computers

MDPI

Article

Computer Vision Approach in Monitoring for Illicit and Copyrighted Objects in Digital Manufacturing

Ihar Volkau [1,*], Sergei Krasovskii [1], Abdul Mujeeb [1] and Helen Balinsky [2,*]

[1] HP–NTU Digital Manufacturing Corporate Lab, Nanyang Technological University, Singapore 637460, Singapore; krasovskii.sergei.gen@gmail.com (S.K.); amujeeb@ntu.edu.sg (A.M.)
[2] Workforce Solutions, HP Inc., Bristol BS1 6NP, UK
* Correspondence: volkau.ihar@ntu.edu.sg (I.V.); helen.balinsky@hp.com (H.B.)

Abstract: We propose a monitoring system for detecting illicit and copyrighted objects in digital manufacturing (DM). Our system is based on extracting and analyzing high-dimensional data from blueprints of three-dimensional (3D) objects. We aim to protect the legal interests of DM service providers, who may receive requests for 3D printing from external sources, such as emails or uploads. Such requests may contain blueprints of objects that are illegal, restricted, or otherwise controlled in the country of operation or protected by copyright. Without a reliable way to identify such objects, the service provider may unknowingly violate the laws and regulations and face legal consequences. Therefore, we propose a multi-layer system that automatically detects and flags such objects before the 3D printing process begins. We present efficient computer vision algorithms for object analysis and scalable system architecture for data storage and processing and explain the rationale behind the suggested system architecture.

Keywords: computer vision; high-dimensional data; digital manufacturing; illicit object; copyright object; illegal printing

Citation: Volkau, I.; Krasovskii, S.; Mujeeb, A.; Balinsky, H. Computer Vision Approach in Monitoring for Illicit and Copyrighted Objects in Digital Manufacturing. *Computers* **2024**, *13*, 90. https://doi.org/10.3390/computers13040090

Academic Editors: Selene Tomassini and M. Ali Akber Dewan

Received: 4 March 2024
Revised: 21 March 2024
Accepted: 22 March 2024
Published: 28 March 2024

1. Introduction

Almost any new technology, along with creating new possibilities, gives rise to immediate attempts to misuse it. For example, the introduction of color printers enabled attempts to print counterfeit currency [1], forge official documents, and so on. It was difficult to conduct counterfeit investigations for illegal activities using color printing, and almost impossible to find the person or people who performed it and the printer itself. As a cybersecurity measure that facilitates the search for the offender, some color laser printer manufacturers started including tracking information as part of the printout [2]. A similar problem emerged in additive manufacturing, or 3D printing, a technology that enables the creation of physical objects from digital blueprints. However, these blueprints can be stolen or tampered with. In addition to illegal 3D printing of counterfeits, another cybersecurity challenge relates to producing 3D-printed weapons, explosives, etc. [3,4]. For example, ghost guns are almost impossible to trace [5], and workshops conducting their manufacturing are discovered mainly by chance [6].

There is an emerging need to detect the printing of objects (hereafter called controlled objects or COs) that potentially infringe on laws, authorship rights, legal or other constraints. We suggest detecting such objects before the 3D printing process begins to avoid legal consequences for manufacturers. We cannot control digital manufacturing at illegal workshops. Still, our approach could help "to keep honest people honest", e.g., online 3D printing digital manufacturers (like Shapeways.com) with large volumes of customers uploading parts for 3D printing. Our approach can prevent the printing of COs and alleviate the accompanying legal and other challenges for an unsuspecting manufacturer. We could help to mitigate the risk to business owners of accidentally manufacturing something forbidden.

This paper proposes a monitoring system for detecting illicit and copyrighted objects in digital manufacturing (DM). Our system is based on extracting and analyzing high-dimensional data from blueprints of three-dimensional objects and can automatically detect and flag such objects before the 3D printing process begins. The system employs efficient computer vision algorithms for object analysis and scalable system architecture for data storage and processing.

The paper is organized as follows: Section 2 discusses the legal issues of DM. Section 3 states the goals and objectives of our work and contains related prior art. Section 4 includes a description of the main parts of our system. Section 5 discusses the results, performance issues, and possible future directions. Section 6 finalizes the article.

2. Legal Framework for Digital Manufacturing and Physical Control at IP Protection

Three-dimensional printing allows the production of a wide variety of objects, ranging from children's toys to weapons, bringing new opportunities and security challenges. In [7], the cybersecurity implications of additive manufacturing are described, and serious concerns have been raised about the security of storage, transmission, and execution of 3D models in digital networks and systems. The International Conference on 3D-Printed Firearms [8] addressed the latest challenges law enforcement faces in tackling the digital manufacturing threat. The Peace Research Institute Frankfurt (PRIF) 2017 report [9] describes the potential of this new technology and analyzes its possible risks concerning the proliferation of small arms, major weapons systems, and even weapons of mass destruction.

Besides the printing of dangerous objects, there are concerns about the 3D printing of counterfeit products, which could be a severe copyright issue [10]. Printing 3D objects without permission is illegal if the original design is protected under copyright law [11,12]. If a 3D model is protected by copyright, copyright holders can use technical protection measures to safeguard patented property. Circumvention of such protection measures is expressly prohibited by the World Intellectual Property Organization (WIPO) [13].

Several theoretical approaches for IP protection in 3D printing have been proposed, in addition to legal measures and prohibitions. In [14], for example, it is offered to tag an object and its associated 3D printing file with a unique identifier to track usage. However, an engineering solution for the implementation was not provided. Similarly, partnering with sharing platforms that make 3D files public can help limit unauthorized use. In [15], proposals were made to incorporate blockchain into the 3D printing process, providing creators with an additional layer of legal protection with copyright information and a watermark. To reduce the illegal use of 3D printers, ref. [16] proposed a method for extrusion manufacturing to trace the origin of printed objects. When a 3D printer has an extruder that pushes the building material through, the hot end of the extruder melts the material and places it on the print platform to create the model. Each extruder's hot end has unique properties, affecting how the 3D model is built. These thermodynamic properties can be used to identify a particular extruder and, therefore, a 3D printer model as unique as a human fingerprint or "ThermoTag". Thus, the model's buyer can be traced for using the printer to make an illegal copy.

