PrinTracker: Fingerprinting 3D Printers using Commodity Scanners

Zhengxiong Li*[1], Aditya Singh Rathore*[1], Chen Song[1], Sheng Wei[2], Yanzhi Wang[3], Wenyao Xu[1]
[1] CSE Department, SUNY University at Buffalo, Buffalo, NY, USA
[2] ECE Department, Rutgers University, Piscataway, NJ, USA
[3] ECE Department, Northeastern University, Boston, MA, USA
Email: [1]{zhengxio, asrathor, csong5, wenyaoxu}@buffalo.edu
[2]{sheng.wei}@rutgers.edu
[3]{yanzhiwang}@northeastern.edu

ABSTRACT

As 3D printing technology begins to outpace traditional manufacturing, malicious users increasingly have sought to leverage this widely accessible platform to produce unlawful tools for criminal activities. Therefore, it is of paramount importance to identify the origin of unlawful 3D printed products using digital forensics. Traditional countermeasures, including information embedding or watermarking, rely on supervised manufacturing process and are impractical for identifying the origin of 3D printed tools in criminal applications. We argue that 3D printers possess unique fingerprints, which arise from hardware imperfections during the manufacturing process, causing discrepancies in the line formation of printed physical objects. These variations appear repeatedly and result in unique textures that can serve as a viable fingerprint on associated 3D printed products. To address the challenge of traditional forensics in identifying unlawful 3D printed products, we present *PrinTracker*, the 3D printer identification system, which can precisely trace the physical object to its source 3D printer based on its fingerprint. Results indicate that *PrinTracker* provides a high accuracy using 14 different 3D printers. Under unfavorable conditions (*e.g.* restricted sample area, location and process), the *PrinTracker* can still achieve an acceptable accuracy of 92%. Furthermore, we examine the effectiveness, robustness, reliability and vulnerability of the *PrinTracker* in multiple real-world scenarios.

KEYWORDS

Embedded Systems; Manufacturing Security; Forensics

ACM Reference Format: Zhengxiong Li, Aditya Singh Rathore, Chen Song, Sheng Wei, Yanzhi Wang, and Wenyao Xu. 2018. PrinTracker: Fingerprinting 3D Printers using Commodity Scanners. In 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18), October 15–19, 2018, Toronto, ON, Canada. ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3243734.3243735

1 INTRODUCTION

Additive manufacturing, also known as 3D printing, has become the main driving force of the third industrial revolution by fundamentally evolving product design and manufacturing [18, 31, 72, 93]. Due to the wide accessibility, 3D printers are increasingly exploited by malicious users to manufacture unethical (*e.g.*, counterfeiting a patented product) and illegal products (*e.g.*, keys and gun parts), shown in Figure 1 [42, 80, 88, 90]. To date, 3D printing has raised a host of unprecedented legal challenges since it could be utilized for fabricating potential untraceable crime tools, making the conventional forensic techniques infeasible in identifying the adversary.

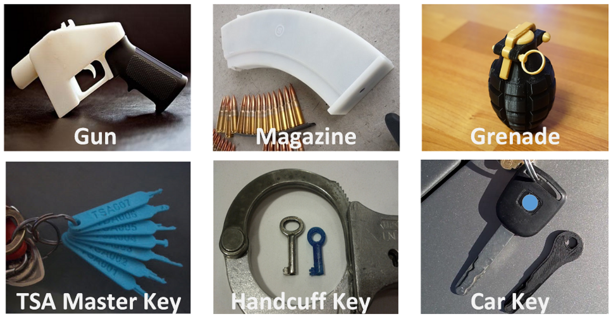


Figure 1: Potential untraceable 3D printed objects acquired from the crime scene [4, 15].

Concerned about the misuse of 3D printing technology, the U.S. Department of State urged International Traffic in Arms Regulation (ITAR) to limit the proliferation of 3D printed criminal tools. However, these regulations have a varying degree of efficacy and are inadequate to deal with the rapid growth of 3D printers [27]. Given the deficiency of law-enforcement agencies in preventing high-impact criminal activities [11, 13, 54, 55], *the ability to identify the source 3D printer, similar to digital image forensics* [77], *can immensely aid the forensic investigation.* Unfortunately, no tool exists for this application in either the computing or manufacturing literature. It is possible to alter the 3D printing process and add identifiable watermarks in either material [21, 63] or process patterns

* The first two authors contribute equally to this work.

CCS '18, October 15–19, 2018, Toronto, ON, Canada

ACM ISBN 978-1-4503-5693-0/18/10...$15.00
https://doi.org/10.1145/3243734.3243735

(*e.g.,* object tagging [68]). Nevertheless, these techniques are not applicable to the 3D printing forensics because the adversary can conveniently access the 3D printer, including design files, and operate it himself without any external supervision. Moreover, these techniques lack support for existing 3D printed objects that have already been manufactured without any watermarks [10].

It is a known fact that the variations arising from the mechatronic process are inevitable. In every manufacturing technique, these variations, typically observable on the resulting products, can serve as an intrinsic signature or fingerprint of the source manufacturing device. Existing studies demonstrate the presence of a concise signature on each paper that uniquely identifies the source document [28, 34, 70]. Furthermore, complementary metal-oxide-semiconductor (CMOS) process variations can be utilized as a physically unclonable method for silicon device identification [86]. Based on the mentioned literature, we hypothesize that each 3D printed product should possess a unique fingerprint and products from the same 3D printer will observe shared features in their fingerprints. If the hypothesis holds, a forensic identification system can be developed to retrieve the provenance of the criminal tool, *i.e.,* the 3D printed product, acquired from the crime scene. The system can provide unprecedented advantages in forensic applications: (1) it benefits the law-enforcement and intelligence agencies by identifying the source 3D printer leveraged by the adversary; (2) it serves as a fundamental solution for authentication of counterfeited products, preventing the substantial loss of intellectual property.

To realize this, the fingerprint of a 3D printer should possess specific properties that are consistent across the 3D printing domain. Firstly, 3D printed products fabricated from the same 3D printer need to comprise common features in their fingerprint. Secondly, distinct features would be observed in the 3D printed products from distinct 3D printers. Finally, the fingerprint should be universal and cannot be spoofed by the adversary. To validate this hypothesis, we address the three main challenges in the current 3D printing paradigm: (1) there is no in-depth study to prove the presence of a fingerprint on a 3D printed object that can establish its correlation to a corresponding printer. Moreover, the 3D printer is a complex system comprising numerous hardware interactions, thereby increasing the challenge in identifying the precise source of the fingerprint; (2) for developing a universal and cost-effective 3D printing forensic tool, the fingerprint must exist in each printed object and can be retrieved without damaging the physical object. In addition, the fingerprint must be resilient to the potential attacks employed by the adversary; (3) in forensic applications, it is strenuous to design a robust forensic tool while ensuring low computational cost, operational correctness and exceptional accuracy.

In this work, we first validate the existence of the fingerprint by studying the source of inevitable variations during the printing process. We investigate a low-cost fingerprint extraction technique capable of precisely measuring the minute textures of the object's surface while causing no damage to the physical object. Subsequently, we perform an extensive attack evaluation to assess the security of our proposed system and the underlying fingerprint. Finally, we present *PrinTracker*, an end-to-end 3D printer identification system, which can effectively reveal the 3D printer identity intrinsically "contained" in its printed objects. By utilizing the fingerprint extracted via a commodity 2D scanner, *PrinTracker* can precisely trace a printed object to its source printer. More importantly, it can be immediately applied in real-world forensic applications without any additional components or design modifications.

Summary: Our contribution in this work is three-fold:

- We conduct the first investigation of a 3D printer's fingerprint. Specifically, we empirically model the intrinsic connection between the 3D printer hardware imperfections and the textures on the associated printed product, which can be utilized as a viable fingerprint.
- We explore and implement an end-to-end 3D printing forensic system, *PrinTracker*, which is an immediately deployable solution and pertinent to 3D printed objects universally and economically.
- We demonstrate the effectiveness, reliability and robustness of *PrinTracker* through extensive experiments using 14 3D printers. Under unfavorable conditions (*e.g.* restricted sample area, location and process), *PrinTracker* can achieve an acceptable accuracy of 92%. We conduct further experiments to demonstrate the resilience of *PrinTracker* against multiple attacks with varying threat levels.

2 3D PRINTER PRELIMINARIES

2.1 Background and Fingerprint Hypothesis

Presently, 3D printers based on the Fused Deposition Modeling (FDM) technology are the most widely used type in commodity 3D printers [53]. As our work is a consolidation of empirical and theoretical efforts, we describe the fingerprint hypothesis using an FDM-type printer for better understanding. Our approach is also compatible with other printing technologies since every 3D printer possesses unique variations based on the corresponding mechatronic structure. These variations are inevitable and originate from the hardware imperfections in the mechanical components.

3D printing is an add-on process where the successive extrusion of material forms the lines and stack of these lines build the object. In addition, the superposition of lines determines the surface attribute of the printed object. The hardware architecture of the FDM-type printer is shown in Figure 2. It primarily includes three parts according to different physical functions, *i.e.,* Feeder, Positioner and Hot end. The control system regulates Feeder, Hot end and Positioner and governs the working process, according to the instructions present in the design file, commonly known as G-code, and the sensor feedback.

Variation from Feeder: The role of the Feeder is to feed the specified material, varying for each printer type, into the material conveyance channel. It includes the feed motor which uniformly moves filament through Hot end. However, there are limitations in precision, such as the motor step size that results in variations [9]. Moreover, the feeding friction varies due to the irregular V-shaped slots on the friction wheel, thereby inciting fluctuations in the steady-state error and response time of the Feeder [91]. These discrepancies lead to *unsteady volumetric flow* (line width) of the extruded filament during the printing process.

Variation from Positioner: It governs the spatial movement of the nozzle in the X-Y-Z direction. Its primary components include belt transmission, a screw rod, three stepper motors (X, Y, Z axis) and a platform. During the printing process, the fluctuations in the rotor position of the stepper motor and the synchronous belt transmission affect the *line trajectory vector* (XY axis) of the nozzle, while the error in the screw rod disturbs the positioning of the platform (Z axis) [71]. Moreover, the kinematics of Positioner determines the trajectory of Hot end, implying that imperfections in Positioner misalign Hot end to some extent.

Variation from Hot End: As a primary component of the 3D printer, Hot end comprises a nozzle through which the melted material is extruded forming a line, repeatedly. To control the heating temperature of the filament, the most optimal and widely used algorithm is the proportional-integral-derivative (PID) control or the fuzzy control [89]. However, both of them can dynamically stabilize the heating temperature only within an accepted range, which results in *non-uniform material fusion* and *unsteady extrusion amount*.

Hypothesis: Owing to the hardware imperfections in the above mechanical components, the variation caused by the system integration leads to a substantial impact on the printing [83]. While the printing performance might remain unaffected, these discrepancies are sufficient to alter the line formation of the printed object and induce a unique and measurable fingerprint which is associated with the mechatronic structure of the source 3D printer. Each printing process on a specific 3D printer is different; however, the fingerprint is consistent and repeatable due to the inevitability of hardware imperfections in the mechanical components according to their processing level [66]. We further illustrate the influence of 3D printer variation on a 3D printed object in Section 3.

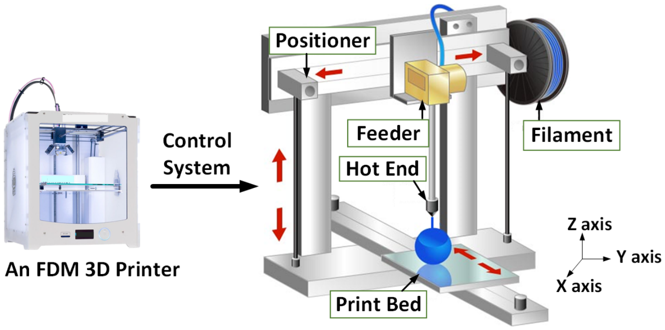


Figure 2: The mechatronic structure of an FDM 3D printer with inevitable variations arising from three primary components: Feeder, Positioner and Hot end.

