to removal attacks. Cui et al. [9-11] proposed to insert watermark through reordering the scan cells in a single scan chain minimizing power overhead. Saha et al. [12-13] proposed to watermark both the scan tree and single scan chain, separately embedding the signatures of the owner of physical design tool and that of the logic design tool. The scheme proposed by Kirovski [14-15] marked the design by restricting some specific registers to appear in the scan chain at the DFT stage. The watermark is verified by comparing some simulation values of the design and the retrieved values in the output vectors in the test mode. It is only applicable to the partial scan architectures but not full scan designs. These techniques solve the problems of watermark embedding time, additional overhead and traceability existed in the previous methods. However, with the increasing complexity of circuit, the correlation of test vector for multiple scan chains may affect the circuit performance. Moreover, these methods are vulnerable to reverse engineering attack. The attackers can damage the overall project only by resynthesis and remapping.

An IP protection method is proposed by watermarking multiple scan chains in sequential circuit. The proposed scheme adopts DFT test model in SOC design, and uses an LFSR for pseudo random test vector generation [16]. All of the test vectors are shifted in scan input for the construction of multiple scan chains with minimum correlation. A watermark logic circuit is designed to change specific registers in multiple scan chains for watermarking the design.

2. Related Work

Usually, digital watermarking [17-20] methods are used along with DFT design in practical application. In this section, some basic definitions lay out the theoretical foundation for the construction of multiple scan chains with the minimum correlativity.
Definition 1: If there is at least one path from input vector \( S_i \) to output vector \( S_o \) in sequential circuit, \( S_i \) is connected with input vectors \( S_j \) and \( S_k \) respectively, then \( S_i \) and \( S_j \) are correlated; otherwise, uncorrelated.

Definition 2: In sequential circuit, \( N \) output vectors connected with input vectors \( S_i \) and \( S_j \) respectively, if it exists, the correlation is \( N \), denoted by \( (S_i, S_j) = N \) or \( (S_i, S_j) = N \), otherwise, \( S_i \) and \( S_j \) are uncorrelated, \( (S_i, S_j) = 0 \) or \( (S_i, S_j) = 0 \).

Definition 3: In multiple scan chains \( M \), supposing each chain has equal length, denoted by \( d \) (except as hereinafter provided). The ordering of scan cells in \( c_1 \) and \( c_2 \) is represented by \( \{s_{1,1}, s_{1,2}, \ldots, s_{1, n}\} \) and \( \{s_{2,1}, s_{2,2}, \ldots, s_{2,m}\} \) respectively. The correlation of scan chains \( c_1 \) and \( c_2 \) is denoted by \( Y(c_1, c_2) \):

\[
Y(c_1, c_2) = \sum_{i=1}^{d} (s_{1,i}, s_{2,i}).
\]  

(1)

Similarly, in multiple scan chains \( M \) with \( n \) scan chains \( c_1, c_2, \ldots, c_n \), correlation of \( M \) is the sum of correlation of every two different scan chains, denoted by \( \Phi(M) \):

\[
\Phi(M) = \sum_{1 \leq i < j \leq n} Y(c_i, c_j) = \sum_{i=1}^{d} \sum_{j=1}^{d} (s_{ij}, s_{jk}) = \sum_{i=1}^{d} \Pi(k).
\]  

(2)

Here, \( \Pi(k) = \sum_{i=1}^{n} (s_{ij}, s_{jk}) \) denotes the sum of correlation of every two different input signals in column \( k \) of the multiple scan chains.

Definition 4: In multiple scan chains \( M \), considering two input signals \( s_{ij} \), \( s_{jk} \) respectively in columns \( k_1 \), \( k_2 \), if the inequation

\[
\sum_{j=1}^{n} s_{ij} \cdot s_{jk} < \sum_{j=1}^{n} s_{ij} \cdot s_{jk} + \sum_{j=1}^{n} s_{ij} \cdot s_{jk}
\]  

(3)

is satisfied, then \( s_{ij} \) and \( s_{jk} \) is exchangeable, the exchange operation is called vector exchange.