The existing solutions for IP protection in 3D printing to combat 3D-printed counterfeiting and forgery are mainly focused on controlling the original production. For example, embedding NFC tags and QR codes in genuine products helps consumers validate their authenticity [17,18]. In [19], it was proposed to use specially placed nanorods in the final product, which do not affect the integrity of the material but could be a compliance "watermark" to distinguish it from a counterfeit, the same way as the watermark is applied to detect fraudulently printed documents.

The control of original production cannot decrease the production of counterfeits using 3D custom printing, which remains and will be the main issue. Along with the violation of trademarks, patents, and other intellectual rights, illegally printed parts could result in severe or even fatal consequences, e.g., due to incorrect materials being utilized or substandard production [20].

3. Problem Statement and the Related Works

Our starting point was to analyze the following situation: There is a 3D printing facility (automated or semi-automated) which receives requests for 3D printing. There is a chance to receive an order to print a controlled object. To avoid legal consequences [4,5], detecting such objects before the 3D printing process begins is recommended. Nowadays, manufactured objects without official permission or license can only be discovered by human inspection, and this process is prone to errors. To the best of our knowledge, currently, there are no existing supporting technical systems, and the enforcement of law mainly relies on the legal bodies' operational activities and information from the public. The introduction of automated tools could be an initial step, allowing at least primary automated law enforcement for 3D printing.

Hereafter, we propose the concept of an automated system for pre-scanning COs in 3D printing, along with the algorithms for the extraction and analysis of high-dimensional data from blueprints of 3D objects. In general, all printable 3D objects can be considered either technical or decorative. The structure and extent of the technical objects are considered fixed. Otherwise, its functionality will be compromised. Currently, we do not consider cases when the specific technical part could be heavily modified aesthetically without changing functionality, nor is there the possibility of including large-scale features that can be easily removed in post-processing.

At first glance, restricting unauthorized objects from printing boils down to checking if two 3D objects represented by blueprints are the same or different. The existing methods for 3D-object matching can be categorized into three groups: shape-based, view-based, and hybrid [21].

3.1. Shape-Based Methods

In the shape-based category, features are extracted from 3D shape representations (such as polygons, voxels, graphs, etc.) and later used for similarity measurement. The descriptor of the shape is found using some algorithm that characterizes the geometric properties of the object. Statistical descriptors employ histograms to encapsulate the distributions of shape features. While they are efficient and quick to compute, their ability to discriminate is limited, as they do not adequately capture the local characteristics of the object's shape. In this category of methods, we mention the following descriptors:

- A 3D shape spectrum descriptor [22] is related to the first and second principal curvature along the object's surface.
- A D2 descriptor [23,24] takes samples of distances between two points on the model's surface and then creates a distance distribution histogram that serves as the model's shape descriptor.
- A descriptor [25] compares the similarity of two 3D objects by generating distance histograms and determining the appropriate alignment of the two objects.
- A graph-based approach [26] utilizes hierarchical structures to represent 3D objects, accompanied by graph-matching techniques.
- A spherical function-based descriptor [27] suggests using a volumetric representation of the Gaussian Euclidean Distance Transform for a 3D object, expressed by the norms of spherical harmonic frequencies.

3.2. View-Based Methods

View-based methods are becoming increasingly popular due to the progress in 2D-3D reconstruction. The primary concept in visual representation for 3D model retrieval involves initially converting the 3D model into a 2D projection image. Subsequently, various image processing techniques are employed to extract diverse features from this image [28]. For example:

- Ansary et al. [29] selected optimal 2D views of a 3D model and created K-mean clustering of views. Then, the similarity between pairwise 3D objects was measured by applying Bayesian models.

- Wang et al. [30] solved the retrieval problem using group sparse coding. The query object was constructed again by the view sets of each shape; then, the restoration error was considered the similarity measurement for retrieval.
- In [31], it was proposed to project a 3D object to a 2D space and use multi-views. These view-based methods combine a trainable system with 2D projection attributes adopted by the Convolutional Neural Networks (CNNs).
- Ref. [32] introduced a 3D shape descriptor known as the spherical trace transform, which generalizes the 2D trace transform. This approach involves calculating a range of 2D features for a collection of planes that intersect the volume of a 3D model.

3.3. Hybrid Methods

The hybrid methods involve fusing various 3D shape features to improve retrieval accuracy [33]. According to [34], a 3D shape representation incorporating more shape features tends to excel in retrieving more relevant models. In a study by Papadakis et al. [35], a novel hybrid 3D model shape descriptor called PANORAMA was introduced. PANORAMA relies on a set of panoramic views of a 3D model. This approach involves projecting an object onto three perpendicular cylinders and, for each projection, calculating the corresponding 2D Discrete Fourier Transform and 2D Discrete Wavelet Transform.

4. System Architecture

The lack of a universally accepted and consistently effective solution is evident from the multitude of methods available. One of the main requirements for an industrial system is stable, error-free work, and one of the ways to improve reliability is by combining existing approaches and using them in the ensemble.

For a real-life proof of concept system, besides comparing two 3D objects, many other issues should be considered, such as:

- How to store COs securely without unauthorized leakage of their blueprints.
- How to represent the objects in the database of controlled objects.
- How to evaluate objects-in-question quickly and provide a fast search of this information to keep up with 3D printing operations.