2.2 Threat Model

We consider a crime scene where an adversary, hereafter Jack, plans to commit a crime, such as stealing valuable information or commodity. Unwilling to leave any trace (*e.g.,* providing ID when purchasing the gun), Jack decides to manufacture the criminal tool by himself with a 3D printer. After the attack is conducted, he leaves the crime scene without leaving any personal marks such as body hair or fingerprint. Instead, he unintentionally or intentionally abandons the tool at the crime scene (*e.g.,* credit card skimmer, cartridge case or magazine) or is unable to retrieve the broken object due to certain circumstances (*e.g.,* grenade debris or broken key in the lock cylinder). He may also employ various preventive strategies, further discussed in Section 9. Meanwhile, the forensic team investigating the crime scene discovers the object and needs to track down the adversary. For instance, a malicious card reader (with a 3D printed card skimmer) has been discovered attached to the real payment terminals [3] shown in Figure 3. A list of prominent suspects is prepared from the limited evidence acquired from the crime scene and stranded 3D printers are secured from the suspects' locality. However, the forensic team encounters several challenges in narrowing down the scope of the investigation. *PrinTracker* is proposed to solve the issue. Specifically, *PrinTracker* utilizes the object's texture and extracts the associated 3D printer's fingerprint contained inside, which acts as a traceable identifier for its source 3D printer. After obtaining the 3D printer ID, the forensic team can match it with the secured printers to reveal the 3D printer Jack used to fabricate the criminal tool. It is worth mentioning that *PrinTracker* can provide the auxiliary information in the presence of other conclusive evidence to identify the adversary.

In our work, we assume that the 3D printed object can be retrieved from the crime scene and it contains a measurable fingerprint. Furthermore, we assume that the adversary will not destroy the 3D printer prior or after committing the crime. These assumptions are practical since even prominent biometric applications (*e.g.,* face, fingerprint) are infeasible under the identical scenario. A non-invasive solution to address the sabotage of 3D printer would be to ensure that the proprietors of 3D printers, including Jack, pre-register the associated printers, along with the images of its printed models, in the *PrinTracker* database. These images will be updated at frequent intervals to ensure that the contained fingerprint is consistent with any alterations of the respective 3D printer. The update frequency is out of scope for this paper and is retained for the future work. During the investigation, the forensic team can easily compare the criminal tool's fingerprint with the *PrinTracker* database to identify the adversary.

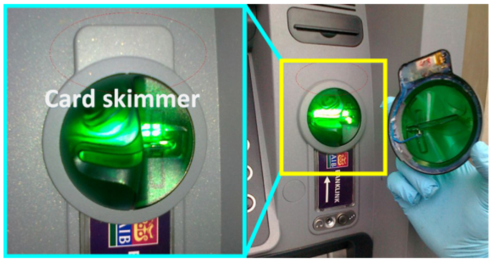


Figure 3: A 3D printed card skimmer acquired during investigation [3].

3 3D PRINTING CHARACTERIZATION: A FIRST PRELIMINARY STUDY

In this section, we characterize the influence of the printer variation upon the printing outcome in a qualitative manner to prove the existence of a viable fingerprint on a 3D printed product.

3.1 Object Surface Exploration

We assume that the components of a 3D printer are correctly installed and the device functions properly. Figure 4 illustrates the discrepancy in line formations between the design model and the physical object.

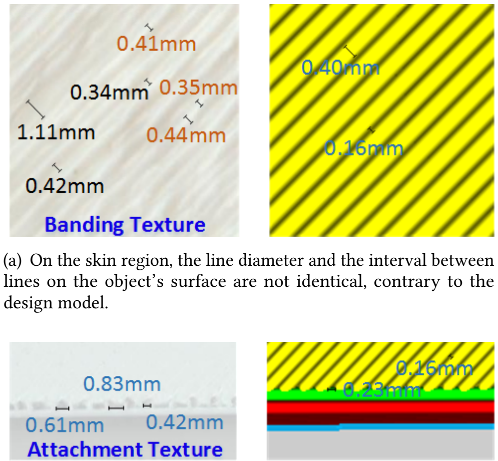
Banding Texture: In Figure 4(a), on the surface of the design model, the line diameter is 0.40mm and the interval between lines is 0.16mm, consistently. While on the object's surface, the line diameter can be 0.34mm, 0.42mm or even 1.11mm. For the interval between lines, the value varies from 0.35mm to 0.44mm. Neither of them is constant due to the unequal filament droplet flow rates, volumes and directions. These discrepancies lead to the formation of a unique texture, namely *banding*, on the object's surface (skin region). The banding is a critical concept in document security and has similar attributes concerning 3D printing [65]. It usually appears as non-uniform light and dark lines across the object's outer layer, perpendicular to the printing process direction. In the banding texture, the major minutia features are a rugged ridge, wide ridge, curved ridge, bifurcation, and short ridge (or dot) as shown in Figure 5(a).

Attachment Texture: A similar situation is observed in Figure 4(b). Near the object's edge, the width and shape of clearances are inconsistent in comparison to the design model, due to a sudden change in the direction of Hot end. Its inertia and loose belt degree cause the improper fusion between the infill and the edge. We leverage the filament filling and the proximity status between the skin and the contour of the object (wall) as a second texture, *i.e.,* the *attachment*. It appears as the continuous or discontinuous and regular or irregular clearance, ridge or air bubble. Also, its major minutia features are clearance, bluff and rugged terrain.

Insights: The acquisition process of these two kinds of textures is independent and universal. The sample location and sample window are not specific resulting in a flawless functioning in cases when only a piece of the object, regardless of its original shape, is obtained from a forensic scene. We have not noticed any inconsistency related to the occurrence of these textures in 10 months experimentation, further elaborated in Section 10. *Unique features found within the texture include aggregated characteristics of banding and attachment. These textures could be considered as the viable fingerprint of the 3D printer.*

3.2 Proof-of-concept

We conduct an experiment to explore the feasibility of using texture features as the fingerprint to differentiate among 3D printers. For a proof-of-concept, we employ four different 3D printers to individually fabricate five cuboids of size 5cm by 5cm by 5mm with the same printing configurations. After generating 20 cuboid objects, we use a commodity scanner (*e.g.*, Canon PIXMA MG2922) to scan every object once. Each image is stimulated with a banding sample of an 8mm by 8mm area, tagged '1', '2', '3' and '4' as shown in Figure 5(a). For ease of comparison, Figure 5(b) illustrates their variations against their sum of average, which reflects the similarity among the texture intensities (refer to Table 1). Each experiment on an image yields a data point on the graph and the points from multiple experiments by the same 3D printer exhibit a cluster. The textures, which are initially similar, begin to isolate on a two-dimensional plane. However, this model is insufficient to precisely identify all devices as the distances are confined between No.1&3 and No.2&4.



(a) On the skin region, the line diameter and the interval between lines on the object's surface are not identical, contrary to the design model.

(b) Near the object's edge, the width and shape of clearances are different from the design model.

Figure 4: Variations exist on 3D printed objects viewed using a digital microscope [16].

Summary: We prove that the 3D printed objects manufactured from the same 3D printer possess similar textures while those from different 3D printers have distinct textures. The printed object incorporates a texture surface which includes the *banding* and the *attachment*. In order to accurately classify among the diverse set of 3D printers, we continue to recruit an appropriate set of feature vectors and develop a 3D printer identification system, *PrinTracker*, elaborated in the following sections.

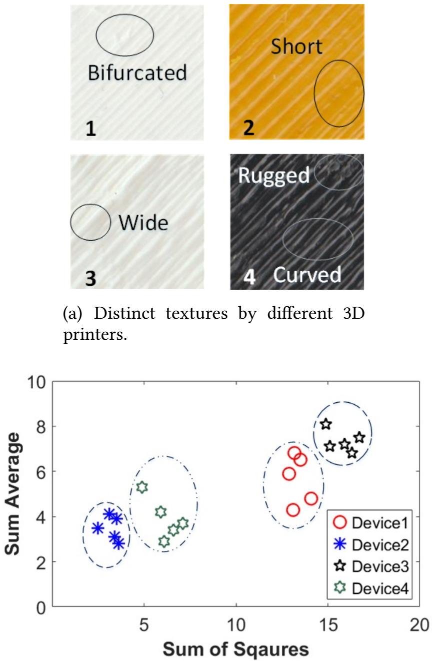
4 *PRINTRACKER* OVERVIEW

We describe our proposed system, *PrinTracker*, in Figure 6, which comprises three sub-modules: (1) Texture acquisition; (2) Texture analysis; (3) Forensic identification. First, we obtain the 3D printed object related to the adversary and use a commodity scanner to acquire the scanned sample of the object (as described in Section 5.1). Then, we analyze the texture from the image and extract its corresponding fingerprint. Through the fingerprint, we precisely identify the 3D printer leveraged by the adversary or discover other relevant information, which serves as a valuable aid during forensic investigations.

5 TEXTURE FINGERPRINT ANALYSIS

5.1 Texture Acquisition

The fingerprint on the printed object is in the form of the texture on the surface. Prior to modeling the fingerprint, we need to determine a robust, easy-to-use and effective way to acquire the texture. The methods of the structured-light, X-ray computed tomography or triangulation-based sensing methods have extensive calibration, strict environment setting or high-cost [96]. The camera in the smartphone has a restricted view, which causes surface deformation [41]. After comparison, we adopt a commodity scanner to scan



(a) Distinct textures by different 3D printers.

(b) Clustering on two feature dimensions.

Figure 5: A Proof-of-Concept for 3D Printer Identification (four different 3D printers with the same design file).

the object's surface and acquire its texture. During the scanning process, the object is placed on the flatbed, and a linear light source is used to illuminate the object. The scan head (built of mirrors, lenses, filters and contact image sensor (CIS) or charge-coupled device (CCD) arrays) moves slowly across the object by a belt to construct a uniformly illuminated and undistorted scanned image of the object. The texture is a pattern of local variations in image intensity, characterized by the spatial distribution of intensity levels in a neighborhood. As shown in Figure 7, a cylindrical object is scanned and there are two prominent textures, the banding and the attachment. Similar characteristics can be observed on other geometric shapes, such as a cube, triangular prism and so on. Thus, we observe that the scanner is attractive and highly competitive against other sensing methods, owing to its noninvasive characteristics and ease-of-operation.

Texture can be indicated as a global property and perceived exclusively from a sufficient image region. After acquiring the scanned image of the object's surface via a commodity scanner, we locate and crop the texture from the scanned image using the sample window as raw data. The acquired raw data includes noise from the imperfection of the sensor array or the environment. To maximize the essential fingerprint, we employ an image enhancement technique that intensifies the texture as well as removes the noise [17]. It maps the intensity values of an original gray-scale image to new values in a new image such that 1% of data are saturated at low and high intensities of the original image. Compared to other methods (*e.g.*, histogram equalization [78]), this technique increases the contrast of the output image, without affecting the original texture characteristics, which is resilient to undesirable artifacts and abnormal enhancement.

5.2 Fingerprint Model

In this section, we utilize the features from the texture on the 3D printed object to model the fingerprint of the 3D printer. To extract the prominent features, we model the texture from the preprocessed data. In 3D printing, the object's surface is comprised of filament droplets and the printer variations are reflected by these accumulated droplets. Consequently, the texture information in an image is contained in the overall spatial relationships among the pixels in the image. Since the spatial distribution of gray values is one of the defining qualities of the texture, we employ the Grey-Level Co-occurrence Matrix (GLCM) model in our work [92]. Specifically, the GLCM model can provide detailed quantification of textural changes and achieve superior performance compared to other texture discrimination methods [43].

GLCM is an estimate of the probability density function of the pixels in the image, which computes local features at each point in the image, and derives a set of statistics from the distributions of the local features.

The probability measure can be defined as Equation (1). N is the number of quantized gray levels. $C(i, j)$ represents the number of occurrences of gray levels i and j within the window. $p(i, j)$, the sum in the denominator represents the total number of gray level pairs (i, j) within the window and is bounded by an upper limit of $N \times N$. We use 8-bit gray level images where the gray levels N is 256:

$$p(i, j) = \frac{C(i, j)}{\sum_{i=0}^{N-1} \sum_{j=0}^{N-1} C(i, j)}. \tag{1}$$

The means for the columns and rows of the matrix are defined as Equation (2) and Equation (3), respectively:

$$u_x = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} i \cdot (i, y), \tag{2}$$

$$u_y = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} j \cdot (i, y). \tag{3}$$

5.3 Fingerprint Exploration

Fingerprint exploration is a crucial step for the 3D printer identification. Using the GLCM model, we extract 20 texture-based features from the model. Each feature influences the identification results, as shown in Section 8.1.3. These features can be categorized into two groups, first-order and second-order statistics. For instance, the features, such as mean and standard deviation, are first-order statistics which estimate the properties of individual pixel values. The second-order statistics (*e.g.*, cluster shade, cluster prominence and homogeneity) determine the properties of two or more pixel values at specific locations relative to each other [81]. We select 11 characteristic features for illustration, including their description and equation in Table 1. Including the remaining nine texture features (dissimilarity, entropy, maximum probability, variance, difference variance, difference entropy, inverse difference, information measure of correlation and inverse difference moment normalized [67]), the overall 20 texture features are used to construct a fingerprint. We further explore the classifiers that can be adopted in our work.

