IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON BLOCKCHAIN-ENABLED TRUSTWORTHY SYSTEMS

Received January 7, 2020, accepted January 23, 2020, date of publication January 28, 2020, date of current version March 20, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2969990

A Blockchain-Based Traceable IP Copyright Protection Algorithm

LIJUN XIAO[1,2], WEIHONG HUANG[2,3], YONG XIE[4], (Member, IEEE), WEIDONG XIAO[4], AND KUAN-CHING LI[5], (Senior Member, IEEE)

[1]Big Data Development and Research Center, Guangzhou College of Technology and Business, Guangzhou 528138, China
[2]School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China
[3]College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China
[4]School of software Engineering, Xiamen University of Technology, Xiamen 361024, China
[5]Department of Computer Science and Information Engineering, Providence University, Taichung 43301, Taiwan

Corresponding author: Weihong Huang (whhuang@hnust.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 61702180.

ABSTRACT Current Intellectual Property (IP) copyright protection technologies have low efficiency of authority management, traceability, and scalability. In this work, a blockchain-based IP copyright protection algorithm is proposed to address these issues by establishing a mathematical model of quadratic matrix transformation for IP circuit trading. This algorithm proposes the design of a distributed random embedding mechanism and position mapping function that, when IP trading occurs in blockchain, the traceable mapping function can trace the copyright information in IP trading with the mapping factor. Besides, this work analyzes the credibility, transparency, overhead, and complexity. Experimental results show that the proposed algorithm can resist replaying attacks, yet the copyright information can be rapidly retrieved after suffered from attacks. Still, the proposed algorithm has higher security, stability, and traceability.

INDEX TERMS Intellectual property, blockchain, copyright protection, position mapping function.

I. INTRODUCTION

The concept of Blockchain originates from the approach of point-to-point electronic payment, initiated in 2008 [1]–[4]. Initially, such an approach was not widely conceived. Though, with the stable running and fast development of Bitcoin, Blockchain increasingly attracts interests from diverse topics from all over the world. At present, the Blockchain is being applied in the fields of finance, wireless communication, intelligent vehicle, health, the Internet of Things (IoT), among several others. The traditional social trust mechanism is established based on trust endorsement of the government, which supports social trust. Therefore, it is difficult to establish trust between two unknown entities directly yet without the participation of a third center, so the Blockchain technology addresses the trust problem in the decentralized system by using the verification of distributed nodes and consensus mechanism. In this case, IP trading can realize information transmission and value transfer that changes the network framework from "information internet" to "value internet". The circuit blockchain achieves trustable trading without the participation of any intermediary agency, so significant the revolution in credible IP trading. The features of Blockchain in-circuit copyright protection are illustrated in [7], [8], as:

(1) IP circuit trading has high efficiency and low cost. Traditional IP protection realized IP circuit trading by utilizing computer cluster that requires significant overhead in running and maintenance. The blockchain-based IP protection method makes nodes rapidly added to the Blockchain by POW, POS, PBFT, among others. In this case, the copyright of the circuit can pass the verification of the Blockchain network, so the participation degree of nodes in the Blockchain is significantly increased. Besides, the speed of IP circuit trading and protection is also improved, realizing low cost in IP trading,

(2) The supervision efficiency of IP circuit protection is improved via Blockchain. The blockchain makes each element in the system completely transparent. The consensus mechanism ensures the balance and data consistency of Blockchain, as the decentralization is realized by using the public distributed supervision. It dramatically reduces fraud behavior, achieving better IP protection in the blockchain,

The associate editor coordinating the review of this manuscript and approving it for publication was Hong-Ning Dai.

(3) Higher Fault-tolerance and robustness. In a distributed Blockchain network, other nodes can normally run even a specific node is impaired, ensuring the security and reliability of a distributed system. Blockchain is an entirely decentralized point-to-point network, including many distributed nodes and servers. It can realize excellent reliability, as each node in Blockchain stores a complete copy of the accounting book, achieving good fault-tolerance and robustness.

To adapt to the intensely competitive electronic market environment, various semiconductor companies consider shortening the IC design cycle and reducing product costs and risks. IP circuit modules are easily being misappropriated and destroyed by malicious users that cause immeasurable economic losses and breaks the fairness of market competition. To protect the copyright of digital products, many research institutes attempt to research chip security and practical technology based on the Blockchain. At present, IP watermarking technologies are aimed to insert copyright information into IP design [9]–[11]. When IP disputes occur, it is convenient to extract watermark information from the suspected IP design, so thus proving the copyright.

II. RELATED WORK

In recent years, the increase of user privacy leakage and security events makes abundant data collection and control of the suspected third party. Blockchain is widely used in the financial field that ensures essential privacy data. Zyskind *et al.* [12] realized a protocol to transform Blockchain into an automatic access controller without a credible third party. This controller carries instructions, store, query, and share data, which addresses the dependable computation issue. Specialized Blockchain lacks performance analysis theory and data support of consistent algorithm, so Hao *et al.* [13] proposed a scheme to evaluate the performance of the consistency algorithm based on Ethereum and Hyperledger, where the results of a consistency algorithm under different transactions can be generated by quantified analysis of delay and throughput that provides quantified data support for researches in the consensus algorithm.

Internet-of-Things (IoT) is widely used in diverse fields nowadays and has higher requirements for data exchange. Huang *et al.* [14] proposed a Blockchain-based trustable data exchange scheme, as it analyzes three credible requirements of data exchange in IoT and demonstrates the basic principle and critical technologies of Blockchain. Besides, it provides detailed architecture and design of the main credible components for a prototype by Ethereum Blockchain and intelligent contract, where the visualized functions are shown. Presently, few researches focused on the reliability of Blockchain in the circuit layer that makes the security and privacy vulnerable to be affected by hardware errors. To reduce such an impact, Xiao *et al.* [15] proposed a reliability-based circuit unit evaluation method that utilizes an iteration probability transmission matrix to calculate the output reliability of any wire. The gradient of the reliability of the circuit unit is generated by gradient and bucket theories. Further, the importance of the circuit unit is reordered by the reliability gradient.

With the sensitized path coverage rate and sequence comparison, the importance based reordering algorithm with the same reliability gradients is constructed. The critical circuit unit is enhanced based on reordering results, improving the security and privacy of Blockchain architecture in the hardware layer. Experimental results show that the proposed scheme achieves higher accuracy, lower complexity, and cost.

IP trading protection technologies can be classified into two categories, including the untraceable method and traceable method. There are some differences between them. A traditional IP protection method cannot ensure the traceable flow, which makes the protected design be easily attacked or misappropriated while the traceable method can record the operation of the uploaded system and trace the whole flow of the design after adding in the Blockchain. The proper behavior of each user is allowed, as it ensures the stability and full protection of the system. Besides, the users who participate in the implementation of consensus mechanisms will be rewarded.