Theorem: Multiple scan chains \( M_p \) is transformed into \( M_p \) after series of vector exchanges. In multiple scan chains \( M_p \), two input signals \( s_{ij} \), \( s_{jk} \) in any two columns \( k_1 \) and \( k_2 \), the inequation

\[
\sum_{j=1}^{n} s_{ij} \cdot s_{jk} + \sum_{j=1}^{n} s_{ij} \cdot s_{jk} \leq \sum_{j=1}^{n} s_{ij} \cdot s_{jk} + \sum_{j=1}^{n} s_{ij} \cdot s_{jk}
\]  

(4)

is satisfied, then \( s_{ij} \) and \( s_{jk} \) is exchangeable, the exchange operation is called vector exchange.

Proof: Consider \( M_p \), if any two input signals in any two columns satisfy the inequation in theorem, \( M_p \) is equal to \( M_p \); otherwise, there must be at least two input signals in different columns not satisfying the inequation. Randomly selecting two input signals \( P \) and \( Q \) in column \( k \) and \( Q \) in column \( k \), \( k \neq k \), \( s_{ij} \), \( s_{jk} \) the vector correlation of \( M_p \) is defined as:

\[
\Phi(M_p) = \gamma(k) + \gamma(k) + \sum_{j=1}^{d} \lambda(k) = \sum_{j=1}^{d} \lambda(k) + \sum_{j=1}^{d} \lambda(k) + \sum_{j=1}^{d} \lambda(k)
\]  

(5)

\( u \) is constant uncorrelated with \( P \) and \( Q \), \( M \) represents vector correlation sum of other columns except \( k \) and \( k \). By exchanging the positions of \( P \) and \( Q \) in \( M_p \), we get multiple scan chains \( M_l \). In \( \Phi(M_l) \), the correlation of the vectors has no change except that of columns \( k \) and \( k \), thus we have

\[
\Phi(M_l) = \gamma(k) + \gamma(k) + \sum_{j=1}^{d} \lambda(k) = \sum_{j=1}^{d} \lambda(k) + \sum_{j=1}^{d} \lambda(k) + \sum_{j=1}^{d} \lambda(k)
\]  

Comparing (4) and (5), since \( \sum_{j=1}^{d} \lambda(k) + \sum_{j=1}^{d} \lambda(k) + \sum_{j=1}^{d} \lambda(k) \), we have \( \Phi(M_l) < \Phi(M_p) \).

We perform the same operations on \( M_p \). Considering \( M_p \), if any two input signals in any two columns satisfy the inequation, \( M_p \) is equal to \( M_p \); otherwise, perform another exchange for new multiple scan chains \( M_p \), having \( \Phi(M_p) < \Phi(M_p) \), repeat by the same logic. Considering multiple scan chains \( M_p \), any two input signals \( s_{ij} \), \( s_{jk} \) in any two columns \( k_1 \) and \( k_2 \), \( \sum_{j=1}^{n} s_{ij} \cdot s_{jk} \) is satisfied. If \( k_1 \) is equal to \( k_2 \), the correlation \( \Phi(M_p) \) will not be affected after exchanging positions; otherwise, the correlation of the new multiple scan chains after exchanging positions must be equal or greater than \( \Phi(M_p) \). Thus the vector correlation of multiple scan chains \( M_p \) is the minimum. Simultaneously, correlation of vectors in new multiple scan chains decreases a positive integer after an exchange operation. Therefore, for any design with multiple scan chains architecture, the minimum correlation must be equal or greater than 0, i.e. multiple scan chains \( M_p \) will be transformed into \( M_p \) after finite times of exchange operations and \( M_p \) has the minimum correlation.

3. Multiple Scan Chains-Based Watermarking

3.1 Watermarking Principle

The test architecture of multiple scan chains has emerged for solving the test time problem in single scan chain [21]. Here, architecture of multiple scan chains with the minimum correlation is presented for better performance. The multiple scan chains \( M_p \) could be transformed into \( M_p \) with the minimum correlation \( \Phi(M_p) \) after exchange operations. Fig. 1 shows the test architecture of multiple scan chains. LFSR shifts test vectors in multiple scan chains for testing. By comparing with single scan chain, multiple scan chains architecture has the advantage of less test time and good resistance.
In the normal mode \((w_{\text{en}}=0)\), the circuit under test executes normal scan test and in the watermark mode \((w_{\text{en}}=1)\), a specific state shifted in ALC may cause 1, thus values of some cells in multiple scan chains will be reversed and then be output. The IP identification could be verified by comparing the output in normal mode and watermark mode for the same input vector.

