IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 28, 2018, accepted July 28, 2018, date of publication August 9, 2018, date of current version August 28, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2864331

Copyright Protections of Digital Content in the Age of 3D Printer: Emerging Issues and Survey

JONG-UK HOU, (Student Member, IEEE), DONGKYU KIM, (Student Member, IEEE), WON-HYUK AHN, AND HEUNG-KYU LEE

School of Computing, Korea Advanced Institute of Science and Technology, Daejeon 34141, South Korea

Corresponding author: Heung-Kyu Lee (heunglee@kaist.ac.kr)

This work was supported by the National Research Foundation of Korea (NRF) Grant through the Korean Government (MSIT) under Grant NRF-2016R1A2B2009595.

ABSTRACT Three-dimensional (3-D) printing has become a key technology, changing industry paradigms in many sectors, including automobiles, aerospace, medical applications, content production, and service areas. However, 3-D printing introduces many copyright infringement issues for digital 3-D objects because the object data can be directly printed and distributed both online and physically. New distribution scenarios not previously considered also pose new content security problems. This paper reviews intellectual property protection issues and solutions in the 3-D printing environment. We summarize various requirements not previously considered in the literature, defining infringement issues for new technology scenarios and requirements. We then analyze existing copyright security technology coverage according to those scenarios and various other aspects, and present the pros and cons of each technology and future research directions. The presented scenarios and reviews will provide significant benefits for the future development of reliable technologies that protect the 3-D printing intellectual property.

INDEX TERMS Additive manufacturing, 3D printing, intellectual property, copyright protection, digital watermarking, digital right management, rapid prototyping.

I. INTRODUCTION

Three-dimensional (3D) printing made its way to the technological world, but its importance was not widely recognized until a few decades ago. However, it is now clear that 3D printing will impact many industries. Many articles and reports published by national institutes, newspapers, and the private sector emphasize the importance of 3D printing in various areas. In particular, since President Barack Obama's State of the Union Address announcing the ''new industrial revolution'' through forming additive manufacturing hubs across the United States, 3D printing has become a critical research and industrial issue in several aspects. Wohler Associates [1] estimated the market for 3D printers and associated software could exceed US$20 billion by 2020.

Introduction of affordable 3D printers marked the beginning of the era of manufacturing democratization [2]. Customers can customize, innovate, and improve existing designs to suit their own tastes and requirements. The scope of 3D printing applications is wide ranging, including business and industrial equipment, automotive, medical, architecture, food, consumer-product, etc. industries.

As the demand for digital 3D model rapidly increased, distribution platforms, such as Thingiverse, Pinshape, and Sketchfab, started to appear on the Internet, and as the distribution of 3D models increased, copyright infringement also significantly increased. Although 3D printing is thriving with new potential, copyright issues are inevitable with its expansion into the content industry, as occurred previously for music and video markets [3]. The law is struggling to cope with legal challenges this technology has produced [2]. Therefore, research for new technologies to protect 3D prints is urgently required to ensure 3D content intellectual property security.

Content providers have attempted to protect 3D objects by cryptographic, access control based digital right management (DRM), and digital watermarking technologies. Most work has concentrated on typical protection scenarios that occur during normal operation in the digital domain. The problem is that most existing 3D content protection methods are ineffective because the 3D printing process disables those protections, as shown in Fig.1. Digital information, such as file headers or the 3D object graphical structure

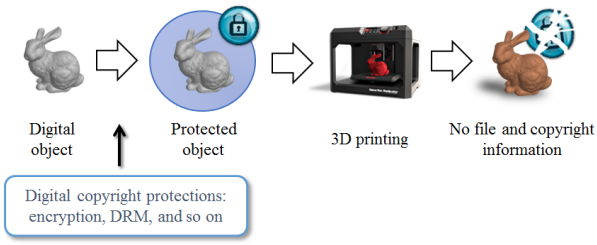


FIGURE 1. Most current 3D object content protection methods are ineffective because file and coordinate information are completely lost during 3D printing.

is completely lost during the 3D printing process. Consequently, 3D objects may be illegally copied and re-distributed in offline and internet markets. This weak point of content protection is called the analog hole [4]. Furthermore, new distribution scenarios not previously defined or considered poses new content security problems. 3D printing brings new requirements for robust copyright protections because they are distributed and handled online and offline. Copyright infringement and protection has had relatively limited research, and 3D content offline distribution environments have been rarely considered.

Various security technologies for 3D printing environments have been proposed. Protection effectiveness differs, and may not be suitable for every copyright infringement scenario, particularly when trying to apply the new technology to existing application scenarios. Therefore, it is critical to define and classify various application scenarios relevant to 3D printing environments. This paper reviews intellectual property protection problems and solutions for 3D printing environments. New copyright infringement scenarios are introduced and analyzed, and previously proposed solution performances are analyzed for each scenario. Finally, we offer future directions for copyright protection technology in 3D printing environments.

The remainder of this paper is organized as follows. Section II reviews the technology and related backgrounds, and Section III discusses illegal distribution scenarios in 3D printing environments. Section IV surveys existing protection solutions and Section V analyzes their effectiveness. Section VI discusses the outcomes of this review and Section VII concludes the paper.