In this work, a traceable IP circuit protection method is proposed under the blockchain environment. The remaining of this paper is organized as follows. Section 2 proposes the mathematical model of traceable trading protection, Section 3 introduces the IP trading algorithm, including embedding, verification and tracing of copyright information, and the performance analyses in terms of credibility, transparency, overhead, and complexity in Section 4. It is conducted in Section 5 experiments to evaluate the stability and security of the proposed algorithm, the validity of the proposed algorithm is verified, and finally, this work is summarized.

III. MATHEMATICAL MODEL

In this section, the design of a mapping function to trace the content of IP circuit trading under the Blockchain environment is discussed, where a circuit can be protected by adding a watermark. As an attacker intends to destroy the content of IP trading, he should attack the watermark in the IP circuit first, given that the copyright requires verification, the traceable mapping function can be used to restore the impaired information [16]–[18]. The mathematical model of quadratic matrix transformation is defined as follows.

Definition 1: Assuming A be a n-rank matrix. If a number λ and n dimensional nonzero vector ξ satisfy $A\xi = \lambda\xi$, λ is called the characteristic value of matrix A. The nonzero vector ξ is the characteristic vector of value λ of matrix A.

Definition 2: If two vectors ξ_1, ξ_2 satisfy $\xi_1^T \xi_2 = 0$, ξ_1 and ξ_2 are orthogonal.

Definition 3: If n-rank matrix A satisfies $A^T = A$, matrix A is symmetric matrix; If n-rank matrix satisfies $A^T A = E$, A is orthogonal matrix, namely, $A^{-1} = A^T$.

Theorem 1: Let λ_1 and λ_2 are the characteristic values of the symmetric matrix A. If $\lambda_1 \neq \lambda_2$, the characteristic vectors ξ_1 and ξ_2 are orthogonal.

Proof: $A\xi_1 = \lambda_1\xi_1, A\xi_2 = \lambda_2\xi_2, \lambda_1 \neq \lambda_2, A^T = A,$

$$\therefore \lambda_1\xi_1^T = (\lambda_1\xi_1)^T = (A\xi_1)^T = \xi_1^T A^T = \xi_1^T A,$$
$$\therefore \lambda_1\xi_1^T\xi_2 = \xi_1^T A\xi_2 = \xi_1^T(\lambda_2\xi_2) = \left(\lambda_2\xi_1^T\xi_2\right),$$
$$\therefore (\lambda_1 - \lambda_2)\,\xi_1^T\xi_2 = 0, \quad \xi_1^T\xi_2 = 0.$$

Namely, ξ_1 and ξ_2 are orthogonal.

Theorem 2: Let A be n-rank symmetric matrix C. There exists an orthogonal matrix, making

$$C^T AC = B = \begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix} \tag{1}$$

Here, $\lambda_1, \lambda_2, \cdots, \lambda_n$ are characteristic values of matrix A.

Proof: Let vectors $\xi_1, \xi_2, \ldots, \xi_n$ be corresponding vectors of characteristic values $\lambda_1, \lambda_2, \cdots, \lambda_n$. Let the unit vectors satisfying

$$\eta_1 = \frac{\xi_1}{|\xi_1|}, \quad \eta_2 = \frac{\xi_2}{|\xi_2|}, \ldots, \eta_n = \frac{\xi_n}{|\xi_n|}, \tag{2}$$

With theorems 1 and 2, we have

$$\eta_i^T\eta_j = 0, \quad i \neq j \tag{3}$$
$$\eta_i^T\eta_i = 1, \quad i = 1, 2, \ldots, n. \tag{4}$$

ξ_i is the characteristic vector of the characteristic value λ_i. Namely, $A\xi_i = \lambda_i\xi_i$, $i = 1, 2, \ldots, n$, then

$$A\eta_i = \lambda_i\eta_i, \quad i = 1, 2, \ldots, n, \tag{5}$$

Matrix $C = (\eta_1, \eta_2, \ldots, \eta_n)$. With (3) and (4), we have $C^T C = E$, $C^{-1} = C^T$. C is orthogonal matrix.

With (3), (4) and (5), we have $C^T AC = B$. Namely, formula (1) is satisfied.

The conclusion of theorem 2 applies in the quadratic matrix, we have theorem 3.

Theorem 3: For any quadratic matrix $f(X) = X^T AX = \sum_{i,j=1}^{n} a_{ij}x_i x_j \left(A^T = A\right)$, there exists orthogonal transformation $X = CY$, making f be standard form, as (6).

$$f = \lambda_1 y_1^2 + \lambda_2 y_2^2 + \cdots + \lambda_n y_n^2, \tag{6}$$

Here, $\lambda_1, \lambda_2, \cdots, \lambda_n$ is the characteristic value of the matrix $A = (a_{ij})$ of f.

Let the rank of quadratic function f be k. According to theorem 3, there exists reversible transformation $X = CY$ and $C^{-1} = C^T$, making f be a standard form.

$$f = \lambda_1 y_1^2 + \lambda_2 y_2^2 + \cdots + \lambda_k y_k^2$$
$$= Y^T \begin{pmatrix} \lambda_1 & & & & & \\ & \ddots & & & & \\ & & \lambda_k & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix} Y = Y^T BY. \tag{7}$$

$s = A$ is the secret data. n linearly independent vectors $X_1, X_2, \cdots, X_n$, are selected.

(1) With $f(X) = X^T AX$, a reversible transformation $X = CY$ exists with theorem 3, making f be a standard form $f = \lambda_1 y_1^2 + \lambda_2 y_2^2 + \cdots + \lambda_k y_k^2 = Y^T BY$. C is public and B is private.

