


Article

An Anti-Counterfeiting Architecture for Traceability System Based on Modified Two-Level Quick Response Codes

Shundao Xie  and Hong-Zhou Tan *

School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou 510006, China; xieshund@mail3.sysu.edu.cn

* Correspondence: issthz@mail.sysu.edu.cn

Abstract: Traceability is considered a promising solution for product safety. However, the data in the traceability system is only a claim rather than a fact. Therefore, the quality and safety of the product cannot be guaranteed since we cannot ensure the authenticity of products (aka counterfeit detection) in the real world. In this paper, we focus on counterfeit detection for the traceability system. The risk of counterfeiting throughout a typical product life cycle in the supply chain is analyzed, and the corresponding requirements for the tags, packages, and traceability system are given to eliminate these risks. Based on the analysis, an anti-counterfeiting architecture for traceability system based on two-level quick response codes (2LQR codes) is proposed, where the problem of counterfeit detection for a product is transformed into the problem of copy detection for the 2LQR code tag. According to the characteristics of the traceability system, the generation progress of the 2LQR code is modified, and there is a corresponding improved algorithm to estimate the actual location of patterns in the scanned image of the modified 2LQR code tag to improve the performance of copy detection. A prototype system based on the proposed architecture is implemented, where the consumers can perform traceability information queries by scanning the 2LQR code on the product package with any QR code reader. They can also scan the 2LQR code with a home-scanner or office-scanner, and send the scanned image to the system to perform counterfeit detection. Compared with other anti-counterfeiting solutions, the proposed architecture has advantages of low cost, generality, and good performance. Therefore, it is a promising solution to replace the existing anti-counterfeiting system.

Keywords: traceability architecture; copy detection; counterfeit detection; 2LQR codes



Citation: Xie, S.; Tan, H.-Z. An Anti-Counterfeiting Architecture for Traceability System Based on Modified Two-Level Quick Response Codes. *Electronics* **2021**, *10*, 320. <https://doi.org/10.3390/electronics10030320>

Academic Editor: D. J. Lee

Received: 5 January 2021

Accepted: 26 January 2021

Published: 29 January 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Over the past decade, consumers around the world have become increasingly concerned about product safety [1]. Traceability is considered a promising solution for product safety, as well as to achieve consumer confidence [2]. Traceability is the ability to access any or all information relating to the product that is under consideration (traceable resource Unit, TRU), throughout its entire life cycle, by means of recorded identifications [3,4]. A traceability system consists of three components, that is, identification of TRUs, documenting connections between TRUs, and attributes of the TRUs [4], as shown in Figure 1. The first component (identification of TRUs) is the most important component that the other two components build on, whereas the other two components are in principle independent [4]. Identification of TRUs includes identifier code type and structure, identifier granularity and uniqueness, and association of identifier to TRU [4].

Traceability usually improves product safety by providing a means for recall as well as proof of the authenticity of the product [2]. However, most publications and reports on traceability only focus on the TRU attributes, because those who build the traceability system are mostly interested in the attributes of TRUs for data analysis and connections between TRUs for product tracking and recall [4]. However, as an essential subsystem of quality management, these traceability systems do not ensure consumers against fraud [2].

The data in the traceability system is only a claim [4] rather than a fact. Therefore, the quality and safety of the product cannot be guaranteed since we can neither ensure the authenticity of the data [5] in the traceability system, nor the authenticity of products in the real world. However, for consumers, their main concern is two problems: the first is whether the information on the system is authentic; the second is whether the information on the system is consistent with the actual product, which is usually called anti-counterfeiting. The two problems are equally important. Failing to solve either of the two problems will lead to a decline in the credibility of the traceability system.

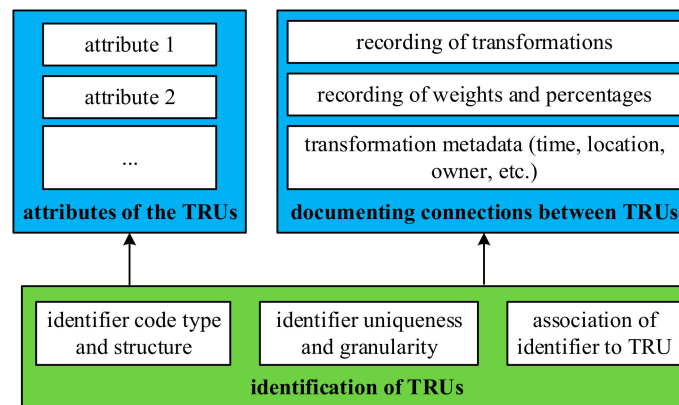


Figure 1. Components of a traceability system. The upper two components, that is, attributes of the TRUs and documenting connections between TRUs, are based on the identification of TRUs. More details are available in [4].

The emergence of blockchain technology has solved the first problem well [5–15], whereas the second problem (anti-counterfeiting) is more difficult to solve. A product is counterfeit if its provenance, specification, quality, and so on are misrepresented [16]. This applies to the product, its container, or other packaging or labeling information [17]. Traditional anti-counterfeiting system and traceability system are generally regarded as two independent systems, which not only causes inconvenience to consumers but also makes them more vulnerable to cracking. Combining the two systems into one can effectively solve the above problems. More specifically, integrating anti-counterfeiting techniques into the traceability system can not only solve the anti-counterfeiting problem in the traceability system, but also make it more convenient to consumers.

In recent years, radio-frequency identification (RFID) is used in traceability to perform anti-counterfeiting. Feng Tian [6] proposed to use RFID to guarantee the quality and safety of the agri-food products in the whole supply chain for the first time. However, this method has two fatal disadvantages. Firstly, the cost of RFID tags is very high, which means that this method can only be applied to high-value goods. Secondly, investments in corollary equipment and updating the original system are huge [6], which greatly limits the application of this method. In addition, RFID tag data is usually static and cannot be updated to reflect the latest conditions of products [16]. Therefore, Kun et al. [16] develop a novel RFID-based system suitable for counterfeit detection, where different types of on-chip sensors and in-system structures collect the necessary information to detect counterfeits. However, this system is designed for internet of things (IoT) devices and cannot apply to products without a printed circuit board (PCB) and integrated circuits (ICs). In [18], the RFID tag is made into high-imitation electronic seed and packed in each seed bag to realize the anti-counterfeiting of seeds. In summary, RFID based solutions have disadvantages of high system complexity, high cost for both tags and equipment. Worse, most of the RFID tags on the market today can be easily cloned, which reduces the anti-counterfeiting performance of these solutions.

Non-RFID based solutions for anti-counterfeiting in the traceability system have been explored for a long time. Agrawal et al. [19,20] proposed a secured tag, which is a randomly

distributed microparticles printed on the textile surface through an uncontrolled screen printing mechanism, for textile products anti-counterfeiting. It is low cost and convenient because only a smartphone with a camera is needed to perform counterfeit detection. However, the secured tag is based on the screen-printing method, so it cannot be applied to products other than textile. In addition, the information in the secured tag is very limited and cannot be manipulated manually. Wang et al. [21] proposed a textile coding tag, where coded yarns having different optical features are used to represent digits, similar to barcodes. The textile coding tag's inherent features link the physical product, therefore eliminate the dependency on external tags. However, the textile coding tag is easy to clone when the yarn coding procedure is provided. Chen et al. [22] proposed to embed codes inside the components made by additive manufacturing (AM) for product authentication and identification of counterfeits but this method can only be applied to AM products and the code can only be captured with a micro-CT scanner. Trenfield et al. proposed to print quick response (QR) codes and data matrices onto the surface of polymeric-based printlets for scanning using a smartphone device and designed a novel anti-counterfeiting strategy, which involved the deposition of a unique combination of material inks for detection using Raman spectroscopy. The above technologies either have poor performance in anti-counterfeiting, or can only be applied to specific products, or the equipment used to detect counterfeiting is too professional to be operated by ordinary consumers.

A few years ago, copy-detection graphical codes (CDGCs) [23,24] were proposed for document authentication. CDGC is a printed machine-readable image that cannot be physically cloned illegally, and its advantages are cheap generation and easy integration [24], because the equipment an ordinary printer is used to make the CDGC tag, and the equipment used for copy detection of CDGC tag is an ordinary scanner. Two examples of CDGC are copy sensitive pattern (CDP) [23] and two-level quick response codes (2LQR codes) [24–26]. Compared to CDP, 2LQR codes have higher data capacity and are compatible with ordinary quick response code (QR code) readers. Therefore, the 2LQR code is a promising technology to solve the problem of anti-counterfeiting in the traceability system, because a 2LQR code is non-cloneable, easy to check, useable by consumers, etc., which are part of the characteristics of ideal anti-counterfeit technology [17]. However, at present, there is no public work to integrate the 2LQR code into the existing traceability system. In addition, the difference between an authentic 2LQR code and its cloned version is tiny [24] during copy detection, which makes the accuracy and robustness of copy detection inferior.

In this paper, we try to solve the safety and quality of the product by integrating an anti-counterfeiting technique (copy detection with 2LQR codes) into the traceability system. Our main contributions are as follows:

- An anti-counterfeiting architecture for traceability systems based on 2LQR codes is proposed to solve the anti-counterfeiting problem in the traceability system. The risk of counterfeiting in the supply chain of the product is analyzed, and the corresponding requirements for the tags, packages, and traceability system are given to eliminate these risks. Based on the analysis above, an anti-counterfeiting architecture for traceability systems based on 2LQR codes is proposed, where the problem of counterfeit detection for the product is transformed into the problem of copy detection for the 2LQR code tag.
- According to the characteristics of the traceability system, the generation progress of the 2LQR code is modified, and there is a corresponding improved algorithm to estimate the actual location of patterns in the scanned image of the modified 2LQR code tag to improve the performance of copy detection.
- A prototype system based on the proposed architecture is implemented, where the consumers can perform traceability information queries by scanning the 2LQR code on the product package with any QR code reader. They can also scan the 2LQR code with a home-scanner or office-scanner, and send the scanned image to the system to perform counterfeit detection.