We need to address three problems:

1. How to describe controlled objects in a compact way that is good for comparison and storage: Confidentiality Preserving Descriptors (CPDs) should be used for object feature representation. Even if a descriptor of a CO is leaked, it cannot be used to manufacture COs.
2. How to keep a Database of Controlled Objects (DCO) containing the descriptions of the controlled objects: this database should be maintained by the authorities, who decide which objects should be controlled.
3. How to compare an object to be manufactured (an object-under-analysis, OUA) to controlled objects from the DCO in rapid, reliable, and efficient ways.

4.1. Storing of Controlled Objects

The decision of what is forbidden and what should be considered controlled objects should be decided by some authority. It might depend on the country and local laws, and local authorities and enforcement organizations should maintain this information.

The information about forbidden and controlled objects (e.g., in airport security) can be kept today in the following forms:

- Human knowledge (a border control officer can recognize a forbidden item).
- Databases of 2D photographs for camera/video recognition.
- In a neural network (NN) for photo/video recognition. This NN should first be trained on many cases to extract the patterns typical for the specific class (classes) of objects to recognize.

These forms cannot be directly utilized for our 3D recognition project. For example, human knowledge cannot be embedded into a device for automation and checks before manufacturing. Two-dimensional photos do not show the internal architecture, so non-functional replicas of the controlled object (for example, a 3D-printed foam gun for hobbyists for play) could be identified as a CO. The usage of a NN could be questionable as sometimes there is only one sample of a controlled object. It does not represent any class, so extracting common patterns from this unique object is pointless.

Both the visual appearance and the object's internal structure should be analyzed to make an informed decision. Furthermore, we do not like to constrain the CO's geometry. COs may have the following: (a) complex geometry with embedded surfaces and structures (this is a unique feature of 3D printers (3DPs) when several objects can be printed at the same time, and some objects may be embedded into others, e.g., a sphere in a hollow cube); (b) a topology with holes and many fine-grain details; and (c) various curvatures with/without edges at the surface, etc.

To date, there are no 3D DCOs or prohibited blueprints in the public domain. If such databases existed, they would be an excellent source for illegal manufacturing and would encourage a proliferation of illicit items, for example, ghost guns. An open-access DCO would substantially increase the scope of attack, so a real DCO (with guns, explosives, etc.) could be created only by relevant government agencies and supervisory authorities and be securely kept out of public access. This consideration sets high-security requirements for a DCO, as the DCO itself would be a target for attacks to extract COs.

One more consideration relates to the question of where to keep the DCO. We assume there should be a centralized DCO, and we propose keeping the local copy of this DCO at the edge (at the printing facility) and keeping both options to perform validation locally at the facility, or as part of a cloud service.

Each edge device subscribes to a centralized DCO (in the cloud) and fetches the latest updates on controlled objects, creating a local DCO copy in-device. The gains from this could be the following:

- Local validation provides performance benefits; large 3D design files do not need to be uploaded through the Internet.
- A deployment model where designs are pre-validated by a cloud service is possible, assuming design owners are ready to get their designs pre-approved from authority services. In some cases, in-device validation could be beneficial as it limits design exposure service. To ensure the confidentiality of designs-to-be-produced, there may be a requirement not to move the blueprint out of the 3D printer to protect intellectual rights and provide secure printing operations.
- Additive manufacturing factories (or devices) could be operating offline.
- A DCO will store information about 3D objects in the form of CPDs.

4.2. Confidentiality Preserving Descriptors: Describing CO

At the system core, there are CPDs—a set of "fingerprints" for 3D objects.
The concept behind CPDs is as follows:

- Each of these descriptors describes a distinctive feature of 3D objects. It could [36–38] be the number of holes in the object, volume of the object, area of the surface, volume of the convex hull, surface- or boundary-based centroid, center of mass, principal axes, convexity, aspect ratios, sphericity, mean radius, ellipsoidal variance, EGI [39], spherical harmonic coefficients [27], etc. Multiple CPDs are used as an ensemble to facilitate rapid object identification.
- Three-dimensional objects are encoded by their feature vector. Each object's CPDs contain essential information about the shape of the 3D object in a compressed and low-dimensionality form, sufficient for object identification.
- Descriptors must be lossy and nonreversible, making the restoration of original blueprints from CPDs impossible even if the 3DP device is breached and fully disassembled.

- Descriptors need to be computationally light/fast for in-device processing. We assume $k = 10^2$–10^3 physical objects per 3DP job, so using object-per-object comparison will require k times the number of controlled objects for comparisons. This processing should not create a "bottleneck" for the primary 3D printing process by demanding too many resources.
- At least some descriptors should be able to capture the internal structure of the 3D object, not only the appearance.
- Descriptors could be efficiently stored in the DCO and allow effective comparison of descriptors.
- As objects in the 3DP job may be rotated for better packing of objects in the printing volume, the descriptors should either provide the same output when the 3D objects are rotated and translated or the most efficient method to compare the descriptors of the rotated and translated objects should be known.

4.3. Identification Process

The objective of the identification process is to analyze the object in a 3D printing (3DP) job as being a CO before printing. CPDs are computed for each object in a 3DP job (for each OUA) and compared to CPDs of controlled objects from the DCO before allowing manufacturing to commence. This identification process should be time- and resource-efficient and include the analysis of the internal structure of the 3D object, not only the surface.

One possible option during the analysis is that the CO in the 3DP job may be rotated and translated for better packing of objects in the printing volume. Assuming that the technical OUA has an established and (almost) unchangeable geometry, its mesh could still be modified to change the number of vertices/triangles (and keep the original geometry and topology) in the blueprint. Such a modification is one of the simplest methods to make the object misidentified if the recognition of the object is based on the number of vertices and triangles of the original blueprint.

We assume that most objects to be printed at the facility are non-controlled. This brings us to a two-level architecture, where at the first level we would like to identify the non-controlled objects as fast as possible and leave only the suspicious objects to be controlled. We use more time-consuming but high-accuracy approaches at the second level to check if the object is a CO.