(2) n participators calculate

$$\begin{cases} X_1^T AX_1 = f_1 \\ X_2^T AX_2 = f_2 \\ \cdots \\ X_n^T AX_n = f_n, \end{cases} \tag{8}$$

and calculate

$$C^T X_i = Y_i, \quad i = 1, 2, \ldots, n. \tag{9}$$

(3) Let the reversible mapping function be $\phi : X_i \rightarrow (f_i, Y_i)$. The set $\{(f_1, Y_1), (f_2, Y_2), \ldots, (f_n, Y_n)\}$ constructs a (k, n) secret sharing scheme [19], [20]. Namely, the secret data s can be reconfigured with any k or more than k sub-secret keys. When k participators $i_1, i_2, \cdots, i_k$, provide the sub-secret keys $\left\{\left(f_{i_1}, Y_{i_1}\right), \left(f_{i_2}, Y_{i_2}\right), \ldots, \left(f_{i_k}, Y_{i_k}\right)\right\}$, we have the following equations set.

$$\begin{cases} Y_{i_1}^T BY_{i_1} = f_{i_1} \\ Y_{i_2}^T BY_{i_2} = f_{i_2} \\ \cdots \\ Y_{i_k}^T BY_{i_k} = f_{i_k}, \end{cases} \tag{10}$$

With (10), the characteristic values $\lambda_1, \lambda_2, \cdots, \lambda_k$ are solved. With the generated B, we have $A = CBC^T$. Namely, s is reconfigured. If there are $k-1$ participators provide the sub-secret keys, $\lambda_1, \lambda_2, \cdots, \lambda_k$ cannot be solved. Therefore, s cannot be reconfigured.

IV. TRACEABLE IP COPYRIGHT PROTECTION ALGORITHM

A. COPYRIGHT INFORMATION PREPROCESSING

Firstly, the copyright information m will be divided into fragments $X_1, X_2, \cdots, X_n$ with the same length. $X_i = \{x_{i1}, x_{i2}, \ldots, x_{in}\}$ is an n-dimensional vector, $i = 1, \ldots, n$. $X_1, X_2, \cdots, X_n$ can form a $n \times n$ matrix A^*.

$$A^* = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{pmatrix} \tag{11}$$

A^* is divided into two symmetric matrices A_1 and A_2 along a diagonal line.

$$A = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{12} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{1n} & x_{2n} & \cdots & x_{nn} \end{pmatrix}, \quad A' = \begin{pmatrix} x_{11} & x_{21} & \cdots & x_{n1} \\ x_{21} & x_{22} & \cdots & x_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{pmatrix} \tag{12}$$

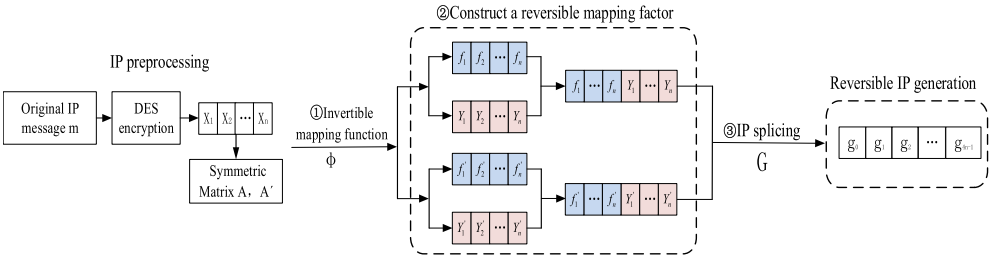

FIGURE 1. The generation of IP watermark.

Let the rank of A_1 and A_2 be k. $s = A, A'$ is regarded as the secret information and the copyright evidence. With the symmetric matrix A, a quadratic $f(X) = X^T AX$ with the rank of k is generated by using the quadratic matrix transformation in section 3. Thus, there exists a reversible transformation $X = CY$ with (8) and (9), from which we obtain the reversible mapping factor $f_i, Y_i, i = 1, 2, \ldots, n$. Similarly, the reversible mapping factor $f_i', Y_i', i = 1, 2, \ldots, n$ for the symmetric matrix A' is generated. $f_i, Y_i, f_i', Y_i', i = 1, 2, \ldots, n$ combine and generate a reversible mapping function sequence $G = \{g_0, g_1, \ldots, g_{4n-1}\}$. Here, each element in G is denoted as follows: $g_i = f_{i+1}; g_{n+i} = Y_{i+1}; g_{2n+i} = f'_{i+1}; g_{3n+i} = Y'_{i+1}; i = 0, 1, \ldots, n-1$. Therefore, the self-recovery mapping function $\phi : X_i \rightarrow \left(f_i, Y_i, f_i', Y_i'\right)$ is constructed. Based on the principle of secret sharing scheme, even a fragment of copyright information is attacked in blockchain, the secret data $s = A, A'$ can be restored by ϕ with any k groups of sequence $\left\{\left(f_{i_1}, Y_{i_1}, f'_{i_1}, Y'_{i_1}\right), \left(f_{i_2}, Y_{i_2}, f'_{i_2}, Y'_{i_2}\right), \ldots, \left(f_{i_k}, Y_{i_k}, f'_{ik}, Y'_{ik}\right)\right\}$. The matrix A^* is generated by combining A and A', obtaining the original copyright information $X_1, X_2, \cdots, X_n$. Additionally, $X_i = CY_i, i = 1, 2, \ldots, n$ can also be used to reconfigure the original copyright information. With the copyright information, the watermark positions $L = \{L_0, L_1, \ldots, L_{4n-1}\}$ can be constructed, which will be selected from the redundant LUT resources for embedding the fragments of copyright information. Besides, this work utilizes the quadratic transformation model to hide the real watermark positions, which enhances the security of watermark positions and the traceability of IP copyright.

B. IP WATERMARK GENERATION, EMBEDDING AND VERIFICATION

The quadratic transformation is a trap-door one-way function [21]. It is introduced in this section the use of quadratic transformation in blockchain-based IP watermark generation, embedding and extraction.

1) IP WATERMARK GENERATION

IP watermark generation includes three parts, including copyright information preprocessing, construction of self-recovery mapping factor, and identification combination [22]. The flow of generation is shown in Fig.1. The original IP message is encrypted by DES algorithm. After that, it is transformed into matrices and finally generates into reversible fragments by mapping function.

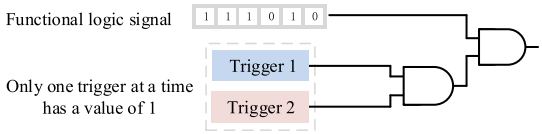

FIGURE 2. Identical logic circuitl.

(1) Original copyright information preprocessing. The IP owner will input the copyright information m first. To prevent the illegal attacks m will be transformed into two $n \times n$ matricescwith the rank of k, which will be used as the evidence of copyright verification. The algorithm transforms the copyright information into a binary sequence, which will be encrypted by the DES algorithm to enhance security and traceability. Based on the thought of distributed storage in blockchain, even the attackers find the positions of copyright information, he cannot extract the related sensitive information. This work realizes the distributed storage of the fragments. The copyright information is divided into fragments with the same length after DES encryption. The remaining part will be padded by zero. The fragments are denoted by $X_1, X_2, \cdots, X_n$.