### 3.2 Watermark Embedding

First of all, the signature, which can intuitively represent one’s identity, is encrypted and then hashed [22]. The generated digital digest is inserted into IP core as watermark. Hash function \(H\) is actually a transformation, using \(x\) as input, the returned value is called hash value, denoted by \(h\), i.e. \(h = H(x)\). Since hash is an oneway function, given a value \(h\), it is impossible to calculate \(x\) by using \(H(x) = h\).

Assume that, the signature is “hnulw…”, firstly, we transform it into ASCII code “110100011…”. The RSA algorithm is used for encryption, with the encrypted text denoted by \(W\). By using hash function \(H\), the digital digest \(M_{\text{sg}} = H(W)\) is generated, i.e. the watermark \(W_m\). After that, we generate a random sequence without repetition, represented by \(R_n = \{r_1, r_2, ..., r_n\}\). With the sequence, the watermark \(W_m\) will be grouped into a number of fragments, denoted by \(w_{\text{en}}, w_{\text{en}}, ..., w_{\text{en}}\). These fragments are mapped into a set of position constraints for watermark embedding.

![Watermark Embedding Diagram](image)

#### Figure 4. The generation of watermark fragments.

Suppose that the generated digital digest \(M_{\text{sg}} = 100110101...\), i.e. the watermark \(W_m\). The random sequence \(R_n = \{3, 2, 4\} \) is used to group watermark into fragments, the numbers in \(R_n\) represent the length of each watermark fragment \(w_{\text{en}} (i=1,2, ..., \lambda)\). As shown in Fig. 4, after grouping, the first three watermark fragments are \(w_{\text{en}} = 100, w_{\text{en}} = 11, w_{\text{en}} = 0101\), and the corresponding decimal numbers are respectively 4, 3, 6. This sequence represents the positions of the watermarked registers. The specific registers at these positions will be changed through watermark circuit for watermarking.

The following pseudo-code summarized the approach:

1. Read in netlist and desired signature \(S\);
2. \(W_s = \text{CHAR TO ASCII}(S)\);
3. \(W_{\text{en}} = \Psi(W_s)\);
4. \(W_m = H(W_{\text{en}})\), store \(W_m\);
5. Generating random sequence \(Rn(k) = \text{Random()}\), store \(Rn(k)\);
6. \(Rn(k): \text{Group } (W_m)\);
7. \(\text{for}(i=1; \text{group number } i<\text{number of watermark fragments } \lambda; i++)\)
8 \hspace{1em} \textit{Position}(i++) = \textit{BIT\_TO\_DEC}(W_m);
9 \hspace{1em} \text{store \textit{Position}(i);} \\
10 \}
11 \hspace{1em} \text{\textbf{\texttt{w_en}}=1, \text{watermark circuit is active;}} \\
12 \hspace{1em} \text{\textit{Position}(i):change specific registers;} \\
13 \hspace{1em} \text{Embedding watermark.}

Lines 1 to 4 preprocess the signature and generate the watermark. The watermark is stored and should be compared with the extracted watermark for copyright identification. Lines 5 and 6 generate a random sequence without repetition and use for grouping watermark into fragments. Lines 7 to 10 transform the watermark fragments into position information. This information is stored for watermark extraction. In line 11, the watermark circuit is active. Finally, line 12 and 13 are executed for watermark embedding.

3.3 Watermark Extraction

When the IP core is suspicious to be misappropriation, the author could apply to the third party for the verification of watermark by the following steps.

First of all, we read in the watermarked design and insert architecture of multiple scan chains. LFSR is used for the generation of test vectors. At present, \texttt{w_en}=1, the watermark circuit is active. The test vectors are shifted in multiple scan chains. The response vectors will be output through the combinational logic in the test circuit. Therefore, the watermarked responses \(R_m\) could be detected at the scan output. Then we set \texttt{w_en} signal as ‘0’, now the scan results become the original response \(R\) since the watermark circuit is not active. Accordingly, given a specific input vector, by comparing the response vector \(R\) and \(R_m\), respectively before and after watermark, the watermark positions will be found. After a series of transformations, the watermark fragments distributed in the whole design are found. Using the stored sequence \(R_m(k)\), the watermark fragments can be recombined as an extracted watermark \(W_m\). The IP identity could be verified by comparing \(W_m\) and \(W_m’\). This process is summarized as follows:

