My Smartphone Recognizes Genuine QR Codes! Practical Unclonable QR Code via 3D Printing

CHEN SONG, ZHENGXIONG LI, WENYAO XU, CHI ZHOU, ZHANPENG JIN, and KUI REN, University at Buffalo, the State University of New York, USA

Additive manufacturing, or 3D printing, has been widely applied in product manufacturing. However, the emerging unauthorized access of 3D printing data, as well as the growth in the pervasiveness and capability of 3D printing devices have raised serious concerns about 3D printing product anti-counterfeit. Electronic product tags are the current standard for authentication purposes; however, often this technology is neither secure nor cost-effective, and fails to take advantage of other unique 3D printing features. Considering the great usability of the QR code, we are motivated to enhance the QR code for the practical and cost-effective 3D printing product identification. Particularly, we bring up the *all-in-one design*, *all-in-one manufacturing* concept incorporating the QR code in the complete 3D printing paradigm. In detail, we explore the possibility of leveraging the random and uncontrollable process variations in the 3D printing system to generate a unique fingerprint for the integrated QR code. To this end, we present an end-to-end 3D-printed QR code verification framework, which does not change the original QR protocol and functionality. The entire solution can be implemented with commodity 3D printers and smartphones. Specifically, we first investigate the inevitable and random process variations in the 3D printing mechanism and analyze the causality between the variations and detectable geometric deformation. We further develop a fingerprint extraction algorithm taking into account both the QR code property and the 3D printer characteristics. The system evaluation indicates that our solution is secure and robust in multiple scenarios.

CCS Concepts: • **Security and privacy**;

Additional Key Words and Phrases: Embedded Systems, Hardware Security, 3D Printing, Authentication

ACM Reference Format:
Chen Song, Zhengxiong Li, Wenyao Xu, Chi Zhou, Zhanpeng Jin, and Kui Ren. 2018. My Smartphone Recognizes Genuine QR Codes! Practical Unclonable QR Code via 3D Printing. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 2, Article 83 (June 2018), 20 pages. https://doi.org/10.1145/3214286

1 INTRODUCTION

Additive manufacturing, also known as 3D printing, has become the main driven force of the industrial revolution. Compared to the traditional *subtractive* way where materials are removed, 3D printing affords greater personalization, less material waste and shorter product lifecycle. Given these advantages, 3D printing has been widely applied in rapid prototyping and product customization. Reports indicate that the global value of the 3D printing market has surpassed 5.1 billion in 2016 [71] and will continuous to grow [35].

Despite its prosperous growth, 3D printing faces the primary challenge of protecting intellectual property, when unauthorized access and use of proprietary 3D printing design files rapidly emerge [63]. Moreover, the growth in

Address comments to wenyaoxu@buffalo.edu.
Authors' address: Chen Song; Zhengxiong Li; Wenyao Xu; Chi Zhou; Zhanpeng Jin; Kui Ren, University at Buffalo, the State University of New York, Department of Computer Science and Engineering, Amherst, NY, 14260, USA.

2474-9567/2018/6-ART83 $15.00
https://doi.org/10.1145/3214286

the accessibility and capability of 3D printing also lowers the launching barrier of the counterfeit. This causes security defects especially when the 3D printing applications range from high-intellectual designs (e.g., branded watches) to high-privacy goods (e.g., biomedical support) that carry health and safety implications [38, 48], and even mission-critical products (e.g., weapon components) that relate the public safety [35]. However, the conventional anti-counterfeit tagging technologies (e.g., 1D barcode [39], watermark [66] and radio-frequency identification [27]) are not effective because: (1) they are prone to security attacks once the attacker hacks the anti-counterfeit protocol; (2) they require extra hardware and specific external devices to process the identity.

Recently, the Quick Response (QR) code has become the booming trademark technology that links real-world products with cyber information via smartphones. Producers attach the QR code to the product to deliver the product-related information to customers. However, we raise the question: *is it possible to integrate the product design with its QR code in 3D printing?* This concept can immediately enhance product security because, different from the traditional QR code usage where the code is detachable from the product, the structure-free characteristic of 3D printing enables the *all-in-one design* and *all-in-one manufacturing* of the QR code and the product *at no extra cost.* More importantly, we notice that each 3D printing process contains inevitable and uncontrollable process variations. Inspired by IC chip process variation for legitimacy verification [34, 58], we hypothesize that the process variation in each 3D printed QR code can be used as a unique and unrepeatable fingerprint. If successful, this QR security-enhancement technology can immediately bring *three* unprecedented advantages to the 3D printed product identification practice (see Fig. 1):

- **High security:** the process variation in each 3D printed QR code is random and uncontrollable. Therefore, it can defend against counterfeits even when the attacker obtains the original design. Also, it will not incur any additional cost because of its natural integration with the product. No such practical security technologies exist in 3D printed products.
- **Full compatibility:** the process variation based verification does not alter the design and content of QR codes. In other words, the integrated QR code contains *two-layer information* in our approach: (1) the product legitimacy verification; (2) the original QR content parsing. Therefore, our approach is fully compatible with the current QR code practice with ubiquitous smartphones.
- **Seamless integration:** the designer generates the QR code and integrates it into the 3D product design. Due to the elegant concept, 3D printing guarantees the natural and seamless integration of the QR code and the product, which makes it impossible for an adversary to detach them for malicious purposes.

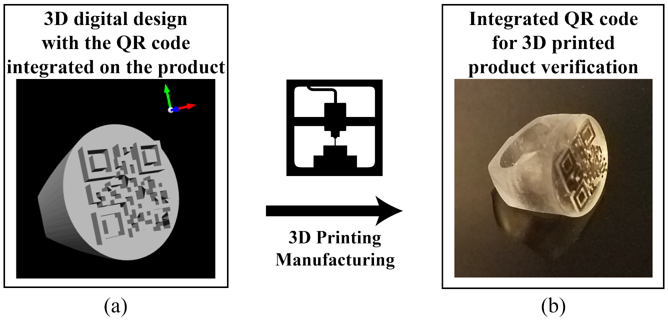


Fig. 1. (a) A customized ring with the integrated QR code is designed with computer-aided-design (CAD) software. (b) The real integrated product via 3D printing. The ring and the QR code are in the *all-in-one design*, *all-in-one manufacturing* style.

To this end, we present an end-to-end QR code verification framework for 3D printed product anti-counterfeit. There are three challenges in the methodology development: (1) how to analyze the process variation of 3D printing manufacturing regarding the multiple hardware components? (2) how to define the QR code fingerprint in the 3D printing physical space without altering its current practice? (3) how to develop an effective matching algorithm considering the physical properties of the QR code and the 3D printer mechanism? We first analyze in-depth the process variation in the hardware and qualitatively formulate it as the geometric trait into the printed result. Then, we define the QR code fingerprint in the 3D printing paradigm by leveraging its universal protocol. Afterward, we specifically purpose a novel fingerprint matching algorithm taking into account the essential characteristic of geometrical traits as well as the systematic features of 3D printers. Extensive experiments are conducted to evaluate the security and robustness of our system according to different attacking scenarios. The results show that process variation in 3D printing is random and uncontrollable, which can be leveraged as the fingerprint for each integrated QR code on the 3D printed product. In other words, each 3D printed QR code contains *two levels of information*: the unclonable fingerprint and the original encoded content. The user employs the smartphone to scan the QR code to validate the legitimacy of the QR code.

Contribution: our work is summarized as follows:

- We explore and implement a secure end-to-end QR code verification system, by generating a unique fingerprint for each integrated QR code on the 3D printed product. This solution is fully compatible with the state-of-the-art QR protocol. To the best of our knowledge, this is the first study on anti-counterfeiting techniques for 3D printed products.
- We investigate the uncontrollable process variation in 3D printing and model the causality between the process variations and the thus-derived geometric traits. We analyze the fingerprint, develop a set of novel fingerprint extraction and matching solutions for practical QR code verification.
- We evaluate the uniqueness of process-variation based fingerprint on integrated QR codes through intensive experiments using commodity 3D printers and smartphones. We particularly examine the security of our solution with regard to different attacking scenarios.

2 BACKGROUND

2.1 3D Printing Process

A standard 3D printing process converts a digital design to a physical object. G-code [1] is the *de facto* 3D printer machine code to control the printing process. Fig. 2 shows the hardware architecture of a 3D printer including the stepper motors, the hot-end, and the transmission systems. The X, Y stepper motors move the printer head via the belt-pulley system. The Z stepper motor vertically moves the platform via the lead-screw system. The material filament is fed by the extrusion stepper motor through a conveyance channel. Initially, the material is in solid status. The heater in the printer header then liquefies the filament. To maintain the heating temperature and avoid damage, the firmware dynamically adjusts the supply current and the cooling fan. The entire process depends on the physical characteristics of hardware units and the environmental content. Therefore, each mechatronic process will generate its own process variations, which cause the random and uncontrollable variance in the printed product. In general, 3D printing manufacturing can be efficiently formulated as [24, 40]: $P = F(D) + \sigma$, where P, D and $F(D)$ denote the printed object, the design and the controllable fabrication function of 3D printing once D is given. σ denotes the geometric content generated by the process variation.

2.2 Quick Response (QR) Code

Released in 1994, QR codes were developed by Toyota subsidiary Denso Wave and are two-dimensional (2D) matrix codes. Unlike the standard UPC barcodes, QR codes can hold more information within the same space. Specifically, one QR code consists of black squares arranged in a square grid on a white background (each black or white module represents a 0 or 1), which can be conveniently scanned with a smartphone app, and processed using the Reed-Solomon error correction [57] until the image can be appropriately interpreted.