2. Materials and Methods

A typical product life cycle, as shown in Figure 2, includes production, packing, warehousing, transportation, and consumption. Participants throughout the product life cycle in the supply chain include producers, distributors, retailers, and customers [15]. The traceability system collects data throughout the product life cycle in each stage of the supply chain and provides query service to consumers.

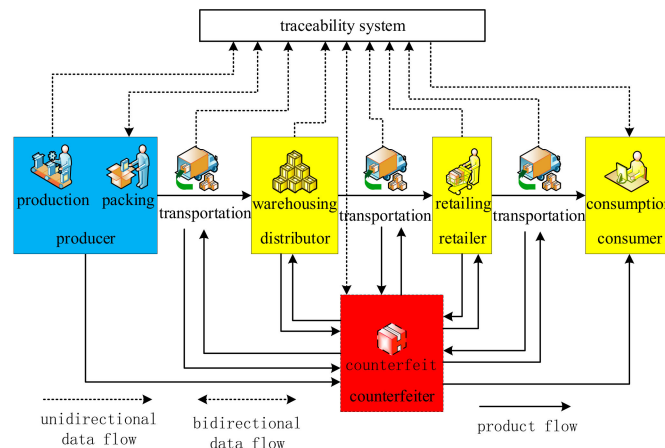


Figure 2. A typical product life cycle and counterfeiting analysis in the supply chain.

- Production is the progress to make new products. For industry, it refers to the manufacturing process. For plant agriculture, it refers to the process of planting and harvesting. For animal husbandry, it refers to breeding and slaughtering. The information about the production progress is usually collected with IoT technology [27].
- Packing is the process to make products into separate trading units, which are usually contained in the packages. The trading units are usually called TRUs in the traceability system, where a unique product identifier (product ID) is assigned to each TRU. The product ID is indexed to all data about the product in the system, such as packing time, packing location, etc. The product ID is then stored into a tag that will be attached to the product. The ID tag connects the products in the physical world with the data in the system. The most used tags are two-dimensional barcodes (2D barcodes) and RFIDs.
- Transportation is the process where the products are transported from one participant to the next. It is usually performed by a producer, distributor, or retailer. The data about the transportation is collected and stored in the traceability system.
- Warehousing is the process of temporary or long-term storage of a product, which is usually done by a distributor. The data about the warehouse is collected and stored in the traceability system.
- Retailing is the process that the product reaching consumers, through either online or offline shopping. The data about the retailing is collected and stored in the traceability system.
- In the consumption stage, the consumer can scan the ID tag attached to the product to query the traceability information.

2.1. Counterfeiting Analysis and Requirements of the Tags, Packages, and System

In this subsection, we consider the counterfeiting that occurs after the product is sent out by the producer. As shown in Figure 2, the participants in the yellow box, that is, the distributor, retailer, and even consumer, are potential counterfeiters. The counterfeiter (red dashed box) may get authentic products from the producer, distributor, and retailer, and then send the counterfeit products to the distributor, retailer, and consumer. What's more, they may have access to a part of the traceability system, such as uploading transportation information, warehousing information, retailing information, and querying traceability

information of products. From the point of view of whether products, packages, and tags have been tampered with, counterfeiting can be divided into the following categories:

- Recycled package: The packages of authentic products are reused to pack the counterfeit products. In this case, the packages, as well as the ID tags, are authentic.
- Recycled ID tag: The ID tags of authentic products are removed from the original packages and reattached to counterfeit packages. In this case, only the ID tags are authentic.
- Cloned ID tag: The ID tags are physically cloned and attached to counterfeit packages. In this case, the ID tags, the packages, and the products are counterfeit though the IDs stored in the ID tags are authentic.
- Forged ID tag: The Counterfeiter generates IDs and then makes them into forged ID tags. In this case, the ID tags as well as the IDs stored in them, the packages, and the products are counterfeit.

To deceive the traceability system, the counterfeiter need only replace the authentic products with the counterfeit ones for the case of the recycled package, recycled ID tag, and cloned ID tag. For the last case, that is, the forged ID tag, the counterfeiter must have sufficient knowledge about how to generate qualified IDs and have access to upload producing and packing information linked to the forged ID.

Therefore, to prevent the above counterfeiting, the traceability and anti-counterfeiting system architecture must meet the following requirement:

- The package must be tamper-evident. Then the consumer can easily tell whether it has been opened.
- The ID tag must be reused-prevented. It will be destroyed once you try to remove it from the original package.
- The ID tag must be clone-detectable. When it is physically cloned, we can distinguish the cloned one from the original one.
- The ID assignment of the system must keep secret from any potential counterfeiter.

For the first requirement, traditional tamper-evident packing technology, such as film wrappers, shrinkable seals, and bands, can be used.

The second and third requirements are the difficulties and emphases of the system. The commonly used 2D barcodes are easy to be cloned. Although there are techniques, such as material ink [28] and secured tag [20], can prevent the code to be cloned, they can only be applied to specific products. It is complicated to prevent the reused of RFID tags. Furthermore, most RFID tags in use can be cloned because they do not have the physical unclonable function [16] (PUF) embedded. The 2LQR code [25], which is designed to increase the capacity and security of the QR code and can be used for document authentication [26], is a promising solution. If it is printed on a void sticker [29] or fragile label, the 2LQR code tag can be both clone-detectable and reused-prevented. However, as a new emerging technology, the performance of 2LQR code in copy detection needs to be improved. The improvement of the 2LQR code will be discussed later in this paper.

The last requirement is easy to meet by restricting access to the ID assignment to those who are trusted.

2.2. Architecture of the System

The anti-counterfeiting architecture for traceability systems based on 2LQR codes is shown in Figure 3, which is divided into four layers: database, back end, front end, and device. On the database and back end layers, the white solid boxes are submodules of a basic traceability system, and the blue dashed boxes are submodules for anti-counterfeiting.

- Database layer: The traceability database stores traceability information of products throughout all their life cycle, and the anti-counterfeiting database stores information for counterfeit detection, such as product status, parameters of the clone-detectable ID tags, etc. The implementation of the databases can be traditional central database, or distributed ledger technologies (DLT) such as blockchain [30].

- Back end layer: There are three modules, ID assignment, data collection, and information query. The ID assignment module generates the product ID as well as the corresponding 2LQR tag for every new product in the packing stage. The ID and the information about the corresponding product are then stored in the traceability database. The parameters for the 2LQR tag are stored in the anti-counterfeiting database. As mentioned in the previous subsection, the ID assignment module can only be accessed by the producer. The data collection module collect data in the stages of production, packing, warehousing, transportation, retailing, and stores the data in the traceability database. Besides, the status about which stage the product is undertaken is stored in the anti-counterfeiting database. The information query module provides query services for consumers, including traceability information and counterfeit detection.
- Front end layer: Provides an operation interface for back end modules. For the ID assignment module and data collection module, a web page and client software for personal computers (PCs) are provided. For the information query module, web page as well as mobile application software (APP), such as iOS APP, Android APP, can be provided.
- Device layer: In the production and packing stage, the producer uses a web page or client software on PC to assign IDs to each product, print the corresponding 2LQR tag with a printer, and attaches it to the product. Besides this, the production and packing information is uploaded to the traceability database. In the warehousing, transportation, and retailing stage, the distributor or retailer can use any QR code scanner or reader to get the product ID and update the corresponding information to the traceability database. In the consumption stage, the consumer can use a mobile phone with a camera to scan the 2LQR tag for traceability information queries. The consumer can also use a home or office scanner to scan the 2LQR tag with specific parameters and send the scanned image to the counterfeit detection submodule for counterfeit detection.

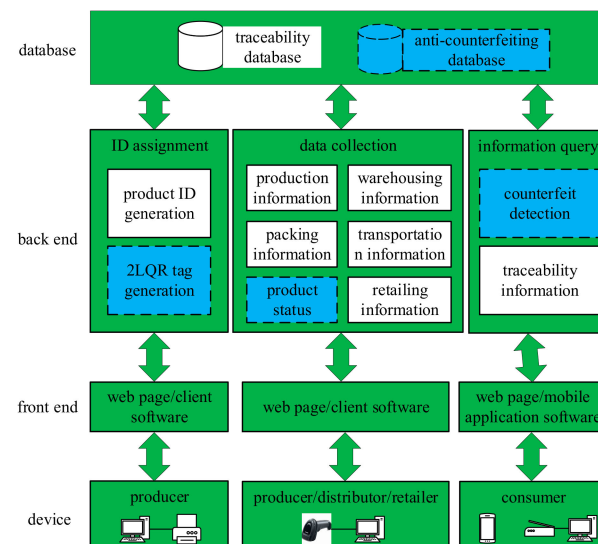


Figure 3. The anti-counterfeiting architecture for traceability system based on 2LQR codes. The white solid boxes are submodules of a basic traceability system. The blue dashed boxes are submodules for anti-counterfeiting.