1 \hspace{1em} \text{Read in the watermarked design } D_w;
2 \hspace{1em} \text{LFSR: generate test vector } V;
3 \hspace{1em} V: R_m = \text{SCAN\_TEST}(V);
4 \hspace{1em} w_{en}=0;
5 \hspace{1em} V: R = \text{SCAN\_TEST}(V);
6 \hspace{1em} \text{\textit{Compare} } (R, R_m), \text{find the changed positions } \textit{Position'}(i);
7 \hspace{1em} \text{for} i=1; \text{group number } i; \text{number of watermark fragments } \lambda; \{i++\};
8 \hspace{1em} \text{extract watermark fragments;}
9 \hspace{1em} W_m’ = \text{DEC\_TO\_BIT} \textit{(Position}(i++)\};
10 \}
11 \hspace{1em} \text{\texttt{Rn}(k): } W_m’ = \text{Combinate} (W_m’); \\
12 \hspace{1em} \text{If } (W_m = W_m’) \text{ then successfully extract watermark;}
13 \hspace{1em} \text{Verify IP copyright.}

4. Experimental Results and Performance Analysis

The proposed scheme by watermarking multiple scan chains with the minimum correlation is implemented in VC on a 1.2 GHz Sun UltraSPARC-TI machine. The watermarking scheme is applied on sequential circuits from ISCAS’85, ISCAS’89 and ISCAS’99 [9] benchmark suites. The performance analysis of the proposed scheme will focus on resource overhead, resistance to attacks and comparison of experimental results.

4.1 Resource Overhead

It is critical to evaluate the resource overhead after watermarking. We select five circuits with the gate number over thousand for experiments. The zero delay models in [23] are used for resource evaluation, through which the transition times will be computed for reflecting the actual resource overhead. The experiment is conducted by the following steps:

1 \hspace{1em} \text{(1) Generate the pseudo random vectors by using LFSR and construct the optimal scan architecture with the minimum correlation, and then output the test vectors;} \\
2 \hspace{1em} \text{(2) load the test vectors in the circuit under test and record the transitions of internal nodes, and then calculate peak power and average power;} \\
3 \hspace{1em} \text{(3) partition the test point in sequential circuit according to the architecture of multiple scan chains;} \\
4 \hspace{1em} \text{(4) use LFSR for the generation of test vectors once again, and obtain the watermarked response vectors; calculate the peak power and average power after watermark by recording the transitions of internal nodes during test.}

As shown in Tab. 1, the cells number of combinational circuit and sequential circuit are shown in column 2 and 3 respectively. The columns, \(“P_w”\), \(“P_f”\) and \(“AK”\) are respectively the average power, peak power and the coverage rate of the test nodes. The experimental results in Tab. 1 show: the average power and peak power both reduce accordingly, while the coverage rate increases slightly. It proves that the proposed scheme has the advantages of lower resource overhead and higher coverage rate without affecting the normal circuit function.

4.2 Resistance to Attacks

In actual application, power attacks will be much more complicated than the attacks applied in benchmark circuits. Therefore, we evaluate the resistance of the proposed scheme to power attacks by resistance of the benchmark to transient power attacks. The evaluation model of resistance to transient power attacks proposed in [8], is used for computing the time for attackers to successfully attack and resource overhead. In this way, the resistance of the watermark to power attacks can be effectively evaluated.
The robustness of the proposed IP watermarking scheme is generally evaluated by the probability of coincidence $P_c$. Basically, $P_c$ represents the probability of a non-watermarked design carrying the legitimate watermark. Let $\lambda$ be the watermark fragments for embedding. The probability of $\lambda$ cells being randomly selected from $n$ scan cells is $\frac{1}{C^*_n}$. Suppose that the selected cells have equal number of “0” and “1”. $P_{01}$ and $P_{10}$ respectively represent the probability of “0” to “1” and that of “1” to “0”, we have $P_{01} = P_{10} \approx 0.5$. Thus the probability of coincidence $P_c$ is shown as

$$P_c = \frac{1}{C^*_n} (p_{01})^{\frac{n}{2}} (p_{10})^{\frac{n}{2}} = \frac{1}{2^n C^*_n}. \quad (6)$$

To have a strong proof of IP identity, the probability must be convincingly low.