II. BACKGROUND

A. 3D PRINTING TECHNOLOGY

Three-dimensional printing, also known as additive manufacturing, rapid prototyping, layered manufacturing, freeform fabrication, etc., enables 3D physical models to be efficiently fabricated without the restrictions usually imposed by geometric complexity. Standard 3D printers build 3D objects by moving the print nozzle along the x, y, and z axes. The modeling process divides the data into a series of 2D cross-sections of finite thickness, which are combined layer by layer sequence to form the physical 3D object. There are many 3D object manufacturing techniques, including computer numerical control (CNC) machining (also known as subtractive manufacturing), injection molding, and investment casting. This paper limits 3D printing considerations to additive manufacturing, because this technology dominates the existing and future 3D printing markets [5].

The general 3D printing process can be characterized as follows, with relatively minor changes depending on the specific technology employed.

The general process sequence of 3D printing is characterized as follows:

1) STL file conversion (triangulation): the 3D object designed by software, such as computer aided design (CAD), is converted to a stereolithography STL) file, which has become a de facto standard. STL files divide external geometry into a series of triangles, also known as the 3D polygonal mesh, and save their vertices, edges, and face normal vectors. Depending on the printing technology, color and texture information may also be stored.

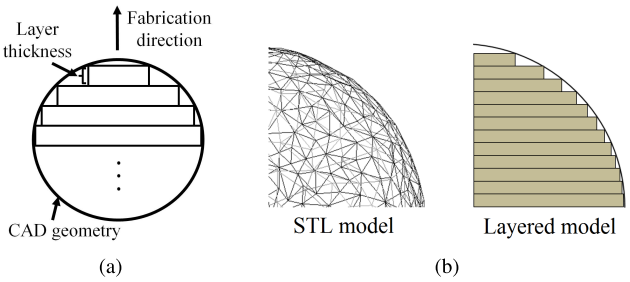
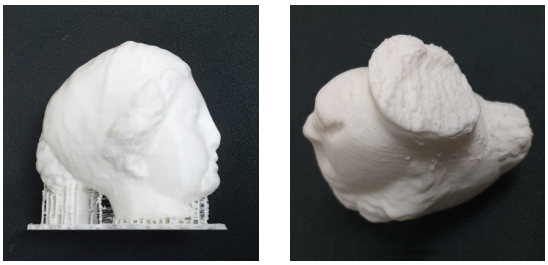


FIGURE 2. (a) General 3D printing parameters, and (b) layering stair step effect.

2) Division into layers, calculation path: size, position, and orientation for the building are set as parameters controlling output resolution, such as fabrication direction and layer thickness (See Fig.2(a)), and the 3D object is digitally sliced by intersecting it with a set of horizontal planes of finite thickness. The printer nozzle motion path is calculated for each plane. Support structure are inserted beneath parts predicted to be weak during fabrication, to help withstand their weight and ensure the parts do not collapse or warp during fabrication (See Fig. 3(a)).
3) Building process: the print nozzle follows the pre-calculated path and builds the 3D object by stacking thin layers. Generally, as each layer is completed, the plate under object descends by the predefined layer thickness along the z axis so the nozzle stacks next layer onto the former layer. Various printing technologies and materials influence output resolution, surface roughness, etc.
4) Post-process: the printed object may require additional cleaning up before being ready for use, including removing supports (See Fig. 3(a)), coating, or



(a) (b)

FIGURE 3. (a) Printed model and support structure, and (b) underneath of the model after removal from the support. When 3D printed objects are removed from their supports, local deformation traces commonly remain on their undersides.

polishing the surface(s), etc., as required for the specific application.

Layer thickness and fabrication direction can significantly affect printed object accuracy [6], [7]. Adding material in distinct layers inherently produces a stair-step effect, a typical artifact of layered manufacturing, as shown in Fig. 2(b). Layer thickness can be thought of as the manufacturing resolution.

Many different 3D printing technologies have been developed, depending on the manufacturing process and materials, including material extrusion technology (FDM), vat photopolymerization (SLA, DLP, CDLP), powder bed fusion (SLS, SLM, EBM), material jetting, binder jetting, and direct energy deposition. Details of each technology are discussed elsewhere [8].

B. CONVENTIONAL COPYRIGHT PROTECTION TECHNOLOGIES

Piracy is the unauthorized use or reproduction of music, movies, books, and other content protected under copyright law. Various technologies have been proposed to prevent copyright infringement, generically called copyright protection. This type of protection usually gives the content owner exclusive rights to perform certain actions or to authorize other actions. This section introduces cryptography based approaches, digital right managements, and digital watermarking, detailing the scope and limitations of each technology.

1) CRYPTOGRAPHY

Cryptography is concerned with secure transmission of data from sender to recipient over an insecure channel. Encrypted data must be converted to an analog signal for human use. Therefore, legitimate consumers are explicitly or implicitly provided with a key to decrypt the content and use the 3D object model. However, cryptography provides no protection once the content is decrypted, which is required for human perception [9], or to print the object. Unfortunately, not all legitimate consumers are trustworthy and an untrustworthy consumer may alter or copy the decrypted content in a manner not permitted by the content owner. Practically, the content is often in an unprotected form in printer device drivers, memory, or storage, and can also be captured at these points. Therefore, encryption is limited to model application, and is inapplicable for 3D printing environments.