The error of the first type (the allowed object is considered controllable) will annoy the customer of the 3D printer as the legitimate order will be rejected. This event will likely negatively affect customer satisfaction and future usage of the manufacturing facility. The error of the second type (the controlled object is considered as allowed) could cause severe consequences for the facility owner/operator for breaking the law. For example, per Singapore law, the operator of the printing facility is responsible for printing illegal objects [4].

The proposed two-layer system can be considered a two-factor authentication (2FA) system, where the printable object is checked and authenticated by distinctively different methods at each stage.

This 2FA system is a cascade of classifiers:

- The decision making about object identification is performed as a cascade of classifiers, i.e., in a hierarchical manner.
- The probability of encountering a CO is low, so we must filter out non-COs quickly and efficiently.
- We start from low-complexity discriminative algorithms to reject the object as being a CO as fast as possible (e.g., it is too small, too "square", has no holes, etc.).
- Then, at later stages, we progress to complex, computationally expensive, and accurate determination algorithms.
- All objects (models) from a 3D print job should pass through a hierarchy of classifiers (it could be imagined as a set of sieves with smaller and smaller chances to make an

inaccurate decision due to being more computationally expensive at each consequent level); refer to Figure 1.

- We aim to identify (eliminate) most objects by the least computationally expensive classifier.
- Ideally, it is expected that identification aims for 100% accuracy within an acceptable time.
- Different methods have different complexity and accuracy (usually, the more complex the approach, the longer the calculations and the better the final accuracy).
- Some models could take a long time to process to reach high-accuracy results.
- The acceptable level of object identification accuracy may depend on the object type. We might need to weigh the importance of correctly identifying the object against the time spent on decision making and the type of the object itself.

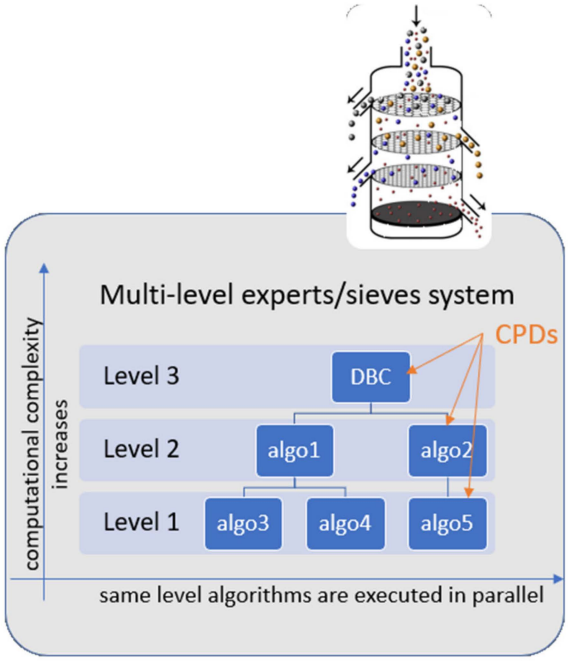

Figure 1. The sieve system is used to identify a CO in a 3DP job.

The method of object identification should be immune to:

- Rotation in R^3 (any degree) and translation (as objects in a 3D printing job could be moved to be better packed in the printing volume).
- Remeshing of 3D object mesh.

Many descriptors for the first layer can be found in [36–38]. We can apply these descriptors according to a decrease in complexity (and an increase in speed) and calculate some descriptors in parallel. The calculation and comparison of different descriptors can be separated into several levels (Figure 1).

We can choose all the descriptors available to perform the object's comparison. However, there is a more advanced way. In [40], different sets of descriptors were analyzed for their usage for object "fingerprinting" and for their efficacy and efficiency. A small set of four descriptors was found to describe and compare 3D objects efficiently. These descriptors are also efficient for information retrieval from the big database of 3D objects. One of the sets of the champion CPDs consists of the convex hull area of the 3D object, convex hull volume, modified extended gaussian image (which is the energy of the spherical harmonics corresponding to the extended gaussian image [39,41] of the 3D object), and the central moment of inertia of the surface of the object calculated relative to the centroid of the 3D object [40]. These CPDs were chosen based on their computational simplicity

and the power of feature extraction, and their efficacy is the same as for the much more comprehensive set of descriptors.

The specialized algorithm called Discriminative Base Comparison (DBC) was used for the second layer. Following Kazhdan's [27] approach, it cuts the 3D object into concentric spheres (shells) and then finds the intersection of the object by each shell. A sequence of spherical harmonic coefficients represents the resulting indicator function for each shell, and then the corresponding energies for each degree and shell are calculated. The valuable property of energies is that an energy is not changed by any rotation in R^3 around the center of mass (or centroid) and does not depend on the object's translation.

In a concentric manner, shell-by-shell and degree-by-degree, the energies of the spherical coefficients are compared for the OUA and COs from the DCO. If a correspondence is found, the object similar to the CO is identified. DBC is a non-iterative and non-gradient method of searching for similarity.

The computational complexity of this method is much higher than the complexity for calculations of the simple descriptors at the first layer of the process. That is why the OUA is first tested by fast and simple descriptors, which provide quick rejection of non-similar objects, and only after passing this sieving-out do we apply the more complex check. Let us recall that most of the objects in the 3DP job are assumed to be non-controllable, so the first layer efficiently identifies and rejects non-COs, leaving only the cases where extra investigation is required.

The overall workflow is depicted in Figure 2. The OUA is represented in the form of a set of descriptors and is compared with the descriptors of the COs from the DCO using the sieve system (Figure 1).