At present, the packaging of most products on the market is sealed. Therefore, is reasonable to assume that the package for each TRU is sealed with tamper-evident packing technology and the tag cannot be removed from the package without damaging it. As a result, the TRU, the package, and the tag are one-to-one and cannot be separated without

being discovered. Therefore, the counterfeit detection of the product is simply the copy detection of the 2LQR code tag on its package.

As the two most important modules of the system, the 2LQR code generation, and counterfeit detection module are described in detail in the following subsections.

2.3. Implementation of the 2LQR Tag Generation Submodule

In this subsection, the 2LQR code and physical cloning process are introduced. Then the modification of the 2LQR code is made according to the requirement of the traceability system for better performance in copy detection.

2.3.1. The 2LQR Codes and Physically Clone Process

2LQR codes are QR codes where dark modules are replaced with specific textured patterns that are sensitive to the P&S process [25]. 2LQR codes are originally designed to improve the storage capacity of QR codes [25] and perform document authentication [26]. Document authentication is to detect whether the document is physically cloned or not. Therefore, document authentication is also called copy detection. Suppose that there are q original patterns $P_i, i = 1, 2, \dots, q$, and the corresponding P&S degraded versions are $S_i, i = 1, 2, \dots, q$, the correlation between the original and degraded patterns $\text{corr}(S_i, P_j)$ satisfies [26]

$$\forall i, j \in [1, q], \text{corr}(P_i, S_i) - \max_{i \neq j}(\text{corr}(P_i, S_j)) \geq \varepsilon \tag{1}$$

Suppose that P_i and S_i are $m \times n$ matrices, i.e., $P_i = P_i(r, c), S_i = S_i(r, c), r = 1, 2, \dots, m, c = 1, 2, \dots, n$, the correlation between them is

$$\text{corr}(P_i, S_i) = \frac{\sum_{r,c}(P_i(r, c) - \mu_P)(S_i(r, c) - \mu_S)}{\sqrt{\sum_{r,c}(P_i(r, c) - \mu_P)^2} \sqrt{\sum_{r,c}(S_i(r, c) - \mu_S)^2}}, \tag{2}$$

where $\mu_P = \frac{1}{nm} \sum_{r,c} P_i(r, c)$ and $\mu_S = \frac{1}{nm} \sum_{r,c} S_i(r, c)$ are the mean value of $P_i(r, c)$ and $S_i(r, c)$, respectively.

An example of a 2LQR code for copy detection is shown in Figure 4. Except for modules in the three finder patterns, all black modules are replaced with textured patterns. The textured patterns used in Figure 4 are shown in Figure 5. The size of the textured patterns, which are the same as that of modules in the QR code image, is 12×12 pixels, and each pixel is black or white.

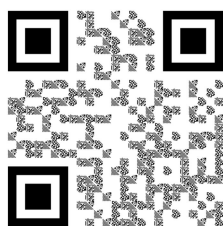


Figure 4. An example of a 2LQR code for copy detection.

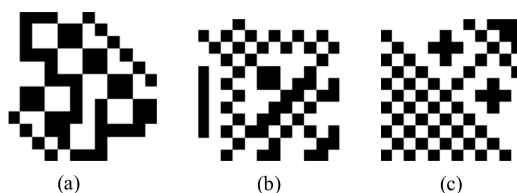


Figure 5. An example of textured patterns used in 2LQR codes. There are three classes of textured patterns here. (a) The first class of textured pattern P_1 . (b) The second class of textured pattern P_2 . (c) The third class of textured pattern P_3 .

The copy detection of 2LQR makes use of the fact that the counterfeiter does not have access to the original patterns P_i [26] and it is impossible to recover the original patterns P_i from its P&S degraded version S_i because the P&S process can be considered as a PUF [31].

The physical cloning (or copy) process of a 2LQR code and a textured pattern is shown in Figure 6. The original image of the 2LQR code I_0 is a digital image generated with a program. The textured patterns $P_i^{(0)} = P_i, i = 1, 2, \dots, q$ in I_0 is an ideal binary image. Then the original image is printed to make a tag, expressed by I_{P0} , which is an analog image in the physical world. The textured patterns $P_i^{(P0)}, i = 1, 2, \dots, q$ in I_{P0} is blurred because of the degradation caused by the printer. We call I_{P0} an authentic tag because it is the printed version of the original image. Then I_{P0} is scanned with a scanner to get a digital image I_1 , which is called the P&S version of I_0 . The textured patterns $P_i^{(1)} = S_i, i = 1, 2, \dots, q$ in I_1 correspond with the P&S versions of $P_i^{(0)}$. The process to get I_1 from I_0 is a P&S process in which the input and output are both digital images. The counterfeiters, who have only access to I_{P0} and I_1 , want to make a counterfeit of the authentic tag I_{P0} . They print I_1 to get a counterfeit tag I_{P1} . The process to make a counterfeit tag I_{P1} from the authentic tag I_{P0} is physical cloning (or copy). The pattern in I_{P0} is further degraded. The counterfeit tag I_{P1} is scanned with scanner to get a digital image I_2 , which is the P&S version of I_1 .

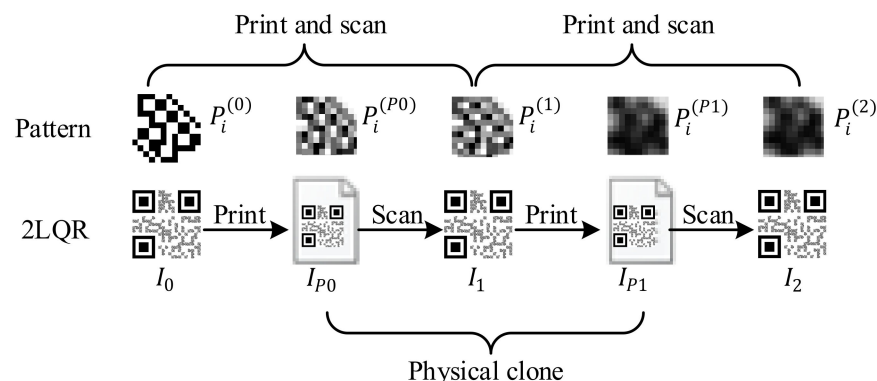


Figure 6. The physical cloning process of a 2LQR code and a textured pattern.

Copy detection is to distinguish between the authentic tag I_{P0} and the counterfeit tag I_{P1} . However, the program can only process digital images. Therefore, the copy detection program is actually to distinguish their scanned versions, that is, I_1 and I_2 . Copy detection of 2LQR codes is based on the information loss principle, that is, every time an image is printed or scanned, some information is lost about the original digital image [24]. The correlation coefficient (or correlation) is an indicator to describe the information loss. The following proposition has been proved in [32]:

- The correlation between textured patterns in I_0 and I_1 is greater than the correlation between textured patterns in I_0 and I_2 , i.e., $\text{corr}(P_i^{(0)}, P_i^{(1)}) > \text{corr}(P_i^{(0)}, P_i^{(2)})$, $i = 1, 2, \dots, q$. More generally, suppose that the k -th P&S version of P_i is $P_i^{(k)}$, $k = 0, 1, 2, \dots$, this proposition is generalized as $\text{corr}(P_i^{(0)}, P_i^{(k)}) > \text{corr}(P_i^{(0)}, P_i^{(k+1)})$, $i = 1, 2, \dots, q, k = 0, 1, 2, \dots$.

The proposition describes the loss of information in the P&S process. The original pattern is used as a reference to measure information loss, as the copy detection program of 2LQR codes does. However, the textured patterns $P_i^{(0)}$ should not be accessible to potential counterfeiters. Therefore, the copy detection program of 2LQR codes should be run in a relatively safe environment, such as the servers where the traceability system is deployed. That is to say, the customer scans the 2LQR image and sends it to the traceability system. Then the system carries out the copy detection and returns the result back to the customer.

2.3.2. Modification of 2LQR Code Generation Process

The 2LQR code generation includes three steps: public message encoding, private message encoding, and replacing black modules in the QR code with textured patterns [25]. The public message is encoded into the QR code directly and can be retrieved with any QR code reader, whereas the private message is scrambled with a key after it is encoded with an error correction code and must be captured with a scanner instead of a camera. However, in the traceability system, the ID tag only needs to store the product ID and the private message is not needed. Therefore, we record the locations of textured patterns instead of the private message encoding step.

The generation of the modified 2LQR code tags is shown in Figure 7. Firstly, the identifier ID for a TRU are generated by the traceability system. Then the producer generates a QR code that stores the ID . The black modules in the QR code are replaced with textured patterns $P_i, i = 1, 2, \dots, q$ to get a 2LQR code. Usually, the patterns P_i are predetermined with a corresponding threshold TH used for copy detection. More details about the threshold can be found in [25]. The replace scheme is about replacing the black modules with P_i . Since we do not need to store information in the private storage level of 2LQR code as in [24–26], we can replace the black modules randomly with textured patterns, or just simply replace all the black modules with P_i in order of $P_1, P_2, \dots, P_q, P_1, \dots$. The patterns, the threshold, and the replace scheme are then stored to the traceability system. The generated 2LQR code is an image that is called an original image. At last, the 2LQR code is printed on paper or other material to make a tag. The tag, also called the authentic tag, is the printed version of the original image. The parameters of tag printing, such as printing resolution, are also stored in the system.

