Computer Science and Information Systems 12(2):823–841 DOI: 10.2298/CSIS141017028L

TDCM: An IP Watermarking Algorithm based on Two Dimensional Chaotic Mapping

Wei Liang[1], Keshou Wu[1],Yong Xie[1] and Jiajun Duan[2]

[1] College of Software Engineering, Xiamen University of Technology,
361024, Xiamen, China
{Wliang, kswu, yongxie}@xmut.edu.cn
[2] Department of Electrical and Computer Engineering, Lehigh University,
18015, Bethlehem, USA
jid213@lehigh.edu

Abstract. With the rapid development of VLSI (Very Large Scale Integration) circuit, IP (Intellectual Property) protection for reused technology is widely concerned. A watermarking scheme for IP protection is proposed on basis of a two dimensional chaotic mapping model (TDCM). The scheme utilizes a secure and controllable embedding model to compute the aggregation level of physical resource positions and the secure threshold of controllability. A two dimensional chaotic sequence is generated with the control of secure threshold. The first dimensional sequence is used to determine random watermark positions and the second dimensional sequence is to control watermark number in each position. Finally, the watermarks are inserted into corresponding places orderly. The experiments show that the proposed scheme has low resource overhead by comparing with other schemes. The resistance to attacks and robustness of the watermark are encouraging as well.

Keywords: IP watermarking, controllable secure threshold, two dimensional chaotic mapping, Robust.

1. Introduction

The rapid advance of LSIC (Large Scale Integrated Circuits) makes it popular to integrate complex system into a single chip, called SoC (System on Chip). Since SoC is highly integrated, traditional design technique cannot meet the design requirements. Therefore, FPGA (Field Programmable Gate Array) becomes a mainstream for SoC implementation because it can improve the inflexibility of custom circuits and the problems of insufficient gates of original programmable device [1], [2], [3], [4]. FPGA is an evolutionary product of PAL (Programmable Array Logic), GAL (Generic Array Logic), etc. It is a semi-custom circuit in specific integrated circuit. The program design of IP circuit is implemented by hardware language. In implementation of SoC, the security of IP circuit is also widely concerned. So far, research on watermarking schemes for IP protection has gotten some achievements. For instance, literature [5], [6], [7] makes a comprehensive conclusion and analysis of developments and challenges in IP watermarking technologies in recent years.

In order to solve security problem of FPGA based IP design, J. Lach's team [8] firstly proposed the concept of FPGA IP watermark and utilized unused LUTs (Lookup Tables) in FPGA for watermark insertion [9], [10], [11], [12], [13], [14], [15], [16]. The basic flow of the proposed algorithms is shown in Fig. 1, each CLB module in the figure can be set as distributed RAM configuration as well as distributed ROM configuration. The data initialization of distributed ROM configuration is realized by setting corresponding parameters. The most important of CLB is the 4 input function generation LUT. It is eventually used to achieve certain logic function. The data flow information of the matched storage is able to be modified without impacting the performance of IP core when LUT is free and the safety insertion of IP core watermark information is achieved.

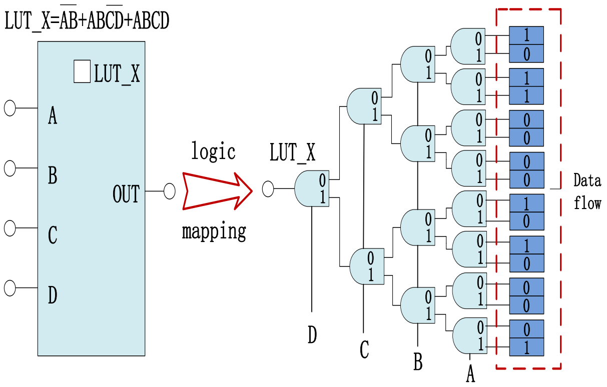


Fig. 1. The internal logical structure of LUT

In last decade, highly integrated circuits make IP reuse technology be popular since it greatly cuts the cycle of IP design. In company with the popular utilization of IP reuse technology, the reused IP is easily to cause disputes on ownership. Meanwhile, chaos theory is introduced in IP watermarking scheme for its good performance on security. For example, literatures [17], [18] employed logistic mapping to generate a sequence as watermark. Furthermore, the chaotic mapping can be used to scramble image space and the watermarks are then inserted. For its effectiveness on digital watermark, chaotic mapping is widely used in recent IP watermarking schemes [19].

In existing IP watermarking schemes based on one dimensional chaotic mapping [20], the ability against attacks and robustness are needed to be improved. For this purpose, a two dimensional chaotic mapping based watermark embedding model and corresponding embedding scheme are proposed. Firstly, the scheme utilizes a secure and controllable embedding model to compute the aggregation level of physical resource positions and the controllable secure threshold. A two dimensional chaotic sequence is generated with the control of secure thresholds. The first dimensional sequence is used to determine random watermark positions and the second dimensional sequence is to control watermark number in each position. Finally, the watermarks are inserted into corresponding places orderly. By comparing with other schemes, the system has higher rate of resource utilization after watermark insertion. The system has good ability against reverse analysis attacks and noise attacks. It will provide a secure and effective watermarking method for IP protection.

2. TPCM mathematical models

The model is designed for security of random watermark insertion. The watermark positions may be easily to be determined once the illegal user utilizes resource discreteness analysis. It will bring great threat to security of the watermarked system. Consequently, we design a secure embedding model based on two dimensional chaotic mapping. The model makes the watermarked resources combine with original design resource which achieves better security.