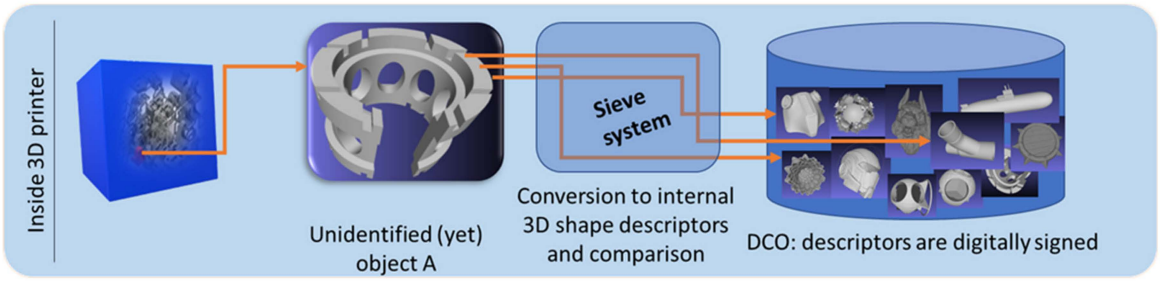

Figure 2. The overall workflow.

5. Results and Discussion

The current developed proof of concept demonstrates its functionality and verifies a principal concept of usage of CPDs for object "fingerprinting" and identification (Figure 3). We also developed an initial prototype that allows for the visualization of how the system will function; there is a working interactive model that gives an idea of the functionality, design, navigation, and layout (Figure 3).

To test the software for the identification of COs, we used several standard internet datasets that contain 3D polygonal models collected from the World Wide Web:

- The ShapeNet dataset (The Princeton Shape Benchmark (PSB), Version 1) [42].
- The Engineering Shape Benchmark (ESB, Purdue University) dataset [43].
- Princeton ModelNet40 [44].
- Free downloadable models from different Internet websites.

All in all, we collected more than 14,000 models and placed them in the database. These 3D objects represented potential objects of interest with unique features.

Our approach was tested in the following way: We took every object from the database (considered as our DCO), then randomly rotated, translated, and re-meshed them, and then performed a database search using our two-layer approach. The first layer checked the correspondence of features of two objects; if the objects are scaled versions of each other, they will be considered as non-matching (as they have, for example, different volumes).

In case we needed to identify the scaled objects as matching, then before the analysis, we additionally needed to scale the objects to the same standard size.

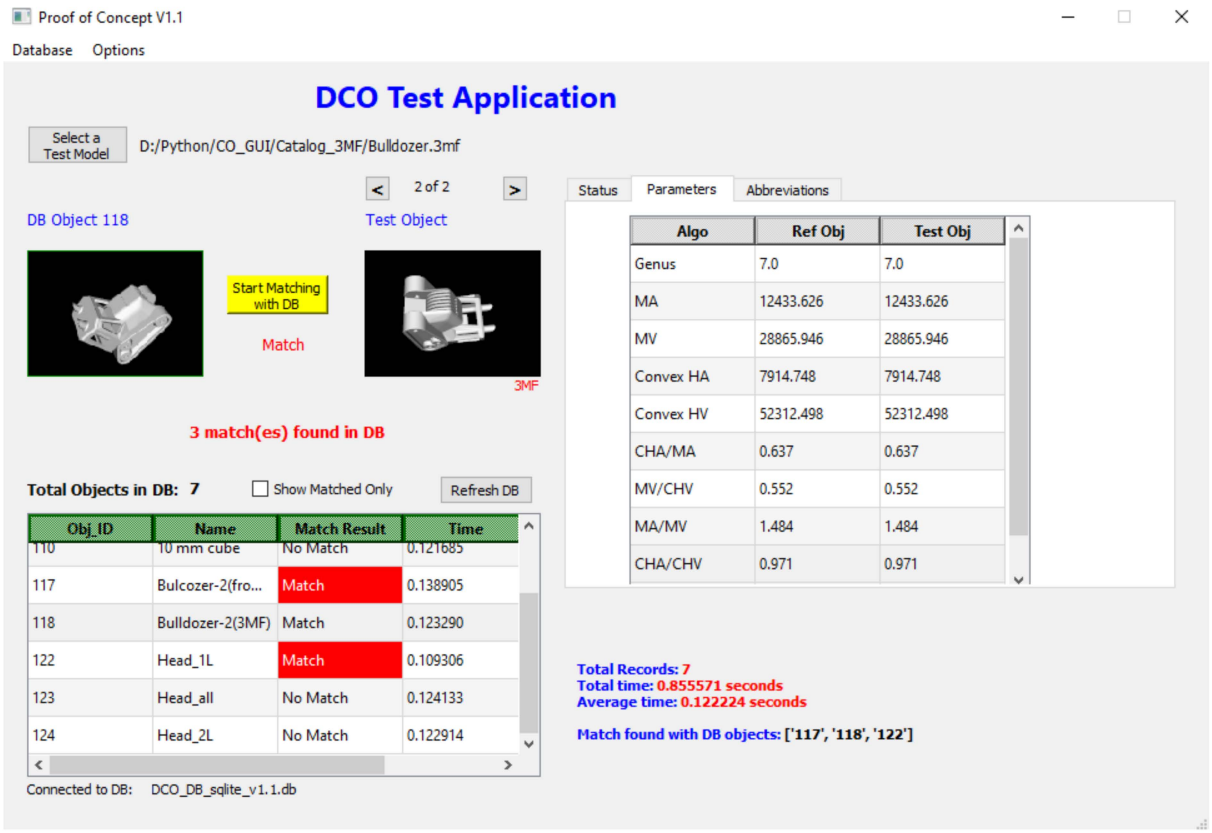

Figure 3. Application interface for comparison of object-under-printing against the DCO objects.

The result showed that, using the architecture suggested and the CPDs described, it was possible in all cases (100% accuracy, 0% false positive/false negative) to successfully identify the models from the database. These identified models could comprise duplicates or mirror images of the OUA, or objects found in the database that possess a slight variation of the surface of the OUA.