Design Evolution: To date, the QR code has 40 different versions with dimensionality ranging from 21 × 21 modules (Version 1) to 177 × 177 modules (Version 40). The larger the symbol, the more the information capacity. For example, the maximum character storage capacity of Version 40 is 7089 in the numeric type.

QR Code Landmarks: All QR codes contain the special position-detection patterns, referred as landmarks hereafter. They are located in three corners of the QR code. The positional relationship of the landmarks allows quick access to the relevant angle, position and size information contained in the code's periphery [18].

QR Code Scanning Flow: First, the QR code scanning app on the smartphone takes a photo of the QR code. Pre-processing operations are conducted such as gray conversion and binarization. Then, the app calculates the orientation with the detected landmarks and corrects the contorted QR code with the angle information. At last, the QR code is divided and the information is extracted according to the standard QR code protocol.

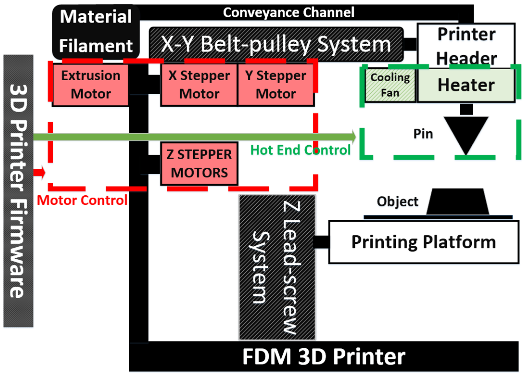


Fig. 2. The 3D printer hardware includes the stepper motors, the hot-end and the transmission systems [4].

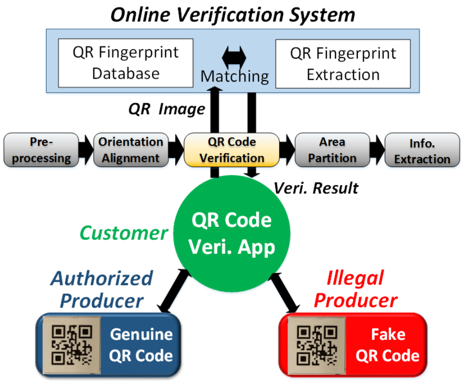


Fig. 3. The threat model of the 3D printed product counterfeit and the corresponding anti-counterfeit approach.

3 APPLICATION SCENARIOS

3.1 Threat Model

Fig. 3 shows the architecture of our threat model. We describe all entities as follows:

- **Authorized Producer**: who fabricates the genuine products. In order to provide each product a unique identity, the authorized producer generates a QR code for each product in the *all-in-one design*, *all-in-one manufacturing* manner. The customer of interest can download an authorized smartphone app and verify if the product in the distributed store is genuine through the QR code verification.
- **Illegal Producer:** who counterfeits high-intellectual or high-value 3D printed products for malicious purposes (e.g., illegal profit). The illegal producer knows that the customer of interest (victim) will use the authorized smartphone apps to verify the genuineness of the products. To convince the customer, he has to replicate genuine QR codes on his fake 3D printed products.
- **Customer:** who is interested in purchasing a 3D printed product. Customers want to verify the genuineness of the product, and they are educated to use the authorized smartphone app to do that. In practice, they launch the app and scan the QR code on the product they are interested in. Note that the customer can also be the authorized producer who conducts the product investigation.

3.2 Anti-Counterfeit Approach

We propose an anti-counterfeit approach for the 3D printed product. The approach is cost-free and practical, which is based on commodity smartphones and 3D printers. Specifically, there are two parts in the proposed approach, i.e., a QR-Code verification app and an online verification system.

QR-Code Verification App: This app is provided by the authorized producer and aims to help the customer verify the legitimacy of the 3D printed QR code (the product). Specifically, the app captures the QR code image

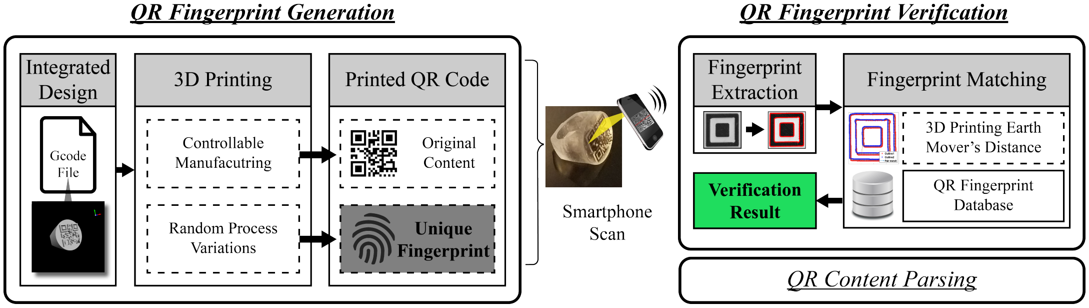


Fig. 4. The end-to-end cyber-physical solution of QR code fingerprint generation and verification. Note that the QR code contains two levels of information: the unique fingerprint and the original content.

and uploads it to the online verification system. We assume that the app is certificated by the authorized producer, and customers of interest know how to install and launch the app.

Online Verification System: Once receiving the uploaded image, the online system verifies the fingerprint of the QR code and returns the result to the app (customer). Note that the verification system is maintained by the authorized producer and contains all the legitimate QR code fingerprints. We assume that the online verification system is secure and not hacked by the adversary (e.g., illegal producers). This makes sense in that such kind of critical resource usually has access limitation and is maintained by the specific person in practice.

3.3 Attack Scenarios

For instance, an illegal producer (hereafter John) maliciously counterfeits the valuable unauthorized products and plans to sell them to a customer (hereafter Mary). To spoof the verification system, John needs to replicate a 3D printed QR code identical to the genuine one. We assume that John achieves the original integrated design file via illegal network access. We consider two attacking scenarios.

Ordinary Attack: John obtains the integrated design file whose content includes both the product and the QR code. To fake the counterfeit product, he purchases the commercial off-the-shelf 3D printers for mass production. The counterfeit products will be further delivered to the selling market.

Advanced Attack: Besides the integrated design, John can also get access to the actual 3D printers that fabricate the genuine product (e.g., John can be the employee). We consider it to be a stronger attack because the printers are exactly the same as the original ones. Note that John cannot break into the verification system.

Mary has no capability of recognizing the genuineness of the purchased product. She installs the QR-Code scan app provided by the authorized producer and scans the QR code on the 3D printed product. The app will notify Mary with the verification result whether the product is legitimate or not.

4 APPROACH OVERVIEW

Fig. 4 illustrates the end-to-end 3D printed product anti-counterfeit solution. The solution comprises the physical part: QR fingerprint generation and the cyber part: QR fingerprint verification. In the former one, we explore the process variation in 3D printing based on its mechanism. Afterward, we leverage the unclonable variation to fingerprint each QR code integrated on the product. In the latter one, we study a smartphone-based verification scheme to extract and verify the fingerprint based on the templates in the secure database. Once its legitimacy is verified, the original content of the QR code will be parsed. In the end, we also perform a quantitative analysis of the fingerprint space with regard to our proposed method.

5 QR FINGERPRINT GENERATION

5.1 Variation-Based Fingerprint

Fabrication variations are caused by uncontrollable factors in machine design and implementation, imposing uncertain quality impacts in the fabrication process [37, 56]. In the current practice of 3D printing, fabrication variation exists universally in the process. It is the collaborative result of multiple physical functional units, containing rich inevitable and uncontrollable process variations due to the complex interaction involved and dynamic ambient conditions [30]. According to the 3D printing in Fig. 2, the 3D printing process relies mainly on the operation of stepper motors, the hot end (including a thermistor) and transmission system.

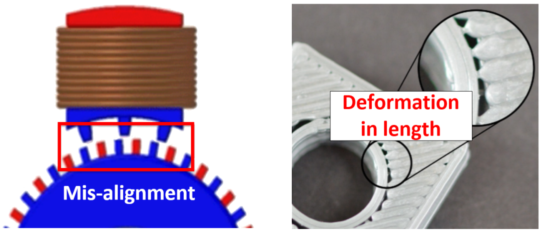


Fig. 5. One example of the geometric deformation in length caused by the random mis-alignment of the stepper motor.

Stepper Motor:A typical stepper motor consists of a slotted stator with two phases (A, B) and a permanent two-polar magnet rotor. The teeth on each side of the rotor are out of alignment by a tooth-width. During the operation, the torque on the motor shaft is generated by a moment of force relationship defined by Lorentz. Due to the mutual or cross-linking of the stator and rotor magnetic flux, the stepper motor produces enough electromagnetic force to drive the load. The mathematical model for the stepper motor is [17, 31, 32]:

$$\begin{cases} \frac{di_a}{dt} = [v_a - Ri_a + K_m \omega sin(N_r\theta)]/L, \\ \frac{di_b}{dt} = [v_b - Ri_b - K_m \omega cos(N_r\theta)]/L, \\ \frac{d\omega}{dt} = [-K_m i_a sin(N_r\theta) + K_m i_b cos(N_r\theta) - B\omega]/J, \\ \frac{d\theta}{dt} = \omega, \end{cases} \tag{1}$$

where v_a, v_b, i_a, i_b are the voltages and currents in Phase A and B. ω, θ and B are the rotor speed, the rotor position and the viscous friction coefficient. J is the inertia of the motor, K_m is the motor torque constant, R is the resistance of the phase winding, L is the inductance of the phase winding and N_r is the number of rotor teeth.