Definition 1: Assume that all CLBs (Configurable Logic Blocks) in FPGA are formed into an array with the size of $\mathrm{m}*n$. The coordinates of all CLBs are established. The CLB at coordinate (i, j) is denoted by C_k , $0 \le k \le m*n-1, k = i*m + j$. All of the CLBs will be classified according to the criterion whether C_k is used. The resources are divided into two parts, used resource sequence C_u and unused resource sequence C_n .

$$\mathrm{C}u = \{u_0, u_1, ..., u_{p-1}\} \tag{1}$$

$$\mathrm{Cn} = \{n_0, n_1, ..., n_{q-1}\} \tag{2}$$

Definition 2: The used resources in FPGA has a standard aggregation level p_0 . The average distance of any cell u_k , $(0 \le k \le p-1)$ in used resource sequence C_u and other cells is denoted as:

$$\overline{ud_k} = \frac{1}{p}\sum_{j=0}^{p-1} D(u_k, u_j) \tag{3}$$

Since the average distance from a single resource u_k cannot represent the global property of C_u. In this case, the average distance will be extended to all resources in C_u. The standard aggregation level p_0 is defined as the average distance of the average distances between all resources in C_u to other resources in C_u. The expression is stated as follows:

$$p_0 = \frac{1}{p+1}\sum_{j=0}^{p-1} \overline{ud_i} \tag{4}$$

The wave range of $\overline{Ud_i}$ is denoted by Δp :

$$\Delta p = \sqrt{\frac{1}{p+1}\sum_{j=0}^{p-1}(\overline{ud_j} - p_0)^2} \tag{5}$$

In definition 2, the aggregation level of used resources in IP design is represented by p_0. Before watermark insertion, we need to know not only the aggregation level of original IP design, but also the watermarked positions with the best security and reliability. In theory, if the values of standard aggregation level p_0 of watermarked IP and original IP are similar, the watermark has high security and strong ability against attacks. But generally, watermark insertion will affect the value of standard aggregation level p_0. Consequently, we introduce the concept of controllable secure threshold in definition 3.

Definition 3: Controllable secure threshold P is an accepted variation rage of aggregation level of used resources after watermark insertion.

$$\cdot\{p | p_0 - \Delta p \le p \le p_0 + \Delta p\} \tag{6}$$

The controllable secure threshold P represents aggregation level of used resources in FPGA and their variation rage. The threshold can be used to constrain the aggregation level of used resources into the minimum. In this case, the watermarks will be elusive and robust.

(1) Firstly, the FPGA design T is prepared. The watermarks are ordered as sequence $R = \{t_0, t_1, t_2, \cdots, t_{n-1}\}$. n is the number of elements in watermark sequence R.

(2) The controllable secure threshold p of T is calculated with definition 2. p will be used to constrain watermark positions. It also control the effect on aggregation level after watermark insertion with the standard aggregation level P_0 and variation range Δp.

(3) The location sequence is selected with the constraint, denoted by $L = \{I_0, I_1, I_2, \cdots, I_{n-1}\}$. Each element I_i in sequence L is chosen to embed watermark with the random position allocation algorithm and secure watermark embedding model. The selection procedure of I_i is as follows:

a) Select the resource I_i $\{0 \le i \le n-1\}$ according to original watermark embedding algorithm.

b) Supposing to add the resource I_i into used resource sequence C_u. I_i will be the $p+1^{\text{th}}$ element of C_u .

c) The value of $\overline{Ud_i}$ can be calculated with expression (5), denoted by p_0. It is the average distance between I_i and the used resources in IP design T .

d) Judge to determine whether the calculated p_w in c) satisfies the controllable secure threshold p in definition 3.

$$p_0 - \Delta p \le p_w \le p_0 + \Delta p \tag{7}$$

(4) Generation of watermark positions

The prepared watermark sequence $R = \{t_0, t_1, t_2, \cdots, t_{n-1}\}$ in step (1) is orderly inserted into the positions in sequence. $L = \{I_0, I_1, I_2, \cdots, I_{n-1}\}$ The watermarked FPGA design is generated, denoted by T_{mark} .

2.1. Two Dimensional Chaotic Mapping Model

Chaos system is a nonlinear dynamical system sensitive to the initial value. For its good randomness, chaos system is widely applied in information security. The Lyapunov exponent is used to describe the nonlinear feature of chaotic map [21], [22], [23]. The number of Lyapunov exponent is consistent with the dimension of system. The system with one Lyapunov exponent great than zero can be called as chaotic system and with more than two Lyapunov exponent great than zero can be called as hyper chaotic system. It is of significance that Lyapunov exponent can describe the instability of chaotic system accurately. Large Lyapunov exponent represents the system is more instable. In this case, the feature of chaotic system is close to random.

The model utilizes the randomness of chaotic system and embeds watermarks into IP circuit in a secure way. The illegal user is hard to analyze the ownership information by analysis attacks.

Definition 4: Two dimensional chaotic mapping can be denoted by two dimensional nonlinear equations. The expressions are as follows:

$$\begin{cases} x_{n+1} = f_1(x_n, y_n) \\ y_{n+1} = f_2(x_n, y_n) \end{cases} \tag{8}$$

$f_1(x_n, y_n)$, $f_2(x_n, y_n)$ can be represented by the following expressions.

$$\begin{cases} f_1(x_n, y_n) = a_1 + a_2 x_n + a_3 x_n^2 + a_4 y_n + a_5 y_n^2 + a_6 x_n y_n \\ f_2(x_n, y_n) = a_7 + a_8 x_n + a_9 x_n^2 + a_{10} y_n + a_{11} y_n^2 + a_{12} x_n y_n \end{cases} \tag{9}$$

The coefficient a_i $(i = 1,2,3,...,12)$ in (10) is constant. a_i is a key factor to determine Lyapunov exponent in two dimensional chaotic system. In this case, the selection of a_i has direct influence on stability of chaotic system. Since two dimensional chaos has more complex timing sequence by comparing with one dimensional chaos. It will lead to the time increase of chaotic mapping and affect the requirement of real time. In this paper, we select a group of coefficients a_i in literature [18] to achieve a two dimensional chaotic system. The procedure shows as follows:

(1) Select a system with large Lyapunov exponent (denotes the system is the most instable) as the chaotic mapping function for watermark insertion, that is:

$$\begin{cases} x_{n+1} = a_2 x_n + a_4 y_n \\ y_{n+1} = a_7 + a_9 x_n + a_{10} y_n \end{cases} \qquad (\mathbf{20})$$

Here, $a_2 = -0.95$, $a_4 = 1.55$, $a_7 = -0.45$, $a_9 = 2.4$ and $a_{10} = 1.05$.