The second experiment conducted to check our method used the ESB [34,43] as a DCO. The set of 3D models input to check against the DCO included transformed and re-meshed models from ModelNet40 [44] (a set of unprotected objects) and ESB (protected objects). Our descriptor-based approach correctly identified whether the input model was contained in the DCO with 100% accuracy; shifted, rotated, and mirrored objects, and objects with minor modifications were identified correctly.

The ultimate validation of the proposed method of CO identification could be accomplished by using a real DCO (with guns, explosives, etc.) To our knowledge, there is no existing open-access database of controlled (prohibited) blueprints, and even keeping a controlled blueprint on a computer without official permission is a criminal offense in some countries, including, for example, Singapore. The existence of such a database would be a significant security threat, and the creation and maintenance of such a DCO should be developed only by relevant government agencies and supervisory authorities. Hence, real-life experiments could be conducted only after the appearance of such a DCO and only by the appointed people.

The system proposed is not a panacea, and expecting the same 100% accuracy in a real-life situation would be really naive. Currently, it can only identify technical objects with (almost) unchangeable geometry. The objects' scaling, rotation, translation, and remeshing do not affect the identification results. This system would mainly help when attempting to

print a known controlled object without significant modification. By analogy, in Internet cyberattacks where people try to use a vulnerability discovered by some pioneer hacker, we hope that most attackers (people who would try to print COs) would use the blueprints found on the Internet without modifications.

We see a rapid adoption of 3D printing technology for manufacturing illegal or counterfeit objects. Wikipedia provides a list of 3D-printed weapons and parts [45] which consists of 50 individual designs printed in metal and plastic. For comparison, only five to six designs were available two years ago. As a result, laws and regulations were rapidly introduced to prohibit/restrict 3D printing, identify legally guilty parties, and introduce penalties. Finding people/organizations illegally printing counterfeit objects and proving that the objects were illegally printed will be an enforcement nightmare for patent holders and relevant law enforcement authorities. Incorporating constraints in 3D printing will allow manufacturers to satisfy current and future legal requirements and enable programmable control for printing unauthorized/copyrighted 3D objects.

Zero-day attacks and different (from those considered above) types of attempts to print COs should be addressed when these new attacks are detected. This is the same never-ending attack and defense game we see for viruses and antiviruses.

One of the types of attacks presently challenging to detect involves modifying the surface of a 3D object in a way that does not impact its functionality but alters the object's shape. Establishing local surface correspondences with the CO could shield them from this attack, and the authors are currently working on this idea. This approach requires time to develop to make it practical (to work in real time and to be accurate and robust under possible modifications).

5.1. Efficiency of Search in a Big Database of Controlled Objects

A potential bottleneck could appear for efficient data retrieval from a big database (~1 M controlled objects and more). A set of CPDs represents each object; hence, for the fast retrieval of an object from a database, we need to find a "good" subset of CPDs to discriminate the database objects efficiently. Next, we need to index and filter the database using the subset of CPDs found. If the database is modified (the number of records is growing), the "good" set of descriptors for fast retrieval might also change. It poses the question: how do you find a quick and efficient method of information retrieval for a database of, say, 1 million or 1 billion records?

The distribution of object features in a database appears to have colossal information "inertia". The distribution does not change a lot when the database grows. It is the same concept as for public opinion surveys: there is no need to ask everyone, and there is a need to choose a representative subset. Statistically representative results for a database of up to 1 million records require a sample size of fewer than 400 records to be analyzed (with a 95% confidence level and 5% margin of error). We conducted experimental checks of the claim as it sounds counterintuitive and found that the statistical approach (unlike intuition) is correct. We can, therefore, discover optimal filtering for a big database based on samples from this database.

5.2. Possible Future Directions

There are a lot of interesting future continuations for this project. For example:

- Making the identification of a CO possible even if no blueprint for this CO is available. This could be done by scanning the object and representing it as a point cloud.
- Identifying a CO even if an intentional change in the design (to escape detection) is made. We assume that this design change does not affect the object's functionality.
- Verifying that the blueprint object was not modified during printing (parts of the blueprint should not be changed during manufacturing due to a malicious attack).
- Performing modeling of attacks and countering attacks.

- Incorporating ML/DL techniques to detect similarity to the class of COs even if we have a limited number (or even one only) of class representatives (e.g., the object looks like a known CO) using one-shot learning.

6. Conclusions

There is a clear need for new solutions in intellectual property protection and the production of controlled objects in the emerging world of 3D printing. In this world, the proliferation of 3D manufacturing of fake spare parts and real weapons is the upcoming reality.

Preventing counterfeiting and printing of controlled objects promises to be a growth market (the same as 3D additive manufacturing) with several clearly defined stakeholders. The incorporation of constraints before the 3D printing process starts might benefit:

- Patents, copyrights, and trademarks holders;
- Three-dimensional manufacturers (this could help address current and future regulatory challenges for the production of COs);
- Law enforcement organizations (to tighten controls for high-risk items).

We have proposed a system architecture for the fast, efficient, and secure identification of whether a design-to-be-produced inside a 3D printing system is a controlled object. The computer vision algorithms developed analyze the features of 3D objects in multi-dimensional space. This project is currently in the process of building a prototype. Pre-screening software could indemnify a 3D printer owner from liability related to the unintentional printing of a controlled object. This technology could help protect manufacturers and rights owners from unscrupulous customers and insider threats (e.g., "after-hours manufacturing", (un)intentional oversight, etc.).

Copyright/trademark holders could protect their intellectual rights, e.g., by subscribing to a service that prevents (prohibits) the reproduction of protected objects through 3D printing at additive manufacturing facilities.