2) DIGITAL RIGHTS MANAGEMENT (DRM)

Digital rights management (DRM) is a set of access control technologies for restricting the use of proprietary hardware and copyrighted work [10]. DRM technologies try to control use, modification, and distribution of copyrighted works, such as software and multimedia content, as well as systems within devices that enforce these policies. The core DRM concept is based on digital licenses. Rather than purchasing the digital content, the consumer purchases a license granting certain rights. A license is a digital data file that specifies certain usage rules for the digital content. Usage rules can be defined by a range of criteria, including access frequency, expiration date, transfer restrictions to other devices, copy permissions, etc. However, similar to encryption, The objects must be converted to 3D forms for user to print it, and content can be sampled at those points in the control flow where it is no longer directly associated with a license [11]. Therefore, 3D objects printed by a legitimate user cannot be protected by DRM, and this approach is inapplicable for 3D printing environments.

3) DIGITAL WATERMARKING AND FINGERPRINTING

Digital watermarking [12] is the process of hiding digital information in a noise tolerant signal, such as multimedia data, and intellectual property design [13], [14] (hardware, software, algorithm etc.). The watermark can then be used to determine authorship should a copyright dispute occur, and can be used as a fingerprint to track a distribution path when a prototype in the hands of only a few people is leaked. Digital watermarking could also be utilized as an active component of an automatic system to regulate unauthorized use in a content sharing environment, where 3D watermarks were covertly embedded in the object content before distribution. Since digital watermarking is directly embedded, copyright information can be followed until the content is consumed. Therefore, watermarking complements cryptography and DRM.

The embedded watermark has to resist possible attempts to infringe the copyright. The most significant aspect is to be robust to digital-to-analog (DA) and analog-to-digital (AD) conversion [4], [15], [16] to ensure the watermark message remains in the content after conversion (See Fig. 4).

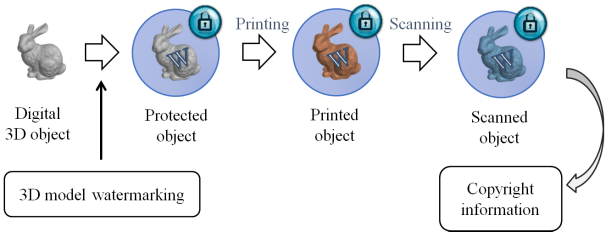


FIGURE 4. An appropriate watermarking system would ensure embedded copyright message(s) in the content survives 3D printing and scanning.

However, most 3D watermarking technologies have focused on scenarios that occur during normal operation in the digital domain [17], which provides limited copyright protection, and requirements for offline environments have only recently begun to be studied. Copyright information may be lost during common processing, including lossy compression or simplification, which are commonly applied to 3D objects. Moreover, in the case of the visible watermark, it is not safe for the copyright holder to maliciously attempt to erase the watermark. Similarly, in the case of the invisible watermark, the copyright information may be lost during common processing such as lossy compression, simplification, which is usually applied to the 3D object.

III. ILLEGAL DISTRIBUTION SCENARIOS

This section introduces several new copyright infringement problems that arise when 3D printers are applied to existing protection systems. Suppose Alice is a copyright holder who creates and transmits digital or printed 3D contents, and Bob is receiving person, who has a possibility to leak a 3D object to a third party.

- Category 1 introduces a digital sharing environment for 3D objects without 3D printing.
- Category 2 introduces three scenarios where Bob uses 3D printers for illegal distribution of digital copies provided by Alice.
- Category 3, introduce three cases that could occur when a 3D printed model from Alice is distributed.

A. CATEGORY 1

Fig. 5 shows a typical conventional scenario for online distribution of digital 3D objects. Alice sends the digital 3D object to Bob over various channels, such as the Internet, contents sharing platform, removable memory, etc. We consider existing copyright protection technologies. DRM is an effective security measure to restrict the use of proprietary hardware and copyrighted works, and cryptography can ensure secure data transmission. However, as discussed above, once the content is decrypted for human perception it is stored unprotected in desktop memory, storage, etc. Although current 3D watermarking can solve this problem, most watermark applications provide less active security than encryption and DRM.

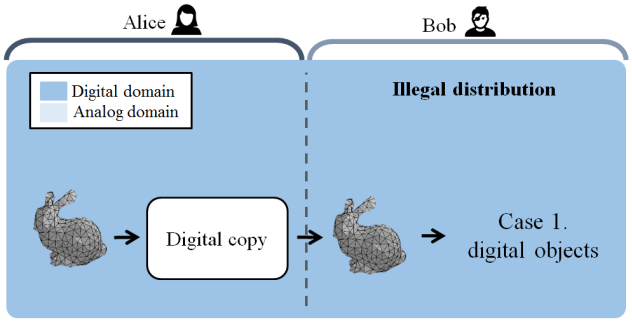


FIGURE 5. Copyright infringement scenario category 1: illegal distribution in the digital domain.

B. CATEGORY 2

Copyright infringement category 2 is a scenario in which 3D printing is intervened after a work is released. In this category, 3D objects produced by Alice are digitally reproduced and delivered to Bob. As shown in Fig. 6, the reproduced model delivered to Bob can be exported as a printed or scanned model through at least one 3D printing or 3D scanning process.

The category 2 includes three cases of copyright infringement scenarios. The details of each scenario are as follows.

1) CASE 2-1

It is the case that Bob leaks the object from Alice using 3D printer. Since Bob is an authorized user, there is no problem to print the protected 3D object. For example, Bob may leak a limited-edition figure that only authorized persons should access. A 3D printer can then replicate the digital object offline, hence Bob can replicate a large number of objects to obtain unfair profit. Furthermore, the digital protection can be removed when Bob prints the object.