(2) Determine a pair of keys as the initial key of the two dimensional chaotic system. The two dimensional chaotic sequence $w = \{w_0, w_1, ...w_{n-1}\}$ is calculated with the expression in (10). Here, *n* is large enough. Each element in *W* consists of x_i and y_i, that is $w = (x_i, y_i)$, $0 \le i \le n-1$.

(3) Assume that the binary sequence of watermark is denoted by $R = \{r_0, r_1, ...r_{L_{mark}-1}\}$ with the length of L_{mark}. The element in generated sequence W is meaningless real number. So it should be first transformed into integrated number. The element W_i is transformed into binary number {0,1}. Then the binary chaotic sequence is divided by m. Each group with m bits will be further transformed into decimal number. After all transformation, a decimal sequence $Z = \{z_0, z_1, z_2, ...z_{p-1}\}$ is generated and each element $z_i = (\alpha_i, \beta_i)$ ($0 \le i \le p-1$). α_i and β_i are decimal number, satisfying $L_{mark} = \sum_{i=0}^{p-1} \beta_i$. The sequence Z can be classified into two sequences with different dimension, $\alpha = \{\alpha_0, \alpha_1, \alpha_2, ...\alpha_{p-1}\}$ and $\beta = \{\beta_0, \beta_1, \beta_2, ...\beta_{p-1}\}$ respectively. α is used to control watermark embedding positions and β is a constraint to limit watermark length in each position.

(4) According to the length of sequence Z and β_i in z_i, the watermark sequence R is grouped and the grouped sequence is obtained. The bit number of each element $g_i(0,1,2,..., p-1)$ is consistent with that of β_i in z_i.

(5) The elements in grouped sequence $G = \{g_0, g_1, g_2, ...g_{p-1}\}$ will be orderly inserted into original IP design with the position constraint $\{\alpha_0, \alpha_1, \alpha_2, ...\alpha_{p-1}\}$ in sequence $Z = \{z_0, z_1, z_2, ...z_{p-1}\}$.

3. Robust IP Watermarking Algorithm based on Two Dimensional

The two dimensional chaotic mapping is employed to achieve better security. Definition 3 gives the definition of controllable secure threshold. It is used as a constraint for the selection of watermark positions. An IP watermarking algorithm based on two dimensional chaotic mapping is proposed. Finally, the watermark embedding and extraction are performed on basis of the proposed algorithm.

As secret key is employed to control the position where IP watermark information is embedded in real time, design of its sequence directly determines the concealment of watermark position. In the process of secret key generation discussed in this paper, we consider the following scenario: It may easily attract the attention of an adversary and increase the chances of exposure to attacks if the generated secret key is not dispersedly distributed and instead positioned closely to the original watermark. Therefore, it is an essential aspect of robustness of watermark methods to devise an effective security strategy that distribute generated secret key as dispersedly and far away from the original watermark as possible. As depicted in Figure 2, we introduce our secret key generation algorithm from three perspectives that guarantees secure use of secret key, including resource searching, resource recording, as well as secret key generation.

(1) Resource searching. All CLB matrices used in FPGA design are read as an entirety. Then, LUT resources inside CLB matrices are scanned using probes. Based on architectural characteristics of FPGA devices, CLB matrices can be traversed in a zig-zag fashion to ensure every single LUT is visited.

(2) Resource recording. In parallel to resource searching, each CLB matrix is accompanied with a two-dimensional matrix which keep track of the utilization of LUT, using 0 to mark free LUTs and 1 to mark used ones.

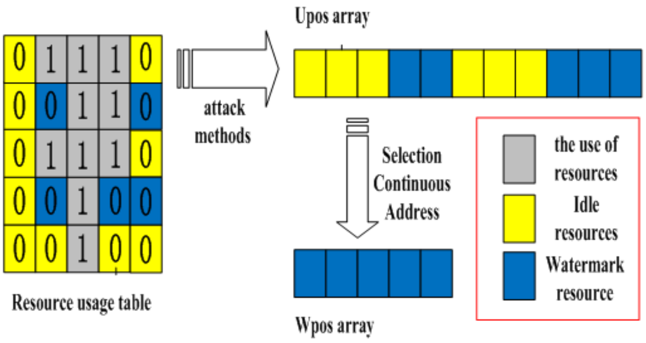


Fig. 2. Schematic diagram of the structure of the key generation

(3) Secret key generation. As illustrated in Figure 2, we need to first use a random number generator to select addresses in the linear list if we want to reconstruct an Upos with linear list structure based on the resource utilization information provided by the resource recorder. As such a linear list only keeps positions of free LUTs, we will be able to guarantee with high probability that information recorded in these position greatly resembles that in the original design, which leads to a set of addresses with two-

dimensional chaotic mappings. Finally, we will be able to save selected address information Wpos into bit-files.

3.1. Watermark Embedding

The embedding algorithm utilizes the feature of LUT in FPGA. The controllable secure model is proposed to constrain the watermark positions. In this paper, DES encryption algorithm is introduced to encrypt watermark information. The encrypted information is further hashed. Since hash is irreversible, watermark extraction can only verify whether the watermark exists. The original watermark information cannot be recovered from watermarked IP design T_{mark}. The algorithm shows as Fig. 3:

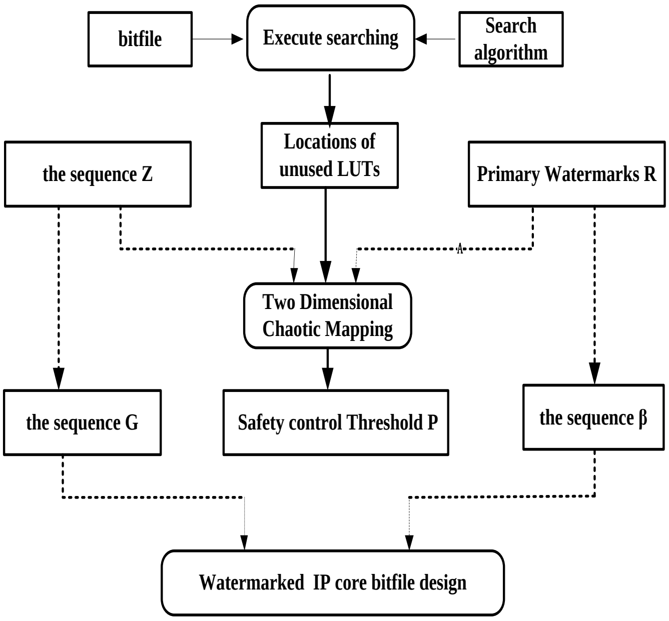


Fig.3. The flow of watermark embedding

Step 1: Preprocess watermark information. The original watermark information S is preprocessed to get sequence R. This procedure is divided into two parts. Firstly, the watermark information S is encrypted by DES algorithm. After that, the cipher text is hashed and the message is regarded as watermark. The binary sequence of watermark is denoted by $R=\{r_0, r_1, ...r_{L_{mark}-1}\}$. $r_i(i=0,1,2,...,L_{mark}-1)$ is the i^{th} bit value L_{mark} , T_{mark} represents the length of watermark bits.

Step 2: Compute controllable secure threshold P. The protected IP design is T. The controllable secure threshold P in definition 3 can be calculated with definitions 1 and 2.

Step 3: Select initial key key and generate two dimensional chaotic sequence Z. The key is used as the initial key of two dimensional chaotic system. With the controllable secure threshold P and requirement in definition 3,a chaotic sequence Z satisfying the requirement is selected. Z consists of α and β ,respectively for controlling watermark positions and watermark bits. Since the generation of Z is limited by the secure threshold P , a part of sequence that cannot satisfy the requirement is removed. The removed items are written in mapping log file for recovery of Z in watermark extraction.

Step 4: The watermark sequence $R=\{r_0,r_1,..,r_{L_{mark}-1}\}$ is divided and transformed into sequence $G=\{g_0,g_1,g_2,..g_{p-1}\}$ with the sequence $\beta=\{\beta_0,\beta_1,\beta_2,...,\beta_{p-1}\}$. The bit number of each element is consistent with the length of $\beta_i(0,1,2,...,p-1)$.

Step 5: All elements in sequence $G=\{g_0,g_1,g_2,..g_{p-1}\}$ are orderly inserted into positions in sequence $\alpha=\{\alpha_{0,}\alpha_1,\alpha_2,...,\alpha_{p-1}\}$ .The watermarked FPGA design is generated and denoted by T_{mark} .

3.2. Watermark Extraction

When the IP ownership is suspected to be infringed, the IP owner can extract and verify the watermarks in the design for ownership proof. The procedure is stated as follows.

Step 1: With the initial key key of two dimensional chaotic mapping and the mapping log file, the chaotic sequence Z can be recovered.

Step 2: The grouped sequence G is extracted in design T_{mark} by using the positions controlling sequence $\alpha=\{\alpha_{0,}\alpha_1,\alpha_2,...,\alpha_{p-1}\}$. Then, the watermark sequence R can be recovered according to sequence $\beta=\{\beta_0,\beta_1,\beta_2,...,\beta_{p-1}\}$.

Step 3: According to the procedure in step 1 of watermark embedding, the original watermark information S is preprocessed to get sequence R.

Step 4: The generated sequence R in step 3 is compared with that in step 2. If they are equal, the ownership verification is successful; otherwise, it is failure.

4. Experiments and Analysis

In this section, we will evaluate and analyze the proposed watermarking algorithm in terms of resource overhead, robustness and ability against attacks.

4.1. Resource Overhead Analysis

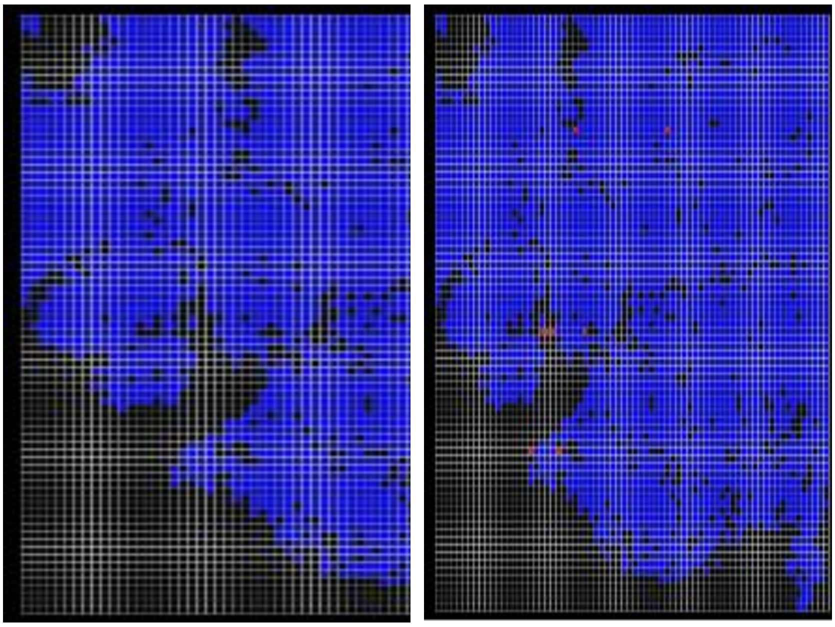
In watermark embedding procedure, original watermark information is encrypted by DES algorithm and then hashed. The data can be compressed by using Hash algorithm. Consequently, despite the length of original watermark, the hashed result is 128bit constantly. The resource overhead will not increase when the length of watermark bits is great than 128. The watermark volume is improved. With the proposed algorithm, the length of watermark bits is unlimited.