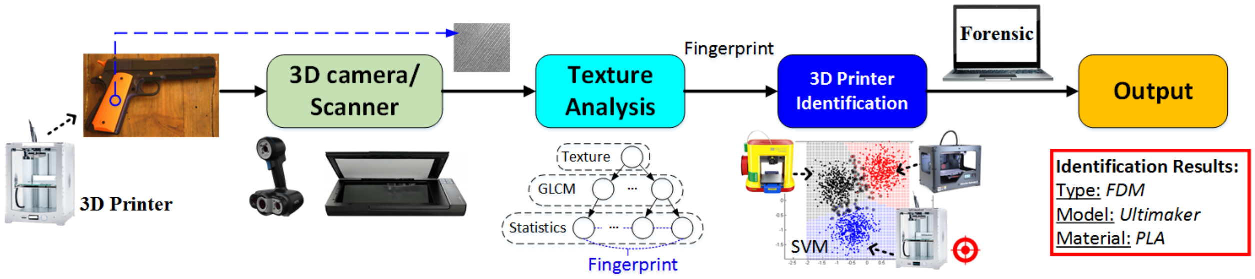


Figure 6: The system overview of *PrinTracker*. With the scanned sample of 3D printed object using a commodity scanner, respective textures are analyzed to extract the fingerprint. Owing to the effective comparison from the fingerprint in the pre-formed database, the physical object in forensic scenes can be precisely traced to its source 3D printer.

Table 1: List of features related to marginal probability.

Num.	Feature Name	Description	Mathematical Definition
1	Correlation	Measures the degree to which two variable's activities is associated and shows the joint probability occurrence of the specified pixel pairs.	$Correlation = \frac{\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}(i,j)p(i,j)-\mu_x\mu_y}{\sigma_x\sigma_y}.$
2	Contrast	Measures the local variations in the gray-level co-occurrence matrix	$Contrast = \sum_{k=0}^{N-1} k^2\{\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} p(i,j), \lvert i-j\rvert = k\}.$
3	Cluster Shade	Measures the skewness of the matrix and is believed to gauge the perceptual concepts of uniformity	$Shade = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1}(i+j-u_x-u_y)^3 p(i,j).$
4	Cluster Prominence	Reflects the cluster-type as Cluster Shade and shows higher range and range/mean (normalized range) values than the other measurements	$Prominence = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1}(i+j-\mu_x-\mu_y)^4 p(i,j).$
5	Energy	Measures the image homogeneousness and provides the sum of squared elements in the GLCM, known as uniformity or the angular second moment	$Energy = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} p(i,j)^2.$
6	Homogeneity	Measures the closeness of the distribution of elements and the statistical stationarity, that certain signal statistics of each texture region have the same values	$Homogeneity = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} \frac{1}{1+(i-j)} p(i,j).$
7	Sum Average	Connects with the enhancement intensity and the internal enhancement patterns	$SumAverage = \sum_{i=2}^{2N} i p_{x+y}(i).$
8	Sum Entropy	Measures the image complexity and is associated with the internal enhancement patterns and the enhancement intensity	$SumEntropy = -\sum_{i=2}^{2N} p_{x+y}(i)\log p_{x+y}(i).$
9	Sum of Squares: Variance	Describes how similar the intensities are within the region	$Variance = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1}(1-\mu)^2 p(i,j).$
10	Sum Variance	Links spatial frequency detection	$SumVariance = \sum_{i=2}^{2N}(i-Entropy)^2 p_{x+y}(i).$
11	Information Measure of Correlation 1,2 (IMC^1,IMC^2)	Measures the joint probability occurrence of the specified pixel pairs.	$IMC^1 = \frac{HXY-HXY1}{\max\{HX,HY\}},$ $IMC^2 = (1-exp[-2.0(HXY2-HXY)])^{1/2},$ $HXY = -\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} p(i,j)log(p(i,j)),$ $HXY2 = -\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} p_x(i)p_y(j)log(p_x(i)p_y(j)).$

6 3D PRINTER IDENTIFICATION

In our work, we employ a surface-based classification model instead of image-based, due to the distinction of a scanned image from the one obtained using a camera or a smartphone. In practical forensic application, we face a variety of constrained situations, including the use of a foreign device by the adversary that is not previously registered by the identification system. To address these challenges, we introduce an alien device detection model to evaluate the performance of the classification model.

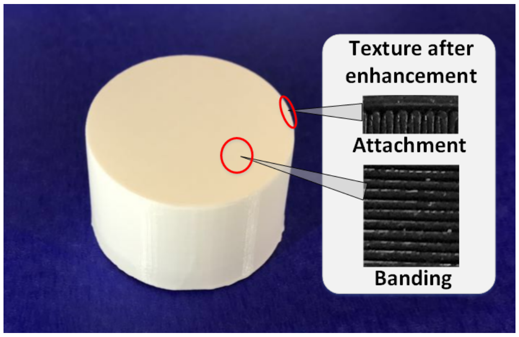


Figure 7: The two types of texture on a 3D printed object.

6.1 ID Provenance Method

3D printer identification can be formulated as a multi-class classification problem. We begin by defining the key terms in the 3D printed objects and then formulate the 3D printer identification problem.

Definition 1 *(Object Surface Set)*: For a 3D printing process, let s denote an area of the object's surface that is attained by a certain sample method. We define surface set S to contain every possible object surfaces. Specifically, we define s_0 as a complete object's surface that has the entire information about intrinsic signature of the source 3D printer. Figure 5(a) illustrates four distinct examples of s. Therefore,

$$\forall s \in S, \emptyset \subset s \subseteq s_0. \tag{4}$$

Definition 2 *(Surface Analysis Function)*: We denote the surface analysis function p as any function that can reflect the surface characteristics. Therefore, let set $\boldsymbol{P}$ represent a collection of selected surface analysis functions:

$$P = \{p_1(), ..., p_k()\}. \tag{5}$$

Definition 3 *(3D Printer Classification Function)*: Assume $C()$ to be a classification function that utilizes several 3D printer features to predict the 3D printer ID. The specific implementation of $C()$ responds to the real-world scenarios and the applied database mentioned in Section 2.2.

Formulation 1 *(Fingerprint Extraction)*: The goal of fingerprint extraction is to acquire the texture features set from the surface s. Specifically, a surface analysis function, denoted by set $\boldsymbol{P}$, is applied. We define $\boldsymbol{I}$ as the result set after applying $\boldsymbol{P}$ on s:

$$\boldsymbol{I}(s) = \{i_1 \leftarrow p_1(s), ..., i_k \leftarrow p_k(s)\}. \tag{6}$$

Therefore, $\boldsymbol{I}$ represents the integration of texture features, marked as feature vector.

Formulation 2 *(3D Printer Identification)*: The purpose of 3D printer identification is to recognize the source 3D Printer of the tested object's surface s using the fingerprint extraction, say $\boldsymbol{I}$, and 3D printer classification function $C()$. Specifically, $\mathbf{R}_{ID}$ is the result of the predicted source 3D Printer ID:

$$\mathbf{R}_{ID} = C(\boldsymbol{I}(s)). \tag{7}$$

Considering our work is the first exploration of 3D printer identification, for classification function $C()$, we employ two universal and easy-to-deploy classifiers, *i.e.,* Support Vector Machine (SVM) and K-Nearest Neighbor (KNN), that can be leveraged to identify 3D printers based on the fingerprint. Previously, SVM and KNN have been successfully applied in scanner and printer identification [65] and multi-touch authentication [73], respectively. SVM locates an optimal hyper-plane in a high-dimensional space to perform the classification, while KNN stores all available cases and classifies new cases based on a similarity measure.

During the training phase, n scanned images of printed objects are obtained from m 3D printers. Each scanned image has a feature vector, and nm sets of feature vectors are used to train the classifier. We employ an ensemble classification approach for training, mainly to achieve robustness over any single classification model. For the testing phase, the system processes the overall predicted result for k test scanned images to output either a positive match with one of the 3D printers that it has been trained with or an *alien* device, implying that the concerned printer is not included in the training database. In such a case, the system initiates a training request that collects n scanned images from the alien printer, inserts a new entry to the classifier database, and re-trains the system. Although false negatives might occur, additional side-information can be leveraged to exercise caution before re-training.

Algorithm 1 Alien 3D printer detection model

```
Input: $I(k)$: K test scan images from an object
       $Thd$: a threshold to distinguish the alien device
Output: $A$: A judgment if it is an alien device
        $R_{ID}$: The predicted classification result for the object
$C_i, T_i, I \leftarrow 0$                                  ▷ Init the parameter
for $i \in \{1, ..., K\}$ do $C(i) = Classify(I(k))$    ▷ Classify each image and get K predicted results
end for
$T = tabulate(C(:))$;                  ▷ Statistical analysis predicted results
$score = max(T(:, 3))$;  ▷ Find the maximum probability value as the classification score
if $score < Thd$ then
    $disp('It\ is\ an\ alien\ device!')$  ▷ If the classification score is less than the threshold, it is considered as the alien device
else
    $I = find(T(:, 3) == score)$;  ▷ Otherwise, find the one with the maximum probability value as the final predicted result
    $R_{ID} = T(I, 1)$;
    $disp(['The\ result\ is\ :', R_{ID}])$;
end if
return $F$
```

6.2 Alien Device

In real-world applications, it is possible that some 3D printers are not included in the identified suspect database (known as alien devices), which may spoof the forensic technique or cause false alarms. To evaluate the overall performance of the multi-class classification in the presence of alien devices, we use a maximum probability value among k predicted results as the classification score as shown in Algorithm 1. To distinguish an alien device from the known devices, we apply a threshold on the classification score. If the classification score is less than the threshold, then the trace is declared

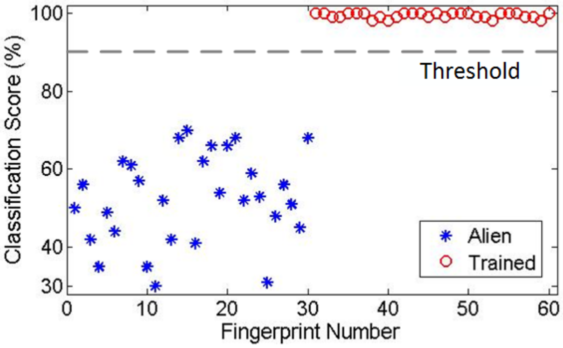


Figure 8: The threshold margin for detection of alien 3D printers.

alien. Figure 8 plots the classification scores for both alien and trained 3D printers (the first half of the X-axis are the fingerprints on the objects from alien devices and the second half is from trained devices). It is observed that the alien printers present a relatively low score, and a threshold for reliable segregation is not hard to find. In *PrinTracker*, we empirically pick one threshold (such as 90%) to separate the alien devices with high accuracy and robustness.

7 BENCHMARKING AND EVALUATION

In this section, we comprehensively evaluate the performance of *PrinTracker* using 14 different 3D printers. We also describe the experimental setup and performance metrics in the evaluation.

7.1 Test-Bench Preparation

Model Fabrication: 3D Printers can be leveraged to produce illegal tools for malicious use. To proof the concept of illegal fabrication in 3D printing, we employ the standard bump keys as the key sample model to evaluate *PrinTracker* performance because (1) bump keys are widely used but subject to counterfeiting in daily life; (2) bump key models contain a rich set of geometric features in different granularity levels to examine the sensitivity of *PrinTracker*. For the sake of generality, we also test the performance with other object models in Section 8.3. We employ 14 commercially off-the-shelf 3D printers, including four Ultimaker series, four MakerBot series, two XYZ printing series and four Formlabs series. These printers operate on two categories of most commonly used working types (*i.e.*, FDM and SLA) and three types of materials (*i.e.*, PLA, ABS and Photopolymer), as presented in Table 2. Each printer produces five key samples with the common printing configurations. Specifically, FDM printers support layer thickness from 60 to 600 microns, while for SLAs it could be from 25 to 100 microns. Each key sample takes from 40 to 60 minutes to fabricate.

Sample Digital Database: As shown in Figure 9, in order to acquire the texture on the bump key, we employ a conveniently accessible commodity scanner Canon MG2922 (US $60), equipped with CIS, whose highest scan resolution is 1200dpi. Manually, we scan the entire set of keys, one at a time, where each key is scanned for 50 times with a 600dpi resolution in an indoor environment. Thus, the sample database contains 70 bump keys and 3500 scanned images. Each scanned image is resized to s_0 (refer to Section 6.1), and stored with the dimensions of 640 × 250px and the size of 90KB in PNG format. In addition, to obtain substantial results, we evaluate our system under each setting 10 times. Unless specified, each time we randomly choose three keys out of the five keys from the individual 3D printer as our training sample set and use the rest for testing. Thus, $3 \times 14 \times 50 = 2100$ randomly chosen images are used for training and $2 \times 14 \times 50 = 1400$ images for testing individually.

Table 2: List of 3D printer setup.