Author Contributions: Conceptualization, I.V. and H.B.; investigation, methodology, writing original draft, review & editing, I.V., S.K., A.M. and H.B.; project administration, I.V. and H.B.; data curation, formal analysis, software, validation, I.V., S.K. and A.M.; supervision, funding acquisition, H.B. All authors have read and agreed to the published version of the manuscript.

Funding: This study is supported under the RIE2020 Industry Alignment Fund—Industry Collaboration Projects (IAF-ICP) Funding Initiative, as well as by cash and in-kind contributions from industry partner HP Inc. through the HP-NTU Digital Manufacturing Corporate Lab.

Data Availability Statement: The open access data [42–44] were used.

Acknowledgments: This study is supported under the RIE2020 Industry Alignment Fund—Industry Collaboration Projects (IAF-ICP) Funding Initiative, as well as by cash and in-kind contributions from industry partner HP Inc. through the HP-NTU Digital Manufacturing Corporate Lab.

Conflicts of Interest: The authors declare that this study received funding from HP Inc. The funder was not involved in the study design, collection, analysis, interpretation of data, the writing of this article or the decision to submit it for publication. In addition, author Helen Balinsky is employed by HP Inc. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. HP Helps U.S. Clamp Down on Counterfeiting. Imaging Expertise Used to Deter Digital Fakes. Available online: https://www.hpl.hp.com/news/2003/july_sept/counterfeit.html (accessed on 31 October 2023).
2. Secret Code in Colour Printers Lets Government Track You. Available online: https://www.eff.org/press/archives/2005/10/16 (accessed on 31 October 2023).
3. When 3D Printing Gets into the Wrong Hands. Available online: https://www.forbes.com/sites/zurich/2016/05/06/when-3d-printing-gets-into-the-wrong-hands/ (accessed on 31 October 2023).

4. Elangovan, N. Parliament Enacts New Law to Keep 3D-Printed Guns off the Streets, Better Regulate Weapons. Available online: https://www.todayonline.com/singapore/parliament-enacts-new-law-keep-3d-printed-guns-streets-better-regulate-weapons (accessed on 31 October 2023).
5. Fact Sheet: The Biden Administration Cracks Down on Ghost Guns, Ensures that ATF Has the Leadership it Needs to Enforce Our Gun Laws. Available online: https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/11/fact-sheet-the-biden-administration-cracks-down-on-ghost-guns-ensures-that-atf-has-the-leadership-it-needs-to-enforce-our-gun-laws/ (accessed on 31 October 2023).
6. Spain Dismantles Workshop Making 3D-Printed Weapons. Available online: https://www.bbc.com/news/world-europe-56798743 (accessed on 31 October 2023).
7. Bridges, S.M.; Keiser, K.; Sissom, N.; Graves, S.J. Cyber security for additive manufacturing. In Proceedings of the 10th Annual Cyber and Information Security Research Conference (CISR'15), Oak Ridge, TN, USA, 7–9 April 2015.
8. Printing Insecurity: Tackling the Threat of 3D Printed Guns in Europe. Available online: https://www.europol.europa.eu/media-press/newsroom/news/printing-insecurity-tackling-threat-of-3d-printed-guns-in-europe (accessed on 31 October 2023).
9. Fey, M. *3D Printing and International Security: Risks and Challenges of an Emerging Technology*; Report No. 144; Peace Research Institute Frankfurt: Frankfurt am Main, Germany, 2017.
10. Ebrahim, T. 3D Printing: Digital Infringement & Digital Regulation. *Northwest. J. Technol. Intellect. Prop.* **2016**, *14*, 2.
11. U.S. Code. Title 17. Ch. 1. § 102—Subject Matter of Copyright: In General. Available online: https://www.law.cornell.edu/uscode/text/17/102 (accessed on 31 October 2023).
12. Ogburu-Ogbonnay, H. 3D Printing as a Copyright Infringement, JIPEL Blog 2016–2017. Available online: https://blog.jipel.law.nyu.edu/2017/03/3d-printing-as-a-copyright-infringement/ (accessed on 31 October 2023).
13. WIPO Copyright Treaty (Adopted in Geneva on December 20, 1996), WIPO IP Portal. Available online: https://wipolex.wipo.int/en/text/295166 (accessed on 31 October 2023).
14. Malaty, E.; Rostama, G. 3D printing and IP law. *WIPO Mag.* **2017**, *1*, 6.
15. Blockchain to Play a Key Part in Ensuring Copyright Laws Can Be Used for 3D Printing. Available online: https://news-archive.exeter.ac.uk/homepage/title_908509_en.html (accessed on 31 October 2023).
16. Gao, Y.; Wang, W.; Jin, Y.; Zhou, C.; Xu, W.; Jin, Z. ThermoTag: A hidden ID of 3D printers for fingerprinting and watermarking. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 2805–2820. [CrossRef]
17. 3D-Printed Counterfeits on the Rise: How to Protect Your Brand. Available online: https://www.nanomatrixsecure.com/3d-printed-counterfeits-on-the-rise-how-to-protect-your-brand/ (accessed on 31 October 2023).
18. Roche, S. The New World of 3D Printing. . . and Counterfeiting. Available online: https://www.linkedin.com/pulse/new-world-3d-printing-counterfeiting-sebastien-roche (accessed on 31 October 2023).
19. O'Heir, J. Protecting a New World of 3D-Printed Products, the American Society of Mechanical Engineers. Available online: https://www.asme.org/topics-resources/content/protecting-new-world-3dprinted-products (accessed on 31 October 2023).
20. Counterfeit Product Alert: How to Identify Counterfeit BMW Group Vehicle Parts. Available online: https://www.thecounterfeitreport.com/product/599/BMW-Group-Vehicle-Parts.html (accessed on 31 October 2023).
21. Zhuang, T.; Zhang, X.; Hou, Z.; Zuo, W.; Liu, Y. A novel 3D CAD model retrieval method based on vertices classification and weights combination optimization. *Math. Probl. Eng.* **2017**, *2017*, 6049750. [CrossRef]
22. Zaharia, T.; Petreux, F. 3D shape-based retrieval within the mpeg-7 framework. In Proceedings of the SPIE Conference on Nonlinear Image Processing and Pattern Analysis XII, San Jose, CA, USA, 30–31 July 2001; pp. 133–145.
23. Osada, R.; Funkhouser, T.A.; Chazelle, B.; Bobkin, D.B. Shape distribution. *ACM Trans. Graph.* **2002**, *21*, 807–832. [CrossRef]
24. Shih, J.-L.; Lee, C.-H.; Wang, J.T. 3D object retrieval system based on grid D2. *Electron. Lett.* **2005**, *41*, 179–181. [CrossRef]
25. Novotni, M.; Klein, R. A geometric approach to 3D object comparison. In Proceedings of the International Conference on Shape Modeling and Applications, Genoa, Italy, 7–11 May 2001; pp. 167–175.
26. Zhang, J.; Siddiqi, K.; Macrini, D.; Shokoufandeh, A.; Dickinson, S. Retrieving articulated 3-d models using medial surfaces and their graph spectra. In Proceedings of the Energy Minimization Methods in Computer Vision and Pattern Recognition: 5th International Workshop, EMMCVPR 2005, St. Augustine, FL, USA, 9–11 November 2005.
27. Kazhdan, M.; Funkhouser, T.; Rusinkiewicz, S. Rotation invariant spherical harmonic representation of 3D shape descriptors. In Proceedings of the 2003 Eurographics/ACM SIGGRAPH Symposium on Geometry Processing (SGP '03), Aachen, Germany, 23–25 June 2003; pp. 156–164.
28. Gao, Y.; Dai, Q. View-based 3D object retrieval: Challenges and approaches. *IEEE Multimed.* **2014**, *21*, 52–57. [CrossRef]
29. Ansary, T.F.; Daoudi, M.; Vandeborre, J. Bayesian 3D search engine using adaptive views clustering. *IEEE Trans. Multimed.* **2007**, *9*, 78–88. [CrossRef]
30. Wang, X.; Nie, W. 3D model retrieval with weighted locality constrained group sparse coding. *Neurocomputing* **2015**, *151*, 620–625. [CrossRef]
31. Hoang, L.; Lee, S.-H.; Kwon, K.-R. A deep learning method for 3D object classification and retrieval using the global point signature plus and deep wide residual network. *Sensors* **2021**, *21*, 2644. [CrossRef] [PubMed]
32. Zarpalas, D.; Daras, P.; Axenopoulos, A.; Tzovaras, D.; Strintzis, M.G. 3D model search and retrieval using the spherical trace transform. *EURASIP J. Adv. Signal Process.* **2006**, *2007*, 23912. [CrossRef]