Table 1. IP watermarking performance indexes in resource utilization and growth

IP core	Model	The length of watermark	Before embedding			After embedding the watermark			Growth rate
			Δ L	L-Num	Δ L (%)	Δ L	L-Num	Δ L (%)	Δ S (%)
DES	XC2V1000	32 bits	3376	10238	32.98	3367	10240	33.04	0.266
STROM	XC2V1500	64 bits	7308	15357	47.32	7382	15360	47.68	0.272
CACHE	XC2V2000	128 bits	13234	21521	61.46	13236	21504	61.57	0.305
RS	XC2V4000	256 bits	25956	46089	56.38	26024	46080	56.44	0.304

Table1 records some performance indexes in resource utilization and growth. ΔL is the total number of utilized LUTs. *L-Num* represents the total number of LUTs in FPGA device. $\Delta L(\%)$ denotes the rate of utilized LUTs and $\Delta S(\%)$ is the growth rate of utilized resource after watermark insertion. The growth rate of utilized resource is constantly close to 0.3% after embedding watermark, which satisfies the requirements resource overhead. Since the proposed algorithm utilizes unused LUTs for watermark insertion, the watermark will lead to increase of resource overhead. However, the watermarked resources will not be accessed when the system is running. Therefore, the power overhead will not increase. The experiments show that the proposed algorithm has good performance on resource overhead and power consumption.

To evaluate the features of low overhead and high watermark volume, we analyze the resource distribution in original design and watermarked design. Xilinx Virtex II XC2V2000 FPGA device is used in experiments. The RS IP core is selected as the target IP design. Fig. 4(a)(b) shows the resource distribution. The proposed model can improve the number of embedded watermark bits. The rate of resource utilization can be also calculated. Meanwhile, we analyze the resource variation and the resource aggregation is better.



(a) Resource distribution of original RS IP design

(b)Resource distribution of watermarked RS IP design

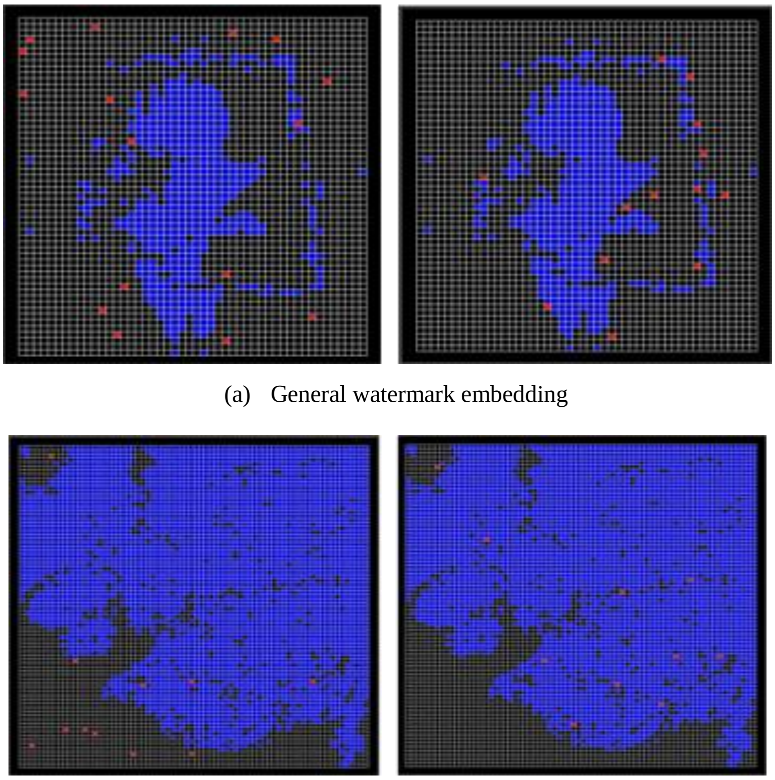
Fig.4. Resource distribution of RS IP designs

4.2. Robustness

In section 2, a concept of standard aggregation level p_0 of utilized resources in design is proposed and controllable secure threshold p is also defined. p is used as constraint to limit the watermarks around the functional resources. In this way, the watermarks are hard to be removed and destroyed. So the robustness is strengthened. Furthermore, the use of two dimensional chaotic mapping has good effects to improve watermark randomness and security.

To evaluate the practical effect of the proposed secure model, we conduct experiments on watermark robustness. Two types of FPGA device are selected, respectively XC2V2000 and XC2V4000. The target IP cores [24] are aes_dec and rs_dec4. We insert the original watermark information “Test IPMark” into IP designs with two watermark embedding algorithm. With the performance testing module in platform implemented by VC language, the resource distributions in original design and watermarked design are compared, as shown in Fig. 5(a)(b).

In Fig. 5(a), the blue area represents the utilized resources in original design and red points are watermarked resources. The scheme in literature [25] is a random insertion. The watermarked positions are uncontrollable and random and may appear in any places. The standard aggregation level p_0 after embedding watermark differs with that of the original design. It will bring great threat to watermark security and robustness. Consequently, In Fig. 5(b), we propose a secure watermark embedding model to guarantee better security and robustness.



(a) General watermark embedding

(b) Watermark embedding under control of p

Fig.5. The resource distribution of rs_dec4 (XC2V4000)

4.3. Security Analysis

The security of IP core mainly reflects the ability of watermark withstanding the malicious tamper or attacks. The normal attack methods include removal attack, physical attack, forgery attack and collusion attack etc. The removal attack removes the watermark directly by certain means. For the brute force attack, it searches the inserted secret information by force. The forgery attack inserts the illegal watermark to IP core which should not exist originally. The passive aggression represents that the attacker who is able to detect the watermark and recognize every mark, but fails to decipher the mark code. The security and performance analysis of proposed algorithm in this paper is conducted under the illegal removal attack and noise attack modes [25], [26], [27].

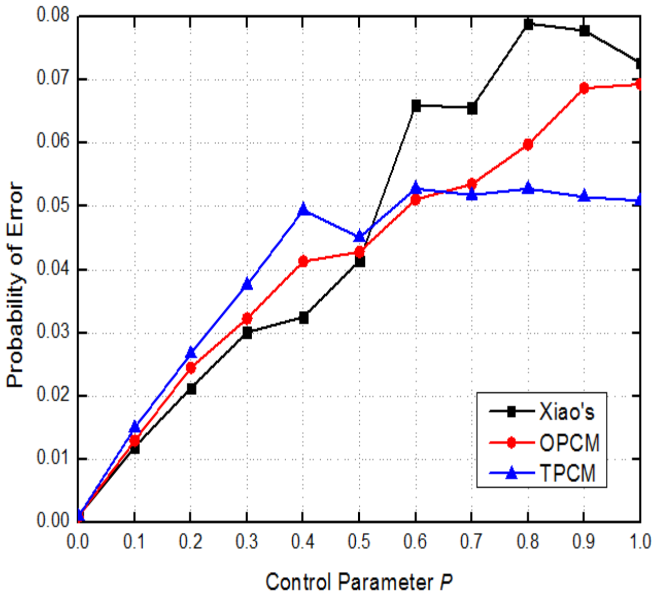
Ability against Reverse Analysis Attacks. In the proposed two dimensional chaotic mapping based IP watermarking scheme, the watermarks insertion can be implemented by configuration of logic function. It is difficult for illegal attackers to get logic function in programmable logic circuit by reverse analysis attacks. To perform reverse analysis attacks, they should firstly obtain all configuration data of FPGA design. There are two ways to get configuration data generally. One is to steal the bit stream and another one is to read configuration data in RAM by using micro-probe.