Num.	Device Model	Type	Material
1	Ultimaker 2 Go	FDM	PLA
2	Ultimaker 2 Go	FDM	PLA
3	Ultimaker 2 Go	FDM	PLA
4	Ultimaker 2 Extended+	FDM	PLA
5	MakerBot Replicator	FDM	PLA
6	MakerBot Replicator	FDM	PLA
7	MakerBot Replicator 2X	FDM	ABS
8	MakerBot Replicator 2X	FDM	ABS
9	XYZ Printing Da Vinci Mini Maker	FDM	ABS
10	XYZ Printing Da Vinci Mini Maker	FDM	ABS
11	Formlabs Form 1+	SLA	Photopolymer
12	Formlabs Form 1+	SLA	Photopolymer
13	Formlabs Form 1+	SLA	Photopolymer
14	Formlabs Form 1+	SLA	Photopolymer

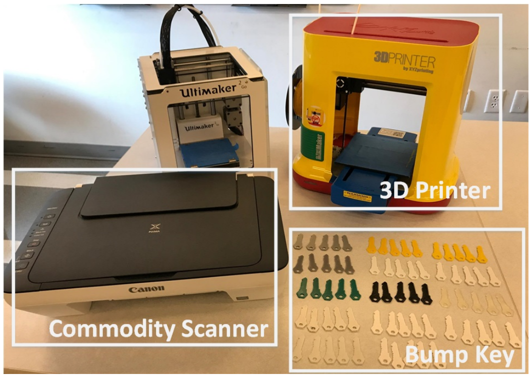


Figure 9: Experimental setup for 3D printer identification where bump keys are fabricated and scanned via a commodity scanner.

7.2 Performance Metrics and Configuration in Forensic Applications

Metrics: As a potential forensic tool, *PrinTracker* will have a significant role in 3D printing forensics if it can reveal valuable information during an unlikely scenario where it barely identifies the

3D printer. Therefore, we evaluate the classification performance from two views: $View1$: Identification of 3D printers; and $View2$: Recognition of 3D printer working types. $View1$ shows the ability to track the source 3D printer and $View2$ aids to narrow the scope for investigation. To evaluate *PrinTracker* in the following sections, we study the metrics of *precision*, *recall*, *F1-measure* and *accuracy* to indicate the performance in different angles. Specifically, *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. *F1-measure* is the harmonic mean of *precision* and *recall*, which is a significant measure, especially with an uneven class distribution. *Accuracy* is the most intuitive performance measure and it is simply a ratio of correctly predicted observation to the total observations [99]. Besides, we also adopt the Equal Error Rate (EER) and the Receiver Operating Characteristic (ROC) since these are the optimal metrics for evaluating identification systems [26]. The ROC curve is created by plotting the true positive rate (TPR) against the false positive rate (FPR) at various threshold settings. EER is the operating point in ROC, where FAR and the false reject rate (FRR=1-TPR) are equal. The lower EER value, the better performance.

McNemar Test: The performance of *PrinTracker* depends on the design of recognition approaches. To investigate the sensitivity of classification model, we perform McNemar Test towards two mostly used classification configurations, *i.e.*, SVM and KNN. For SVM, considering the sample database is linearly inseparable, we use the radial basis function (RBF) kernels [65]. For KNN, we test the K configuration from 1 to 15, and K=3 achieves the best performance. We configure KNN as K=3 in the following analysis.

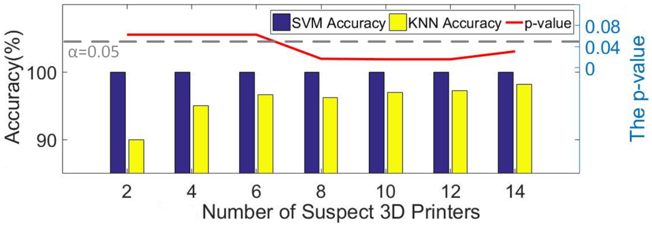


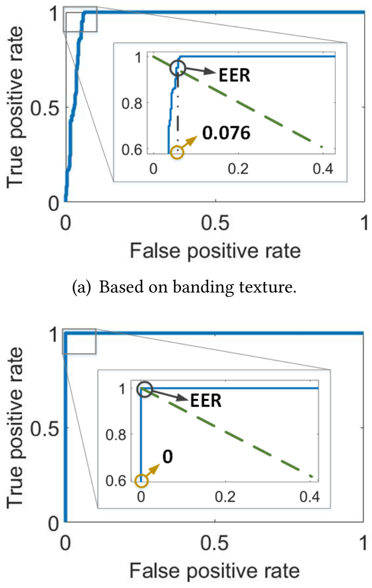
Figure 10: Comparison of two classifiers on accuracy for 3D printer identification, indicating the superiority of SVM.

Besides measuring accuracy, we conduct a set of McNemar tests to determine if there is a significant difference in performance of SVM and KNN on the sample database [45]. McNemar test is a frequently used test for matched-pair data, with a significance level $\alpha = 0.05$. Under the null hypothesis, the two algorithms should have the same error rate. If the null hypothesis is correct, the p value is below 0.05. Figure 10 shows that along the class number from 2-14, the accuracy of the SVM is close to 100% throughout all case, higher than the KNN performance. Furthermore, the McNemar test shows when there are more than eight classes, the p value maintains around 0.02, which is less than 0.05 and rejects the null hypothesis. This result indicates that SVM has superior performance over KNN in this application. In the following sections of evaluation, *PrinTracker* will be configured with the SVM classifier.

7.3 Overall Performance of Identifying 3D Printers

To maximize the efficiency of *PrinTracker* for 3D printer identification, a fingerprint comprising of sufficient textural characteristics, *i.e.,* the banding and attachment texture, needs to be extracted from the 3D printed object. However, it is not uncommon to discover only a segment of an object during the forensic investigation. Therefore, it would be ideal for the PrinTracker to precisely identify the source 3D printer ($View1$) in a scenario where only one of the two textural information is available. To this end, we evaluate the performance of $View1$ by considering individual textures for 14 printer classes. In the testing sample set, each class owns 100 scanned images. The resulting classification score is shown as a confusion matrix in Figure 12(a) and 12(b). In the confusion matrix plot, the darker the color contrast of a cell, the higher is the classification score. Seemingly, the diagonal cells are the darkest, indicating that the fingerprint from a 3D printer was accurately classified to its associated class.

Performance of Banding Texture: The 3D printer identification results from Figure 12(a) demonstrate an average precision and recall of 91.81% and 92.59% respectively. The F1-measure is 92.20%, while the EER is observed to be 0.076, as illustrated in Figure 11(a). Upon careful analysis, we notice that No.5 3D printer is misclassified as No.9 and No.10 3D printer even though it utilizes visibly different material from the other two printers. The reason is due to the nature of our algorithm which statistically describes the textures, primarily based on the interleaving of material filaments, rather than their visual characteristics.

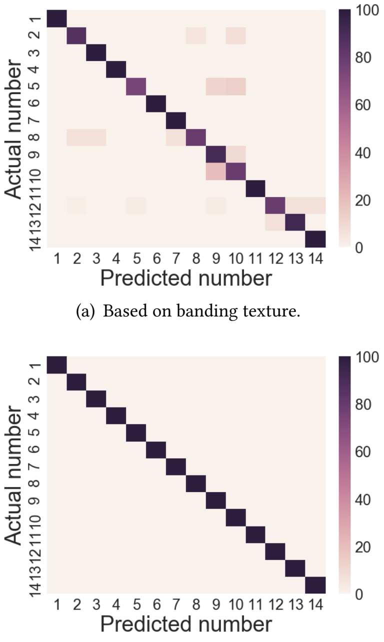


(a) Based on banding texture.

(b) Based on attachment texture.

Figure 11: The ROC curve of the overall performance.

Performance of Attachment Texture: As indicated from the Figure 12(b), the classification performance is exceptional with precision, recall and F1-measure as 100%. Correspondingly, the EER



(a) Based on banding texture.

(b) Based on attachment texture.

Figure 12: The confusion matrix of identifying printers on 14 3D printers with banding and attachment textures.

is 0, as shown in Figure 11(b). Compared to the banding texture, the attachment texture achieves a superior performance due to the drastic fluctuations in the speed and direction of motor movements within the connection area between the skin and the wall. Therefore, the printer variations (mentioned in Section 2) have a significant influence on the attachment texture leading to profound textural information on the contour of the 3D printed object.

In conclusion, our results demonstrate that a 3D printer could be precisely identified through its artifacts by using either the banding or attachment texture as a fingerprint. We continue to study the performance evaluation based on the attachment texture unless stated otherwise.

7.4 Overall Performance of Identifying Machine Types

Considering the rare occurrence when *PrinTracker* barely identifies the 3D printer, it would be crucial to diagnose the 3D printing machine type to narrow the investigation scope. In $View2$, there are two mainstream machine types in the sample database. In our testing sample set, FDM and SLA classes contain 1000 and 400 scanned images, respectively. Table 3 describes that these two machine types are classified with 99.79% precision and 99.79% recall on average. F1-measure is 99.79%. It can be observed that *PrinTracker* has a better performance on SLA. It is because the texture feature is more significant with SLA, due to its advanced processing technology [51]. The results indicate that *PrinTracker* could accurately recognize the machine type of a 3D printer to narrow down the scope of suspects.

Table 3: The confusion matrix of recognizing machine types of 3D printers using the attachment texture.

		Predicted		
		FDM	*SLA*	Recall
Actual	*FDM*	997	3	99.70%
	SLA	0	400	100%
	Precision	100%	99.26%	

7.5 Impact of Alien Device

In the real-world application, the database would include every 3D printer brand and model. However, it would be ideal if *PrinTracker* could recognize the alien devices, for which it is not trained in advance. We design an experiment to explore the performance of the alien devices based on the attachment texture. All the 3D printers fabricate five keys, and we acquire 50 scanned images for each key. Out of 14 3D printers, we randomly choose eight devices for the training set but never use them for testing. From the remaining six printers, we first randomly select two devices for testing and evaluate the performance of *PrinTracker*. Next, we randomly select four devices from the six printers and repeat the previous step. We include these six printers gradually to obtain an evaluation of alien devices.

The results, in Figure 13, indicate that *PrinTracker* can successfully reject the alien devices using the threshold value of the classification score. The overall performance of the system does not change considerably with the increasing number of alien devices.

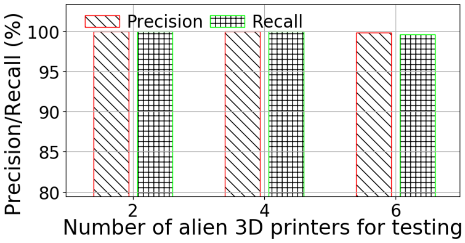
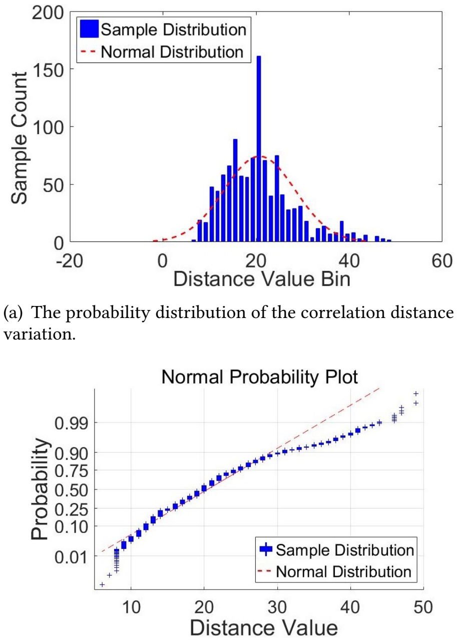


Figure 13: Precision/Recall with alien devices.

7.6 Fingerprint Space Analysis

For an authentication system, the security of the fingerprint is critical. If the outcome of each textural feature is limited or specific, it can be guessed easily. To verify the security of *PrinTracker*, we examine if the textural feature output is a unique, uniformly distributed, and independent random number. It is worth mentioning that it is the fingerprint that reflects each 3D printer distinction, not the textural feature. Considering our feature data are decimal within a range, not binary [75], we inspect if the normal distribution is fitted to the data of the Correlation (refer to Table 1). For the ease of the analysis, we consider the Correlation feature, which is essential for both $Views$ (refer to Section 8.1.3). Similar characteristics could be observed on other textural features as well.



(a) The probability distribution of the correlation distance variation.

(b) The normal distribution test.

Figure 14: Evaluation to determine the uniqueness of Correlation feature.

Figure 14(a) illustrates the probability distribution of the Correlation feature value after testing 1120 scanned images, where 16 of 50 scanned images are randomly selected for each object from the sample database. The y-axis represents the count of images in each bin. The x-axis shows the Correlation value range of each bin. The histogram presents our experimental results, where the dotted line shows a fitted normal distribution with parameters. Its mean, $\mu = 2.07$, is in its 95% significance level [2.02,2.11] with high accuracy. In Figure 14(b), we employ the normal probability plot to verify the fingerprint's security [94]. The result resembles the diagonal line, implying that the distribution is similar to the normal. Lastly, we conduct a t test. The test decision h is 1.0 and p value is 0.01, significantly lower than $\alpha = 0.05$, which indicates that the result distribution is intensely akin to the normal distribution.