We observe that the variation in the factors can affect the motor operation in an unpredictable manner. Besides, there are other complex interferences such as the slight magnetic coupling between the phases and the variation in inductance due to the magnetic saturation. Therefore, the actual operation variation is almost impossible to predict or reproduce, and so are thus-derived geometric discrepancies. For example, the gear tooth can be randomly misaligned due to the variation in ω, θ and cause step loss. As shown in Fig. 5, this can cumulatively result in the deformation of length in a printed line. If the step loss happens in the extrusion motor, it will vary the extrusion amount of the material filament and cause inconsistency in printed traits.

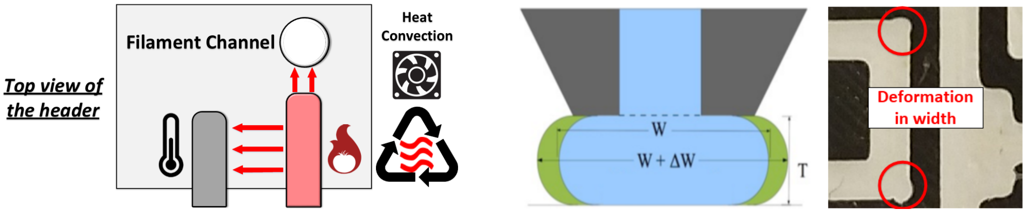
Hot-end: The hot-end locates in the extruder and is arguably the most complex part as it is in charge of the tricky tasks of melting and extruding material filament, such as polylactic acid (PLA) [50] or acrylonitrile butadiene styrene (ABS) [3]. Fig. 6(a) shows a hot-end structure and the heat conduction process in an isotropic medium. Typically, the hot end contains a cartridge heater and a thermistor. The heater is positioned next to the filament channel and generates adequate heat to melt the extruded material. To prevent the temperature from going too high, the thermistor and the cooling fans are deployed to monitor and adjust the temperature.

The heat conduction can be generally modeled as the following heat transfer governing equation [33]:

$$\frac{\partial T}{\partial t} = \frac{k}{C_p \rho} \left(\frac{\partial^2 T}{\partial x^2} + \frac{\partial^2 T}{\partial y^2} + \frac{\partial^2 T}{\partial z^2} \right) + q, \tag{2}$$

where $\frac{\partial T}{\partial t}$ denotes the temperature change rate, k is the thermal conductivity, ρ is the material density, C_p is the heat capacity, $\frac{k}{C_p \rho}$ is called thermal diffusivity and q is the internal heat generation. We find that these factors fluctuate in an uncontrollable way and eventually bring variations to the heating conduction. For example, the values of k, ρ, C_p highly depend on the uncertain material purity, mutative material conductivity at different temperature and the real-time heat convection of the surrounding air. Even with the same material, $\frac{k}{C_p \rho}$ varies due to unpredictable manufacturing imperfections [29]. Fig. 6(b) illustrates that the variation in the hot-end affects the liquefaction of the material, causing the fluctuations of the printed line width.

Transmission System: The actuation systems are the crucial components which connect the motors to the printing head and the platform. Due to different working frequency and load force, the 3D printer employs the belt-pulley system for the head movement and the lead-screw system for the platform movement. Specifically, the belt-pulley system is the complex joint of the belt and the pulley [11]. Belt span tension F at the belt cord centerline increases in the belt velocity direction. The random vibration component of tensioner-arm and pulley angular rotation, velocity and acceleration will cause the inhomogeneous driving force conductivity from one side to the other. On the other hand, the torque in the lead-screw system [7, 52] is determined by the load on the screw, the mean diameter, the coefficient of friction, the lead angle and other factors, which are affected by manufacturing imperfections and the random wear-and-tear conditions along the printer usage.



(a) The thermal conduction diagram.

(b) The geometry variation in line width.

Fig. 6. The deviation in the temperature control system and the thus-derived small deformation.

Summary: (1) The process variation in 3D printing is a natural integration of multiple sources and its existence is *inevitable*; (2) The variation is *non-repeatable* because it is the complex interaction result among the variations of multiple physical components; (3) The process variation leads to *persistent* and *measurable* traits (e.g., geometric deformation) embedded on the printed part (e.g., the integrated QR codes).

5.2 QR Fabrication with Fingerprint

We design and fabricate each 3D printed QR code with the unique fingerprint via process variation.

Step 1: 2D QR Code Generation. Users can encode any product information into a 2D QR code. Different types of the embedded information (e.g., url or text) need to apply different protocol.

Step 2: 3D QR Code Design. We use Materialise Magics [2] to upgrade the 2D QR code into a 3D version, which will be further integrated into the product as one unit. We employ the dual color to represent the black and white area of the QR code. Because 3D printing is a layer-wise process, two areas are formed in different layers.

Step 3: 3D QR G-code Generation. We adopt an open source software Cura [64] to convert the 3D QR code to the machine-readable G-code file. Preprocessing such as slicing [21] and path-planning is conducted.

Step 4: 3D QR Code Fabrication. The G-code file is downloaded onto the 3D printer for fabrication. The random variation affects factors such as the head position or the extrusion material, resulting in the geometric deformation on the QR code. Therefore, each printed QR code naturally contains two levels of information: the original content ($F(D)$) from the design and the unique fingerprint (σ) from the process variation.

6 QR FINGERPRINT VERIFICATION

6.1 Fingerprint Extraction

We extract the fingerprint using the smartphone to capture the micro-scale geometric deformation generated by the process variation (we prove the smartphone's sensing ability in Sec. 9). In the digital domain, the geometric shape is commonly represented by vertices because they can best represent the global and local details [6, 12]. The geometric contour of an area-of-interest, which is the combination of vertices, contains abundant information about the geometric discrepancies. Since a good solution should be compatible with all QR codes regardless of version or content, we focus on the three landmarks, which are owned by every QR code. CANNY edge detection is an efficient tool to extract the contour of the landmark [10]. We utilize the improved CANNY edge detection method to better reduce the noise disturbance via the self-adaptive filter and the morphological thinning [28, 69].

6.2 Fingerprint Matching

Once the fingerprint of a 3D printed QR code is extracted, we compare it with the genuine ones in the database to verify its legitimacy. In the following, we introduce a new matching approach towards robustly quantifying the similarity between two extracted fingerprints.

Earth Mover's Distance: We select *Earth Mover's Distance* (EMD) [44, 45] as the basic distance metric because: 1) the unclonable process variation essentially generates the unique geometric distortion in the printed outline, i.e., *the movement (dislocation) of the corresponding vertices on the image*, which naturally fits the principle of EMD; 2) naive Euclidean distance requires the same size of two sets. Instead, EMD supports the N-to-M matching when the vertex number differs in the fingerprints [13, 45]. Specifically, EMD is commonly formulated as the well-known transportation problem [25] which is described as follow: let $A = \left\{(p_1, w_{p_1}) \cdots (p_m, w_{p_m})\right\}, 1 \leq i \leq m$; $B = \left\{(q_1, w_{q_1}) \cdots \ (q_n, w_{q_n})\right\}, 1 \leq j \leq n$; and $D = [d_{ij}]$ the ground distance matrix where $d_{ij} = ||p_i - q_j||$. We want to find a flow $F = [f_{ij}]$ that transports set X to set Y with the least cost [45]:

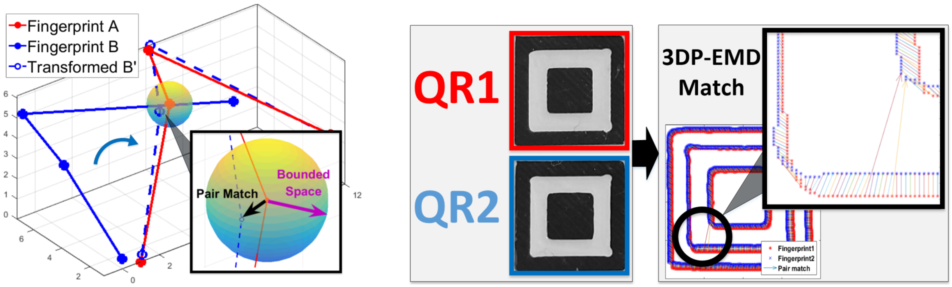
$$EMD(A, B, F) = \frac{min_F(\sum_{i=1}^{m} \sum_{j=1}^{n} f_{ij}||p_i - q_j||)}{\sum_{i=1}^{m} \sum_{j=1}^{n} f_{ij}}, \tag{3}$$

with subject to: 1) $f_{ij} \geq 0; 1 \leq i \leq m, 1 \leq j \leq n$; 2) $\sum_{i=1}^{m} w_{x_i} = \sum_{j=1}^{n} w_{y_j}$; 3) $\sum_{j=1}^{n} f_{ij} \leq w_{x_i}; 1 \leq i \leq m$; 4) $\sum_{i=1}^{m} f_{ij} \leq w_{y_j}; 1 \leq j \leq n$; 5) $\sum_{i=1}^{m} \sum_{j=1}^{n} f_{ij} = min(\sum_{i=1}^{m} w_{x_i}, \sum_{j=1}^{n} w_{y_j})$.

These constraints: 1) move points from X to Y; 2) state that the overall weight of points in X equals the one in Y and therefore, weight normalization is not required; 3) limit the amount of points in the target that can be sent by the clusters in X to their weights; 4) limit the clusters in Y from receiving points more than their capacity; 5) move the maximum amount of points.