With the way of stealing bit stream, attackers need to import the programmable data in every time of system booting. The way makes it possible to analyze circuit function from bit stream. In our proposed scheme, a stabilized power is used to keep the information in storage nonvolatile. The configuration data is no need to be imported again in system booting. In this case, the attackers cannot steal the bit stream of IP circuit.

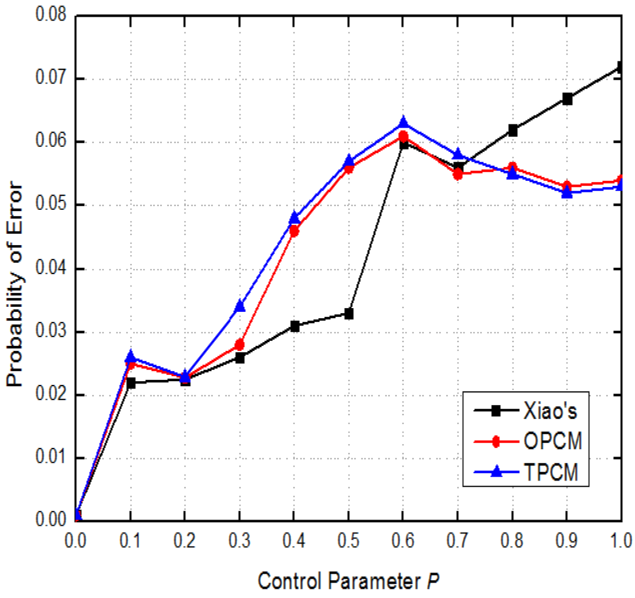
Besides the way of stealing bit stream, attackers may use micro-probe to read configuration information in RAM. Therefore, the RAM units and the output signal in our scheme are set at the low level of chip. The attackers cannot probe related configuration logic by micro-probe. Consequently, IP circuits with our proposed watermark scheme has good ability against reverse analysis through stealing bit stream, especially reverse analysis on layout.

The noises in above experiments are Gaussian noise. In following experiments, we focus on noise attacks of GGD type and MSS type. The noise intensity is denoted by P, $0<P<1$. Fig. 6(c) compares the proposed scheme with the method based on one dimensional chaotic mapping (ODCM).The experimental results in Fig. 6(c) show that the performance of ODCM against GGD noise attack is low with the increase of P. The reason is that the position aggregation parameter becomes small after suffering GGD noise attacks when P increases. In this case, the error probability of IP circuit increases correspondingly. In Fig. 6(d), when P becomes larger, our scheme has better ability against MSS noise attack by comparing with that in literature [30].

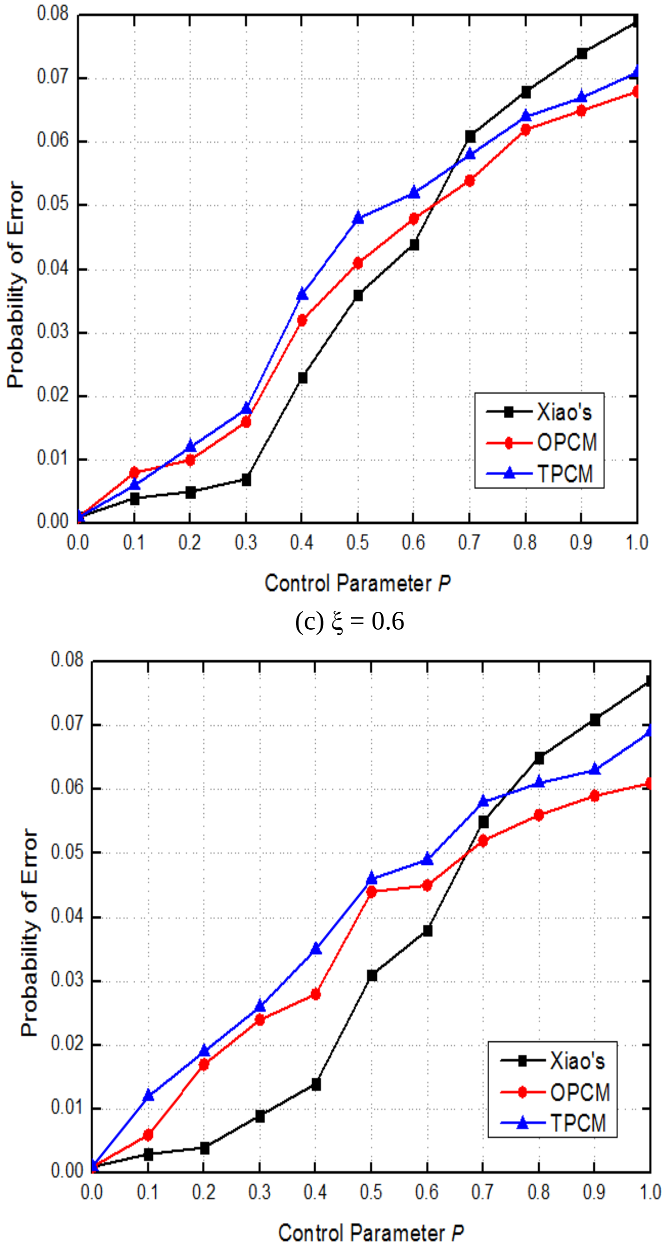
Noise Attacks. If the signals of the watermarked circuits with our scheme are not in Gaussial distribution, Where ξ denotes the optimal threshold for attack of noises. Using optimization methods in [28] which gives ξ values of 0.2, 0.4, 0.6, 0.8, we are able to compare the performance of various algorithms in terms of resistance to noise attack. The performance after suffering noise attacks can be obtained by using numerical method. Fig.6 (a) shows a comparison of OPCM [29] and TDCM scheme with that in literature [30]. With $P<0.6$ and low noise intensity, the security of two schemes are better than that in Xiao’s [30]. Fig.6 (b) shows the ability against noise attacks of our proposed two schemes are better than the method based on one dimensional chaotic mapping when $P>0.9$. In contrast, the proposed method based on two-dimensional chaotic mappings are superior to previously proposed approaches in terms of resistance against noise attack.