It is a known fact that if the fingerprint capacity is limited, its security will be severely undermined. In our work, one texture feature contains at least 8 bits, indicating the minimum capacity of the fingerprint to be 160 bits. Therefore, our feature vector possesses excellent security with a large capacity.

8 PERFORMANCE ANALYSIS

In this section, we consider several factors that could affect our ability to model fingerprint and classify devices. These factors are grouped into: (a) Sensitivity; (b) Reliability; (c) Robustness [38, 99].

8.1 Sensitivity Analysis

8.1.1 Effect of Sample Area: Evidence left in the forensic scene often has a huge distinction with respect to its area. Even a minute piece of an object can be valuable to narrow down the investigation if the forensic tool is resilient. We examine the performance of *PrinTracker* with different sample areas of the banding and attachment texture as displayed in Table 4. For the banding texture, the area varies from $64mm^2$ to $4mm^2$, marked from $B1$ to $B5$. For the attachment texture, the area ranges from $10mm^2$ down to $2mm^2$, marked from $F1$ to $F5$.

Table 4: List of sample areas for respective textures.

Area num.	B1	B2	B3	B4	B5
Banding (mm^2)	64	49	36	16	4
Area num.	F1	F2	F3	F4	F5
Attachment (mm^2)	10	8	6	4	2

The experimental result is shown in Figure 15. We observe that the larger the sample area is, the higher the precision and recall. Specifically, for the banding texture $B1$, the precision and recall are 91.81% and 92.59%. The F1-measure is 92.20%, respectively. The precision declines by more than 4% on both $B2$ and $B4$, while in others by 0.01% and 0.58%, which implies that the precision and recall reduce in a stepped manner. The reason is that the banding texture is based on the interleaving of filaments whose diameter is diversified for different 3D printers. In our sample database, most diameters are less than 1.6mm. Therefore, the result depends on the filament count in the sample area, which is not altered continuously. Lastly, $4mm^2$ sample area is the theoretical boundary based on the banding texture. However, for the attachment texture, the boundary could be as small as a $2mm^2$ area. We observe that all precision and recall values are higher than 98% for the attachment texture. The distinctiveness in this area could be clearance or air bubble, which could be microscopic (less than 1mm). *PrinTracker* can provide a robust performance as long as the sample area is larger than $2mm^2$.

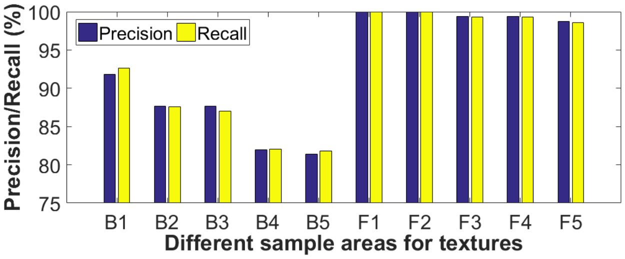


Figure 15: The classification performance with different sample areas for respective textures on the printed keys.

8.1.2 Effect of Sample Location: In scenarios where only a fraction of the evidence is acquired from the forensic scene, it is not uncommon that the object may not contain the entire details of the skin or wall. Instead, the object could consist of partial segments of the skin or wall, increasing the difficulty in obtaining individual textures. Therefore, we evaluate the changes in performance when the sample location covers different portions of the skin and wall.

To certify the relationship between the texture location and the classification performance, we first choose a $50mm^2$ area on a key, encompassing the banding and attachment textures. We use a $6mm^2$ sample window to scan the area from the origin by 0.5mm steps towards the right and upwards. In Figure 16(a), the color indicates the F1-measure. It can be observed that as the scanning region approaches the attachment texture, the value of the F1-measure increases. It is close to 100% when the entire attachment texture is analyzed. Moreover, a high-low transition is present around 2mm upwards, where there is a dividing line between both textures. To evaluate the performance of *PrinTracker* under different sample locations with different areas, we select four evenly distributed sample areas, $B1$ and $B2$ for the banding texture, and $A1$ and $A2$ for the attachment texture, shown in Figure 16(b). Evidently, similar results can be observed as Section 8.1.1, indicating that the selection of sample location for individual banding and attachment texture has a limited influence on the system performance.

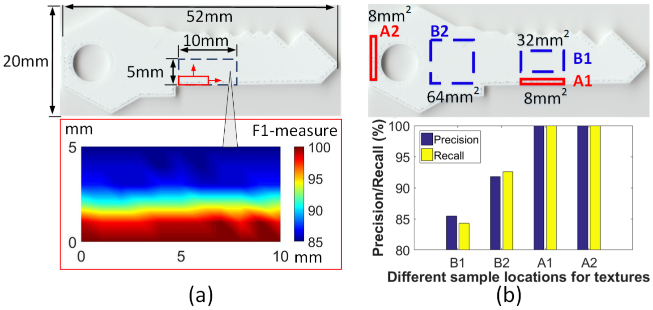
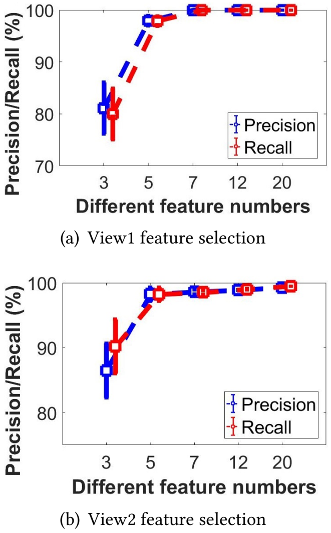


Figure 16: The classification performance for respective textures on the keys with variation in sample locations (a) within a specific area; (b) across the whole object.

8.1.3 *Effect of Feature Selection:*

As the size and dimensionality of database containing 3D printer samples increases, accessing which features has the greatest outcome on the *PrinTracker* performance can aid in saving time and resources, which is an essential advantage during forensic investigations. In this experiment, we investigate the impact of feature dimension on the performance of our system for $View1$ and $View2$. In our work, we extract 20 features. We start with the entire set of 20 features and reduce the number gradually. The precision and recall for each test feature are described in Figure 17. For $View1$, the precision of classification decreases from 100% to 97.92%, with the feature dimension decreasing from 20 to 5. Afterward, the precision quickly decreases to 81.11%, when the feature number reduces to three. The variation of the precision/recall increases with the decrease in the number of features. A similar turning point, around the feature number 5, is observed for $View2$. For $View2$, the precision is 99.28%, 98.25% and 86.50% for 20, 5, 3 features respectively.

We further analyze the two $Views$ based on the five features. For $View1$, Contrast, Cluster Prominence, Sum average, Sum Entropy and Information Measure of Correlation1 are the essential features. For $View2$, we choose Cluster Prominence Maximum Probability, Sum of Squares: Variance, Information Measure of Correlation2 and Sum Variance. All features are scrutinized in Table 1. Compared to $View2$, $View1$ excessively utilizes the texture homogeneity, while $View2$ takes advantage of deviation value among the texture [92]. Therefore, for different forensic applications, it is essential to select the optimal features in order to maximize the system performance.



(a) View1 feature selection

(b) View2 feature selection

Figure 17: The classification performance with variation in texture feature number.

8.2 Reliability Analysis

8.2.1 *Effect of Working Environment:*

Manufacturing room environment control is noticeably vital in standard industry working process. However, the individual workshop can also be the conventional workplaces for 3D printing. To investigate the impact of variation in a working environment on the fingerprint, we design the following experiment. We evaluate the performance of No.1, 2 and 3 3D printers in four environmental setups with different humidity and temperature settings. Specifically, each printer fabricates three keys in each environment and each key is scanned 15 times for the testing set. We use the training set from the sample database. The results of our experiment are shown in Table 5. The precision and recall are all 100%. Similarly, the F1-measure is 100%. The fingerprint possesses a strong tolerance to working environment within the range of 10-20°C temperature and 30-70% humidity, and the performance of *PrinTracker* remains unaffected.

8.2.2 *Effect of Printing Process Configuration:*

In the manufacturing domain, a mindful selection of printing process parameters is crucial for ensuring ideal product quality. Furthermore, in the real-world application, the nature of these configurations are unknown for the criminal tool, *i.e.,* the 3D printed object acquired from the crime scene. Therefore, it is critical for *PrinTracker* to precisely identify the source 3D printer, regardless of the printing parameters utilized to manufacture the 3D object. We employ the No.1, 2 and 3 3D printers and consider three situations with varying speed, resolution and print materials. There are three settings under each situation. In each setting, we produce three keys. Each key is scanned three times (totally 81 scanned images for each situation) and the images are then tested against the training set in the sample

Table 5: The recognition result of *PrinTracker* in external environments. Note: 10°C=50°F, 20°C=68°F.

		Temp. (°C)	
		10	*20*
Humid. (%)	*30*	100& 100	100& 100
	70	100& 100	100& 100

*In the cell: Precision(%) & Recall(%).

database. In the *speed situation*, we set the nozzle speed at 120mm/s (S1), 110mm/s (S2) and 100mm/s (S3). In the *resolution situation*, we set the layer thickness at 0.06mm (R1), 0.1mm (R2) and 0.15mm (R3). In the *materials situation*, we select three material, one 3D Universe 2.85mm PLA in white (M1), two Ultimaker 2.85mm PLA in white (M2) and gray (M3). Figure 18 describes the results with accuracy in every situation to be higher than 99%, thereby implying that *PrinTracker* is resistant to the variation in printing parameters within 120-100mm/s nozzle speed and 0.06-0.15mm layer thickness in different materials. Out-of-range configuration might pose a risk of spoofing our solution, but the products will suffer from severe deformation and poor quality, which compromises the usability.

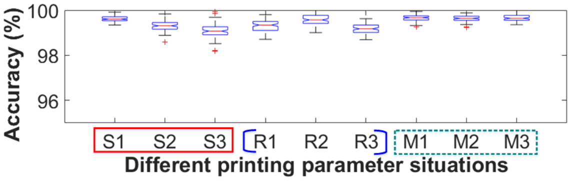


Figure 18: The system performance of 3D printed keys with different printing process parameters.

8.2.3 Effect of Working Status: In practical manufacturing, the 3D printer functions favorably without interruption. However, it may confront some unexpected scenarios. Three situations are summarized. Firstly, the 3D printer works continually without any interruption or intermission. Secondly, the material suffers from a fracture during the extrusion, and new material needs to be reloaded. Lastly, the printing process is paused owing to certain accidents and is resumed after the situation is resolved. To examine the impact of 3D printer working statuses on the fingerprint, we conduct the following experiment.

We manipulate No.1, 2, 3 3D printers for 10 hours in identical fashion. In the first six hours, we continuously produce nine keys and have a 40 minutes break to avoid "machine fatigue" on the next part. Then, we reload the material and continue to fabricate two keys and have another 40 minutes break. In the last 80 minutes, we fabricate the last two keys, while pausing in the middle of each task for one minute. Eventually, we scan each key 15 times as the testing set and use the training set from the sample dataset. The results of the experiment are shown in Figure 19. The precision and recall are both 100%, implying that the fingerprint remains consistent during an extensive working period and is insensitive to the 3D printer's working status.

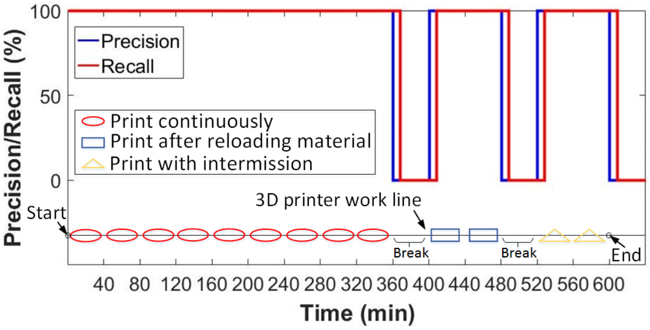


Figure 19: The system performance along the entire work duration under different situations.

8.3 Robustness Analysis

8.3.1 Effect of Objects with Different Geometries: In forensic applications, valuable evidence can include objects with different geometric shapes, such as unexploded bombs [1] and cartridge cases [55]. Therefore, it is important to investigate the robustness of *PrinTracker* with various 3D prints. To this end, we conduct the further evaluation with *five* designs of distinct shapes and curvatures, including standard car key, handcuff key, grenade, magazine and bullet (see samples in Figure 20). For ease of evaluation, each design is fabricated with three selected 3D printers, and each 3D printer produces five sample copies. Other experimental procedures are the same with above experiments, and the experimental setup is with Table 2. As shown in Figure 20, both precision and recall in the case of the car key, grenade and magazine are close to 100%. For all objects, the average F1-measure is 92.20%. In comparison, the precision and recall in the case of handcuff key and bullet drop down to around 83% due to limited effective areas in scanned samples. It is because that these two samples both have cylindrical-shape, and commodity scanner cannot provide a high imaging quality with objects with the large curvature. We further discuss the specific solution for these curved objects in Section 10. These results show an encouraging indication that *PrinTracker* is scalable to a large number of objects.