3DP-EMD: Considering the 3D printing mechanism and QR code practice, we propose an extended *3D Printing Earth Mover's Distance*, namely 3DP-EMD, by enhancing two particular aspects:

- First, the process variation will not cause any geometric dislocation larger than one line width because otherwise it is considered to be a printing defeat [6]. Thus, for a printed product with satisfactory quality, we can assume the deformation range is bounded. As shown in Fig. 7(a), for each vertex, we set the bounded space as a sphere with a radius of δ and any matching vertex pair (p_i, q_j) with a distance larger than δ has no practical meaning. Accordingly, we add the distance penalty as $d_{ij} = inf$ when $||p_i - q_j|| > \delta$.



(a) 3DP-EMD considers the bounded space and rigid transformation in 3D space.

(b) The matching result of two QR fingerprints on one landmark.

Fig. 7. The concept and demonstration of 3DP-EMD for QR fingerprint matching.

- Second, the characteristic of QR code allows people to scan from a flexible angle. As a result, the extracted point set (A) can be regarded as being applied to certain rigid transformations upon the stored point set (B) captured via another angle (e.g., orthogonal 0°). To ensure the accurate matching between set A and set B, we need to eliminate the rigid transformation. Specifically, the transformation in 3D space can be represented by a rotation (i.e., a 3×3 matrix) $\mathcal{M}$ and a translation (i.e., a 3×1 matrix) $\mathcal{Z}$. As shown in Fig 7(a), set A is the pre-stored fingerprint and set B is the one captured from another angle. Instead of directly calculating the EMD of set A and set B, we want to align set B to set A as close as possible to remove the capturing noise ($B' = \mathcal{M}B + \mathcal{Z}$).

  Based on Eq. 3, we define a cost function to find $\mathcal{M}$, $\mathcal{Z}$ that gives us the smallest EMD of two sets:

$$Cost(A,B,F) = \frac{min_F(\sum_{i=1}^{m}\sum_{j=1}^{n} f_{ij}||p_i - (\mathcal{M}q_i + \mathcal{Z})||)}{\sum_{i=1}^{m}\sum_{j=1}^{n} f_{ij}}. \tag{4}$$

The problem of minimizing Eq. 4 is a standard L_2^2-norm convex optimization problem with respect to 12 variables in $\mathcal{M}$ and $\mathcal{Z}$. We adopt a flow-transformation iterative algorithm [13, 20, 65] to find the best transformation to align the two point set and calculate the minimum 3DP-EMD.

Fig. 7(b) shows the matching of two fingerprints. In practice, we compare all three landmarks against the corresponding templates. Only when each match achieves the 3DP-EMD cost less than a pre-defined threshold will the QR code be regarded as the genuine one. Note that we only need to store the point set in the database instead of the entire image. Assume the coordinates of each point are stored in float (4×2 bytes) and we extract 200 points from each landmark, the entire storage is $3 \times 200 \times 8 = 4.8KB$. The data size can be further reduced by lossless compression algorithms such as Run Length Encoding [46] or Huffman Coding [70]. Therefore, our approach is scalable for a large series of printed parts.

6.3 Feature Space Analysis

To understand the security of our solution, we formulate and analyze the potential feature space of the extracted fingerprint. Assume each module in the QR code is represented by $a \times a$ pixels in the captured image, and the distortion range of each pixel u is less than a pixels: $0 < u < a$. Considering the comparison on one landmark, the maximum number of extracted vertex is $N = 8a \times 8a$ because each landmark is 8×8 modules. Therefore, in the extreme case, the maximum 3DP-EMD is $Max_{3DP-EMD} = Nd \leq 2^6a^3$, and the theoretical space is $0 < \int < Max_{3DP-EMD}$. For three landmarks, the upper bound of the feature space is $\mathcal{S} = \int^3 = 2^{18}a^9$. In the camera system, let the size of the sensing unit be d, the focal length be f, the FOV (field of view) angle in vertical be θ and the capture distance be D. Based on the geometric relationship, the vertical FOV can be derived as: $\theta = 2 * \arctan(\frac{\frac{d}{2}}{f})$, $FOV_1 = 2D * \tan\frac{\theta}{2}$.

For example, the 8MP camera has the pixel size of $d = 1.4um$ and focal length of $f = 4mm$. If $D = 30$cm, $FOV_1 \approx 0.1mm$. Given a QR code of $5cm \times 5cm$, the side length of one module in a landmark $\approx \frac{8}{8} = 1mm$. Therefore, $a = \frac{1}{0.1} = 10$. The potential feature space in the ideal condition can reach as large as $2^{18}10^9$, which proves that our method is secure.

7 EVALUATION

In this section, we conduct comprehensive experiments to evaluate the security performance of our proposed QR code fingerprint. Specifically, we adopt two scenarios where the malicious attacker obtains the original design file and has access to either the commercial 3D printers or the original printer (see Sec. 3.3).

7.1 System Setup

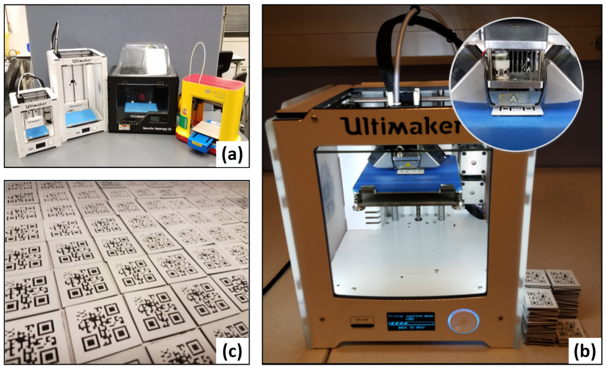


Fig. 8. We apply four different commercial 3D printers to fabricate 100 QR codes in total.

QR Code Fabrication: As shown in Fig. 8(a), we employ 4 different printers, i.e., Ultimaker 2 Go, Ultimaker 2 Extended+, MakerBot Replicator 2X and XYZ da Vinci Mini Maker (Table 1). For simplicity, we fabricate the QR code alone instead of the entire product. Each printer fabricates 25 QR codes based on the same design file. All the 3D printers support the resolution of 20 microns, with the nozzle diameter of 0.4 *mm*. For the sake of fabrication quality, we set the printing speed at 1800 mm/min and the nozzle temperature at 215°C. PLA is used as the filament. Fig. 8(b) shows the fabrication process, and Fig. 8(c) depicts the fabricated QR cluster. The QR code design contains 3000 sliced layers, and each QR code takes about 2 hours to print.

Sample Database: Afterward, we manually take 100 images for each QR code in the indoor environment. The images are captured by Galaxy S7, equipped with the built-in rear camera sensor Sony IMX260. Specifically, the size of camera pixels is 12MP, each single pixel area is $1.4um$ and the camera aperture is F/1.7. Initially, we apply the capture distance as $15cm$ (we will evaluate the distance effect in Sec. 8.2). To avoid the pixel-wise noise caused by the smartphone position, we apply the burst mode to capture images at fast speed (> 10 images per second). The sample database contains 100 QR codes and $10,000$ QR code images.

7.2 Performance Metrics

To evaluate the verification performance, we employ *precision*, *recall* as the metrics [19]. *Precision* is the ratio of correctly predicted positive observations to the total predicted positive observations. *Recall* is the ratio of correctly predicted positive observations to all observations in actual positive class. These two metrics emphasize different aspects in terms of the application scenarios.

For the overall performance, we adopt the balanced accuracy metric (BAC) (see Eq. 5), given its advantage of non-sensitivity to instance distribution [55]. Let k be the total number of the QR codes (classes) stored in the database. For each class i ($1 \le i \le k$), TP_i is the true positive and TN_i is the true negative. Similarly, FN_i and FP_i, respectively refer to the false negative and the false positive.

$$BAC(\%) = \frac{0.5 * \sum_{i=1}^{k} TP_i}{\sum_{i=1}^{k}(TP_i + FN_i)} + \frac{0.5 * \sum_{i=1}^{k} TN_i}{\sum_{i=1}^{k}(TN_i + FP_i)}. \tag{5}$$

Table 1. Specifications of the employed 3D printers.

Num.	Printer Model	Layer Res. (μm)	X/Y Acc. (μm)
1	Ulti. 2 Go	20~600	12.5/12.5
2	Ulti. 2 Extended+	20~600	12.5/12.5
3	MakerBot Rep. 2X	100	11/11
4	XYZ. Mini Maker	100~400	20/20

7.3 System Accuracy

We evaluate the verification performance mainly from three aspects: (1) *inter-printer performance*, i.e., can our approach distinguish the QR codes manufactured by different 3D printers? (2) *intra-printer performance*, i.e., is our approach able to distinguish the QR codes manufactured by the same 3D printers? (3) *alien QR codes*, i.e., can our approach reject unknown cases?