2) CASE 2-2

Suppose Bob 3D prints the object and then scans it to remove digital identification information by taking advantage of the analog hole [4]. For example, if the object was protected by access control based protections that allow only single (or any other restricted) printing, Bob can then create countless digital replicas, bypassing the copyright protection. Most current copyright protections are disabled through this 3D printing process, including techniques that inserting copyright information within the object, such embedded watermarks [18] and all encryption and DRM techniques.

3) CASE 2-3

Suppose Bob reproduces an illegal printed object acquired through case 2-2 using 3D printer. Not only Bob can produce countless replicas from unprotected model, but this process can be repeated by any interested third party, with consequential significant commercial damage.

4) PROTECTION SCENARIOS FOR CATEGORY 2

In general, the copyright holder identification information is inserted to 3D object in the Alice's side. In addition, Alice can embed identifying information when uploading the 3D object to the online sharing platform, or the information may be inserted shortly before Bob downloads the object. In this case, the online sharing platform provides its own security measures to protect the objects.

C. CATEGORY 3

Rather than distributing digital objects online, Alice can print the 3D object (either in-house or using a printing agency) and then distribute, share, or sell the object. The object is

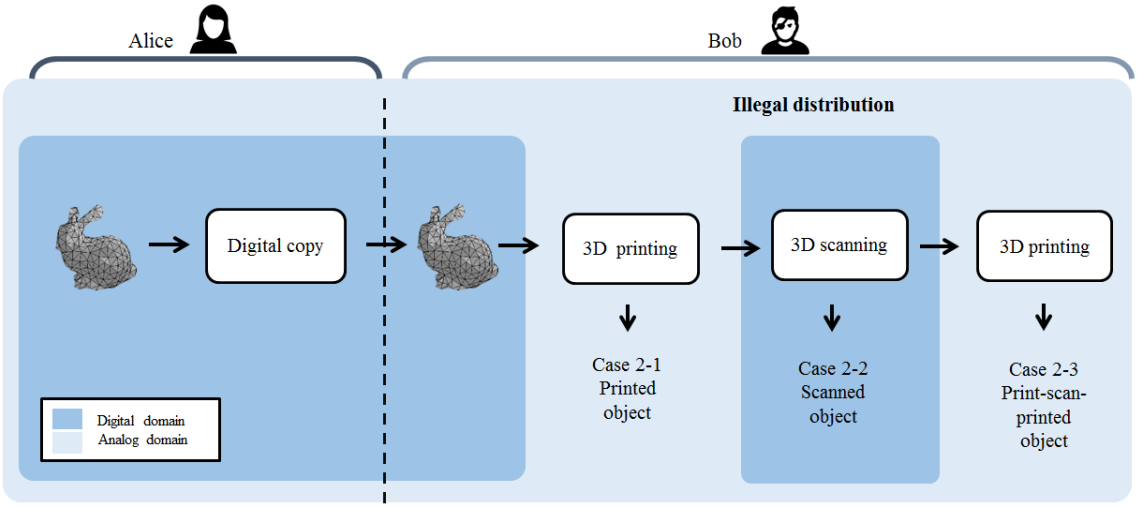


FIGURE 6. Copyright infringement scenario category 2: illegal distribution of 3D digital content using 3D printer.

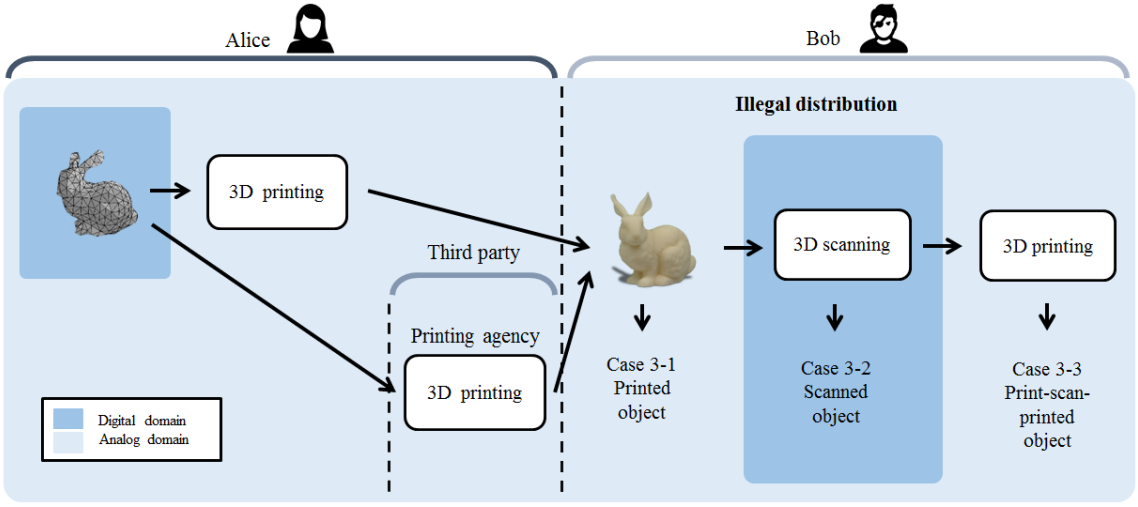


FIGURE 7. Copyright infringement scenario category 3: illegal distribution of 3D printed content from Alice.

delivered to Bob offline. Fig.7 shows how Bob can illegally distribute the printed object from Alice to third parties. Bob can also distribute a scanned digital model obtained from the printed model.