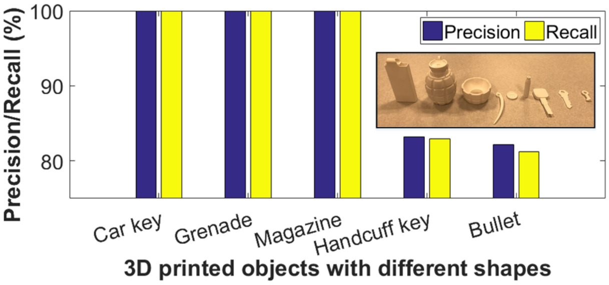


Figure 20: The identification performance of 3D printed objects with different geometric shapes, implying the strong robustness of our *PrinTracker*.

8.3.2 Effect of Scalability: To ensure an immediate and effective real-world deployment of *PrinTracker*, it is necessary to evaluate the

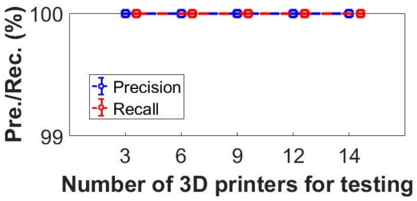


Figure 21: The identification performance with increasing 3D printers as test dataset.

scalability with increasing 3D printers. We conduct an experiment where we increase the number of objects gradually and measure the performance of *PrinTracker* at each stage. In the first stage, we consider only three randomly chosen devices to train and evaluate the system with their traces. Next, we increase the scope to six devices and again evaluate the performance of our system. We gradually increase the number of devices in each stage and measure the *PrinTracker* performance.

Figure 21 shows that the precision and recall of the system for different objects considered is nearly 100%. The performance of *PrinTracker* and the fingerprint remains consistent across a broad set of objects.

9 ATTACK ANALYSIS

In this section, we examine the security of our *PrinTracker* in the following attack scenarios.

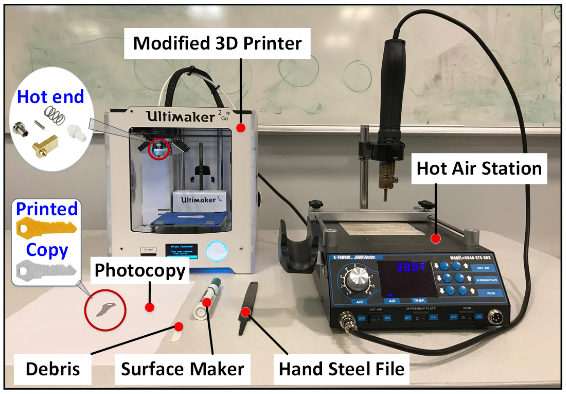


Figure 22: Experimental setup for attack analysis using photocopying, modified 3D printer, surface maker, hand steel file, debris and hot air station.

Zero-Informed Attack: The naive attacker luckily acquires a 3D printer, which has a mechatronic structure similar to an authorized printer in the database. He is confident that when a forensic team obtains the evidence, no forensic tool can help them trace the evidence to his 3D printer. However, *PrinTracker* can even recognize fingerprints from the same model of 3D printers in the same batch, as proved in Section 7.3. In addition, the attacker cannot guess the textural feature outcome since the feature value is randomly distributed (refer to Section 7.6).

Photocopying Attack: In the scenario where the attacker is not able to obtain the authorized 3D printer but acquires the texture of associated object's surface, he copies it onto another object to surpass the authentication. To evaluate its effectiveness, we utilize six 3D printers (*i.e.*, No.2, 4, 6, 8, 10 and 12) to manufacture five keys individually. Subsequently, we generate three photocopies of each bump key (totally 90 photocopies) at the highest print resolution (1200 × 1200 dots per inch) on a commodity printer. An example of a photocopy from a key is illustrated in Figure 22. During testing, the *PrinTracker* refuses the entire set of photocopies and identifies them as an alien device. Due to the halftoning effects of the photocopying process [98], the scanned texture would differ from the original one, which significantly depletes the possibility to break the system. In real practice, this attack can be easily detected by the investigator due to a significant change in the exterior of the object.

Forgery Attack: We assume that the attacker has access to the specification of an authorized 3D printer, rather than machine itself, and exploits another printer to produce an identical fingerprint with the authorized one. There are two methods to achieve this goal. First, he can utilize a fine-grained printer to mimic the coarse one. By using millions of dollars worth of advanced manufacturing machine, it is possible to imitate a few hundred dollars worth of desktop 3D printer. However, it is not economically feasible and the investigator can easily verify the trading record to acquire the details of this extraordinary 3D printer's purchase. Moreover, given the extensive detail of all texture elements, computing or simulating the texture pattern is computationally expensive, where the complexity increases exponentially with the texture area.

Second, he can modify the 3D printer with some components from the authorized printer. We believe this to be the most plausible attack. To explore this, we consider three 3D printers (No.1, 2 and 3) and remove their *Hot ends*. Progressively, we install the *Hot end* of the No.1 onto the No.2, the *Hot end* of the No.2 onto the No.3 and *Hot end* of the No.3 onto the No.1. An example of a modified 3D printer can be seen in Figure 22. For each modified 3D printer, we manufacture five bump keys (total 15 newly printed keys) and scan each new key five times (total 75 scanned images). Upon testing the scanned images using *PrinTracker*, we observe that the entire set of these images is refused and classified as an alien device. The reason is that the fingerprint not only generates from the manufacture variations but also from the complex integrated effect of mechanical components. Thus, *PrinTracker* would remain unaffected.

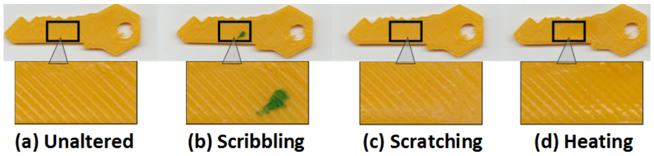


Figure 23: One original key and three altered keys for denial-of-service attack.

Denial-of-Service Attack: We consider a scenario where the attacker neither has access to a million-dollar manufacturing machine nor is experienced to modify the components of a 3D printer. He is a conventional attacker who is assured that the alteration or sabotage of the 3D printed object's surface would aid in avoiding detection by the law-enforcement agencies. Before leaving the crime scene, he leverages traditional approaches of scribbling, cracking, scratching or heating of the object's surface in a time-restricted situation. We investigate the security of our method against the non-ideal handling of the 3D printed object by utilizing three 3D printers (No.1, 7 and 9) to produce three keys for each printer under individual non-ideal condition. Furthermore, each key is scanned five times.

- ▷ **Scribbling:** On the surface of every key, we drew random patterns with a surface marker such that each pattern covers close to 10% area of the sample box. An example of a scribbling pattern is shown in Figure 23(b). We observe that alcohol can be used to clean the ink from the key's surface effortlessly. We test the scanned images of the cleaned surface's texture with results showing an accuracy of 100%, implying the *PrinTracker* has a high tolerance to the scribbling attack.
- ▷ **Cracking:** Assuming the bump key is broken when opening a lock, debris may be observed at the crime scene as shown in Figure 22. We crack the front end of the sample key and validate the associated scanned images using *PrinTracker*. Our results show an accuracy of 100% in precisely identifying the 3D printer ID, implying that the cracking method is futile. The reason is due to the robustness of *PrinTracker* to the sample location and area, as mentioned in Section 8.1.
- ▷ **Scratching:** We scratch 10% of the sample box area using a hand steel file. The hand steel file and the resulting scratched surface are illustrated in Figure 22 and Figure 23(c), respectively. The initial results using the scanned images of the scratched surface demonstrate an accuracy of 100%. In order for the attack to be successful, this method has to be performed precisely in order to destroy each texture minutia feature since the feature's diameter is 0.4mm. Even in the scenario where the entire surface is destroyed, it would still be possible to acquire the fingerprint from the 3D object as described in the following attack.
- ▷ **Heating:** We consider an attack where the adversary destroys the surface of the concerned 3D printed object. To perform this, we employ the *XTronic* hot air station [2] (refer to Figure 22) to partially melt the surface of the sample keys at a temperature of 230 °C, higher than the common working temperature 210 °C. It is worth to mention that for completely destroying the object surface, the adversary would take the risk of totally losing the products for malicious use (*e.g.*, bend keys with heat) besides additional intensive time effort. The resulting surface, described in Figure 23(d), is deprived of intricate textures containing the fingerprint of the source 3D printer. However, in most design files, several outer layers are identical and share the same minutia features. Even if the outer layer is destroyed, it can be removed to analyze the characteristics of the inner layer. We acquire the scanned images of the inner layer and leverage the *PrinTracker* to identify the 3D printer ID. The accuracy is observed to be 100%, validating the ineffectiveness of this attack.

The mentioned approach employing the examination of inner layers can also be utilized to improve the performance with respect to curved 3D printed objects. We believe that the dependency of the fingerprint on an object's geometry and heating requires closer investigation, and will be a next critical step to *PrinTracker*.

10 DISCUSSION

Aging: *Aging effect* on the object is a conventional process in the physical and polymer material domain [95]. However, with the development of preservation techniques [14], it is possible to have a long-term, stable, non-volatile, clean corrosion protection for the printing material. To evaluate the *Aging effect* on the object, we re-sample the objects as the test group after *10 months* by using the original template group as the training set. We also evaluate the presence of *Aging effect* on the device by re-producing the two bump keys for each device (No. 1, 2, 4, 9 and 12 3D printers) as the test group after *10 months* by using the original template group as the training set. In both cases, the identification performance for the new testing group remains exceptional. Furthermore, it is unlikely that suspects will wait several years after printing the criminal tool to perform a crime. 3D printer's *Aging effect* is an open problem in hardware security. We continue to research on this problem.

Other Material Types: PLA, ABS and photopolymer, which are the most popular materials in 3D printing, are used in the evaluation. Learned from the rationale, every 3D printer has its unique variations and our method could be applied to other types of printing material like plastic, metal, ceramics and porcelain. However, additional experiments are required for validation which would involve custom upgrades in the method for different materials.

Scanner Property: Concerning the scanner, there are three problems worth exploring. Firstly, scanner resolution is critical for acquiring clear and detailed textures. Presently, a majority of scanners support the resolution at 600dpi. We performed the identification experiments with a *300dpi* resolution using the attachment texture (refer to Section 7.3), with results showing an acceptable performance of 90.27% precision and 90.03% recall. Secondly, to evaluate the performance of *PrinTracker* for different scanner types, we employ two distinct commodity scanners (HP OfficeJet 5255 and Canon MB2720) to scan the sample bump keys and repeat the identification experiments on the attachment texture. The results show an average performance of 99.96% precision and 99.91% recall. Finally, we need to consider the case where the flatbed scanner cannot scan the object effectively, such as any curved surface objects. In such a scenario, an expensive 3D scanner having accuracy up to 7μm could be used [12], which would require advanced operational skills.

Alien Device: Although *PrinTracker* can accurately reject the alien devices, it has a limited effect since there is no information about the specific alien device that printed the object. A typical solution is to continuously update the pre-formed database to include an extensive set of 3D printer IDs. Another method is to efficiently combine the watermarking and our proposed technique, by ensuring that individual textures survive the printing process. The forensic team can leverage these textures to obtain additional information about the device and its proprietor. Presently, this is an open problem for device forensics, *e.g.,* firearms investigation [50]. Considering our work is the first exploration of 3D printer identification, this challenge will be addressed in future work.

11 RELATED WORK

Object and Product Fingerprinting: Miscellaneous technologies are developed in surface fingerprint readers, which utilize the microstructure of the surface or its physical characteristics. The microstructure of the surface represents its profound details and material properties upon examination at close range or under magnification [40, 87]. In paper fingerprinting, the fiber structure of the paper [28, 34, 64, 84], the texture speckle pattern [70] and the material translucent patterns [79] serve as unique identifiers for the paper document. For silicon devices, physical characteristics, known as the intrinsic PUF (Physically Unclonable Functions), are widely leveraged for identification [47]. Moreover, considerable efforts have been devoted to two approaches based on digital signals delay [59, 62, 75, 76] and bi-stable logic cells [49, 52, 58, 74, 85, 86]. These studies validate that the intrinsic component microscopic variation in the physical system is random and inevitable. To the best of our knowledge, *PrinTracker* is the first study to employ fingerprint characterization in the 3D printing domain.