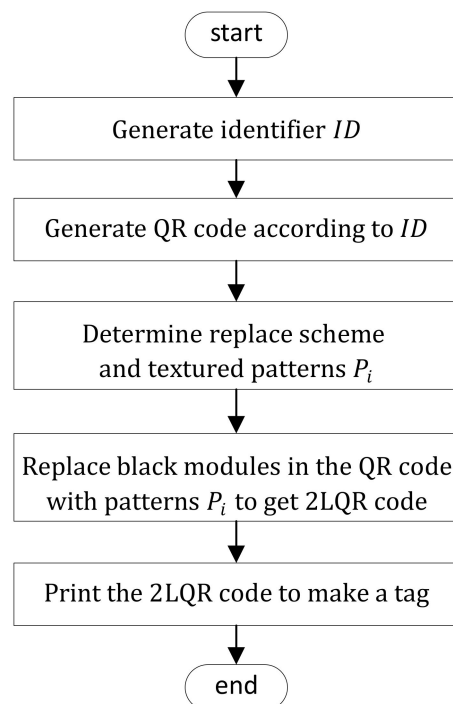


Figure 7. Generation process of the modified 2LQR code tag.

2.4. Implementation of Counterfeit Detection Submodule

As mentioned above, the counterfeit detection of a product is the copy detection of the 2LQR code tag in this system. Therefore, a copy detection process of the modified 2LQR code tag is introduced here. Making use of the fact that the locations of textured patterns are recorded, an improved algorithm to estimate the actual location of patterns in the scanned image is proposed.

2.4.1. Copy Detection Process of the Modified 2LQR Code Tag

The copy detection process for the modified 2LQR code tag is shown in Figure 8. Firstly, the identifier ID is extracted using a QR code reader. Then the printing parameters (such as printing resolution) are queried from the system with ID . The 2LQR code tag is then scanned using a scanner with the same resolution as the printing. The test 2LQR code image I_t is extracted from the scanned image. The authentic indicator $\text{ind}(I_t)$ of I_t is calculated after the textured patterns P_i with corresponding threshold TH , the replace scheme are queried from the system. The indicator $\text{ind}(I_t)$ is the mean value of all correlations between patterns in I_0 and the corresponding patterns in the same location of I_t [26]. The correlations between patterns are calculated with Equation (2). If the indicator is not less than TH , the tag is considered to be authentic. Otherwise, the tag is considered to be an illegal copy.

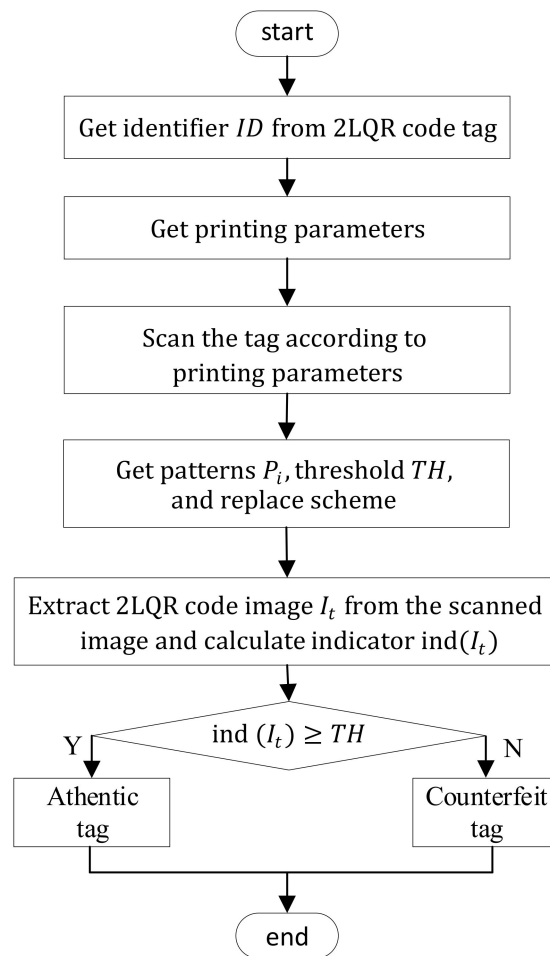


Figure 8. Copy detection progress for 2LQR code tag.

2.4.2. An Improved Algorithm to Estimate the Actual Location of Patterns

The accuracy of locations of patterns in the scanned image I_t is very important to calculate $\text{ind}(I_t)$. In [26] the locations of patterns are determined using the reference decode algorithm for QR code [33], and the detected patterns are classified into q classes $P_i, i = 1, 2, \dots, q$ using pattern recognition algorithm. There are two problems with the method above. Firstly, local distortion of the 2LQR image, which is very common and can affect the accuracy of pattern location, is not handled by the reference decode algorithm. Secondly, the accuracy of the pattern recognition algorithm in [26] is not 100%, resulting in the wrong correspondence between some detected patterns and their original patterns. The two problems make the indicator $\text{ind}(I_t)$ for authentic tag decrease and reduce the

accuracy of copy detection. Therefore, we proposed an improved algorithm to estimate the actual location of patterns.

Instead of recognizing each pattern in the test 2LQR image I_t , we store the ideal locations of each class of patterns P_i in the system. For example, the ideal locations (coordinates of the upper left of the patterns) of the first class of patterns P_1 in the 2LQR code in Figure 4 are $(96, 0), (168, 0), (180, 12), \dots$, where the origin $(0, 0)$ is on the upper left corner of the 2LQR code, and the positive direction of the y axis is downward.

Assume that there are N patterns in I_t , expressed by $SP_j, j = 1, 2, \dots, N$, their corresponding original patterns are $OP_j \in \{P_i, i = 1, 2, \dots, Q\}, j = 1, 2, \dots, N$, respectively, and their ideal coordinates of the upper left are $(x_j, y_j), j = 1, 2, \dots, N$, respectively. Set the width and height of the original patterns are w and h , respectively. The key schematic of the process of estimating the actual locations of the patterns is shown in Figure 9, where the same 2LQR code as in Figure 4 is used, that is, $Q = 3$.

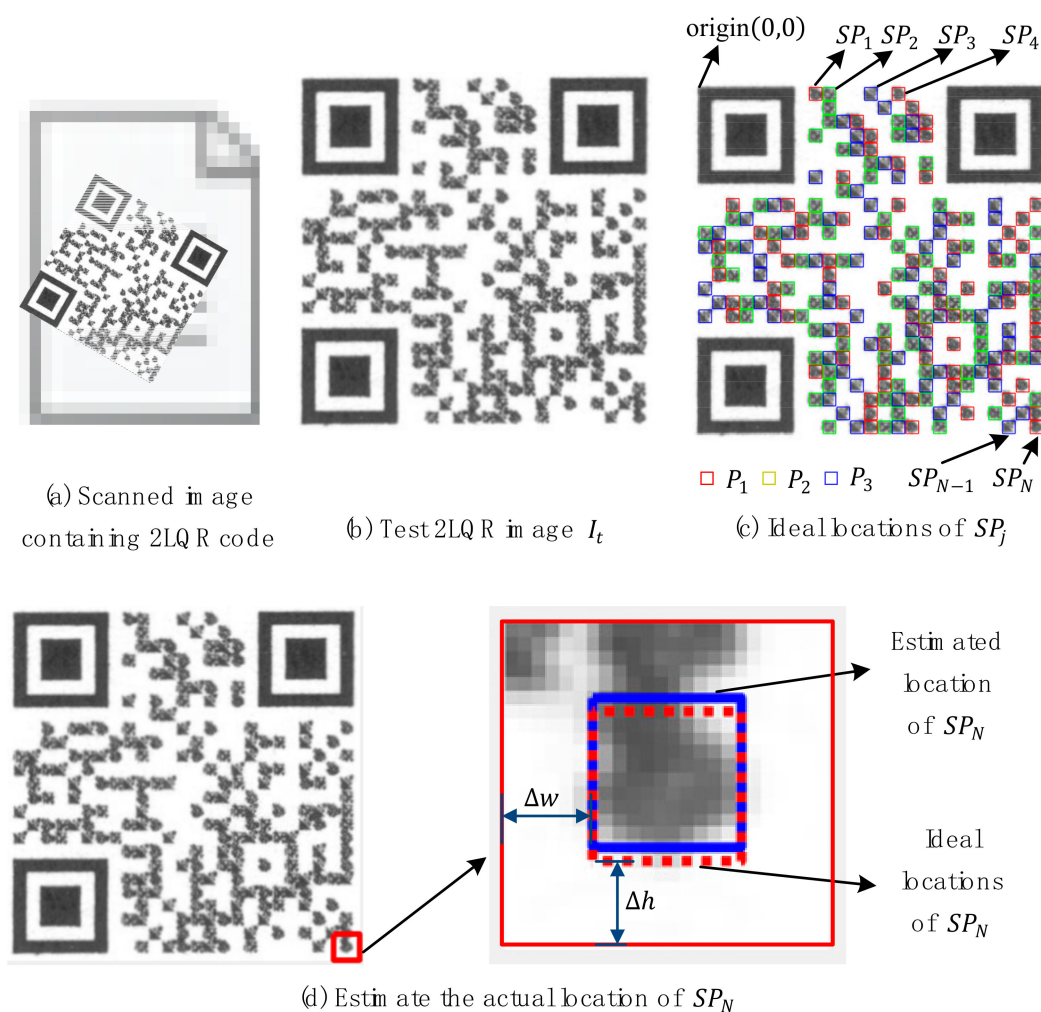


Figure 9. Key schematic of the process of estimating the actual locations of the patterns.

Firstly, the 2LQR code tag is scanned and an image containing the 2LQR is obtained, as shown in Figure 9a.