1) CASE 3-1

Suppose Bob leaks the printed object to an unauthorized user. For example, prototypes often go through intermediate testers before market release, and commercial returns can be significantly impacted if the prototype design is leaked. Therefore, a method to protect 3D printed objects, such as multimedia fingerprinting [19], is required. We consider illegal copying of 3D printed objects in cases 3-2 and 3-3.

2) CASE 3-2

Suppose Bob 3D scans the provided 3D object, where he may also remove digital identification information. After scanning, Bob can create countless digital replicas, bypassing Alice's copyright protections. Similar to case 2-2, a large number of existing copyright protections for 3D printing environments are disabled, e.g. inserting copyright information inside an object [20], or embedding a watermark using other materials [18].

3) CASE 3-3

Suppose Bob reproduces an illegal object acquired through case 3-2 using a 3D printer. Similar to case 2-3, this case results in a more challenging copyright protection issue. Smartphone applications or 3D scanners can be used to digitize printed 3D objects. Using the scanned data, Bob can then reproduce countless replicas of the provided model, and the model can be replicated by third parties, compounding the commercial damage.

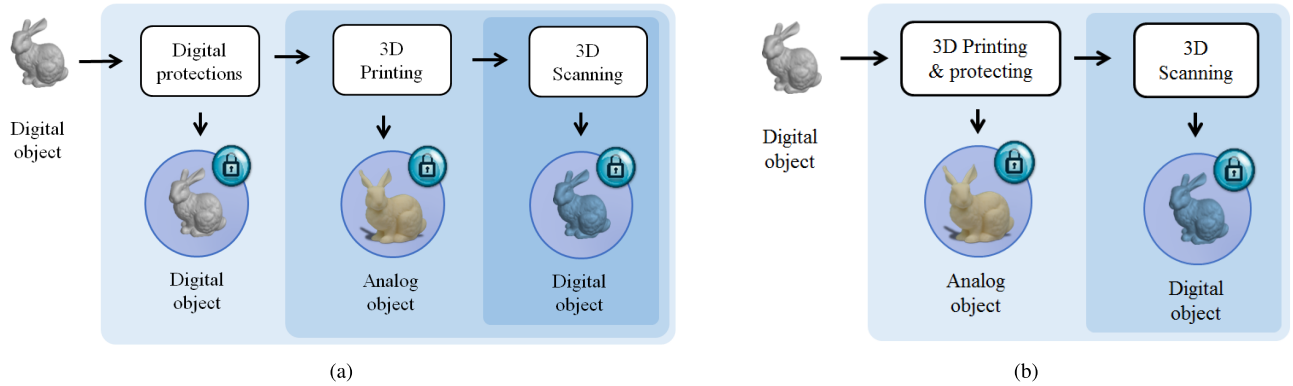


FIGURE 8. Two ways of copyright protections in printing environment. (a) protections in a digital domain and then printing the cover model, (b) protections during or after printing.

4) PROTECTION SCENARIOS FOR CATEGORY 3

For copyright infringement category, 3D objects are generally distributed, shared, or sold using an online or offline market. Thus, Alice can embed copyright owner identification information in a 3D object before delivering the 3D object to an sharing platform or Bob. In general, the copyright holder identification information is inserted to 3D object in the Alice's side.

However, the protection scenario when Alice uses a 3D printing agency is a bit more complicated. The identification information can be inserted by the printing agency. In this case, this protection scenario is the same as the scenario considered in this category. Alternatively, if Alice embed identifying information when sending 3D objects to the agency, protection scenario is the same as the scenario considered in Category 2.

IV. EXISTING COPYRIGHT PROTECTIONS FOR 3D PRINTING ENVIRONMENTS

Current proposed 3D copyright protection techniques only consider digital domain security issues. However, digital security techniques such as DRM and cryptography are not applicable for 3D printing, as discussed above. This section introduces proposed digital and physical copyright protection technologies for various 3D printing applications.

There are two types of techniques introduced here. The first type is a technology class that is directly applied to a digital model (See Fig.8(a)). The technology can be designed to provide security on the digital side. The second type is a technique applied to the printed model, presented in Fig.8(b), in which the security process is applied physically during/after the printing process.

A. DIGITAL DOMAIN TECHNIQUES

The basic requirements for digital domain copyright protection in the 3D printing environment can be defined as follows.

(i) Provide information identifying the copyright holder.
(ii) Robust to DA and/or AD conversion.
(iii) Imperceptibility

Imperceptibility must be acquired not only in terms of conservation of product value but also in enhancing the security of the mark in copyright infringement situations. Depending on the detailed design of the technology, the satisfaction range of (ii) may vary.

This approach is generally called digital watermarking, where copyright information is embedded into the geometric structure of the digital 3D object. This includes techniques to insert copyright marks using through 3D signal processing techniques that cannot be recognized by a person, as well as inserting visible marks, e.g. barcodes or QR codes in non-visible positions, such as inside or on the bottom of the 3D object.

1) NON-BLIND WATERMARKING TECHNIQUES

Non-blind watermarking is the original model to detect copyright information, and has advantages of very high robustness and reliable identification of copyright information. However, non-blind technology preserves both the original model and the watermark to protect the copyright information, hence application is limited. Non-blind techniques can be applied to the following application scenario.