33. Daras, P.; Axenopoulos, A.; Litos, G. Investigating the effects of multiple factors towards more accurate 3-D object retrieval. *IEEE Trans. Multimed.* **2012**, *14*, 374–388. [CrossRef]
34. Jayanti, S.; Kalyanaraman, Y.; Iyer, N.; Ramani, K. Developing an engineering shape benchmark for CAD models. *Comput.-Aided Des.* **2006**, *38*, 939–953. [CrossRef]
35. Papadakis, P.; Pratikakis, I.; Theoharis, T.; Perantonis, S. Panorama: A 3D shape descriptor based on panoramic views for unsupervised 3d object retrieval. *Int. J. Comput. Vis.* **2010**, *89*, 177–192. [CrossRef]
36. Peura, M.; Iivarinen, J. Efficiency of simple shape descriptors. In Proceedings of the 3rd International Workshop on Visual Form (IWVF3), Capri, Italy, 28–30 May 1997; pp. 443–451.
37. Wäldchen, J.; Mäder, P. Plant species identification using computer vision techniques: A systematic literature review. *Arch. Comput. Methods Eng.* **2008**, *25*, 507–543. [CrossRef] [PubMed]
38. Sonka, M.; Hlaváč, V.; Boyle, R.D. *Image Processing, Analysis and Machine Vision*, 4th ed.; Springer: New York, NY, USA, 1993.
39. Kang, S.B.; Horn, P.K. Extended Gaussian image (EGI). In *Computer Vision*; Ikeuchi, K., Ed.; Springer: Cham, Switzerland, 2021; pp. 420–424.
40. Volkau, I.; Krasovskii, S.; Mujeeb, A.; Balinsky, H. Whether 3D object is copyright protected? Controlled object identification in additive manufacturing. In Proceedings of the IEEE 22nd International Conference on Cyberworlds (CW2023), Sousse, Tunisia, 3–5 October 2023.
41. Horn, B.K.P. *Robot Vision*; The MIT Press: Cambridge, MA, USA, 1986.
42. Shilane, P.; Min, P.; Kazhdan, M.; Funkhouser, T. Princeton Shape Benchmark. Available online: https://shape.cs.princeton.edu/benchmark/benchmark.pdf (accessed on 15 May 2023).
43. Engineering Shape Benchmark (ESB, Purdue University). Available online: https://engineering.purdue.edu/cdesign/wp/downloads/ (accessed on 31 October 2023).
44. Wu, Z.; Song, S.; Khosla, A.; Yu, F.; Zhang, L.; Tang, X.; Xiao, J. 3D ShapeNets: A Deep Representation for Volumetric Shapes. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2015), Boston, MA, USA, 7–12 June 2015; pp. 1912–1920.
45. List of 3D Printed Weapons and Parts. Available online: https://en.wikipedia.org/wiki/List_of_3D_printed_weapons_and_parts (accessed on 31 October 2023).