Secondly, the reference decode algorithm for QR code [33] is used to process the scanned image. In this step, the geometric deformation is corrected and the 2LQR code is rotated to a specific direction, that is, the three finder patterns are in the lower left, upper left, and upper right, respectively. Besides, the 2LQR code is resized to the same size as its original image, resulting in the test image I_t , as shown in Figure 9b.

The ideal locations of all patterns that were queried from the traceability system are shown in Figure 9c, where the original patterns of detected patterns SP_i , in red, green, blue boxes are P_1, P_2, P_3 , respectively.

For each detected pattern SP_j , the estimated location of it is searched within the neighborhood of its ideal location, as shown in Figure 9d. The solid red box is the neighborhood of the ideal location of the last detected pattern SP_j , where $j = N$ in the case in Figure 9d. Set the distance between the edges of the dotted red box and solid red box in horizontal and vertical are Δw and Δh , respectively. The coordinate of upper left of the neighborhood of each detected pattern SP_j is $(x_j - \Delta w, y_j - \Delta h)$. The width and height of them is $w + 2\Delta w$ and $h + 2\Delta h$, respectively. The estimated location of SP_j is

$$(\hat{x}, \hat{y}) = \arg \max_{\substack{x_j - \Delta w \leq x \leq x_j + \Delta w \\ y_j - \Delta h \leq y \leq y_j + \Delta h}} \left(\text{corr} \left(OP_j, SP_j^{(x,y)} \right) \right), \tag{3}$$

where $SP_j^{(x,y)}$ is the detected pattern SP_j when its location is (x, y) .

Obviously, the correlation between the original pattern OP_j and the detected pattern in the estimated location $SP_j^{(\hat{x}, \hat{y})}$ is not less than the correlation between the original pattern OP_j and the detected pattern in the ideal location $SP_j^{(x_j, y_j)}$, i.e.,

$$\text{corr} \left(OP_j, SP_j^{(\hat{x}, \hat{y})} \right) \geq \text{corr} \left(OP_j, SP_j^{(x_j, y_j)} \right). \tag{4}$$

Because all patterns satisfy Equation (1), the algorithm above can find the exact location of the patterns in large probability and improve the accuracy of $\text{ind}(I_t)$, which will increase the accuracy of copy detection for the 2LQR code tag.

Now we discuss the complexity of the proposed algorithm. For each pattern, there are $(2\Delta w + 1) \times (2\Delta h + 1)$ correlations to be calculated and compared, as shown in Equation (3). According to Equation (2), $m \times n$ loops are needed to calculate a correlation between two $m \times n$ patterns. Therefore, the overall complexity for the proposed location estimation algorithm is $O(Nmn(2\Delta w + 1)(2\Delta h + 1)) = O(Nmn\Delta w\Delta h)$, where N is the number of patterns in a 2LQR code tag.

2.4.3. Calculation of Threshold for Copy Detection

Ideally, the threshold TH is calculated with all the scanned images of the authentic and counterfeited 2LQR code tags. However, it is impossible to get all counterfeited 2LQR code tags. What is more, in practical application, the number of authentic 2LQR code tags is usually large and it is not practical to scan all the authentic 2LQR code tags by the producer. Therefore, a compromise is to use a small part of the authentic and counterfeited 2LQR code tags to calculate the threshold TH .

Suppose that the scanned image of the authentic and counterfeited 2LQR code tags are $I_{t,i}, i = 1, 2, \dots, N_{t1}$ and $I_{t,j}, i = 1, 2, \dots, N_{t2}$, respectively, where N_{t1} and N_{t2} are the number of authentic and counterfeited 2LQR code tags. The threshold TH is

$$TH = \frac{\sum_{i=1}^{N_{t1}} \text{ind}(I_{t,i})}{N_{t1}} + \frac{\sum_{j=1}^{N_{t2}} \text{ind}(I_{t,j})}{N_{t2}}. \tag{5}$$

3. Results

In this section, two experiments are performed to measure the performance of the modified 2LQR code and the corresponding improved algorithm in copy detection. Then a prototype system for the proposed architecture is implemented to verify how the architecture works to fight against counterfeiting. At last, a comparison of the proposed architecture and other solutions, such as RFID based solutions, is made, which shows that

counterfeit detection using 2LQR code has the advantages of low cost, high reliability, and high usability.

3.1. Performance of the Modified 2LQR Code and the Corresponding Improved Algorithm

To measure the performance of the modified 2LQR code in copy detection and the improved algorithm to estimate the actual location of patterns, 120 2LQR codes with random content were generated with the algorithm described in Figure 7 and printed to make 120 authentic tags with printer HP LaserJet Pro M126 MFP. Then the tags were copied to make 120 counterfeit tags with HP Color LaserJet Pro MFP M377. The print and copy processes were both performed with a 600-dpi resolution. There were 240 2LQR code tags in total to be tested. The paper used to make the tags in the above process was A4 printer paper. The algorithm was implemented using MATLAB R2019a and ran on HP Z230 Tower Workstation with an Intel Xeon E3-1246 v3 processor and 8 GB memory.

In the first experiment, we scanned the tags using the same machine as the printing machine, that is, HP LaserJet Pro M126 MFP. Then the copy detection process described in Figure 8 is performed. This experiment is similar to that in [26], as shown in Figure 10.

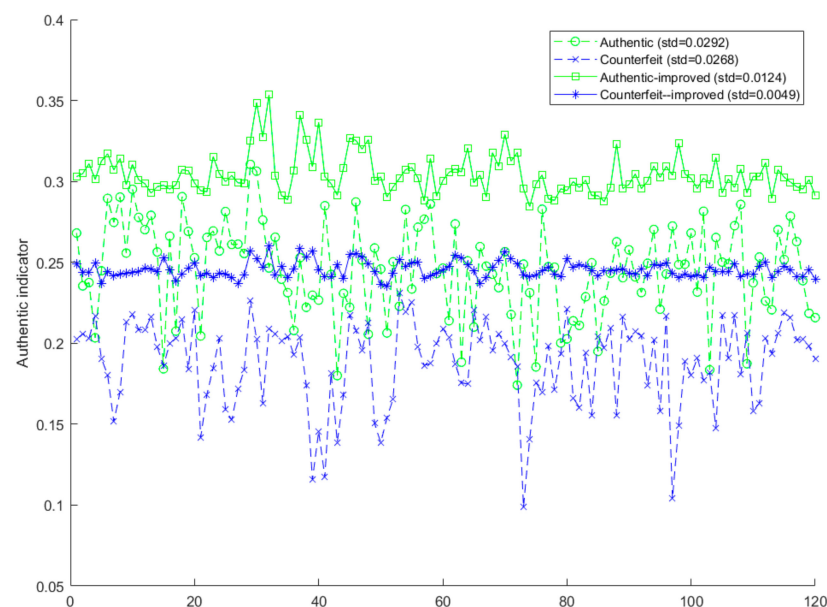


Figure 10. Authenticity indicators for authentic and counterfeit 2LQR code tag images scanned with HP LaserJet Pro M126 MFP. The plus sign and square are authenticity indicators for authentic and counterfeit 2LQR code tag images without the improved algorithm, respectively. The circle and asterisk are authenticity indicators for authentic and counterfeit 2LQR code tag images with the improved algorithm, respectively.

Without the improved algorithm to estimate the actual location of patterns, the authenticity indicators for authentic and counterfeit 2LQR code tag images overlap seriously in some areas, such as data points around 20, 50, etc. When the improved algorithm is applied, the authenticity indicators increase for both authentic and counterfeit 2LQR code tag images. However, the standard deviation of indicators for authentic and counterfeit 2LQR code tag images decreases by 57.53% and 81.72%, respectively, which means that the improved algorithm improves the robustness of copy detection. Therefore, it is easy to distinguish between them according to the authenticity indicators.

The average runtimes to calculate authenticity indicators for a single 2LQR code tag with and without the improved algorithm are 0.0754 s and 1.8203 s, respectively. The runtime overhead is significant. However, compared to other steps, such as scanning the tag, which usually needs tens of seconds, a few seconds runtime overhead is acceptable.

To perform copy detection, we select three sets of scanned images to calculate the threshold TH with Equation (5). The first set includes all the 240 authentic and counterfeited 2LQR code tags. The second set includes 10 tags randomly selected from the 120 authentic tags and 10 tags randomly selected from the 120 counterfeited tags. The three sets include the first 10 tags of the 120 authentic tags and the first 10 tags of the 120 counterfeited tags. The thresholds calculated with the three sets of data before the improved algorithm applied are $TH_1 = 0.2167$, $TH_2 = 0.2084$, $TH_3 = 0.2273$, respectively. After the improved algorithm applied, the thresholds are $TH'_1 = 0.2750$, $TH'_2 = 0.2739$, $TH'_3 = 0.2759$, respectively. It is clear that the difference of thresholds calculated with the different sets of images is very small.

Without the improved algorithm, the accuracies of copy detection are 84.61%, 81.25%, 98.89%, respectively, when $TH = TH_1$, $TH = TH_2$, $TH = TH_3$, respectively. After the improved algorithm applied, the threshold, the accuracies of copy detection are 100%, 100%, 100%, respectively, when $TH = TH'_1$, $TH = TH'_2$, $TH = TH'_3$, respectively. Obviously, a small error of threshold will affect the accuracy of copy detection significantly, whereas when the improved algorithm is applied, the accuracy is unchanged when the threshold varies. This means that the proposed algorithm improves both the accuracy and robustness of copy detection.