(2) Construction of reversible mapping factor. Based on the quadratic matrix transformation model, the quadratic $f(X) = X^T AX$ with the rank of k is generated with the symmetric matrix A. Therefore, the reversible transformation $X = CY$ is established. With (8) and (9), the reversible mapping factor $f_i, Y_i, i = 1, 2, \ldots, n$ is obtained. Similarly, the reversible mapping factor $f_i', Y_i', i = 1, 2, \ldots, n$ for the symmetric matrix cA' is also generated. By combining both the reversible mapping factor, the reversible mapping function sequence is generated.

(3) Identification information combination. The reversible mapping factors f_i, Y_i, and $f_i', Y_i', i = 1, 2, \ldots, n$ are combined as $G = \{g_0, g_1, \ldots, g_{4n-1}\}$. Here, $g_i = f_{i+1}; g_{n+i} = Y_{i+1}; g_{2n+i} = f'_{i+1}; g_{3n+i} = Y'_{i+1}; i = 0, 1, \ldots, n-1$. With (8), (9), and (10), even some fragments are impaired, the secret data can be reconfigured with the reversible mapping function ϕ with only k groups of sequence $\left\{\left(f_{i_1}, Y_{i_1}, f'_{i_1}, Y'_{i_1}\right), \left(f_{i_2}, Y_{i_2}, f'_{i_2}, Y'_{i_2}\right), \ldots, \left(f_{i_k}, Y_{i_k}, f'_{ik}, Y'_{ik}\right)\right\}$.

TABLE 1. Generation of watermark positions.

Watermark	g_0	g_1	g_2	g_3	$\cdots$	g_{4n-2}	g_{4n-1}
Watermark Positions	(g_0, g_1)	(g_1, g_0)	(g_2, g_3)	(g_3, g_2)	$\ldots$	(g_{4n-2}, g_{4n-1})	(g_{4n-1}, g_{4n-2})
	L_0	L_1	L_2	L_3	$\ldots$	L_{4n-2}	L_{4n-1}

The matrix A^* is generated by combining A and A', obtaining the original copyright information $X_1, X_2, \cdots, X_n$. Additionally, $X_i = CY_i, i = 1, 2, \ldots, n$ can also be used to reconfigure the original copyright information.

The pseudo-code of the IP watermark generation algorithm is described as follows.

Algorithm 1 Watermark Generation Algorithm

Input: Copyright information m, symmetric matrix A, A'
Output: Watermark sequence G

1. m is transformed into a binary sequence and divided into $X_1, X_2, \cdots, X_n$ the same length after DES encryption;
2. $f(X) = X^T AX, f'(X) = X^T A'X$;
3. With theorem 3, $X = CY$ and $X = C'Y$;
4. i=1
5. while i≤n do
6. $f_i = X_i^T AX_i, f_i' = X_i^T A'X_i$;
7. $Y_i = C^T X_i, Y_i' = C'^T X_i$;
8. $g_{i-1} = f_i, g_{n+i-1} = Y_i, g_{2n+i-1} = f_i', g_{3n+i-1} = Y_i'$;
9. end while

2) WATERMARK EMBEDDING ALGORITH

With the quadratic matrix transformation model, the embedding algorithm selects the watermark positions $L = \{L_0, L_1, \ldots, L_{4n-1}\}$. All the programmable units CLB are read from the original FPGA design. The LUT resources are scanned with the Z-traversal method due to the feature of FPGA [23]–[25], as it ensures each LUT be accessed. Finally, the target positions are found to embed the watermarks. Also, the symmetric matrix D represents the watermark position. 0 denotes unused resource and 1 denotes used resource. Therefore, a quadratic $f(X) = X^T DX$ can be constructed. With (7), there exists an orthogonal transformation $X = C'Y$. A new matrix D' is generated. Even the attacker captures the matrix D', he cannot know the real watermark positions. Therefore, the embedded watermark information will not be removed, which improves the security of the watermark. Finally, the sequence G is embedded into LUTs by logic configuration under the constraint of L [26].

The procedure of watermark embedding is illustrated as follows.

Position generation: With the generation procedure of reversible copyright information, we have $g_i = f_{i+1}; g_{n+i} = Y_{i+1}; g_{2n+i} = f'_{i+1}; g_{3n+i} = Y'_{i+1}; i = 0, 1, \ldots, n-1$. As listed in Table 1, we denote

$$(f_1, f_2), (f_2, f_1), \ldots, (f_{n-1}, f_n), (f_n, f_{n-1}), (Y_1, Y_2), (Y_2, Y_1), \ldots, (Y'_{n-1}, Y'_n), (Y'_n, Y'_{n-1}), \quad (13)$$

In Table.1, the first row is watermark and the second row is watermark position. All the programmable units CLB are read from the original FPGA design. The LUT resources are scanned with the Z-traversal method due to the feature of FPGA. The embedding positions are generated by searching the corresponding coordinates.

The embedding positions can be denoted by the corresponding matrix. 0 is unused and 1 is used resources. It can establish a symmetric matrix D. The quadratic transformation model is used to enhance the security of real positions. Therefore, a quadratic $f(X) = X^T DX$ can be constructed. With (7), there exists an orthogonal transformation $X = C'Y$. A new matrix D' is generated. Even the attacker captures the matrix D', he cannot know the real watermark positions. Therefore, the embedded watermark information will not be removed, improving the security of the watermark.

(2) Identical logic configuration. The generated watermarks will be configured into the LUT resource by identical logic. The identical logic circuit will not change the output. Namely, the input of the logic is the same as the output. For any signal $S_i, i = 0, 1, 2, \ldots$, it satisfies $S_i \| 0 = S_i$, $S_i \& 1 = S_i$. The logic 0 and 1 are respectively named identical logic 0 and identical logic 1. By analyzing the feature of identical logic, when two flip-flops are reversed, the output is constant 0 after an And gate.

If a functional signal is or-ed with the identical logic 0, the output will not be changed. Therefore, the output will be equal to the functional signal, demonstrating that the redundant logic will not change the normal functionality of the circuit.

The pseudo-code of the traceable watermark embedding algorithm is illustrated as follows.

3) TRADING INFORMATION VERIFICATION ALGORITHM

In the Blockchain-based trading environment, trading information verification includes determining positions of copyright information, splitting copyright information, preprocessing and information verification [27]–[29].

(1) $D = C^* D' C^{*T}$ can be calculated with the matrix D' and C^*. Matrix D is used to restore the embedding position

Algorithm 2 Watermark Embedding Algorithm

Input: Original design S, sequence $G = \{g_0, g_1, \ldots, g_{4n-1}\}$
Output: watermarked design S', D'
1. With $G = \{g_0, g_1, \ldots, g_{4n-1}\}$, the watermark positions $L = \{L_0, L_1, \ldots, L_{4n-1}\}$ are generated,
2. $L = \{L_0, L_1, \ldots, L_{4n-1}\}$ is transformed into the symmetric matrix D,
3. Construct a quadratic $f(X) = X^T DX$,
4. With (7), an orthogonal transformation $X = C^*Y$, exists and a new matrix D' is generated,
5. A sequence G is embedded with the constraint of L,
6. $S' = S$.