(i) Alice has the 3D object, M, and generates a watermark, w.
(ii) Alice creates watermarked 3D object, M', by embedding w to M.
(iii) Alice publishes M', retaining M and w securely.
(iv) Bob creates a 3D print from M', and claims it to be his own.
(v) Alice 3D scans the object and reconstructs a suspect 3D mesh, M^*.
(vi) Alice extracts a suspect watermark w^* *by comparing* M *and* M^*, and proves w and w^* are equivalent.

The watermark can include additional security using pseudo-random numbers and a secret key. Watermark application and security are discussed in more detail elsewhere [21].

Yamaguchi *et al.* [22] first proposed a method to extract watermarks from 3D printed objects. The watermark is embedded in the spectral region of the digital 3D mesh using

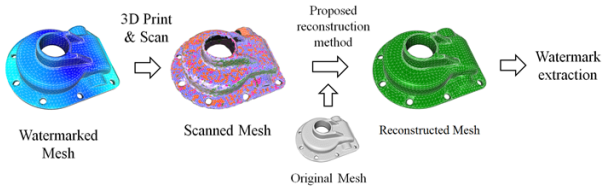


FIGURE 9. Non-blind watermark extraction following Yamaguchi *et al.* [22]. Embedded information is extracted from 3D printed objects by reconstructing the 3D mesh homologous to the original.

a robust, unrecognized, and informed algorithm based on spread spectrum techniques. Fig.9 shows how. the embedded copyright information is extracted from 3D printed objects by reconstructing the 3D mesh homologous to the original. Suspicious 3D meshes are repeatedly optimized using a variant of the nearest point technique to reconstruct sparse subsets, providing accurate and robust reconstructions of noisy and incomplete 3D prints. The mesh is structurally registered to the original mesh in terms of geometry and topology, and the suspicious watermark(s) extracted using simple algebraic operations.

Since the method is non-blind, both the embedding and extracting steps can only be performed by the owner of the original 3D mesh with complete access to the secret data. They also assume that the owner can access the suspicious 3D print to obtain a 3D scan of the surface. This was the first attempt to embed and detect digital watermarks in 3D printed objects, and greatly influenced subsequent research.

Hou *et al.* [23] proposed a robust watermarking domain for 3D print and scan processes based on signal processing. Since the surface normal vector is robust to the stair-stepping manufacturing effect, they proposed a non-blind watermark embedding and extraction method using statistical features of the surface normal vector. However, the proposed technique has only successfully detected watermarks for a limited range of laboratory environments, and cannot guarantee imperceptibility of the embedded watermark.

2) BLIND WATERMARKING APPROACHES

It is important that no prior information about the original content be required at the watermark detection stage. Blind watermarking schemes have several practical advantages over non-blind schemes, because we do not need to know every corresponding key of the 3D printed object. A typical blind watermarking application is as follows.

(i) Alice has the 3D object, M, and generates a watermark, w.
(ii) Alice creates watermarked 3D object, M', by embedding w to M.
(iii) Alice publishes M', retaining w securely.
(iv) Bob creates a 3D print from M', and claims it to be his own.
(v) Alice 3D scans the object and reconstruct a suspect 3D mesh M^*.
(vi) Alice extracts a suspect watermark w^* from M^*, and proves w and w^* are equivalent.

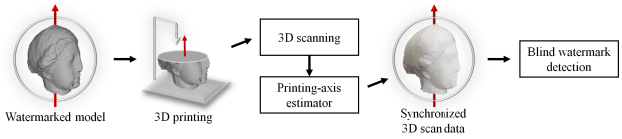


FIGURE 10. Blind watermark extraction procedure of Hou *et al.* [24]. The printing artifact, instead of being regarded as severe distortion, are treated as a template that provides orientation information to the watermark detector.

Hou *et al.* [24] proposed a robust blind watermarking scheme for 3D printing using a component that is unchanging to the printing direction for robustness against the printing process. Printing artifacts, rather than being regarded as distortion, are treated as templates, providing orientation information for the watermark detector (See Fig. 10). They also proposed a blind estimation algorithm for printing direction based on analyzing the layering artifact. The watermark extracted from the printed and scanned model using the proposed estimator is then synchronized with the original orientation. They showed that their proposed watermark scheme with watermark primitive perpendicular to the printing-axis, and watermark synchronization using the printing-axis estimator achieved blindness and robustness in 3D printing environments. However, they also showed that usage and performance are limited. The content provider must align model z-axes and the printing direction to benefit from the printing axis estimator, and imperceptibility and robustness are not insufficient for practical deployment.

Pham *et al.* [25] proposed a 3D printing model watermarking technique using Menger facet curvature and K-means clustering. 3D printing model facets were grouped by K-means clustering of their Menger curvature values, and a watermark embedded by transforming the vertices of a facet with curvature closest to the changed mean curvature. However, their algorithm was based on a naive assumption about geometric transforms in 3D printing and scanning, making it difficult to provide robustness against various distortions, and experimental results were unreliable. They also proposed 3D slicer [26] based watermarking [27] and perceptual encryption [28] to prevent illegal copying or illegal access from unauthorized users and attacks from hackers. However, these algorithms did not consider 3D printing scenarios, and are vulnerability to DA conversion. Therefore, they only provide the same level of protection as encryption and DRM and cannot be applied in complex scenarios or 3D printing systems.