In the second experiment, we scanned the tags using the same machine as the copy machine, that is, HP Color LaserJet Pro MFP M377. The results are shown in Figure 11. The standard deviation of indicators for authentic and counterfeit 2LQR code tag images decrease by 64.46% and 80.65%, respectively, which is similar to the results in the first experiment.

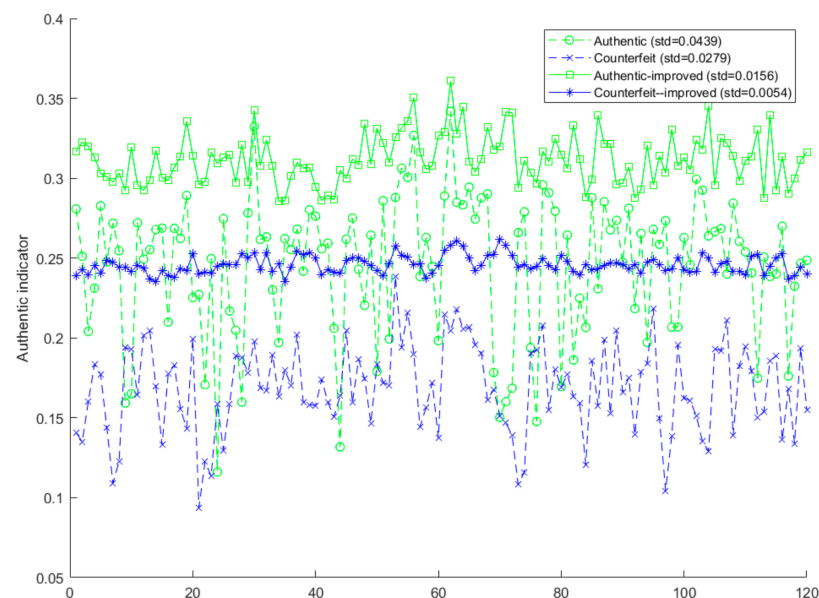


Figure 11. Authenticity indicators for authentic and counterfeit 2LQR code tag images scanned with HP Color LaserJet Pro MFP M377. The plus sign and square are authenticity indicators for authentic and counterfeit 2LQR code tag images without the improved algorithm, respectively. The circle and asterisk are authenticity indicators for authentic and counterfeit 2LQR code tag images with the improved algorithm, respectively.

Using the same thresholds calculated in the first experiment to perform copy detection, the accuracies before and after the improved algorithm is applied are 96.84%, 93.94%, 98.85% and 100%, 100%, 100%, respectively, which is very similar to that in the first experiment.

The average runtimes to calculate authenticity indicators for a single 2LQR code tag with and without the improved algorithm are 0.0754 s and 1.8163 s, respectively, which is very similar to that in the first experiment.

The two experiments have shown that:

- The improved algorithm can increase the accuracy of copy detection for 2LQR code to 100% with lesser standard deviation of indicators, meaning that the improved algorithm improves the robustness of copy detection.
- The scanner used for copy detection has little effect on the accuracy of copy detection for 2LQR code.

3.2. Comparison of 2LQR Code with Other Barcodes

Originally, barcodes do not have the feature of copy detection. However, there are researches on the copy detection of 2D barcodes in recent years. To compare the performance of copy detection for different barcodes, the normalized accuracy (NACC) [34] is used:

$$\text{NACC} = 1 - \frac{(FAR + FRR)}{2}, \quad (6)$$

where *FAR* is the percentage of counterfeited samples that have been falsely accepted as genuine, *FRR* is the percentage of genuine samples that have been falsely accepted as counterfeit.

We used the data samples of the first experiment in Section 3.1 to calculate *FAR*, *FRR*, and NACC of 2LQR codes and modified 2LQR codes (the improved algorithm is applied) with different thresholds, as shown in Table 1, where the performance of DFT-based, LBP-based, and DFT+LBP-based barcodes proposed in [34] are also listed.

Table 1. Performance of different barcodes in copy detection.

Barcode	<i>FAR</i>	<i>FRR</i>	NACC
DFT-based [34]	2.36%	5.00%	96.32%
LBP-based [34]	0.64%	10.83%	94.27%
DFT+LBP-based [34]	0.00%	2.50%	98.75%
2LQR code (TH = TH_1)	11.67%	17.50%	85.42%
2LQR code (TH = TH_2)	20.00%	13.33%	83.33%
2LQR code (TH = TH_3)	0.83%	25.83%	86.67%
Modified 2LQR code (TH = TH'_1)	0.00%	0.00%	100.00%
Modified 2LQR code (TH = TH'_2)	0.00%	0.00%	100.00%
Modified 2LQR code (TH = TH'_3)	0.00%	0.00%	100.00%

Table 1 shows that the performance of DFT-based, LBP-based, and DFT+LBP-based barcodes is better than the 2LQR code because they have lower *FRR*. However, the performance of the modified 2LQR code is the best no matter which threshold is used.

3.3. The Prototype System for the Proposed Architecture and Comparison with other Solutions

To verify the anti-counterfeiting capability of the proposed architecture, a prototype system based on the architecture is implemented, as shown in Figure 12. The software platform of the prototype system is Windows 10. In the database layer, the databases are implemented with MariaDB. In the back end, the submodules for anti-counterfeiting are implemented with MATLAB and encapsulated with a windows batch file, which is called by the information query module written in PHP. The system is running on HP Z230 Tower Workstation with Intel Xeon E3-1246 v3 processor and 8 GB memory. The mobile phone used for traceability information query is iPhone XR with iOS 14.2, and the Camera application is used to scan the 2LQR code.

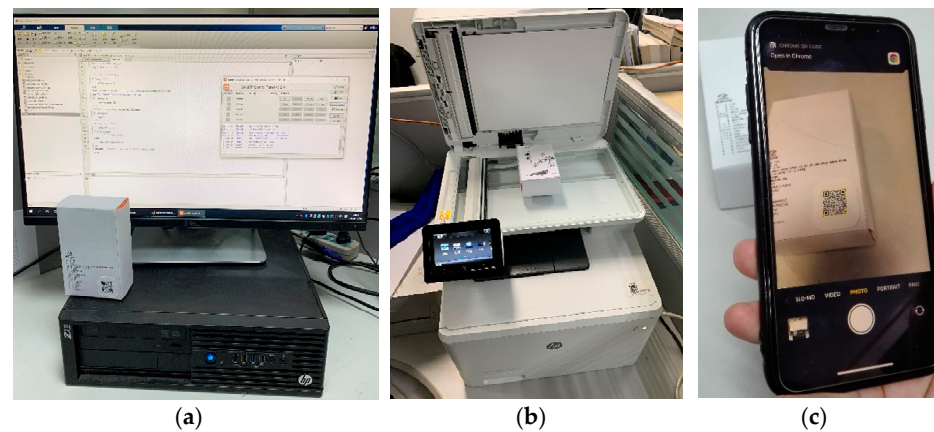


Figure 12. The prototype system. (a) The computer running the system and the product package with the 2LQR code tag attached. (b) Scan the 2LQR code tag attached to the package with a scanner. (c) Traceability information query with a mobile phone.

The tags generated in the previous subsection are used to test the prototype system. An example of the tags is shown in Figure 13, where the original image, the scanned images of the authentic and counterfeit tag are shown in (a), (b), and (c), respectively. In order to simulate the case of forged tag, we intentionally delete the data of a tag from the traceability database and anti-counterfeiting database, as shown in Figure 13d.



Figure 13. Example tags used to test the prototype system. (a) The original image of an authentic tag. (b) The scanned image of an authentic tag (printed version of image in (a)). (c) The scanned image of a counterfeit tag (cloned version of the authentic tag in (b)). (d) The scanned image of a forged tag.

3.3.1. Traceability Information Query Test

Firstly, the traceability information query of the prototype system is tested. Reading the tag with any QR code reader, such as the iPhone camera program, a web page showing the traceability information of the product is opened, as shown in Figure 14. Note that the product ID stored in the counterfeit tag is the same as that in the authentic tag. Therefore, the traceability information for the two tags is the same. Obviously, no data is shown for the forged tag because there no data in the databases that links to the forged ID.