$L = \{L_0, L_1, \ldots, L_{4n-1}\}$. The corresponding LUT resources with specific identical logic can be searched.

(2) Based on the embedding position $L = \{L_0, L_1, \ldots, L_{4n-1}\}$, the reversible mapping factor $f_i, Y_i, f_i', Y_i', i = 1, 2, \ldots, n$ can be calculated, namely the watermark sequence $G = \{g_0, g_1, \ldots, g_{4n-1}\}$. As in the procedure of watermark generation, the length of the fragment is fixed. Thus, it can be combined with the reversed procedure. Finally, encrypted watermarks $X_1, X_2, \cdots, X_n$ can be calculated as $X_i = CY_i, i = 1, 2, \ldots, n$.

(3) In the Blockchain-based IP trading procedure, the watermark generation realizes DES encryption. Thus, the verification should decrypt the extracted information and finally restore the original copyright information m.

(4) The restored copyright information m is compared to the declared one of the IP owner. If both are consistent, the trading is legal.

The pseudo-code of the trading information verification algorithm is described as follows.

Algorithm 3 Trading Information Verification Algorithm

Input: D', secret file C^*, C', C
Output: Original copyright information m
1. Calculate $D = C^*D'C^{*T}$
2. Restore watermarked positions $L = \{L_0, L_1, \ldots, L_{4n-1}\}$ with D;
3. Search the watermark sequence $G, f_i, Y_i, f_i', Y_i', i = 1, 2, \ldots, n$ with L;
4. while i≤n do
5. $X_i = CY_i, X_i = C'Y_i'$;
6. end while;
7. X_i is decrypted to restore m

4) THE TRACEABILITY OF IP CIRCUIT

In IP copyright trading, attackers attempt to destroy or remove the copyright information in the IP circuit. Some detection tools are used to evaluate or analyze the target IP circuit. After determining the existence of copyright information, they may remove it and obtain next the non-watermarked design. Traditionally, the content of copyright information is difficult to be restored after suffered an attack, so the authentication fails. In this section, a restoration mechanism is used to trace the behavior of attackers and restore accurate copyright information. After restoring the embedding position $L = \{L_0, L_1, \ldots, L_{4n-1}\}$, the reversible mapping factor $f_i, Y_i, f_i', Y_i', i = 1, 2, \ldots, n$, namely the sequence $G = \{g_0, g_1, \ldots, g_{4n-1}\}$ can be extracted. As the procedure of the watermark generation, the length of the fragment is fixed, and therefore, it can be combined with the reversed procedure. With the secret-sharing mechanism presented in section 3, any k groups of sequence can restore the original copyright information. The matrix B, B' can be calculated by solving the equation set in (10).

$$\left\{\left(f_{i_1}, Y_{i_1}, f_{i_1}', Y_{i_1}'\right), \left(f_{i_2}, Y_{i_2}, f_{i_2}', Y_{i_2}'\right), \ldots, \left(f_{i_k}, Y_{i_k}, f_{ik}', Y_{ik}'\right)\right\}$$

Therefore, $X_1, X_2, \cdots, X_n$ is generated by calculating and combing $A = CBC^T, A' = C'B'C'^T$. In the end, the original copyright information can be restored by decryption.

V. ALGORITHM ANALYSIS

In this work, we proposed a quadratic matrix transformation model based traceable IP protection algorithm. In the IP trading procedure, we utilize the model and realize a (k, n) secret sharing scheme, as the impaired IP copyright fragments can be reconfigured. The proposed algorithm can compensate for the drawbacks of the existing IP protection algorithms in resistance against attacks. This section mainly analyzes the performance in terms of credibility, transparency and overhead.

A. CREDIBILITY ANALYSIS

The proposed algorithm combines the quadratic matrix transformation model and the secret-sharing mechanism, ensuring the credibility of the proposed algorithm. The probability of coincidence is the probability that the non-watermarked IP circuit carries the same watermarks with the watermarked IP circuit, which depends on the number of inserted watermarks. If more watermarks are inserted, the probability of coincidence is smaller. Still, it can be used as a metric to evaluate the credibility of copyright authentication.

Based on the approach of Blockchain-based distributed trading algorithms, the copyright information is transformed into fragments for embedding. Let the number of fragments is n_0, and n the number of unused lookup tables. The probability to detect m watermark positions from n unused positions is $1/C_n^m$. Assuming that the probability that the selected positions "include" watermark fragments is P_0 and "not include" the watermark fragments is P_1. The probability of coincidence P_c can be calculated as follows:

$$\mathrm{P}_c = \frac{1}{\mathrm{C}_n^m}(\mathrm{P0})^{n_0}(\mathrm{P1})^{(n-n_0)} \tag{14}$$

The proposed algorithm transforms the copyright information into a group of reversible mapping factors, which are

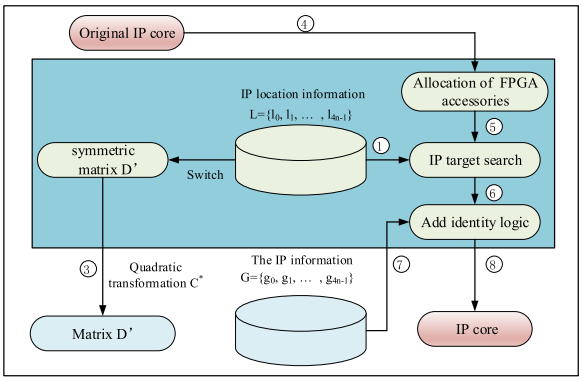

FIGURE 3. The traceable watermark embedding algorithm.

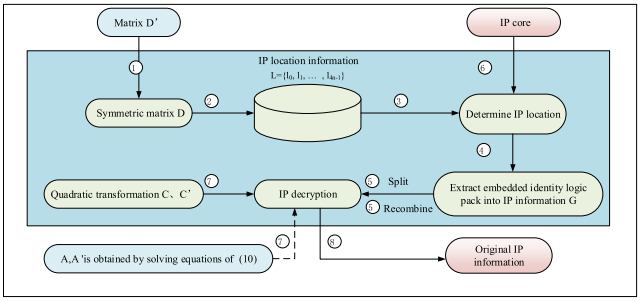

FIGURE 4. The trading information verification algorithm.

embedded in the design. If the number of embedded watermarks is larger, the probability of coincidence is smaller, demonstrating the higher credibility of the circuit.