Electronic System Identification: With respect to a complex system or a device consisting of multiple components, several studies analyze fingerprints to distinguish among devices by externally observing the response of a specific signal according to device distinctions. In scanner and printer identification [57], the measured noise data of the imaging sensor and the banding texture on the paper are leveraged as an intrinsic signature. In recent years, studies describe methods to extract fingerprint of the smartphone from accelerometer readings stimulated with an identical vibration sequence by recording the signals via a microphone [25, 37, 39, 97]. For different RFID devices, the modulation shapes and spectral features of the signal emitted by transponders are different, which is employed as a fingerprint for the device [36]. Furthermore, a camera fingerprint has been extensively studied based on CFA interpolation [22], demosaicing artifacts [23], pixel defects condition [48] and PRNU noise of video-camera imaging sensors [19, 30, 61]. The cross-browser, bugs and electronic device fingerprints are analyzed with respect to the hardware features [29, 32, 33, 44, 46, 69].

3D Object Watermarking: 3D watermarking [20, 24, 35, 56] is a specific technology employed to validate the product's authenticity. It induces a watermark by modifying the model's local geometric configuration and shape topology. However, it is mainly used in the digital domain [60, 63, 82] and remains severely under-explored for 3D printed real-world products. Moreover, 3D printing enables fabrication shift from manufacturer to the user which allows the adversary to ensure that no evidence/trace information, resulting from any watermarking approach, is present on the printed object.

12 CONCLUSION

This paper shows that 3D printers possess unique fingerprints. With 3D printer's vast availability and personalization, the exponential rise in the novel threats related to 3D printing requires immediate attention. Specifically, we demonstrate that the fingerprint stems from the 3D printer hardware imperfections during the manufacturing process. The profound texture of the printed object's surface reflects the fingerprint which is adequate to identify the device leveraged by the adversary. Our comprehensive analysis of 14 3D printers validates the existence of fingerprints on every printed object, which is viable even in uncontrolled environments. More importantly, we conduct extensive experiments to confirm the effectiveness, reliability and robustness of our proposed system, with results indicating exceptional precision and recall rates in the classification of 3D printers and their process types. The research findings are an essential step for understanding 3D printer fingerprints and their applications at large.

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] Accessed: 2017-1-27. *3D printers are new weapon in fight against landmines.* https://www.usatoday.com/story/news/world/2015/09/23/printers-fight-against-landmines/72666674/.

[2] Accessed: 2017-10-11. *X-TRONIC MODEL 5040 XTS Hot Air Rework Station and Preheating Station.* https://xtronicusa.com/X-TRONIC-5000-SERIES-MODEL-5040-XTS-Hot-Air-Rework-Station-&-Preheating-Station-p25881615.

[3] Accessed: 2017-2-12. *What you need to know about card skimming.* https://www.engadget.com/2014/07/28/credit-card-skimming-explainer/.

[4] Accessed: 2017-3-21. *Anyone can now print out all TSA master keys.* https://www.engadget.com/2016/07/28/tsa-master-key-3d-models/.

[5] Accessed: 2017-4-12. *PT100 datasheet.* https://www.itsirl.com/datasheets/RTM13.pdf.

[6] Accessed: 2017-4-18. *Belt datasheet.* http://www.optibelt-usa.com/fileadmin/files/Catalogs_and_Manuals/TECH_MANUAL_TIMING_BELTS.pdf.

[7] Accessed: 2017-4-18. *Gear datasheet.* http://qtcgears.com/tools/catalogs/PDF_Q420/Section%207.pdf.

[8] Accessed: 2017-4-18. *Screw datasheet.* http://www.thomsonlinear.com/downloads/actuators/Worm_Gear_Screw_Jacks_ctuk.pdf.

[9] Accessed: 2017-5-18. *Motor datasheet.* https://mecheltron.com/sites/default/files/webresources/MechanicalElectroMech/StepperMotors/pdf/42BYGH_data_sheet.pdf.

[10] Accessed: 2017-6-10. *AB-857 Firearms: identifying information.* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?billid=201520160AB857.

[11] Accessed: 2017-6-20. *3D Printing New Kinds of Crime.* http://www.policechiefmagazine.org/3d-printing-new-kinds-of-crime/.

[12] Accessed: 2017-6-21. *CyberGage360.* http://cyberoptics.com/3dscanning-metrology/cybergage360/.

[13] Accessed: 2017-6-26. *3D Printer Confiscated in Organized Crime Raid.* http://www.engineering.com/3DPrinting/3DPrintingArticles/ArticleID/8642/3D-Printer-Confiscated-in-Organized-Crime-Raid.aspx.

[14] Accessed: 2017-6-27. *Anti-Corrosion Intercept Technology Now Available in 3D Printable Form.* https://3dprint.com/159174/intercept-technology-3d-printable/.

[15] Accessed: 2017-8-23. *Fear of downloadable guns becoming a reality.* https://www.zdnet.com/article/fear-of-downloadable-guns-becoming-a-reality/.

[16] Accessed: 2018-2-17. *XCSOURCE 20X-800X 8 LED USB 3D Digital Zoom Microscope Endoscope Magnifier PC Video Camera with Stand TE071.* http://microscopesunlimited.com/product/xcsource-20x-800x-8-led-usb-3d-digital-zoom-microscope-endoscope-magnifier-pc-video-camera-with-stand-te071/.

[17] Y Abdallah and R Yousef. 2015. Augmentation of X-Rays Images using Pixel Intensity Values Adjustments. *International Journal of Science and Research (IJSR)* 4, 2 (2015), 2425–2430.

[18] 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.* ACM, 419–433.

[19] KR Akshatha, AK Karunakar, H Anitha, U Raghavendra, and Dinesh Shetty. 2016. Digital camera identification using PRNU: A feature based approach. *Digital Investigation* 19 (2016), 69–77.

[20] Patrice Rondao Alface and Benoit Macq. 2007. From 3D mesh data hiding to 3D shape blind and robust watermarking: A survey. In *Transactions on data hiding and multimedia security II.* Springer, 91–115.

[21] Christian Bayens, Garcia L Le T, R Beyah, M Javanmard, and S Zonouz. 2017. See No Evil, Hear No Evil, Feel No Evil, Print No Evil? Malicious Fill Patterns Detection in Additive Manufacturing. In *26th USENIX Security Symposium (USENIX Security 17).* USENIX Association, 1181–1198.

[22] Sevinc Bayram, H Sencar, Nasir Memon, and Ismail Avcibas. 2005. Source camera identification based on CFA interpolation. In *Image Processing, 2005. ICIP 2005. IEEE International Conference on*, Vol. 3. IEEE, III–69.

[23] Sevinc Bayram, Husrev T Sencar, and Nasir Memon. 2008. Classification of digital camera-models based on demosaicing artifacts. *digital investigation* 5, 1 (2008), 49–59.

[24] Oliver Benedens. 1999. *Geometry-based watermarking of 3D models*. Technical Report. FRAUNHOFER INST FOR COMPUTER GRAPHICS DARMSTADT (GERMANY) VIRTUAL REALITY DEMONSTRATION CENTRE.

[25] Hristo Bojinov, Yan Michalevsky, Gabi Nakibly, and Dan Boneh. 2014. Mobile device identification via sensor fingerprinting. *arXiv preprint arXiv:1408.1416* (2014).

[26] Ruud M Bolle, Jonathan H Connell, Sharath Pankanti, Nalini K Ratha, and Andrew W Senior. 2013. *Guide to biometrics*. Springer Science & Business Media.

[27] Danton Bryans. 2015. Unlocked and loaded: government censorship of 3D-printed firearms and a proposal for more reasonable regulation of 3D-printed goods. *Ind. LJ* 90 (2015), 901.

[28] 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), 475–475.

[29] SL Yinzhi Cao and E Wijmans. 2017. Browser Fingerprinting via OS and Hardware Level Features. In *Proceedings of the 2017 Network & Distributed System Security Symposium, NDSS*, Vol. 17.

[30] Lit-Hung Chan, Ngai-Fong Law, and Wan-Chi Siu. 2012. A two dimensional camera identification method based on image sensor noise. In *Acoustics, Speech and Signal Processing (ICASSP), 2012 IEEE International Conference on*. IEEE, 1741–1744.

[31] Wenyao Xu Chi Zhou Zhanpeng Jin Kui Ren Chen Song, Zhengxiong Li. 2018. My Smartphone Recognizes Genuine QR Codes! Practical Unclonable QR Code via 3D Printing. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 3 (2018).

[32] Kyong-Tak Cho and Kang G Shin. 2016. Fingerprinting Electronic Control Units for Vehicle Intrusion Detection.. In *USENIX Security Symposium*. 911–927.

[33] Kyong-Tak Cho and Kang G Shin. 2017. Viden: Attacker Identification on In-Vehicle Networks. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 1109–1123.

[34] William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J Alex Halderman, and Edward W Felten. 2009. Fingerprinting blank paper using commodity scanners. In *Security and Privacy, 2009 30th IEEE Symposium on*. IEEE, 301–314.

[35] Adam Dachowicz, Siva Chaitanya Chaduvula, Mikhail Atallah, and Jitesh H Panchal. 2017. Microstructure-Based Counterfeit Detection in Metal Part Manufacturing. *JOM* 69, 11 (2017), 2390–2396.

[36] Boris Danev, Thomas S Heydt-Benjamin, and Srdjan Capkun. 2009. Physical-layer Identification of RFID Devices.. In *Usenix Security Symposium*. 199–214.

[37] 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.

[38] Anupam Das, Nikita Borisov, and Matthew Caesar. 2016. Tracking Mobile Web Users Through Motion Sensors: Attacks and Defenses.. In *NDSS*.

[39] Sanorita Dey, Nirupam Roy, Wenyuan Xu, Romit Roy Choudhury, and Srihari Nelakuditi. 2014. AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable.. In *NDSS*.

[40] Maurits Diephuis and Sviatoslav Voloshynovskiy. 2013. Physical object identification based on famos microstructure fingerprinting: comparison of templates versus invariant features. In *Image and Signal Processing and Analysis (ISPA), 2013 8th International Symposium on*. IEEE, 119–123.

[41] Maurits Diephuis, Sviatoslav Voloshynovskiy, and Taras Holotyak. 2015. Sketchprint: physical object micro-structure identification using mobile phones. In *Signal Processing Conference (EUSIPCO), 2015 23rd European*. IEEE, 834–838.

[42] Davis Doherty. 2012. Downloading infringement: patent law as a roadblock to the 3D printing revolution. *Harv. JL & Tech.* 26 (2012), 353.

[43] Alaa Eleyan and Hasan Demirel. 2011. Co-occurrence matrix and its statistical features as a new approach for face recognition. *Turkish Journal of Electrical Engineering & Computer Sciences* 19, 1 (2011), 97–107.

[44] Sebastian Eschweiler, Khaled Yakdan, and Elmar Gerhards-Padilla. 2016. discovRE: Efficient Cross-Architecture Identification of Bugs in Binary Code.. In *NDSS*.

[45] Morten W Fagerland, Stian Lydersen, and Petter Laake. 2013. The McNemar test for binary matched-pairs data: mid-p and asymptotic are better than exact conditional. *BMC medical research methodology* 13, 1 (2013), 91.

[46] David Formby, Preethi Srinivasan, Andrew Leonard, Jonathan Rogers, and Raheem A Beyah. 2016. Who's in Control of Your Control System? Device Fingerprinting for Cyber-Physical Systems.. In *NDSS*.

[47] Blaise Gassend, Dwaine Clarke, Marten Van Dijk, and Srinivas Devadas. 2002. Silicon physical random functions. In *Proceedings of the 9th ACM conference on Computer and communications security*. ACM, 148–160.

[48] Zeno J Geradts, Jurrien Bijhold, Martijn Kieft, Kenji Kurosawa, Kenro Kuroki, and Naoki Saitoh. 2001. Methods for identification of images acquired with digital cameras. *Proc. of SPIE, Enabling Technologies for Law Enforcement and Security* 4232 (2001), 505–512.

[49] Jorge Guajardo, Sandeep S Kumar, Geert Jan Schrijen, and Pim Tuyls. 2007. FPGA intrinsic PUFs and their use for IP protection. In *CHES*, Vol. 4727. Springer, 63–80.

[50] Julian Sommerville Hatcher, Frank J Jury, Jac Weller, and Thomas G Samworth. 1997. *Firearms investigation, identification and evidence*. Univ. Book Agency.

[51] David D Hernandez. 2015. Factors affecting dimensional precision of consumer 3D printing. *International Journal of Aviation, Aeronautics, and Aerospace* 2, 4 (2015), 2.

[52] Daniel E Holcomb, Wayne P Burleson, and Kevin Fu. 2009. Power-up SRAM state as an identifying fingerprint and source of true random numbers. *IEEE Trans. Comput.* 58, 9 (2009), 1198–1210.