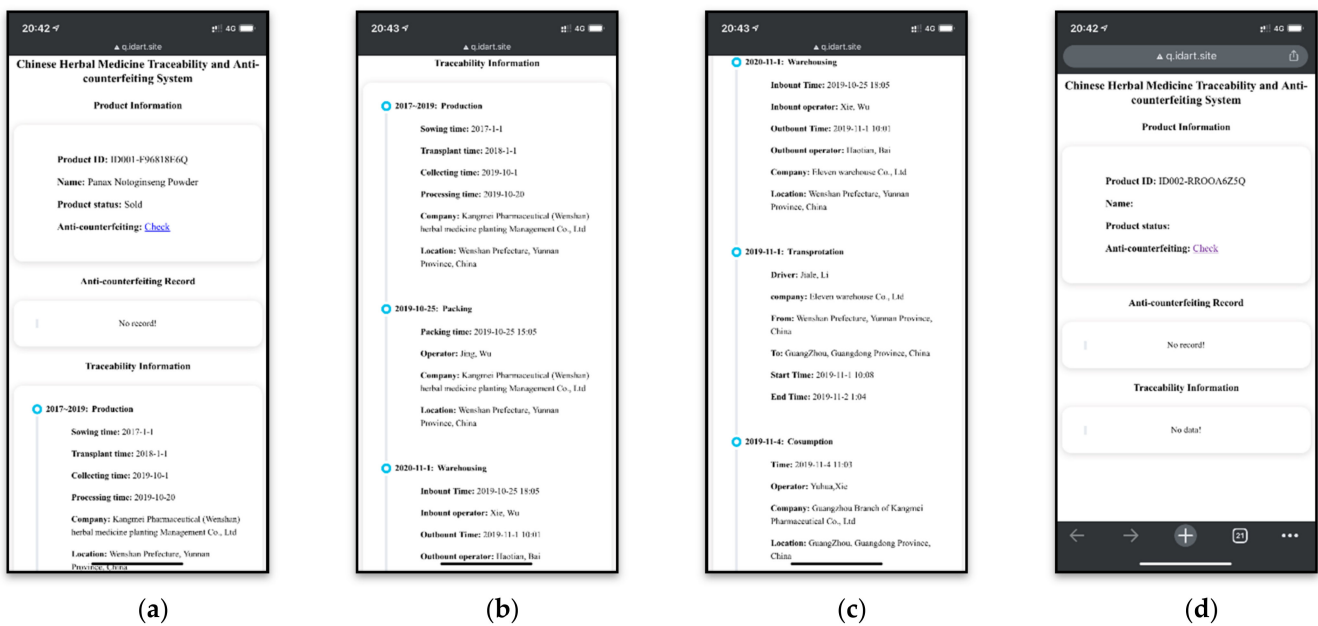


Figure 14. Traceability information query web page of the prototype system. (a–c) Traceability information for the authentic and counterfeit tag. (d) Traceability information for the forged tag.

3.3.2. Anti-Counterfeiting Test

Click the *check* button in the traceability information query web page to open the anti-counterfeiting page, as shown in Figure 15. All tags are correctly classified by the prototype system and detailed instructions are given to consumers. After anti-counterfeiting checking of the tags, all checking records are stored in the database and will be shown in the traceability information query web page, as shown in Figure 16.

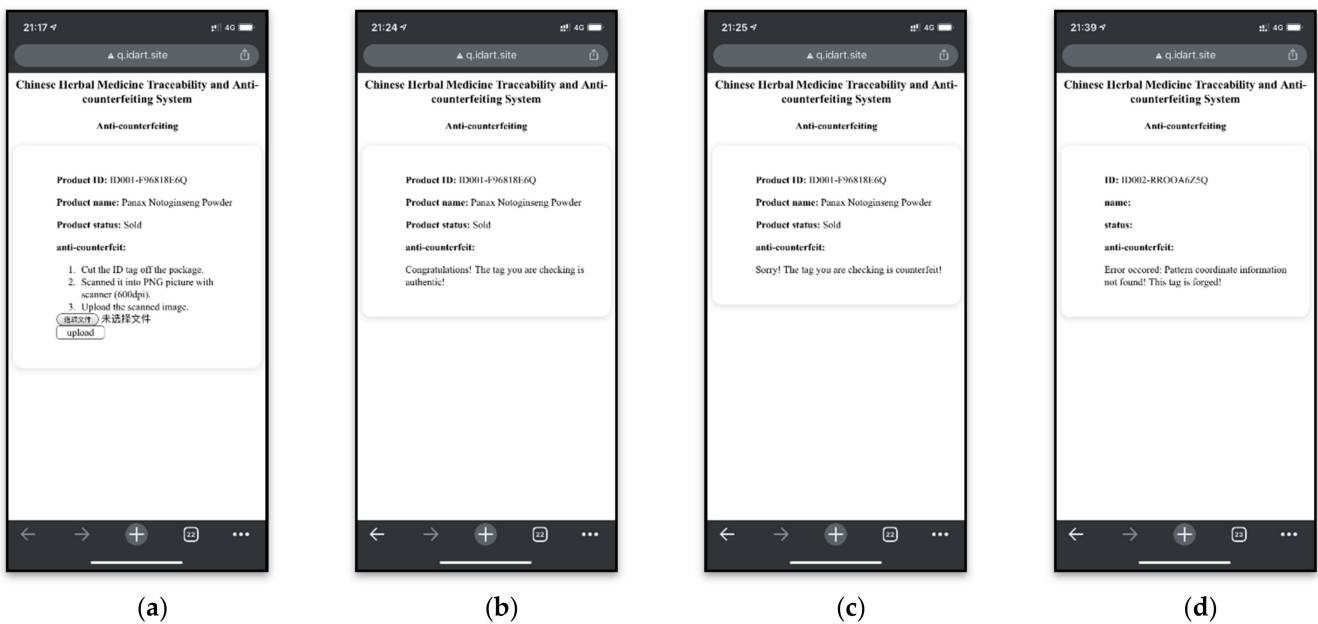


Figure 15. Anti-counterfeiting web page of the prototype system. (a) Scan image uploading page. (b–d) Anti-counterfeiting results for the authentic, counterfeit, and forged tags, respectively.

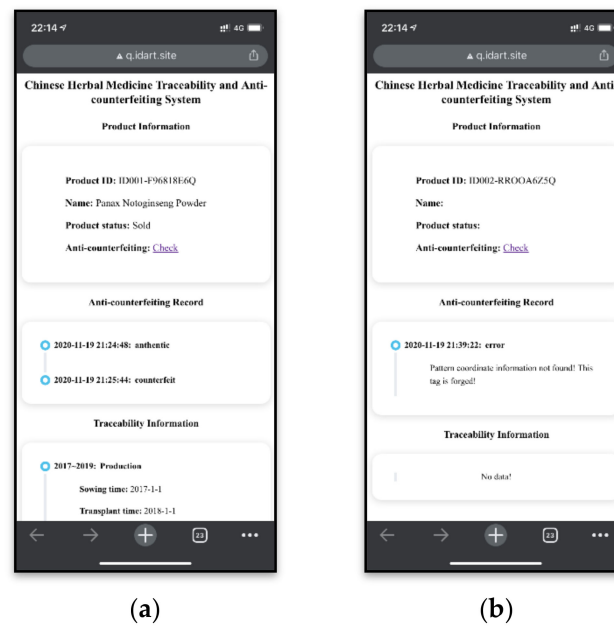


Figure 16. Anti-counterfeiting records in traceability information query web page. (a,b) Anti-counterfeiting records for the authentic (or counterfeit) tags and forged tag, respectively.

The response time of the counterfeit detection is an important index to show the efficiency of the anti-counterfeiting method. The response time mainly includes two parts: time to scan the 2LQR tag (t_{scan}) and time to upload the scanned image to get counterfeit detection result (t_{upload}). To get the response time, we scanned 10 2LQR tags and calculated the average time as the t_{scan} , and calculate the average time of uploading the 10 scanned images to get counterfeit detection results as the t_{upload} . The response times for different scanners are shown in Table 2. The response time is less than 1 minute, showing the high efficiency of the proposed method in counterfeit detection.

Table 2. The response time of the counterfeit detection.

Scanner	t_{scan} (s)	t_{upload} (s)	Response Time(s)
M126	15.88	15.19	31.07
M377	10.99	14.56	25.55

3.3.3. Comparison with Other Works

The comparison of the proposed architecture with other anti-counterfeiting solutions is shown in Table 3. We compare them in three areas, that is, application scope, cost (tag cost, reading device cost, and anti-counterfeiting device cost), and anti-counterfeiting performance (recycled package detection, recycled ID tag detection, cloned ID tag detection, and forged ID tag detection). Compared with CDTA [16] and Textile Coding Tag [21], the proposed architecture is more general and low cost. Compared with Frequent pattern mining [35] and Textile Coding Tag [21], the proposed architecture has better performance in anti-counterfeiting. Therefore, the proposed architecture is a promising solution for product anti-counterfeiting with the advantages of low cost, generality, and good performance.

Table 3. Comparison of the proposed architecture with other anti-counterfeiting solutions.

Solutions	Proposed	CDTA [16]	Frequent Pattern Mining [35]	Textile Coding Tag [21]
application scope	general	IoT devices	general	textile
tag cost	very low	very high	unknown	low
reading device	mobile phone	RFID reader	unknown	mobile phone
anti-counterfeiting device	office/home scanner	RFID reader	unknown	mobile phone
recycled package detection	yes	unknown	yes	unknown
recycled ID tag detection	yes	yes	yes	yes
cloned ID tag detection	yes	yes	no	no
forged ID tag detection	yes	yes	yes	unknown

4. Discussion and Conclusions

In this paper, the problem of product counterfeiting in its life cycle is discussed and an anti-counterfeiting system architecture for traceability based on modified 2LQR codes is proposed to solve this problem, where the problem of counterfeit detection for the product is transformed into the problem of copy detection of the 2LQR code tag. To effectively perform copy detection of 2LQR code tags, an improved algorithm is proposed to estimate the accurate location of patterns in the scanned 2LQR code image. Experiments show that the accuracy and robustness of copy detection for 2LQR codes improve when the improved algorithm is applied. Besides this, the experiments also show that the scanner used for copy detection has little effect on the accuracy of copy detection for the 2LQR code tag. Therefore, customers can use any qualified scanner to scan the 2LQR tag for copy detection. In summary, using 2LQR codes is a low-cost, reliable, and convenient solution for product counterfeit detection in traceability systems.

The prototype system of the proposed architecture proves the feasibility of the proposed architecture. Compared with other anti-counterfeiting solutions, the proposed architecture has advantages of low cost, generality, and good performance. Therefore, it is a promising solution to replace the existing anti-counterfeiting system.