B. TRANSPARENCY ANALYSIS

For the IP trading protection algorithm, transparency is the embedded copyright information and does not affect the standard functionality of the original design. This algorithm utilizes the logic configuration and inserts watermarks into unused resources in the original design. In the IP trading procedure, the circuit will not activate the watermarked resources and change the normal function. Therefore, the transparency directly affects the security of the algorithm in Blockchain-based IP trading.

C. PERFORMANCE OVERHEAD ANALYSIS

Performance overhead is the extra resources and power after embedding the copyright information. The proposed algorithm utilizes the unused resources in the original design for watermark embedding. Therefore, the resource occupation increase to some degree though less impact on performance overhead, since there are abundant programmable resources in FPGA. Besides, watermarks are embedded into the unused resource. When a core is running, the watermarked resources will not be activated, so it will not cause extra power overhead. Meanwhile, the watermark generation in the proposed algorithm transforms the copyright information into the reversible mapping factors by using the quadratic matrix transformation model, and the generated mapping factors will be embedded in the design. Therefore, with the same length of copyright information, the proposed algorithm has less actually embedded content, causing less impact on resource and delay.

D. COMPLEXITY ANALYSIS

The core of the quadratic matrix transformation model-based reversible protection algorithm is to rapidly calculate the reversible mapping factors of the copyright information and restore the original copyright. For the symmetric matrix A, the quadratic matrix transformation model is established in section 3. With the formulas (8) and (9), the reversible mapping factors $f_i, Y_i, i = 1, 2, \ldots, n$ and $f_i', Y_i', i = 1, 2, \ldots, n$ are generated. The time complexity of the algorithm is $O(n)$. Moreover, the embedded information is $G = \{g_0, g_1, \ldots, g_{4n-1}\}$ and the secret information is $s = A.A'$ is a $n \times n$ matrix. The space complexity of the algorithm is $O(n^2)$. In other words, the time complexity of the proposed algorithm is not high and the space complexity has better superiority.

VI. EXPERIMENTS AND ANALYSIS

In this section, several experiments to evaluate the performance of the proposed algorithm are conducted. Typical benchmarks are selected for testing, and the utilized platform is Xilinx Virtex II Pro XC2VP4 FPGA. The performance is mainly evaluated in terms of stability and security. The detection stability is the probability of detection accuracy of the embedding watermark and the security is analyzed by false alarm rate of detection.

A. STABILITY ANALYSIS

The four IP cores are embedded 32-bit and 256-bit watermarks, so the performance results are listed in Table 2, with W denoting the detection stability and X the area under the curve. Changes in detection stability are shown in Fig. 5, where larger values of X and W demonstrates the better performance of detection.

In Table 2, four benchmark circuits occupying different numbers of resources, to best evaluate the performance of the proposed detection algorithm. The performance is evaluated by embedding 32-bit and 256-bit watermark information respectively. When embedding a 32-bit watermark, both the stability and detection time increase significantly. Though, when the number of the watermark is 256 bit, the change of stability increases gently despite it decreases, but the detection time still increases. Due to the increase of embedding watermarks, the LUT resources of the IP circuit and the detection time are adjusted optimally in the detection procedure. Therefore, the adjustment makes false dismissal probability decrease to some degree may the number of embedding watermarks is large.

To evaluate the resource overhead and delay, the proposed algorithm is compared to the one proposed by Cui *et al.* [16]. The MD5 IP core is used as the benchmark, respectively representing embedded 100%, 75%, 50% and 25% watermark.

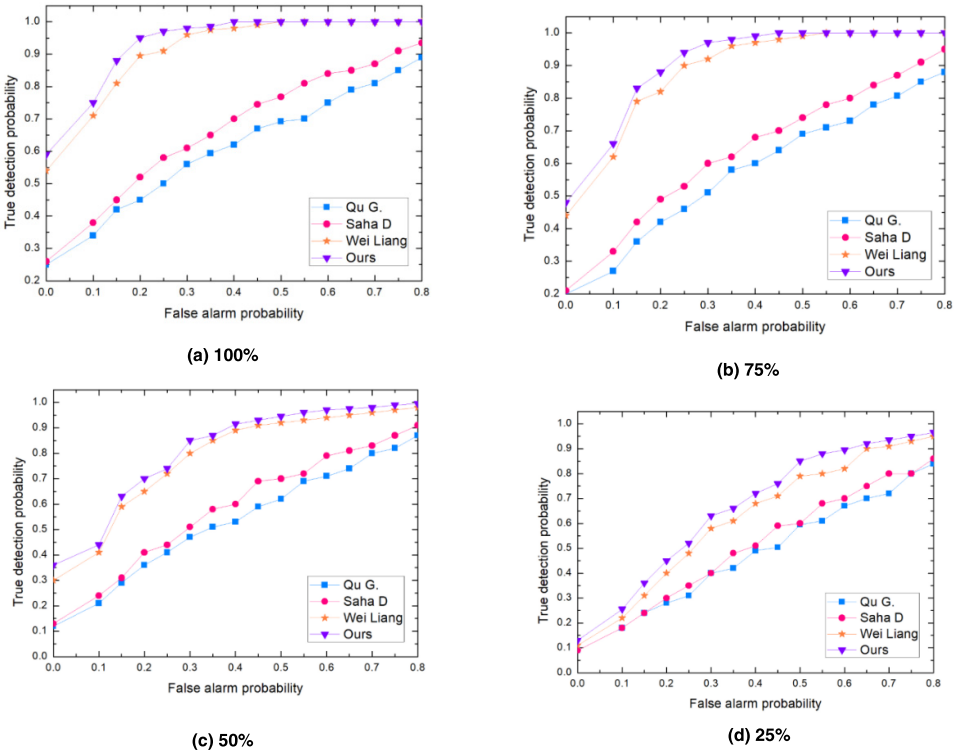

FIGURE 5. The comparison of detection probability of four algorithms with different embedding rate.

TABLE 2. Stability comparison after embedding watermark.

Circuit	Original design		32 bit		256 bit	
	Cells(slices)	Timing(ns)	W	X	W	X
RSA	490	9.130	0.865	0.730	0.965	0.930
MD5	1171	18.018	0.773	0.546	0.843	0/686
SHA	1695	12.765	0.665	0.330	0.771	0.542
DES	1438	11.231	0.641	0.282	0.819	0.638

The relationship between detection probability and false alarm probability of four algorithms is shown in Fig. 5. With the increase of embedding rate, the detection probability changes accordingly, the proposed algorithm tends to 1 rapidly though by comparing it to the algorithm by Qu *et al*, which demonstrates that the stability of the proposed algorithm is optimal with a high watermark embedding rate.