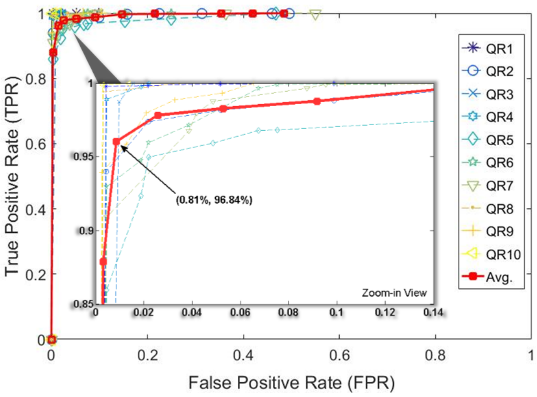
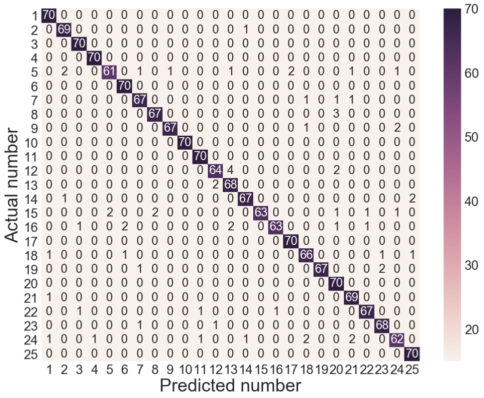


Fig. 9. The ROC curves of the QR codes.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1	70	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	69	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
3	0	0	70	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	70	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	2	0	0	61	0	1	0	1	0	0	0	1	0	0	0	2	0	0	0	1	0	0	1	0
6	0	0	0	0	0	70	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	67	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	0	0
8	0	0	0	0	0	0	0	67	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0
9	0	0	0	0	0	0	0	0	67	0	0	0	0	0	0	0	0	1	0	0	0	0	0	2	0
10	0	0	0	0	0	0	0	0	0	70	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	70	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	64	4	0	0	0	0	0	0	2	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	2	68	0	0	0	0	0	0	0	0	0	0	0	0
14	0	1	0	0	0	0	0	0	0	0	0	0	0	67	0	0	0	0	0	0	0	0	0	0	2
15	0	0	0	0	2	0	0	2	0	0	0	0	0	0	63	0	0	0	0	1	0	1	0	1	0
16	0	0	1	0	0	2	0	0	0	0	0	0	2	0	0	63	0	0	0	1	0	1	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	70	0	0	0	0	0	0	0	0
18	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	66	0	0	0	0	1	0	1
19	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	67	0	0	0	2	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	70	0	0	0	0	0
21	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	69	0	0	0	0
22	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	67	0	0	0
23	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	68	0	0
24	1	0	0	1	0	0	0	0	0	0	1	0	0	1	0	0	0	2	0	0	2	0	0	62	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	70

Fig. 10. The confusion matrix of 25 QR codes.

7.3.1 *Inter-Printer Verification Performance.*

For each QR code, we randomly select 30 out of 100 images as the template set, and use the rest for testing. In total, 3000 images are used as templates and 7000 images are used as samples. For each sample, we extract its fingerprint and compare it with each template. We determine the sample to be the specific template's class as long as the 3DP-EMD distances of three landmark pairs are within the threshold. If multiple classes meet the criteria, we employ the majority voting strategy to determine the class. If multiple classes have the same count, we select the one with the minimum average distance. If the genuine sample is rejected by all classes, we regard it as an FN event.

The receiver operating characteristic (ROC) curve can graphically compare the system performance under various settings. Specifically, we brute force the threshold and record the corresponding results. For the purpose of demonstration, we randomly pick 10 curves to depict (Fig. 9). The average result over all 100 QR codes is colored in red. Zooming into the results, we observe that the average result of 100 QR codes achieves an AUC (area under curve) of 99.36%, which means that the fingerprint of each QR code remains significantly distinguishable in terms of different thresholds. Take one specific threshold as an example (as pointed out), we achieve the high TPR of

96.84% and the low FPR of 0.81% at the same time. This performance is favorable for the customer as she wants guarantee of a genuine product. On the other hand, the manufacturer will emphasize high TPR since the last thing she wants is for a genuine product to be incorrectly marked as fake. In the future, we will further improve the TPR while keeping the low FPR.

7.3.2 ***Intra-Printer Verification Performance.*** We validate the system performance when the QR codes are manufactured by one 3D printer. Similar to the above experimental setup, for each QR code, we withdraw 30 images as the templates and the rest of the images are applied for testing. For the purpose of demonstration, we illustrate the confusion matrix of the classification result over the 25 QR codes printed by Ulimaker 2 Go. Fig. 10 shows that 96.27% of the instances are correctly recognized. Such a result substantially proves that the unclonable process variation exists not only among different printers, but also in the identical one.

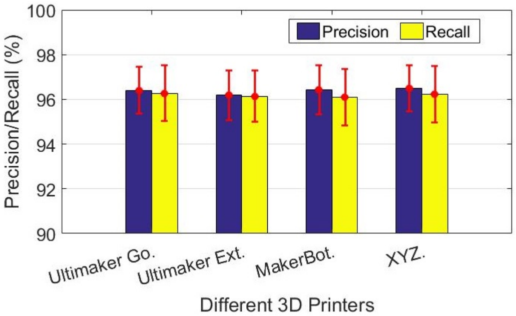


Fig. 11. Avg. precision/recall of four 3D printers.

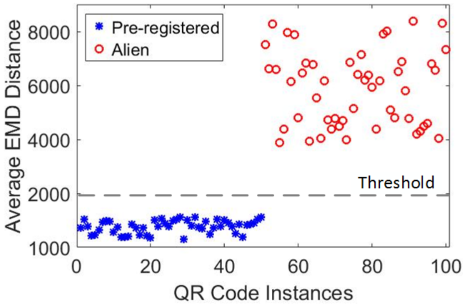


Fig. 12. We use threshold to segregate alien QR codes.

Fig. 11 summarizes the average precision and recall of Ultimaker 2 Go, Ultimaker 2 Extended+, MakerBot Replicator 2X and XYZ da Vinci Mini Maker. Specifically, the average precisions are 96.41%, 96.18%, 96.42%, 96.49%, respectively and the average recalls are 96.27%, 96.14%, 96.11%, 96.24%, respectively. Here, we focus more on precision because we want to minimize the chance that the counterfeit product is falsely recognized as the legitimate one. In this sense, our system achieves good security performance with regard to all four printers, which shows its capability to deny the advanced adversary attack. Moreover, the overall high recalls indicate that most of the legitimate products can be verified.

7.3.3 ***Performance with Alien QR Codes.*** To identify an alien QR code, we apply a threshold on the 3DP-EMD distance. First, we randomly split 100 QR codes into the pre-registered group (50 QR codes) and the alien group (50 QR codes). For each pre-registered one, we use 30 images as templates and select 20 out of the remaining 70 images as samples. Then, we calculate the average 3DP-EMD among the templates and the samples. Similarly, we select 20 out of 100 images for each alien QR code and calculate the average 3DP-EMD among them and all the registered templates. In Fig. 12, we observe that the alien QR codes have a larger distance and a threshold for reliable segregation can be empirically set. We refer to the settings in [19] and select 20 QR codes for training only. For testing, we regard the remaining 80 QR codes as the alien ones. Fig. 13 reports that even with the increase of alien codes, our methods can still identify them correctly, with an average precision of 99.75% and recall of 99.73%.

7.3.4 ***Performance with Increasing QR Codes.*** Because the printing duration is time-consuming, it is impractical to analyze the fingerprint capacity on a large amount. Therefore, we heuristically evaluate this aspect by investigating the performance tendency with the increasing number of QR codes. To be specific, we increase the data size from 20 QR codes to 100. As shown in Fig. 14, we report the average BAC and the standard deviation in each case. With the increase of the QR codes, the classification accuracy remains high and stable, with only

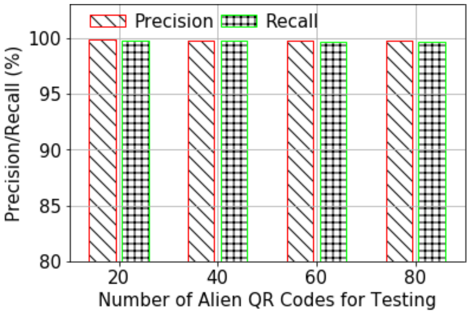


Fig. 13. Avg. precision/recall for alien QR codes.

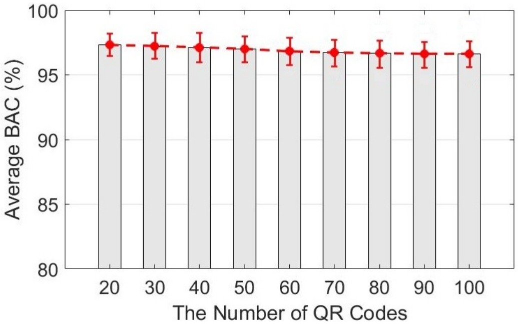


Fig. 14. BAC tendency when the QR code increases.

0.02% fluctuation from 90 to 100. This provides encouraging signs that our system is likely scalable to a large amount of QR codes (products).

8 SENSING SENSITIVITY ANALYSIS

We carry out the sensing sensitivity analysis to evaluate robustness and usability. We use the same dataset as aforementioned, which consists of 100 QR codes.

8.1 Camera Type

Smartphones have different built-in camera sensors. The main parameters are resolution, single pixel area and aperture. Camera resolution determines the ability to describe the detail in the field of view. The single pixel area is the sensitive area that receives photons to represent as a pixel. The camera aperture means an opening of the sensor through which light travels. Larger aperture means more photons (details) can be received.

Without losing generality, we adopt three popular smartphones: Nexus 5, Galaxy S7 and iPhone 6s. The supported maximum resolution for three smartphones is 8MP, 12MP and 12MP. Both Nexus 5 and Galaxy S7 have the single pixel area of 1.4um, while the one for iPhone 6s is 1.22 *um*. They have different default camera apertures, which are F/2.4, F/1.7 and F/2.2. Considering the commonly supported resolution, we evaluate 8M, 5M and 0.9M (some settings are not originally supported and we use 3rd-party software to do the configuration [22]).

Table 2. The performance of different phone types with regard to different resolutions.

Phone Type Picture Size	Nexus 5	Galaxy S7	iPhone 6s
8M (3264x2448)	95.34±0.82	96.57±1.12	96.26±1.43
5M (2560x1920)	96.27±1.57	96.86±1.46	95.38±1.39
0.9M (1280x720)	95.59±1.60	96.32±1.55	96.57±1.82

The average BAC is shown in Table 2. Overall, three smartphones obtain the average BAC of 95.73%, 96.58% and 96.07% respectively under different resolutions. Among them, Galaxy S7 has the comparatively highest BAC because it has a larger pixel area and aperture, which enables it to capture more fingerprint details. In general, our approach can provide good performance with most commercial smartphones.