However, the data samples for 2LQR codes are limited in the experiments, and more experiments to test different printers and scanners should be done in the future. Moreover, copy detecting of 2LQR codes by taking photos instead of scanning with a scanner is also an attractive research direction.

Author Contributions: Conceptualization, S.X. and H.-Z.T.; methodology, S.X.; software, S.X.; validation, S.X.; writing—Original draft preparation, S.X.; writing—Review and editing, S.X. and H.-Z.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Science and Technology Planning Project of Guangdong Province, grant number 2017B090908006.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

- Li, J.; Yu, Y.; Hu, S.; Zhang, C. An Authority Management Framework Based on Fabric and IPFS in Traceability Systems. In Proceedings of the Blockchain and Trustworthy Systems, Guangzhou, China, 7–8 December 2019; pp. 761–773.
- Aung, M.M.; Chang, Y.S. Traceability in a Food Supply Chain: Safety and Quality Perspectives. *Food Control* **2014**, *39*, 172–184. [\[CrossRef\]](#)
- Olsen, P.; Borit, M. How to Define Traceability. *Trends Food Sci. Technol.* **2013**, *29*, 142–150. [\[CrossRef\]](#)
- Olsen, P.; Borit, M. The Components of a Food Traceability System. *Trends Food Sci. Technol.* **2018**, *77*, 143–149. [\[CrossRef\]](#)
- Tian, F. A Supply Chain Traceability System for Food Safety Based on HACCP, Blockchain Internet of Things. In Proceedings of the 2017 International Conference on Service Systems and Service Management, Dalian, China, 16–18 June 2017; pp. 1–6.

6. Tian, F. An Agri-Food Supply Chain Traceability System for China Based on RFID Blockchain Technology. In Proceedings of the 2016 13th International Conference on Service Systems and Service Management (ICSSSM), Kunming, China, 24–26 June 2016; pp. 1–6.
7. Caro, M.P.; Ali, M.S.; Vecchio, M.; Giaffreda, R. Blockchain-Based Traceability in Agri-Food Supply Chain Management: A Practical Implementation. In Proceedings of the 2018 IoT Vertical and Topical Summit on Agriculture—Tuscany (IOT Tuscany), Tuscany, Italy, 8–9 May 2018; pp. 1–4.
8. Lin, J.; Shen, Z.; Zhang, A.; Chai, Y. Blockchain and IoT Based Food Traceability for Smart Agriculture. In Proceedings of the 3rd International Conference on Crowd Science and Engineering, New York, NY, USA, 28 July 2018; pp. 1–6.
9. Salah, K.; Nizamuddin, N.; Jayaraman, R.; Omar, M. Blockchain-Based Soybean Traceability in Agricultural Supply Chain. *IEEE Access* **2019**, *7*, 73295–73305. [[CrossRef](#)]
10. Eberhardt, J.; Tai, S. On or Off the Blockchain? Insights on Off-Chaining Computation and Data. In *Proceedings of the Service-Oriented and Cloud Computing, Oslo, Norway, 27–29 September 2017*; De Paoli, F., Schulte, S., Broch Johnsen, E., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 3–15.
11. Xu, X.; Lu, Q.; Liu, Y.; Zhu, L.; Yao, H.; Vasilakos, A.V. Designing Blockchain-Based Applications a Case Study for Imported Product Traceability. *Future Gener. Comput. Syst.* **2019**, *92*, 399–406. [[CrossRef](#)]
12. Xu, X.; Pautasso, C.; Zhu, L.; Gramoli, V.; Ponomarev, A.; Tran, A.B.; Chen, S. The Blockchain as a Software Connector. In Proceedings of the 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA), Venice, Italy, 5–8 April 2016; pp. 182–191.
13. Ding, Q.; Gao, S.; Zhu, J.; Yuan, C. Permissioned Blockchain-Based Double-Layer Framework for Product Traceability System. *IEEE Access* **2020**, *8*, 6209–6225. [[CrossRef](#)]
14. Schinle, M.; Erler, C.; Vetter, A.R.; Stork, W. How to Disclose Selective Information from Permissioned DLT-Based Traceability Systems? In Proceedings of the 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), Oxford, UK, 3–6 August 2020; pp. 153–158.
15. Liu, J.; Sun, X.; Song, K. A Food Traceability Framework Based on Permissioned Blockchain. *J. Cybersecur. Henderson* **2020**, *2*, 107–113. [[CrossRef](#)]
16. Yang, K.; Forte, D.; Tehranipoor, M.M. CDTA: A Comprehensive Solution for Counterfeit Detection, Traceability, and Authentication in the IoT Supply Chain. *ACM Trans. Des. Autom. Electron. Syst.* **2017**, *22*, 1–31. [[CrossRef](#)]
17. Bansal, D. Anti-Counterfeit Technologies: A Pharmaceutical Industry Perspective. *Sci. Pharm.* **2013**, *81*, 1–13. [[CrossRef](#)]
18. Wang, Z.; Zhang, H. *Design of Traceability and Forgery Prevention Management System for Agricultural Products Breeding*; Atlantis Press: Paris, France, 2018; pp. 1185–1188.
19. Agrawal, T.K.; Koehl, L.; Campagne, C. A Secured Tag for Implementation of Traceability in Textile and Clothing Supply Chain. *Int. J. Adv. Manuf. Technol.* **2018**, *99*, 2563–2577. [[CrossRef](#)]
20. Agrawal, T.K.; Campagne, C.; Koehl, L. Development and Characterisation of Secured Traceability Tag for Textile Products by Printing Process. *Int. J. Adv. Manuf. Technol.* **2019**, *101*, 2907–2922. [[CrossRef](#)]
21. Wang, K.; Kumar, V.; Zeng, X.; Koehl, L.; Tao, X.; Chen, Y. Development of a Textile Coding Tag for the Traceability in Textile Supply Chain by Using Pattern Recognition and Robust Deep Learning. *Int. J. Comput. Intell. Syst.* **2019**, *12*, 713–722. [[CrossRef](#)]
22. Chen, F.; Luo, Y.; Tsoutsos, N.G.; Maniatakos, M.; Shahin, K.; Gupta, N. Embedding Tracking Codes in Additive Manufactured Parts for Product Authentication. *Adv. Eng. Mater.* **2019**, *21*, 1800495. [[CrossRef](#)]
23. Picard, J. Digital Authentication with Copy-Detection Patterns. In Proceedings of the Optical Security and Counterfeit Deterrence Techniques V, San Jose, CA, USA, 20–22 January 2004; Volume 5310, pp. 176–184.
24. Tkachenko, I.; Destruel, C.; Strauss, O.; Puech, W. Sensitivity of Different Correlation Measures to Print-and-Scan Process. *Electron. Imaging* **2017**, *2017*, 121–127. [[CrossRef](#)]
25. Tkachenko, I.; Puech, W.; Destruel, C.; Strauss, O.; Gaudin, J.-M.; Guichard, C. Two-Level QR Code for Private Message Sharing and Document Authentication. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 571–583. [[CrossRef](#)]
26. Tkachenko, I.; Puech, W.; Strauss, O.; Destruel, C. Printed document authentication using two level or code. In Proceedings of the 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Shanghai, China, 20–25 March 2016.
27. Farooq, M.S.; Riaz, S.; Abid, A.; Umer, T.; Zikria, Y.B. Role of IoT Technology in Agriculture: A Systematic Literature Review. *Electronics* **2020**, *9*, 319. [[CrossRef](#)]
28. Trenfield, S.J.; Tan, H.X.; Awad, A.; Buanz, A.; Gaisford, S.; Basit, A.W.; Goyanes, A. Track-and-Trace: Novel Anti-Counterfeit Measures for 3D Printed Personalized Drug Products Using Smart Material Inks. *Int. J. Pharm.* **2019**, *567*, 118443. [[CrossRef](#)]
29. Chen, Y.-T.; Chen, C.-C. Improve the Performance of Traceability System by Using a Digital Certificate Enabled Anti-Counterfeit QR-Code Mechanism. *Int. J. Soc. Sci. Humanit.* **2017**, *7*, 5.
30. Demestichas, K.; Peppes, N.; Alexakis, T.; Adamopoulou, E. Blockchain in Agriculture Traceability Systems: A Review. *Appl. Sci.* **2020**, *10*, 4113. [[CrossRef](#)]
31. Ho, A.T.P.; Hoang, B.A.M.; Sawaya, W.; Bas, P. Document Authentication Using Graphical Codes: Reliable Performance Analysis and Channel Optimization. *Eurasip J. Inf. Secur.* **2014**, *2014*, 9. [[CrossRef](#)]
32. Xie, S.; Zhong, S.; Chen, R.; Tan, H.-Z. Two-Stage Textured-Patterns Embedded QR Codes for Printed Matter Authentication. *Eurasip J. Image Video Process.* **2013**, *58*, 1056–1071.

-
33. Information Technology—Automatic Identification and Data Capture Techniques. QR Code 2005 Bar Code Symbology Specification. Available online: <https://www.iso.org/standard/43655.html> (accessed on 18 January 2021).
 34. Chen, C.; Li, M.; Ferreira, A.; Huang, J.; Cai, R. A Copy-Proof Scheme Based on the Spectral and Spatial Barcoding Channel Models. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 1056–1071. [[CrossRef](#)]
 35. Benatia, M.A.; Baudry, D.; Louis, A. Detecting Counterfeit Products by Means of Frequent Pattern Mining. *J. Ambient. Intell. Hum. Comput.* **2020**. [[CrossRef](#)]