B. SECURITY ANALYSIS

1) ANALYSIS OF FALSE ALARM RATE

In this section, the false alarm rate of detection is used to evaluate the security of the detection algorithm and can be calculated by the formula (14). To achieve better security, the false alarm rate of detection is expected to tend to zero. The DES core is used in this section as a benchmark. The result is compared to the algorithm by Saha *et al*. as shown in Fig. 6. With the increase of the embedding rate, the false alarm rate of the proposed algorithm decreases sharply compared to

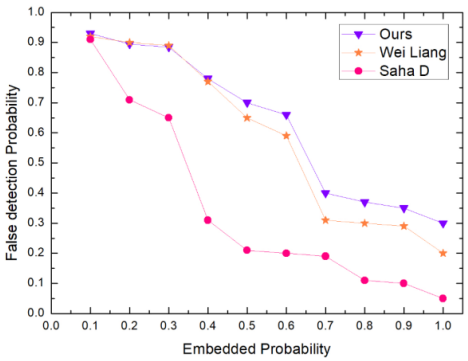

FIGURE 6. False detection probability comparison with different embedding rate.

Saha *et al*., tending rapidly to zero. From this observation, it demonstrates that the proposed algorithm achieves a lower false alarm rate of detection than comparative algorithms, achieving better security of detection.

TABLE 3. Detection performance comparison.

IP circuit	Embedding rate	Saha' algorithm			The proposed algorithm		
		W	T	P_β	W	T	P_β
RSA	100%	0.865	0.224	0.012	0.865	0.026	0.009
	75%	0.791	0.257	0.022	0.791	0.221	0.017
	50%	0.645	0.358	0.024	0.645	0.256	0.014
	25%	0.382	0.479	0.031	0.382	0.289	0.025
MD5	100%	0.773	0.245	0.008	0.773	0.221	0.005
	75%	0.685	0.457	0.014	0.685	0.254	0.009
	50%	0.452	0.668	0.031	0.452	0.202	0.011
	25%	0.324	0.709	0.039	0.324	0.271	0.017
DES	100%	0.641	0.313	0.015	0.641	0.021	0.003
	75%	0.561	0.421	0.022	0.561	0.162	0.013
	50%	0.378	0.518	0.026	0.378	0.273	0.015
	25%	0.256	0.725	0.027	0.256	0.388	0.018

In IP circuit trading, the false alarm rate of detection is not directly related to the false alarm rate of embedding even though it has a particular relationship with the embedding method. Generally, the method with a higher embedding rate can easily detect watermarks. The quantified IP watermark embedding method has a lower embedding rate than that of replacement or exchange based embedding method. As shown in Fig. 6, the number of embedded watermarks is 32-bit. When the embedding rate is 100%, the proposed algorithm has superiority in the false alarm rate of detection by comparing to the one proposed by Saha *et al.*

Table 3 lists the detection performance of three algorithms with different embedding rates. The proposed algorithm constructs an overall scrambling algorithm that achieves lower calculation complexity and less calculation time than Z scrambling algorithm by Saha *et al*., requiring less detection time. Also, it is more suitable for real-time IP detection. Results in Table 3 show the superiority of the proposed algorithm in stability and detection performance.

2) RESISTANCE AGAINST MULTIPLE EMBEDDING ATTACKS

Multiple embedding attack is to add another forged copyright information into a watermarked IP design and declare forged ownership. It causes degradation of circuit performance, and the attack will confuse the authentication institution, however.

The IP trading scheme in this work mainly utilizes the value of SHA-1 hash function to realize the random trading query of the verification party. It can prevent illegal multiple embedding attackers from realizing information steganography. That is, the hash function is designed under a random assumption. If the verifier has the commitment value Z for the signature r, Z will not leak available information about r under the condition of a discrete logarithm problem. In this work, the use of quadratic matrix transformation is intransitive for the authentication of IP watermark. The public key Y in the proof is combined with the identity information of the prover via the public key certificate since only the signer can construct a zero-knowledge proof. Also, it avoids the verifier distributing the signature M of the prover. In IP protection, the identity information of the verifier can be added. In this case, the proof of the prover is regarded as proof of the verifier and the only proof of authorized use of the verifier. Therefore, the proposed algorithm is secure under multiple embedding attacks.

VII. CONCLUSION AND FUTURE WORK

To address the issues of low security and traceability in traditional IP protection technologies, it is proposed in this work a traceable IP protection algorithm in the Blockchain environment. The quadratic matrix transformation model is emphasized during the design of this model based on a traceable IP protection algorithm, as the algorithm embeds a group of reversible self-recovery mapping factors in IP design that dramatically improves the robustness of copyright information and enhances the ability against replay attacks.

Based on the experimental results, the contributions of this work validated are as follows: (1) In Blockchain-based IP circuit trading, quadratic matrix transformation transforms the copyright information into a group of identification sequence, and (2) With the feature of distributed storage in blockchain, the traversal search algorithm randomly selects multiple identification information from the distributed LUT resources and generates the coordinates of IP copyright rapidly. As future directions, we will aim at researches on

secure intelligent contract protocol of IP circuit protection under the Blockchain environment to enhance the security and reliability further.

REFERENCES

[1] W. Liang, M. Tang, J. Long, X. Peng, J. Xu, and K.-C. Li, "A secure fabric blockchain-based data transmission technique for industrial Internet-of-Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3582–3592, Jun. 2019.

[2] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," *Future Gener. Comput. Syst.*, vol. 105, pp. 475–491, Apr. 2020.

[3] W. Liang, K.-C. Li, J. Long, X. Kui, and A. Y. Zomaya, "An industrial network intrusion detection algorithm based on multifeature data clustering optimization model," *IEEE Trans. Ind. Inf.*, vol. 16, no. 3, pp. 2063–2071, Mar. 2020.

[4] H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, p. 352–375, 2018.

[5] W. Liang, J. Long, X. Lei, Z. You, H. Luo, J. Cai, and K.-C. Li, "Efficient data packet transmission algorithm for IPV6 mobile vehicle network based on fast switching model with time difference," *Future Gener. Comput. Syst.*, vol. 100, pp. 132–143, Nov. 2019.

[6] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019, doi: 10.1109/jiot.2019.2920987.

[7] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 839–858.

[8] A. Savelyev, "Copyright in the blockchain era: Promises and challenges," *Comput. Law Secur. Rev.*, vol. 34, no. 3, pp. 550–561, Jun. 2018.