The architecture of multiple scan chains $M_p$ with the minimum correlation is constructed on the basis of $M_0$. The proposed scheme embeds 32 bits and 128 bits watermark into the optimal architecture. Then, we conduct 1000 random attacks on the watermarked benchmark circuits.

If the attackers attempt to remove the watermark and add their own test circuits, they need to modify the logic circuit and replace part of functional logic. The difficulty may be basically equal to redesign. Five larger circuits in the benchmark suites are selected for experiment. The $P_c$ change rate after embedding watermark, 32bits and 128bits respectively, are shown in Fig. 5. The experimental results show that the number of chains is increasing with the complexity of the test circuits, while $P_c$ presents a downtrend. The decline of $P_c$ change rate in (b) is slower than that in (a), which precisely proves that embedding watermark with larger size in complicated circuit has strong resistance to attacks.

<table>
<thead>
<tr>
<th>Circuit</th>
<th>Combinational Logic N</th>
<th>Sequential Logic C</th>
<th>Original Circuit</th>
<th>Watermarked Circuit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>$P_e$ $P_f$ $\Delta K$ (%)</td>
<td>$P_e$ $P_f$ $\Delta K$ (%)</td>
</tr>
<tr>
<td>S5378</td>
<td>2779</td>
<td>179</td>
<td>3797 1968 84.56</td>
<td>3461 1876 90.11</td>
</tr>
<tr>
<td>S9234</td>
<td>5597</td>
<td>211</td>
<td>6785 3622 90.12</td>
<td>6123 3601 98.54</td>
</tr>
<tr>
<td>S13207</td>
<td>7952</td>
<td>669</td>
<td>10908 6471 82.16</td>
<td>9875 5947 88.34</td>
</tr>
<tr>
<td>S35932</td>
<td>16066</td>
<td>1728</td>
<td>41235 19677 89.64</td>
<td>32471 17983 91.44</td>
</tr>
<tr>
<td>S38584</td>
<td>19354</td>
<td>1546</td>
<td>20657 14906 92.82</td>
<td>18195 12876 96.01</td>
</tr>
</tbody>
</table>

Tab. 1. The performance comparison of the original and watermarked circuit

4.3 Comparison of Experimental Results

The experiments are conducted on the multiple scan chains with the minimum correlation. The comparison of the proposed scheme with methods in [9] and [15] are shown in Tab. 2.

Assume that, $\Phi(M_p)$ is the minimum correlation, $P_e$ denotes the probability of coincidence and $\Delta S$ represents the coverage rate of watermark detection. Tab. 2 shows that the proposed scheme has lower $P_e$ than other methods, which verify the stronger resistance of our scheme to attacks. The coverage rate of watermark detection $\Delta S$ is larger. Since the architecture of multiple scan chains we use in the scheme, the watermark has become more observable and testable. Therefore, the proposed scheme has lower probability of coincidence $P_e$ and better coverage rate of watermark detection.
Proposed \([15]\) \([9]\)