8.2 Capture Distance

The landmarks in three corners allow the fast, omnidirectional scanning of a QR code from a large angle, eliminating the need to align the scanner with the code. Considering a QR code with common size (5 $cm \times 5$ cm), we vary the capture distance reasonably from 15 to 55 cm. Fig. 15 reports the average BAC. We can observe that the average performance fluctuates between 96 $\sim$ 97% when the capture distance changes. For the most practical capture range of 15 ∼ 35 *cm*, the performance achieves an average BAC of 97.00%. Therefore, the performance of our approach will not be affected by the capture distance.

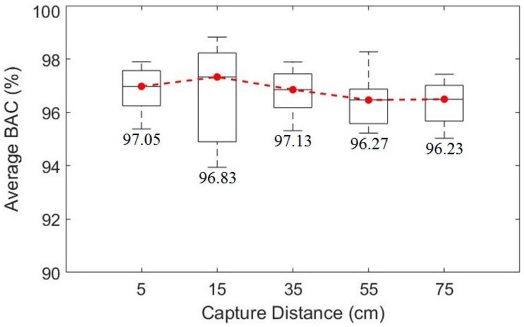


Fig. 15. Avg. BAC under different capture distances.

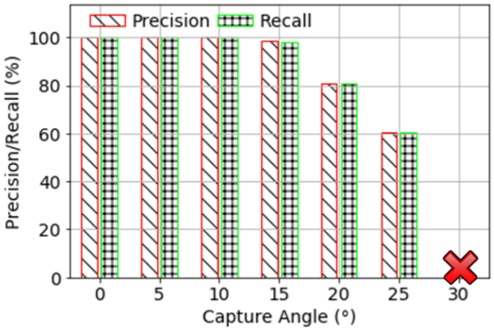


Fig. 16. The performances under different capture angles.

8.3 Capture Angle

The 2D QR code supports a flexible capture angle due to its resistance to distortion. Different from the plain 2D code, the integrated 3D QR code has elevation in the surface topology (remember the black and white areas have different heights). Therefore, the tilting reading can cause the rear part to be covered by the front part. Specifically, we define the orthogonal capture as 0° and gradually tilt the capture angle. Results in Fig. 16 show that our system achieves almost 100% precision for the capture angle within 15°. Beyond that, overlap occurs and we cannot fully extract the fingerprint. When the capture angle is larger than 30°, even the QR code cannot be properly parsed. Note that larger elevation can narrow the angle range because the viewing angle towards the bottom black area is smaller.

8.4 Landmark Resolution

The resolution of the landmarks directly determines the integrity of the captured fingerprint. For example, if the landmark capture is too blurred, it will be difficult to extract the accurate fingerprint.

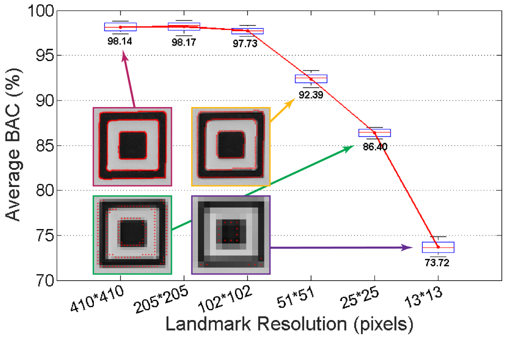


Fig. 17. Avg. BAC under different landmark resolutions.

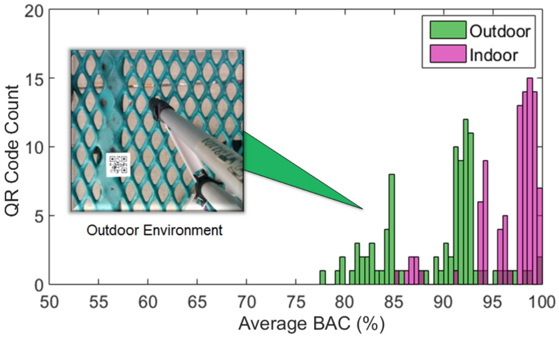


Fig. 18. Indoor and outdoor performance.

As shown in Fig. 17, we evaluate 5 landmark resolutions from 410 × 410 to 13 × 13 pixels. The average BACs are 97.34%, 97.05%, 97.11%, 91.35%, 85.69% and 72.55% respectively. Performance largely degrades after the resolution is smaller than 51 × 51 pixels. To better understand this phenomenon, we take one landmark as an example. When the resolution remains high (the first three cases), the edge boundary can be precisely detected and the extracted fingerprint is integral. However, when the resolution becomes too low, the capture can no longer provide the detailed information about the geometric edge. As a result, the fingerprint cannot be accurately extracted. Considering the fact that the camera sensor on current mobile devices are capable of capturing a high resolution of the landmark within the reasonable distance, our system is practical to extract the prints' fingerprint.

8.5 Ambient Light

QR-based applications are diverse in daily life and the application scenario can be both indoor and outdoor. The difference in the ambient light can affect the way the camera senses the QR code.

Indoor: We consider the indoor environment as a comparatively constrained place where fluorescent lamps are placed in fixed positions and generate a certain amount of illuminance according to the Central Nation System (CNS). In such an environment, white balance may vary in a slight way, but it can be easily adjusted by the adopted algorithm during the camera sensing process. There are cases where the surface of the material reflects the light at a specific angle. However, those can be easily addressed by adjusting the camera's position or using non-reflective material.

Outdoor: The outdoor environment is much more complex in the sense that the light condition is determined by various factors. Since it's impossible to include all the light conditions, we conduct a proof-by-concept evaluation. As shown in Fig. 18, we capture the QR code image in an open place with a tripod.

Eventually, we plot the average BAC distribution in two scenarios, where the red color represents the indoor case and the green color represents the outdoor case. Specifically, the overall BAC of indoor and outdoor scenarios are 96.87% and 91.70% respectively. This means that although the QR code can still be read in the outdoor space, the sunlight influences the camera when it senses the details of the QR code. Noticeably, the outdoor scenario also has a larger standard deviation of 6.47%. In future work, we will explore advanced image processing algorithms to reduce ambient noises and increase the usability of our approach in the outdoor environment.

9 DISCUSSION

Nozzle Travel Speed: 3D printers support a wide range of travel speed (e.g., Ultimaker 2 Go supports up to 18, 000 mm/min) and the determination is usually empirical based on the factors such as temperature and a material's thermoplastic properties. For example, the recommended speed for PLA filament is 1800 ∼ 5400 mm/min. If the speed is too high, the printed result may have more variations because of the incomplete liquefaction when the material is pulled out of the nozzle. In this work, we focus on the uncontrollable process variation given the recommended speed configuration. Particularly, we set the travel speed at 1800 mm/min.

Heating Temperature: The heating temperature is a critical factor in melting the solid material and affects the printing result in geometry. Specifically, this parameter setting is closely related to the material bonding. Material with good bonding properties, such as PLA, can have a constant performance across different temperatures. Therefore, any temperature within the PLA's recommended range from 175 ∼ 230°C can be applied.

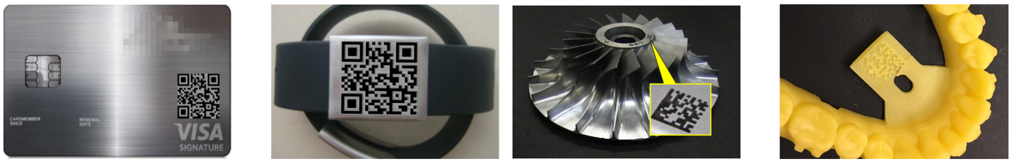
Filament Type: 3D printing has been applied in various domains involving diverse materials from plastic to metal. For FDM printers, PLA and ABS are the two most widely used types. Based on the unique property, each material performs differently. Our approach can be applicable with other materials because the process variation is an inherent feature in the 3D printing system.

3D Scanner: 3D scanning is an alternative way to obtain the digital design and counterfeit the genuine product. The scanner captures the geometric information of the object and generates the point clouds or polygon meshes in digital for forgery. However, scanners with ultra-high precision to reconstruct the digital design in the dimension of the practical QR code are costly and therefore, raise the launching barrier of the attack.

Sensing Dimension: Our method can be further improved with smartphones with advanced sensing modality. For example, iPhone X is equipped with the TrueDepth Camera System to capture the depth information in 3D space [15]. With that, we can obtain the product fingerprint in 3D space and such a system is invulnerable to image-based attack since it can differentiate the real integrated 3D QR code from the fake 2D image.

Sensing Resolution: The absolute minimum resolvable spot the camera can sense on the object is determined by its object space resolution (OSR) [23]. For example, Samsung S8 [47] has the camera with $1.4\mu m$ pixel size. The image space resolution is $\frac{1000\mu m/mm}{2\times 1.4\mu m} = 357lp/mm$[1]. Given the horizontal dimension of 3456 and Field-of-View of $77mm$, the Primary Magnification is $\frac{1.4\mu m\times 1440}{27mm} = 0.0747$. Thus, $OSR = 357lp/mm \times 0.0747 \approx 26\mu m$, which means that the current smartphone can perceive the micron-scale. Considering that the nano-scale 3D printing is still immature and extremely expensive [36], our method is feasible with the smartphone.

10 IMPLICATION



(a) Finacial field: the bank card.

(b) Medical field: the patient wristband.