[9] W. Liang, K. Wu, Y. Xie, and J. Duan, "TDCM: An IP watermarking algorithm based on two dimensional chaotic mapping," *Comsis. Jcomsis Comput. Sci. Inf Syst. Comput.*, vol. 12, no. 2, pp. 823–841, 2015.

[10] W. Liang, W. Huang, W. Chen, K.-C. Li, and K. Li, "Hausdorff distance model-based identity authentication for IP circuits in service-centric Internet-of-Things environment," *Sensors*, vol. 19, no. 3, pp. 487–505, Jan. 2019.

[11] A. Sengupta and S. Bhadauria, "Exploring low cost optimal watermark for reusable IP cores during high level synthesis," *IEEE Access*, vol. 4, pp. 2198–2215, 2016.

[12] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops*, May 2015, pp. 180–184.

[13] Y. Hao, Y. Li, X. Dong, L. Fang, and P. Chen, "Performance analysis of consensus algorithm in private blockchain," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2018, pp. 280–285.

[14] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, and L. Xie, "A decentralized solution for IoT data trusted exchange based-on blockchain," in *Proc. 3rd IEEE Int. Conf. Comput. Commun. (ICCC)*, Dec. 2017, pp. 1180–1184.

[15] J. Xiao, J. Lou, J. Jiang, X. Li, X. Yang, and Y. Huang, "Blockchain architecture reliability-based measurement for circuit unit importance," *IEEE Access*, vol. 6, pp. 15326–15334, 2018.

[16] A. Cui, G. Qu, and Y. Zhang, "Ultra-low overhead dynamic watermarking on scan design for hard IP protection," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 11, pp. 2298–2313, Nov. 2015.

[17] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K.-K.-R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Comput. Netw.*, vol. 129, pp. 429–443, Dec. 2017.

[18] X. Li, A. K. Sangaiah, S. Kumari, F. Wu, J. Shen, and M. K. Khan, "An efficient authentication and key agreement scheme with user anonymity for roaming service in smart city," *Pers. Ubiquit. Comput.*, vol. 21, no. 5, pp. 791–805, Oct. 2017.

[19] A. Sengupta, "Intellectual property cores: Protection designs for CE products," *IEEE Consum. Electron. Mag.*, vol. 5, no. 1, pp. 83–88, Jan. 2016.

[20] Y. -F. Chang and W. -L. Tai, "A block-based watermarking scheme for image tamper detection and self-recovery," *Opto-Electron. Rev.*, vol. 21, no. 2, pp. 182–190,2013.

[21] M. Kumm, K. Moller, and P. Zipf, "Partial LUT size analysis in distributed arithmetic FIR Filters on FPGAs," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2013, pp. 2054–2057.

[22] S. Y. Park and P. K. Meher, "Efficient FPGA and ASIC realizations of a da-based reconfigurable FIR digital filter," *IEEE Trans. Circuits Syst., II, Exp. Briefs*, vol. 61, no. 7, pp. 511–515, Jul. 2014.

[23] B. Habib, K. Gaj, and J.-P. Kaps, "FPGA PUF based on programmable LUT delays," in *Proc. Euromicro Conf. Digit. Syst. Design*, Sep. 2013, pp. 697–704.

[24] K. Juretus and I. Savidis, "Reduced overhead gate level logic encryption," in *Proc. 26th Ed. Great Lakes Symp. VLSI (GLSVLSI)*, 2016, pp. 15–20.

[25] J. M. Winograd and R. P. J. Zhao, "Content access management using extracted watermark information," U.S. Patent 8 838 978, Sep. 16, 2014.

[26] J. Long, D. Zhang, C. Zuo, J. Duan, and W. Huang, "A robust low-overhead watermarking for field authentication of intellectual property cores," *Comsis Jcomsiscomput Sci. Inf.*, vol. 13, no. 2, pp. 609–622, 2016.

[27] Z.-W. Zhang, "Double reversible watermarking algorithm for image tamper detection," *J. Inf. Hiding Multimedia Signal Process.*, vol. 7, no. 3, pp. 530–542, 2016.

[28] B. D. Rouhani, H. Chen, and F. Koushanfar, "Deepsigns: A generic watermarking framework for ip protection of deep learning models," Apr. 2018, *arXiv:1804.00750*. [Online]. Available: https://arxiv.org/abs/1804.00750

[29] M. E. Riffi, Y. Saji, and M. Barkatou, "Incorporating a modified uniform crossover and 2-exchange neighborhood mechanism in a discrete bat algorithm to solve the quadratic assignment problem," *Egyptian Informat. J.*, vol. 18, no. 3, pp. 221–232, Nov. 2017.

LIJUN XIAO received the bachelor's degree from the Hunan University of Technology and Business, in 2014, and the master's degree from the Hunan University of Science and Technology, Xiangtan, in 2017. From 2017 to 2018, she was an Assistant Researcher with the Hunan University of Science and Technology. She has been an Assistant Professor with the Guangzhou College of Technology and Business, Guangzhou, since 2009. She has published six refereed journal articles and conference papers. Her current research interests include theories of software engineering, IP protection, and software security.

WEIHONG HUANG received the M.S. and Ph.D. degrees in computer science and technology from Hunan University, China, in 2005 and 2019, respectively. He is currently working with the School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, China. He has published more than 20 refereed journal articles and conference papers. His research interests include network and information security, hardware security, and IP protection.

YONG XIE (Member, IEEE) received the Ph.D. degree in computer science and engineering from Hunan University, China, in 2013. He is currently an Associate Professor with the Xiamen University of Technology. He has published more than 50 refereed journal article and conference papers. His major interests include in-vehicle networks, embedded real-time systems, and cyber-physical systems. He is a member of ACM and CCF.

WEIDONG XIAO received the bachelor's degree from Jiangxi Normal University, in 1992, and the M.S. degree from Xiamen University, in 2003. He is currently a Professor with the School of software Engineering, Xiamen University of Technology. He has published more than 20 refereed journal articles and conference papers. His research interests include networks security protection, embedded systems and hardware/IP protection, and fog computing, and security management in WSN.

KUAN-CHING LI (Senior Member, IEEE) is currently a Distinguished Professor with the Department of Computer Science and Information Engineering, Providence University, Taiwan. He received distinguished and chair professorships from universities in China and other countries. He was a recipient of awards and funding support from several agencies and high-tech companies. He has been actively involved in several major conferences and workshops in program/general/steering conference chairman positions. He has organized numerous conferences on high-performance computing and computational science and engineering. Besides publishing numerous research articles and articles, he is coauthor/co-editor of several technical professional books published by CRC Press/Taylor & Francis, Springer.