Probability of Error
0.00
0.01
0.02
0.03
0.04
0.05
0.06
0.07
0.08
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1.0
Control Parameter *P*
Xiao's
OPCM
TPCM

(a) ξ = 0.2


Probability of Error
0.00
0.01
0.02
0.03
0.04
0.05
0.06
0.07
0.08
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1.0
Control Parameter *P*
Xiao's
OPCM
TPCM

(b) ξ = 0.4



(c) ξ = 0.6

(d) ξ = 0.8

Fig. 6. When ξ values of 0.2, 0.4, 0.6, 0.8, the compare the performance of various algorithms in terms of resistance to noise attack

5. Conclusions and further work

This paper is focused on the intellectual protection problem of the very large integration circuit and a novel algorithm which is suitable for the IP protection of integration circuit has been proposed. The presented method utilized the two-dimensional chaotic encryption to design the safety hidden modal of intellectual property core, and then applied it on the intellectual property core algorithm which is based on the idea of two dimensional chaotic scrambling. The contributions of this paper are as follows.

1) Define the aggregation degree of the resources of physical location in the intellectual property core by safety hidden mathematical modal, and then make the prediction of the used resources aggregation degree of the inserted intellectual property core. In order to guarantee that the information of intellectual property core watermark is effectively inserted surrounding the used circuit resources, the real time inserting mode is selected according to the aggregation degree of the modal.

2) Use the safety valve built up in safety modal to control the hidden algorithm which has the super chaos effect on the two dimensional chaotic sequence. The first dimension sequence is used to control the position of the watermark which the second dimension sequence decides the bits of inserted watermark on each position. By this method, the algorithm succeeded in reducing the power consuming as well as largely increasing the watermark information concealment of the safety modal. Thus, it indeed improved the resistance ability of the watermark algorithm against the illegal attacks.

Although the intellectual property core watermark technique has provided many effective watermark algorithms for the research area of integration circuit secure design in recent years, these achievements is not mature enough for the industrial application. Thus, more research and exploration is still required to find the solution which has a high recognition by both academic and industrial fields. For the future work,we will focus on the following two perspectives:

(1) Active and low cost security control algorithm. The existing IP protection methods mainly include active and passive watermark. The effectiveness and performance of active IP protection technique is limited because it can only take the hysteresis measure to testify and prosecute the suspicious illegal. However, the passive blind watermark technique is more effective to control the fake and illegal infringement in the public scenario by putting the protection right into the hands of IP core processor. How to realize the low cost positive security technique is one of our future directions.

(2) Propose a watermark detection algorithm with high security and high practicability. Lots of existing IP protection methods are based on certain assumptions, some may even require a trustful third party. But in practical industry, the third party is untrustworthy and those methods that based on the assumption of reliable technique e.g. PUF which is not mature enough in the industry. These practical problems are the key factors which decide whether the IP protection methods can be applied into the market safely and effectively. Thus, one of the future directions is also about to propose a real time watermark detection method which is suitable for the public scenario.

Acknowledgments. This work is supported by the National Nature Science Foundation of China (Grant 61202462), the National Nature Science Foundation of Hunan province (Grant 13JJ3091, 14JJ3062), A Project Supported by Scientific Research Fund of Hunan Provincial Education Department (Grant 14A047) and the China Postdoctoral Science Foundation funded project (Grant 140778).