(c) Industrial field: the turbine blades.

(d) Healthcare field: the tooth aligner.

Fig. 19. The real-world examples where QR codes are naturally integrated within products via 3D printing.

Integration of QR Codes and Products: The elegant layer-by-layer concept grants 3D printing a unique feature: structure-free, i.e., independence of design complexity. Taking advantage of this attribute, inventors can integrate the QR Code into the product design such that the product and QR code are fabricated as a whole. Fig. 19 shows a few examples of the existing applications where QR codes are embedded in the products. Such seamless integration can further improve product security, cost-effectiveness and aesthetics in multiple aspects.

Fingerprint Formation: In this work, we utilize the QR code as the carrier of the fingerprint because of its popularity. However, our method can also be extended to other geometrical patterns due to the existence of unclonable variation in any 3D printed geometry. Introducing random variations in the G-code to fingerprint the product is an interesting but orthogonal research topic. It requires the systematic design to make sure that the firmware/hardware can properly support the modified operations in terms of printing overhead and quality.

Unclonable 3D Printing: The implication of our methodology can go beyond the QR code applications. 3D printing is becoming the next generation manufacturing driven force, and has been applied in many domains [68]. However, recent studies [5, 26, 54] manifests that 3D printing has security unknowns which might lead to intellectual property leaks. Our study discovers that 3D printing can weave the unique fingerprint into any products, and users can conveniently read verify it via smartphones. Our discovery has the potential to yield success in anti-counterfeit markets and lead to a far-reaching breakthrough of "unclonable 3D printing".

11 RELATED WORK

Production Identification Technologies: Miscellaneous anti-counterfeit technologies are developed in the conventional manufacturing area [51]. **(1)** *1D Barcode*, such as Universal Product Code [39], is a well-established optical-machine readable symbol. It contains simple, but high-density linear codes to embed the specific ID information. **(2)** *Holography* [14] is a photographic recording of a light field based on the principle of interference. It is generated from the interference patterns obtained through the contact of laser beams by either angular image or laser technology. The high-definition hologram is used as a security identity. **(3)** *Watermark* is originally

[1] This unit stands for line-pairs per millimeter.

an identifying image or pattern in paper that appears as various shades of lightness/darkness when viewed by transmitted light. Later on, it is more widely extended to the digital domain by coding invisible ID into the noise-tolerant carrier [66]. **(4)** *RFID tag* uses electromagnetic fields to automatically identify and track tags attached to objects. The tag contains electronically stored ID and communicates with the nearby RFID reader [27]. However, the aforementioned methods do not fit well in the 3D printing paradigm in that: They are all *design-based* and can be easily forged once the design pattern is leaked; (2) They require extra cost and are isolated from the 3D printing mechanism. No effective method is explored for 3D printed product anti-counterfeit.

QR Security Enhancement: With the increase of QR code applications in identity-aware augmented domains, many enhancement methods are explored to make the QR code more secure. Researchers tried to integrate the traditional encryption methods onto the QR code to increase its complexity. For example, Zhenbo *et al.* employ a prevalent holographic encryption method, double random-phase encoding in the Fresnel domain, to embed the hologram upon a QR code [43]. Vongpradhip *et al.* [67] proposed a method of embedding the watermark text with the QR code by applying DCT (Discrete-Cosine-Transform) transform. However, both methods can be hacked by the reverse methods once the attacker knows the integration domain [41, 49, 67]. Tkachenko *et al.* proposed a two-level QR code [59] for private message sharing and document authentication. The key idea is to design a private level independent of the public level (the standard QR code protocol). However, the security of the embedded information fully depends on the assumption that the attacker does not know the private protocol. Existing QR security enhancement technologies increase the design complexity but are still vulnerable.

Hardware Fingerprint: Using intrinsic random physical features to identify hardware has a rich history. An early version of the unclonable identification system was proposed by Tolk [60] based on random optical reflection patterns generated by the reflective particle tag. Similar works [42, 62] utilized different optical microstructures based on transparent media. Random, unforgeable fiber texture was studied in [8, 9]. Lukas *et al.* [34] studied the camera identification by investigating the unique sensor noise pattern from the captured images. Dey *et al.* [19] explored smartphone fingerprints based on the hardware imperfections during the sensor manufacturing process. Similarly, Das *et al.* [16] proposed to fingerprint devices through on-board acoustic components. The randomness of capacitance measurements [53, 61] and the inherent delay characteristics of wires and transistors [58] were also developed. Therefore, the intrinsic variation in the physical system is random and inevitable.

12 CONCLUSION

With the increasing versatility of QR codes in the identity-aware applications, we present an end-to-end approach for 3D printed product anti-counterfeit through unclonable QR code generation and verification using commodity 3D printers and smartphones. Considering the general trend of applying 3D printing in product manufacturing, our paper is the first work to explore and leverage the uncontrollable process variations in the 3D printing mechanism through the widely accepted QR code. Our extensive experiments verify the viability of the unclonable QR code fingerprint, which is effective against the 3D printed product counterfeit.

ACKNOWLEDGMENTS

We thank all anonymous reviewers for their insightful comments on this paper. This work was in part supported by the National Science Foundation under grant No. 1547167.

REFERENCES

[1] First edition in 1950s. *G-code (RS-274).* http://reprap.org/wiki/G-code.

[2] First edition in 1950s. *Materialise Magics.* http://software.materialise.com/magics.

[3] Sung-Hoon Ahn, Michael Montero, Dan Odell, Shad Roundy, and Paul K Wright. 2002. Anisotropic Material Properties of Fused Deposition Modeling ABS. *Rapid Prototyping Journal* 8, 4 (2002), 248–257.

[4] Jerry Ajay, Chen Song, Aditya Singh Rathore, Chi Zhou, and Wenyao Xu. 2017. 3DGates: An Instruction-Level Energy Analysis and Optimization of 3D Printers. In *Proceedings of the Twenty-Second International Conference on Architectural Support for Programming*

Languages and Operating Systems, ASPLOS 2017, Xi'an, China, April 8-12, 2017. 419–433.

[5] Mohammad Abdullah Al Faruque, Sujit Rokka Chhetri, Arquimedes Canedo, and Jiang Wan. 2016. Acoustic Side-Channel Attacks on Additive Manufacturing Systems. In *2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 1–10.

[6] Samuel N Bernier, Bertier Luyt, and Tatiana Reinhard. 2015. *Design for 3D Printing: Scanning, Creating, Editing, Remixing, and Making in Three Dimensions*. Maker Media, Inc.

[7] VB Bhandari. 2010. *Design of Machine Elements*. Tata McGraw-Hill Education.

[8] James DR Buchanan, Russell P Cowburn, Ana-Vanessa Jausovec, Dorothee Petit, Peter Seem, Gang Xiong, Del Atkinson, Kate Fenton, Dan A Allwood, and Matthew T Bryan. 2005. Forgery:"Fingerprinting" Documents and Packaging. *Nature* 436, 7050 (2005), 475.

[9] Philippe Bulens, F-X Standaert, and J-J Quisquater. 2010. How to Strongly Link Data and Its Medium: The Paper Case. *IET Information Security* 4, 3 (2010), 125–136.

[10] John Canny. 1986. A Computational Approach to Edge Detection. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 6 (1986), 679–698.

[11] Gregor Čepon and Miha Boltežar. 2009. Dynamics of A Belt-drive System Using A Linear Complementarity problem for the Belt-pulley Contact Description. *Journal of Sound and Vibration* 319, 3 (2009), 1019–1035.

[12] Chee Kai Chua and Kah Fai Leong. 2003. *Rapid Prototyping: Principles and Applications*. Vol. 1. World Scientific.

[13] Scott Cohen and L Guibasm. 1999. The Earth Mover's Distance under Transformation Sets. In *Computer Vision, 1999. The proceedings of the seventh IEEE International Conference on*, Vol. 2. IEEE, 1076–1083.

[14] Robert Collier. 2013. *Optical Holography*. Elsevier.

[15] Apple Worldwide Developers Conference. 2017. Capturing Depth in iPhone Photography. Retrieved 2018-4-17 from https://developer.apple.com/videos/play/wwdc2017/507/

[16] Anupam Das, Nikita Borisov, and Matthew Caesar. 2014. Do You Hear What I Hear?: Fingerprinting Smart Devices Through Embedded Acoustic Components. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 441–452.

[17] Vincent Del Toro. 1985. Electric Machines and Power Systems. (1985).

[18] ADC Denso. 2011. QR Code Essentials. *Denso Wave* 900 (2011).

[19] Sanorita Dey, Nirupam Roy, Wenyuan Xu, Romit Roy Choudhury, and Srihari Nelakuditi. 2014. AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable. In *The 2014 Network and Distributed System Security (NDSS) Symposium*.

[20] Hu Ding and Jinhui Xu. 2014. Finding Median Point-Set Using Earth Mover's Distance. In *The 28th AAAI Conference on Artificial Intelligence (AAAI-14)*. 1781–1787.

[21] André Dolenc and Ismo Mäkelä. 1994. Slicing Procedures for Layered Manufacturing Techniques. *Computer-Aided Design* 26, 2 (1994), 119–126.

[22] FGAE. 2018. Camera FV-5. Retrieved 2018-4-2 from https://play.google.com/store/apps/details?id=com.flavionet.android.camera.pro

[23] Jay Gao. 2008. *Digital Analysis of Remotely Sensed Imagery*. McGraw-Hill Professional.

[24] Ian Gibson, David W Rosen, and Brent Stucker. 2010. Design for Additive Manufacturing. In *Additive Manufacturing Technologies*. Springer, 299–332.