Adobe systems [29] proposed a technique for storing and retrieving data embedded in the 3D printed object surface. The proposed method embedded a 3D symbol matrix in the electronic file used for 3D printing the object as part of its surface structure. Data embedded in the surface structure was processed using 2D image analysis of the embedded pattern. However, the proposed method can affect product quality

because the eventual watermark is humanly visible, and hence vulnerable to malicious removal by an unauthorized user.

3) WATERMARK INSIDE THE PRINTED OBJECT

Okada *et al.* [30] proposed inserting a pattern inside a 3D printed object, as shown in Fig. 11(a). The micro-pattern copyright information is embedded near the object surface and extracted from thermal images obtained with a thermographic camera and two halogen lamps. However, experiments using flat and curved objects showed detection performance was significantly affected by pattern size and surface radius. Hence application to practical 3D printed objects is questionable. Subsequently, Silapasuphakornwong *et al.* [31] improved detection performance using thermal video frames, and other groups have considered near infrared [32] and x-ray [33] based approaches rather than thermographic cameras. Fig.11(b) shows the example of the lighting and recoding system based on near infrared camera devised in [32]. Using x-rays allows copyright information to be included not only in the pattern distribution, but also in the depth information.

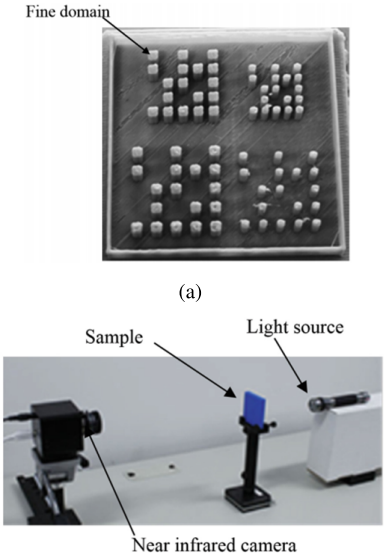


FIGURE 11. Non-destructive detection of data embedded within printed objects: (a) cavity patterns inserted in 3D printed object, and (b) lighting and recording system devised in [32].

Suzuki *et al.* [34] proposed low infill density objects, inserting and detecting copyright information coded by infill density, which is widely used in 3D printing process. They [35] investigated detection performance relative to cavity (or pattern) size, distance between adjacent cavities, and cavity distance from the surface.

B. ADDITIONAL HARDWARE AND MATERIAL

This technology embeds copyright information into the 3D printed object using materials distinct from the printing materials or special identifiers, such as radio-frequency identification (RFID) tags. These techniques are only generally applicable to printed models and do not provide security for the digital domain.

Wee *et al.* [36] proposed several copyright protection methods based on additional materials, inserting an identifier into the object during printing. The identifier could be a bar code, QR code, RFID tag, specific geometric form, etc. Wee *et al.* [37] also proposed a technique to insert an identifier by controlling printer hardware or firmware. However, all the proposed identifiers must be visible in some way to authenticate the object without requiring additional hardware, i.e., the identifier must be on the object surface or the object material must be transparent. Both cases degrade the object value.

Therefore, various techniques to insert identifiers inside 3D printed objects have also been proposed. Wee *et al.* [36], [37] suggested placing an RFID chip inside the 3D object to authenticate copyright information. Disney enterprises [20] proposed a practical copyright protection scheme based on RFID tag, as shown in Fig. 12(a) and Fig.12(b), where a print layer including an RFID tag is inserted during 3D printing. Copyright information can be detected or extracted using an RFID reader. Since the RFID tag is located inside the printed object, it is difficult to remove the tag without damaging the object.

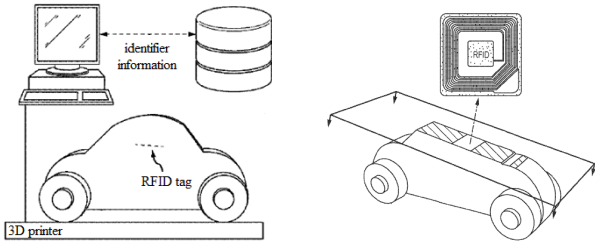


FIGURE 12. Copyright protection scheme based on RFID tags: (a) overall scheme [20], (b) RFID tag layer included during 3D printing.

Several techniques have also been proposed based on special materials and hardware that operate during 3D printing. William *et al.* [18] proposed a watermarking technique inside the 3D model using special equipment to inserting a watermark in the 3D printer hardware. Similarly, Misfeldt *et al.* [38] proposed a technique to insert an identifier inside the object's surface using special materials during printing. The material was distinct from the other printing material, e.g. different magnetic characteristics, and could be detected using a magnetic detector. Both technologies are human visible, and difficult to remove. However, since additional hardware and material are required, they cannot be applied for all current printers.

Quantum Materials Corporation proposed a 3D printing anti-counterfeiting technology based on quantum dot detection [39], [40], which is almost impossible to counterfeit. This method inserted random quantum dots into the

object while printing to produce a unique, physically unclonable fingerprint known only to the manufacturer.

Authentication technologies using chemical materials have also been proposed. Sharon *et al.* [41]–[43] demonstrated fast and accurate authentication for 3D printed products using spectral signatures produced from chemical taggants, yielding covert material based fingerprinting. The ability of UV-cured commodity chemicals to apply and adhere to a wide range of materials and remain undetectable in the visible spectral region is a key enabler of the technology [41]. Fingerprints were created using a directed energy deposition multi-material additive manufacturing system and detected with x-ray fluorescence spectroscopy [42].