<table>
<thead>
<tr>
<th>Circuit</th>
<th>(\Phi(M_p))</th>
<th>(P_c)</th>
<th>(\Delta S) (%)</th>
<th>(P_c)</th>
<th>(\Delta S) (%)</th>
<th>(P_c)</th>
<th>(\Delta S) (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>i7</td>
<td>18</td>
<td>2.17E-21</td>
<td>91.02</td>
<td>2.91E-21</td>
<td>86.49</td>
<td>7.52E-20</td>
<td>90.23</td>
</tr>
<tr>
<td>i9</td>
<td>19</td>
<td>1.02E-14</td>
<td>90.62</td>
<td>3.49E-14</td>
<td>85.07</td>
<td>1.05E-13</td>
<td>88.48</td>
</tr>
<tr>
<td>i2</td>
<td>22</td>
<td>1.91E-23</td>
<td>97.83</td>
<td>6.38E-23</td>
<td>83.24</td>
<td>2.64E-19</td>
<td>79.41</td>
</tr>
<tr>
<td>i8</td>
<td>15</td>
<td>5.77e-32</td>
<td>94.27</td>
<td>1.67E-32</td>
<td>88.36</td>
<td>2.60E-31</td>
<td>91.86</td>
</tr>
<tr>
<td>frg2</td>
<td>14</td>
<td>1.23E-19</td>
<td>92.06</td>
<td>6.02E-18</td>
<td>91.68</td>
<td>1.91E-19</td>
<td>70.77</td>
</tr>
<tr>
<td>alu4</td>
<td>25</td>
<td>1.93E-41</td>
<td>94.82</td>
<td>7.14E-34</td>
<td>79.91</td>
<td>1.70E-39</td>
<td>86.09</td>
</tr>
<tr>
<td>apex6</td>
<td>20</td>
<td>5.77E-33</td>
<td>99.15</td>
<td>3.06E-24</td>
<td>95.28</td>
<td>8.16E-31</td>
<td>93.62</td>
</tr>
<tr>
<td>rot</td>
<td>20</td>
<td>4.98E-26</td>
<td>100.00</td>
<td>8.75E-25</td>
<td>94.76</td>
<td>1.41E-21</td>
<td>87.71</td>
</tr>
<tr>
<td>x3</td>
<td>18</td>
<td>4.66E-36</td>
<td>95.37</td>
<td>8.08E-25</td>
<td>89.41</td>
<td>6.28E-35</td>
<td>71.44</td>
</tr>
<tr>
<td>k2</td>
<td>33</td>
<td>2.42E-32</td>
<td>96.53</td>
<td>3.24E-32</td>
<td>92.09</td>
<td>8.64E-32</td>
<td>83.57</td>
</tr>
</tbody>
</table>

Tab. 2. Comparison of watermarking methods.

5. Conclusions

A novel DFT watermarking scheme is proposed based on sequential circuit for IP protection. The scheme has solved the problems of large overhead, low resistance to attacks and coverage rate of watermark detection in previous DFT watermarking methods. The test vectors generated by LFSR are shifted in scan input for the construction of multiple scan chains with minimum correlation. A watermark logic circuit is designed to change specific registers in multiple scan chains for watermarking the design. The watermark can be effectively detected without interference with normal function of the circuit, even after the chip is packaged. The experimental results show that the proposed scheme has lower resource overhead, probability of coincidence \(P_c\) and higher coverage rate of watermark detection by comparing with the existing methods. We will study on DFT watermarking techniques on the basis of scan tree and scan forest in the future.

Acknowledgments

This work is supported by National Basic Research Program of China (973 Program, Grant Nos. 2009CB326202, 2010CB334706), Key Program of National Natural Science Foundation of China (Grant No. 60736016), National Natural Science Foundation of China (Grant Nos.60973128, 61073191, 61070196 and 60973113) and PAPD, Scientific Research Fund of Hunan Provincial Education Department (Grant No.09C403), Natural Science Foundation of Xiangtan United Fund of Hunan Province (Grant No. 09JJ9006).

References


About Authors...

Wei LIANG was born in 1978. He received his BS in Automation from the Central South University, China, in 2003, MS in Computer Science and Technology from Hunan University of Science and Technology, China, in 2008, and he is currently pursuing his PhD in Computer Science and Technology from Hunan University, China. His current research interests include steganography, steganalysis, real-time embedded systems, intellectual property protection, and field programmable gate arrays.

Xingming SUN (Corresponding author) received his BS in Mathematics from Hunan Normal University, China, in 1984, MS in Computing Science from Dalian University of Science and Technology, China, in 1988, and PhD in Computer Science from Fudan University, China, in 2001. He is currently a professor in the School of Computer and Communication, Hunan University, China. His research interests include network and information security, digital watermarking, digital forensic, database security, and intellectual property protection.

Zhiqiang RUAN was born in 1982. Since 2009, he has been a Ph. D. candidate in Computer Science from Hunan University. His current main research interests include security in wireless sensor networks, intellectual property protection and field programmable gate arrays.

Jing LONG received her BE in Hunan University of Science and Technology, China, in 2009, and is currently pursuing her M.S. in Computer Application at the School of Computer Science and Engineering of Hunan University of Science and Technology, China. Her research interests include real-time embedded systems, intellectual property protection, field programmable gate arrays, wireless sensor networks.

Chengtao WU received his BE in Hunan University of Science and Technology, China, in 2010, and is currently pursuing his M.S. in Computer Science and Technology at the School of Computer and Communication of Hunan University, China. His research interests include information security, intellectual property protection, field programmable gate arrays.