[25] Frank L Hitchcock. 1941. The Distribution of A Product from Several Sources to Numerous Localities. *Journal of Mathematics and Physics* 20, 1 (1941), 224–230.

[26] Avesta Hojjati, Anku Adhikari, Katarina Struckmann, Edward Chou, Thi Ngoc Tho Nguyen, Kushagra Madan, Marianne S Winslett, Carl A Gunter, and William P King. 2016. Leave Your Phone at the Door: Side Channels that Reveal Factory Floor Secrets. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 883–894.

[27] Ari Juels. 2006. RFID Security and Privacy: A Research Survey. *IEEE Journal on Selected Areas in Communications* 24, 2 (2006), 381–394.

[28] AMRUTA L KABADE. 2016. Canny Edge Detection Algorithm. (2016).

[29] William Morrow Kays, Michael E Crawford, and Bernhard Weigand. 2012. *Convective Heat and Mass Transfer*. Tata McGraw-Hill Education.

[30] Liza Wallach Kloski and Nick Kloski. 2016. *Getting Started with 3D Printing: A Hands-on Guide to the Hardware, Software, and Services Behind the New Manufacturing Revolution*. Maker Media, Inc.

[31] Paul C Krause, Oleg Wasynczuk, and Steven D Pekarek. 2012. *Electromechanical Motion Devices*. Vol. 90. John Wiley & Sons.

[32] BC Kuo and J Tal. 1978. Incremental Motion Step Motors and Control Systems, Volume II. *SRL. Publishing* (1978).

[33] John H Lienhard. 2013. *A Heat Transfer Textbook*. Courier Corporation.

[34] Jan Lukas, Jessica Fridrich, and Miroslav Goljan. 2006. Digital Camera Identification from Sensor Pattern Noise. *IEEE Transactions on Information Forensics and Security* 1, 2 (2006), 205–214.

[35] James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, and Alex Marrs. 2013. *Disruptive Technologies: Advances that Will Transform Life, Business, and The Global Economy*. Vol. 180. McKinsey Global Institute San Francisco, CA.

[36] Nanoscribe. 2016. Photonic Professional GT. Retrieved 2017-08-11 from https://www.photonics.com/pr61179/Photonic_Professional_GT

[37] Sani R Nassif. 2001. Modeling and Analysis of Manufacturing Variations. In *Custom Integrated Circuits, 2001, IEEE Conference on*. IEEE, 223–228.

[38] Newsweek. 2015. Counterfeit Drug Industry. Retrieved 2018-4-17 from http://www.newsweek.com/2015/09/25/fake-drug-industry-exploding-and-we-cant-do-anything-about-it-373088.html

[39] The Global Language of Business. 2017. Universal Product Code (UPC). Retrieved 2018-4-17 from http://www.gs1us.org/resources/standards/ean-upc-visuals

[40] Tom Page. 2011. Design for Additive Manufacturing. (2011).

[41] Jantana Panyavaraporn, Paramate Horkaew, and Wannaree Wongtrairat. 2013. QR Code Watermarking Algorithm Based on Wavelet Transform. In *Communications and Information Technologies (ISCIT), 2013 13th International Symposium on*. IEEE, 791–796.

[42] Ravikanth Pappu, Ben Recht, Jason Taylor, and Neil Gershenfeld. 2002. Physical One-way Functions. *Science* 297, 5589 (2002), 2026–2030.

[43] Zhenbo Ren, Ping Su, Jianshe Ma, and Guofan Jin. 2014. Secure and Noise-free Holographic Encryption with A Quick-Response Code. *Chinese Optics Letters* 12, 1 (2014), 010601.

[44] Yossi Rubner and Carlo Tomasi. 2001. The Earth Mover's Distance. In *Perceptual Metrics for Image Database Navigation*. Springer, 13–28.

[45] Yossi Rubner, Carlo Tomasi, and Leonidas J Guibas. 2000. The Earth Mover's Distance as A Metric for Image Retrieval. *International Journal of Computer Vision* 40, 2 (2000), 99–121.

[46] David Salomon. 2004. *Data Compression: the Complete Reference*. Springer Science & Business Media.

[47] Samsung. 2017. Samsung Galaxy S8 Specifications. Retrieved 2018-4-17 from http://www.samsung.com/global/galaxy/galaxy-s8/specs/

[48] Science. 2018. Drug Manufacturing via 3D Printing. Retrieved 2018-4-17 from http://www.sciencemag.org/news/2018/01/you-could-soon-be-manufacturing-your-own-drugs-thanks-3d-printing

[49] Vellaisamy Seenivasagam and Ramesh Velumani. 2013. A QR Code Based Zero-Watermarking Scheme for Authentication of Medical Images in Teleradiology Cloud. *Computational and Mathematical Methods in Medicine* 2013 (2013).

[50] Tiziano Serra, Josep A Planell, and Melba Navarro. 2013. High-resolution PLA-based Composite Scaffolds via 3D Printing Technology. *Acta Biomaterialia* 9, 3 (2013), 5521–5530.

[51] Ruchir Y Shah, Prajesh N Prajapati, and YK Agrawal. 2010. Anticounterfeit Packaging Technologies. *Journal of Advanced Pharmaceutical Technology & Research* 1, 4 (2010), 368.

[52] Joseph E Shigley, Charles R Mischke, and Richard G Budynas. 2004. *Mechanical Engineering Design*. McGraw-Hill.

[53] Boris Škorić, Stefan Maubach, Tom Kevenaar, and Pim Tuyls. 2006. Information-theoretic Analysis of Capacitive Physical Unclonable Functions. *Journal of Applied Physics* 100, 2 (2006), 024902.

[54] Chen Song, Feng Lin, Zhongjie Ba, Kui Ren, Chi Zhou, and Wenyao Xu. 2016. My Smartphone Knows What You Print: Exploring Smartphone-based Side-channel Attacks Against 3D Printers. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 895–907.

[55] Chen Song, Aosen Wang, Kui Ren, and Wenyao Xu. 2016. EyeVeri: A Secure and Usable Approach for Smartphone User Authentication. In *Computer Communications, IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on*. IEEE, 1–9.

[56] Stefan H Steiner and R Jock MacKay. 2005. *Statistical Engineering: An Algorithm for Reducing Variation in Manufacturing Processes*. Vol. 1. ASQ Quality Press.

[57] Madhu Sudan. 1997. Decoding of Reed Solomon Codes Beyond the Error-correction Bound. *Journal of Complexity* 13, 1 (1997), 180–193.

[58] G Edward Suh and Srinivas Devadas. 2007. Physical Unclonable Functions for Device Authentication and Secret Key Generation. In *Proceedings of the 44th Annual Design Automation Conference*. ACM, 9–14.

[59] Iuliia Tkachenko, William Puech, Christophe Destruel, Olivier Strauss, Jean-Marc Gaudin, and Christian Guichard. 2016. Two-Level QR Code for Private Message Sharing and Document Authentication. *IEEE Transactions on Information Forensics and Security* 11, 3 (2016), 571–583.

[60] Keith M Tolk. 1992. *Reflective Particle Technology for Identification of Critical Components*. Technical Report. Sandia National Labs., Albuquerque, NM (United States).

[61] Pim Tuyls, Geert-Jan Schrijen, Boris Škorić, Jan Van Geloven, Nynke Verhaegh, and Rob Wolters. 2006. Read-proof Hardware from Protective Coatings. In *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 369–383.

[62] Pim Tuyls and Boris Škorić. 2006. Physical Unclonable Functions for Enhanced Security of Tokens and Tags. In *ISSE 2006-Securing Electronic Busines Processes*. Springer, 30–37.

[63] Ultimaker. 2013. As 3D Printing Becomes More Accessible, Copyright Questions Arise. Retrieved 2017-5-1 from http://www.npr.org/sections/alltechconsidered/2013/02/19/171912826/as-3-d-printing-become-more-accessible-copyright-questions-arise

[64] Ultimaker. 2017. Ultimaker Cura Software. Retrieved 2018-4-17 from https://ultimaker.com/en/products/cura-software

[65] Shinji Umeyama. 1991. Least-squares Estimation of Transformation Parameters Between Two Point Patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 13, 4 (1991), 376–380.

[66] Ron G Van Schyndel, Andrew Z Tirkel, and Charles F Osborne. 1994. A Digital Watermark. In *Image Processing, 1994. Proceedings. ICIP-94., IEEE International Conference*, Vol. 2. IEEE, 86–90.

[67] Sartid Vongpradhip and Suppat Rungraungsilp. 2012. QR Code Using Invisible Watermarking in Frequency Domain. In *2011 Ninth International Conference on ICT and Knowledge Engineering*. IEEE, 47–52.

[68] Aosen Wang, Tianjiao Wang, Chi Zhou, and Wenyao Xu. 2017. LuBan: Low-Cost and In-Situ Droplet Micro-Sensing for Inkjet 3D Printing Quality Assurance. In *Proceedings of the 15th ACM Conference on Embedded Networked Sensor Systems (SenSys '17).* ACM, Delft, Netherlands, 1–14.

[69] Bing Wang and ShaoSheng Fan. 2009. An Improved CANNY Edge Detection Algorithm. In *Computer Science and Engineering, 2009. WCSE'09. Second International Workshop on*, Vol. 1. IEEE, 497–500.

[70] Ian H Witten, Radford M Neal, and John G Cleary. 1987. Arithmetic Coding for Data Compression. *Commun. ACM* 30, 6 (1987), 520–540.

[71] Terry Wohlers. 2017. *Wohlers report 2017: 3D Printing and Additive Manufacturing State of the Industry.* Wohlers Associates.

Received November 2017; revised January 2018; accepted April 2018