References

1. Sur-Kolay S. and Bhunia S.: Tutorial T4: Intellectual Property Protection and Security in System-on-Chip Design, in VLSI Design (VLSID), 2012 25th International Conference on, Hyderabad, India, 18-19. (2012)
2. Caldwell, A. E., Choi, H., Kahng, A. B, Mantik, S., Potkonjak, M., Qu, G., J. L, W.: Effective Iterative Techniques for Fingerprinting Design IP, 36th ACM/IEEE Design Automation Conference Proceedings, New York, NY, USA 843-848. (1999).
3. Abdel-Hamid, A.T., Tahar, S., and Aboulhamid E. M.: A Survey on IP Watermarking Techniques, Design Automation for Embedded Systems, Vol. 9, No. 3, 211-227.(2004)
4. Castillo, E. L., Parrilla, A. Garcia, U. Meyer-Baese, G. Botella, and A. Lloris.: Automated Signature Insertion in Combinational Logic Patterns for HDL IP Core Protection, in 4th Southern Conference on Programmable Logic, San Carlos de Bariloche, 183-186.(2008)
5. Oliveira, A.L.: Techniques for the Creation of Digital Watermarks in Sequential Circuit Designs, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 20, No . 9,1101-1117. (2001)
6. T.V. L and Desmedt. Y.: Cryptanalysis of UCLA Watermarking Schemes for Intellectual Property Protection, in IH02: Revised Papers from the 5th International Workshop on Information Hiding. London, UK: Springer-Verlag, 213-225. (2003)
7. Ziener.D and Teich.J.: Power Signature Watermarking of IP Cores for FPGAs, Journal of Signal Processing Systems,Vol. 51, No. 1, 123-136. (2008)
8. Ziener. D., Techniques for Increasing Security and Reliability of IP Cores Embedded in FPGA and ASIC Designs, Dissertation, University of Erlangen-Nuremberg, Germany, verlag Dr.Hut, Munich, Germany. (2010)
9. Abdel-Hamid, A.T., Tahar, S., and Mostapha, A. El: IP watermarking techniques: survey and comparison, in System-on-Chip for Real-Time Applications, 2003. Proceedings. The 3rd IEEE International Workshop on, 60-65. (2003)
10. Wei, L., Dafang, Z., Zhiqiang, Y., Osama, H.: A Survey of Techniques for VLSI IP Protection. Information Technology Journal, Vol. 12, No. 12, 2324-2332. (2013)
11. Lach, J., Mangione-Smith, W., and Potkonjak, M.: Signature hiding techniques for FPGA intellectual property protection, in Proc.Int. Conf. Compute-Aided Design, 186-189. (1998)
12. Castillo E., et al.: IPP@HDL: efficient intellectual property protection scheme for IP cores. IEEE Transactions on VLSI Systems, Vol. 15, No. 5, 578-591. (2007)
13. Ji Liang, Z.: Efficient verification of IP watermarks in FPGA designs through lookup table content extracting.IEICE Electronics Express, 1735-1741. (2012)
14. Cui, A., Ch, C., Taha ,S.: IP watermarking using incremental technology mapping at logic synthesis level. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 27, no. 29, 1565-1570. (2008)
15. Qu, G.: Publicly detectable watermarking for intellectual property authentication in VLSI design. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems", Vol. 21, No. 11, 1363-1368. (2002)
16. Le Gal. B: Lilian Bossuet Automatic low-cost IP watermarking technique based on output mark insertions. Design Automation for Embedded Systems, Vol. 16, No. 2, 71-92. (2012)
17. Fan,Y.: Testing-based watermarking techniques for intellectual-property identification in SOC design. IEEE Trans. on Instrumentation and Measurement, Vol. 57, No. 3, 467-479. (2008)
18. Schmid, M., Ziener, D., Teich, J.: Netlist-Level IP Protection by Watermarking for LUT-Based FPGAs. In: Proceedings of IEEE International Conference on Field-Programmable Technology (FPT 2008), Taipei, Taiwan 209-216. (2008)
19. A.B, K, Lach, J., Mangione-Smit, .H, Mantik. S, I.L, M., Potkonjak, M., Tucker, P., Wang, H., and Wolfe, G.: Constraint-based watermarking techniques for design IP protection, IEEE transactions on computer-aided design and integrated circuits system, Vol. 20, No. 10, 1236-1251. (2001)

20. Aijiao, C., C. H., C., Tahar, S.: A robust FSM watermarking scheme for IP protection of sequential circuit design. IEEE Trans Comput Aid D, Vol. 30, No. 5, 678-690. (2011)
21. Tefas, A., Nikolaidis, A., Nikolaidis, N. Solachidis, V. Sekeridou, S., Pitas, I.: Markov chaotic sequences for correlation based watermarking schemes, chaos, solitons & fractals Vol. 17, No. 2, 567-573. (2003)
22. L-Y.X, Tang-W. K.S., Chen-G, R.: Generating hyperchaos via state feedback control. International Journal of Bifurcation and Chaos, Vol. 15, No. 10, 3367-3375. (2005)
23. Y. X, L, W. T, K. S., G. R, C.: Hyperchaos evolved from the generalized Lorenz Equation. International Journal of Circuit Theory and Applications, Vol. 33, No.4, 235-251. (2005)
24. Basic Crypto Core: Overview.,(2013). [Online]. Available: http://www.opencores.org/projects.cgi/web/basicdes.pdf (opencores.org: Overview.urrent October 2013)
25. Qian-chuan, Z., Qing-xin, Z.: A DCT domain color watermarking scheme based on chaos and multilayer Arnold transformation. Proc of International Conference on Networking and Digital Society, Chengdu, China, 209-212. (2009)
26. Rong-rong, N., Qiu-qi, R., Yao, Z.: Pinpoint authentication watermarking based on a chaotic system. Forensic Science International, Vol. 179, No. 1, 54-62. (2008)
27. Shen, Z. W., Liao, W. W., Shen, Y. N.: Blind watermarking algorithm based on henon chaos system and lifting scheme wavelet, International Conference on Wavelet Analysis and Pattern Recognition, Baoding, 308-313. (2009)
28. Basu, A., Roy, D. B., Banerjee, D. et al.: FPGA Implementation of IP Protection through Visual Information Hiding. International Journal of Engineering Science and Technology, Vol. 3, No. 5, 4191-4199. (2011)
29. Wei, L., Xingmin, S., Zhihua, X.: A Chaotic IP Watermarking in Physical Layout Level Based on FPGA. Radio engineering.Vol. 20, No.1, 118-125. (2011)
30. Xiaoyan Sun, Maosheng Zhang, Huanguo Zhang.: Two-Dimension Chaotic-Multivariate Signature System .Vol. 10, No. 1, 1694-0814. (2013)

Wei Liang received his BS in automation from Central South University, China, in2003, MS in computer science and technology from Hunan University of Science and Technology, China, in 2008, and PhD in computing science from Hunan University, China, in 2013. He is currently a Associate Professor in College of Software Engineering, Xiamen University of Technology, China. His current research interests include steganography, real-time embedded systems, intellectual property protection, and field programmable gate arrays. Contact him at Wliang@xmut.edu.cn.

Keshou Wu received the PhD degree in computational mathematics from Huazhong University of Science and Technology, China, in 2011. He is currently at Xiamen University of Technology as a professor. His research interests include intellectual property protection, field programmable gate arrays, data mining, and machine learning. Contact him at kswu@xmut.edu.cn.

Yong Xie received his BE in computer science and technology from Hunan University of Science and Technology, China, in 2007, and PhD in computing science from Hunan University, China, in 2013. His research interests include real-time embedded systems, intellectual property protection, field programmable gate arrays, wireless sensor networks. Contact him at yongxie@xmut.edu.cn.

Jiajun Duan is a research assistant and a PhD in Electrical Engineering the Lehigh University, USA, in 2014. His current research interests include real-time embedded systems, intellectual property protection, and field programmable gate arrays. Contact him at jid213@lehigh.edu.

Received: October 17, 2014; Accepted: April 23, 2015.