[53] 3D Hubs. *Digital Manufacturing Trends 2018*. https://www.3dhubs.com/trends Accessed: 2018-2-2.

[54] Rick Hurd. 2016. Homemade gun in Stanford student's murder-suicide spurs question on 'ghost guns'. (Aug 2016). https://www.mercurynews.com/2015/08/06/homemade-gun-in-stanford-students-murder-suicide-spurs-question-on-ghost-guns/

[55] Beau Jackson, Rushabh Haria, Michael Petch, Katie Armstrong, Michael Molitch-Hou, Alicia Miller, Jenny Shang, Lydia Mahon, and Nick Hall. 2018. AR-15 with 3D Printed Lower Receiver Seized in Oregon. (Jan 2018). https://3dprintingindustry.com/news/ar-15-with-3d-printed-lower-receiver-seized-in-oregon-52234/

[56] Zachary C Kennedy, David E Stephenson, Josef F Christ, Timothy R Pope, Bruce W Arey, Christopher A Barrett, and Marvin G Warner. 2017. Enhanced anti-counterfeiting measures for additive manufacturing: coupling lanthanide nanomaterial chemical signatures with blockchain technology. *Journal of Materials Chemistry C* 5, 37 (2017), 9570–9578.

[57] Nitin Khanna, Aravind K Mikkilineni, George T-C Chiu, Jan P Allebach, and Edward J Delp. 2008. Survey of Scanner and Printer Forensics at Purdue University. *IWCF* 8 (2008), 22–34.

[58] Sandeep S Kumar, Jorge Guajardo, Roel Maes, Geert-Jan Schrijen, and Pim Tuyls. 2008. The butterfly PUF protecting IP on every FPGA. In *Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on*. IEEE, 67–70.

[59] Jae W Lee, Daihyun Lim, Blaise Gassend, G Edward Suh, Marten Van Dijk, and Srinivas Devadas. 2004. A technique to build a secret key in integrated circuits for identification and authentication applications. In *VLSI Circuits, 2004. Digest of Technical Papers. 2004 Symposium on*. IEEE, 176–179.

[60] Suk-Hawn Lee, Tae-Su Kim, Byung-Ju Kim, Seong-Geun Kwon, Ki-Ryong Kwon, and Kuhn-Il Lee. 2003. 3D polygonal meshes watermarking using normal vector distributions. In *Multimedia and Expo, 2003. ICME'03. Proceedings. 2003 International Conference on*, Vol. 3. IEEE, III–105.

[61] Chang-Tsun Li. 2010. Source camera identification using enhanced sensor pattern noise. *IEEE Transactions on Information Forensics and Security* 5, 2 (2010), 280–287.

[62] Daihyun Lim, Jae W Lee, Blaise Gassend, G Edward Suh, Marten Van Dijk, and Srinivas Devadas. 2005. Extracting secret keys from integrated circuits. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 13, 10 (2005), 1200–1205.

[63] Benoît Macq, Patrice Rondao Alface, and Mireia Montanola. 2015. Applicability of watermarking for intellectual property rights protection in a 3d printing scenario. In *Proceedings of the 20th International Conference on 3D Web Technology*. ACM, 89–95.

[64] Eric Métois, Paul Yarin, Noah Salzman, and Joshua R Smith. 2002. FiberFingerprint identification. In *Proc. 3rd Workshop on Automatic Identification*. 147–154.

[65] Aravind K Mikkilineni, Osman Arslan, Pei-Ju Chiang, Roy M Kumontoy, Jan P Allebach, George T-C Chiu, and Edward J Delp. 2005. Printer forensics using svm techniques. In *NIP & Digital Fabrication Conference*, Vol. 2005. Society for Imaging Science and Technology, 223–226.

[66] Dieter Muhs, Herbert Wittel, Dieter Jannasch, and Joachim Voßiek. 2003. *Roloff/Matek Maschinenelemente*. Springer.

[67] Ke Nie, Jeon-Hor Chen, J Yu Hon, Yong Chu, Orhan Nalcioglu, and Min-Ying Su. 2008. Quantitative analysis of lesion morphology and texture features for diagnostic prediction in breast MRI. *Academic radiology* 15, 12 (2008), 1513–1525.

[68] Marios Papas, Thomas Houit, Derek Nowrouzezahrai, Markus H Gross, and Wojciech Jarosz. 2012. The magic lens: refractive steganography. *ACM Trans. Graph.* 31, 6 (2012), 186–1.

[69] Hemant Sengar. 2014. VoIP Fraud: Identifying a Wolf in Sheep's Clothing. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 334–345.

[70] Ashlesh Sharma, Lakshminarayanan Subramanian, and Eric A Brewer. 2011. PaperSpeckle: microscopic fingerprinting of paper. In *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 99–110.

[71] Robert L Skubic and James W Comb. 2012. Adjustable platform assembly for digital manufacturing system. (April 10 2012). US Patent 8,153,183.

[72] 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.

[73] Yunpeng Song, Zhongmin Cai, and Zhi-Li Zhang. 2017. Multi-touch Authentication Using Hand Geometry and Behavioral Information. In *Security and Privacy (SP), 2017 IEEE Symposium on*. IEEE, 357–372.

[74] Ying Su, Jeremy Holleman, and Brian Otis. 2007. A 1.6 pJ/bit 96% stable chip-ID generating circuit using process variations. In *Solid-State Circuits Conference, 2007. ISSCC 2007. Digest of Technical Papers. IEEE International*. IEEE, 406–611.

[75] 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.

[76] Daisuke Suzuki and Koichi Shimizu. 2010. The Glitch PUF: A New Delay-PUF Architecture Exploiting Glitch Shapes.. In *CHES*, Vol. 10. Springer, 366–382.

[77] Ashwin Swaminathan, Min Wu, and KJ Ray Liu. 2008. Digital image forensics via intrinsic fingerprints. *IEEE transactions on information forensics and security* 3, 1 (2008), 101–117.

[78] Richard Szeliski. 2010. *Computer vision: algorithms and applications*. Springer Science & Business Media.

[79] Ehsan Toreini, Siamak F Shahandashti, and Feng Hao. 2017. Texture to the Rescue: Practical Paper Fingerprinting based on Texture Patterns. *arXiv preprint arXiv:1705.02510* (2017).

[80] Jasper L Tran. 2014. The law and 3D printing. *J. Marshall J. Info. Tech. & Privacy L.* 31 (2014), 505.

[81] Mihran Tuceryan and Anil K Jain. 1993. Texture analysis. In *Handbook of pattern recognition and computer vision*. World Scientific, 235–276.

[82] Francesca Uccheddu, Massimiliano Corsini, and Mauro Barni. 2004. Wavelet-based blind watermarking of 3D models. In *Proceedings of the 2004 workshop on Multimedia and security*. ACM, 143–154.

[83] Ansel Ugural. 2003. *Mechanical design: an integrated approach*. McGraw-Hill Science/Engineering/Math.

[84] Frerik van Beijnum, EG van Putten, KL Van der Molen, and AP Mosk. 2006. Recognition of paper samples by correlation of their speckle patterns. *arXiv preprint physics/0610089* (2006).

[85] Vincent Van der Leest, Geert-Jan Schrijen, Helena Handschuh, and Pim Tuyls. 2010. Hardware intrinsic security from D flip-flops. In *Proceedings of the fifth ACM workshop on Scalable trusted computing*. ACM, 53–62.

[86] Ingrid Verbauwhede and Roel Maes. 2011. Physically unclonable functions: manufacturing variability as an unclonable device identifier. In *Proceedings of the 21st edition of the great lakes symposium on Great lakes symposium on VLSI*. ACM, 455–460.

[87] Svyatoslav Voloshynovskiy, Maurits Diephuis, Taras Holotyak, and Nabil Standardo. 2014. Physical object identification using micro-structure images. (2014).

[88] Gerald Walther. 2015. Printing insecurity? The security implications of 3d-printing of weapons. *Science and engineering ethics* 21, 6 (2015), 1435–1445.

[89] BT Wang. 2014. A temperature analysis˜ control strategy on 3D printing nozzle. *Hunan Normal University* (2014).

[90] Mark Yampolskiy, Todd R Andel, J Todd McDonald, William B Glisson, and Alec Yasinsac. 2014. Intellectual property protection in additive layer manufacturing: Requirements for secure outsourcing. In *Proceedings of the 4th Program Protection and Reverse Engineering Workshop*. ACM, 7.

[91] D-S Yan, Z-Q Cao, and G-R Kong. 2003. Analysis of the driving force by friction in a driving structure of FDM. *Journal of Beijing University of Chemical Technology(Natural Science Edition)* 30, 3 (2003), 71–73.

[92] Xiaofeng Yang, Srini Tridandapani, Jonathan J Beitler, David S Yu, Emi J Yoshida, Walter J Curran, and Tian Liu. 2012. Ultrasound GLCM texture analysis of radiation-induced parotid-gland injury in head-and-neck cancer radiotherapy: An in vivo study of late toxicity. *Medical physics* 39, 9 (2012), 5732–5739.

[93] Wenyao Xu Chi Zhou Zhanpeng Jin Yang Gao, Borui Li. 2018. Watching and Safeguarding Your 3D Printer: Online Process Monitoring Against Cyber-Physical Attacks. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 3 (2018).

[94] Soweon Yoon. 2014. *Fingerprint recognition: models and applications*. Michigan State University.

[95] Robert J Young and Peter A Lovell. 2011. *Introduction to polymers*. CRC press.

[96] Longyu Zhang, Haiwei Dong, and Abdulmotaleb El Saddik. 2016. From 3D sensing to printing: A survey. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)* 12, 2 (2016), 27.

[97] Zhe Zhou, Wenrui Diao, Xiangyu Liu, and Kehuan Zhang. 2014. Acoustic fingerprinting revisited: Generate stable device id stealthily with inaudible sound. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 429–440.

[98] Baoshi Zhu, Jiankang Wu, and Mohan S Kankanhalli. 2003. Print signatures for document authentication. In *Proceedings of the 10th ACM conference on Computer and communications security*. ACM, 145–154.

[99] Sebastian Zimmeck, Jie S Li, Hyungtae Kim, Steven M Bellovin, and Tony Jebara. 2017. A privacy analysis of cross-device tracking. In *26th USENIX Security Symposium (USENIX Security 17)*. USENIX Association, 1391–1408.

Appendices

A HARDWARE VARIATIONS MODEL

In the printing process, the invariant and repeatable fingerprints on the 3D printed objects arise from the inevitable variations in the mechanical components. We elaborate the source of the variations as follows.

The 3D printer relies on a stepper motor driving system to move the nozzle in the X-Y-Z axis under specific instructions. In inter-band motors, the coefficient of viscous friction, the torque constant, the system inertia and the load torque is different, making it unlikely to output the same rotor position with the same load. In intra-band motors, there are 10% and 20% tolerances in the resistance and inductance respectively, which causes:

- Variation of 5% in the rotor position.
- 5% and 20% variations in the stepper motor accuracy and power consumption, respectively [9].

During the printing process, the spatial movement of the nozzle is achieved by the Positioner. The kinematics of the Positioner determines the trajectory of the Hot end, implying that imperfections in the Positioner misalign the Hot end to some extent. The Positioner includes a belt transmission (including synchronous gear, belt, pulley, shaft and bearing), a screw rod, three stepper motors and a platform. There are 6% and 0.5% tolerances in the cross-sectional area of a belt and the distance between the teeth respectively, which causes variations in synchronous belt transmission. Concerning the Positioner, the error of gear shape (height and diameter) is within ±3% [7]. For the belt, the differentiation of the reference diameter, the V truncated shape and the elongation rate is under 3%. Its center distance variation is around 2% [6]. In addition, for screw rod, its pitch error, medium diameter error and tooth type half-angle error are fluctuated according to the processing level, which leads to friction fluctuations between 5%-8% [8] causing:

- Discrepancies in the rotor position of the stepper motor and synchronous belt transmission affect the line's trajectory vector (XY axis) of the nozzle.
- Error in screw rod disturbs the positioning of the platform (Z axis) during the printing process.

The thermal process initiates after the material arrives at the Hot end, whose temperature is monitored by the control system. While governing the temperature during extrusion, there is a 10% variation in the coefficient of the heater power. The A/D amplifier (INA826) gain error is ±5%. The thermal sensor is PT100 with the resistance value variation of $\pm 0.06\Omega$. It has a 0.384ohm drift when temperature changes, while its measuring accuracy ranges from ±0.15°C to ±0.30°C and thermal response time is within 0.3s-0.9s before $\tau 0.5$ [5]. The nozzle hole diameter error is between 1%-5%. The heater diameter error is around 2%. These variations lead to:

- Fluctuation in temperature of the hot end, thereby leading to improper material fusion.
- Variation in actual volumetric flow (line width) of the material from unsteady friction in the Feeder.