V. PERFORMANCE SUMMARY AND ANALYSIS

This section summarizes the applicability of current copyright protection techniques for 3D printing environments introduced in Section III. We summarize the advantages and disadvantages of each technology, imperceptibility, and robustness to malicious removal.

A. IMPERCEPTIBILITY

Imperceptibility is a significant requirement not only to conserve product value, but also to enhance security in copyright infringement situations. Copyright protection serves little purpose if the identifiers are exposed to every user and are not robust to malicious removal. DRM and cryptography do not reduce model quality, because they preserve the original model form. Technologies that require additional hardware, such as internal watermarking techniques [30]–[35], have very high imperceptibility, since the protection or identifier is not exposed on the model surface. RFID tags are located inside the printed object [20], hence are difficult to see or remove without damaging the object. Quantum dots [39], [40] and chemical materials [41]–[43] cannot be detect visually detected, whereas specific detectors for each fingerprint can easily identify them.

However, digital watermarking techniques change the model surface slightly, causing slight damage. For example, watermark distortion may affect printed model performance for very delicate designs, such as mechanical parts. For example, Kumar *et al.* [29] proposed method is perceptible and vulnerable to malicious removal. Geometric watermarks or identifiers [36], [37] are also perceptible, since the identifier must be on the object surface or the overlaying material must be transparent.

B. AGAINST INFRINGEMENT SCENARIO 1

This scenario includes digital domain scenarios considered by current security technologies (see Section III-A for details). All digital watermarking technologies distort the digital 3D model, providing security on the digital domain. However, offline technologies [20], [36], [37], and physical addition [18], [38] (e.g. RFID) technologies cannot provide protection in the digital domain. Special material based techniques also have security limitations in the digital domain. Although internal watermarking [30]–[35] and geometric watermarking [36], [37] did not provide protection scheme in the digital domain when originally proposed, it is not difficult to modify the watermarking algorithms to provide this security.

C. AGAINST INFRINGEMENT SCENARIO 2

Fig.6 shows that the physical model delivered to Bob can be exported as a printed or scanned model through at least one 3D printing or scanning process. Since it cannot be guaranteed that Bob will use a 3D printer with a security system, any technology that cannot be applied in the digital domain is inapplicable to scenario 2. On the other hand, strictly digital domain protection, i.e., DRM and cryptography, are inapplicable to physical objects. Although digital watermarking copyright information can be retained through 3D printing and scanning, this requires a system to detect watermarks offline, such as model surface reconstruction [22], and watermark synchronization [24], [29].

D. AGAINST INFRINGEMENT SCENARIO 3

The content provider (Alice) has fully control over when the digital model is printed, hence she can benefit from a variety of print security technologies. In particular, using a device that inserts a physical watermark not only provides complete security for case 3-1, but also ensures imperceptibility. However, case 3-2 and 3-3 are more challenging copyright protection issues. Digitizing, i.e., optical 3D scanners or cameras, removes all identifiers based on special materials or internal watermarks, whereas digital watermarking based technologies ensure copyright information survives digitizing. Hence, digital watermarking is not vulnerable to digitizing, even in subsequent printing and scanning (case 3-3). However, watermarking can be disabled if digital processing, e.g. post-scan processing or surface smoothing, is performed.

VI. DISCUSSION

A. 3D PRINTING TECHNOLOGIES AND COPYRIGHT PROTECTIONS

Copyright protection technologies discussed here were classified by whether they were affected by 3D printing technology. Current 3D printers tend to be either high cost with high capability or low cost with low capability [44], with higher end printers generally targeted at enterprises and 3D printing agencies, and lower end printers at consumers and hobbyists.

Based on this survey, digital [29] and geometric [36], [37] watermarking techniques are not affected by 3D printing technology type. However, most other techniques are significantly influenced by printing technology type and materials. For example, internal watermarking techniques [30]–[32] or distinguishable material based techniques [18], [38] can only be applied to materials that do not cause interference with the detector. For example, detection using magnetic fields or infrared cameras would not be feasible when printing using metal lamination techniques. On the other hand,

TABLE 1. Scenario applicability of copyright protection methods for 3D printing environments.

Technique	Category	Invisibility[1]	Illegal distribution scenario[2]							Comment
			1	2-1	2-2	2-3	3-1	3-2	3-3	
Conventional techniques	Cryptography	++	○○	×	×	×	×	×	×	Only digital domain
	DRM	++	○○	×	×	×	×	×	×	
	Digital watermarking	+	○○	×	×	×	×	×	×	
Pham *et al.* [28]	Visual cryptography	++	○○	×	×	×	×	×	×	Only digital domain
Yamazaki *et al.* [22]	Digital watermarking	+	○○	○	○	○	○	○	○	Non-blind, 3D scanner
Hou *et al.* [23]	Digital watermarking	+	○○	○	○	○	○	○	○	Non-blind, 3D scanner
Hou *et al.* [24]	Digital watermarking	+	○○	○	○	○	○	○	○	Blind, 3D scanner
Pham *et al.* [27]	Digital watermarking	+	○○	○	○	×	○	○	×	Blind, 3D scanner
Kumar *et al.* [29]	Digital watermarking	−	○○	○○	○	○	○○	○	○	Blind, 3D scanner
Takashima *et al.* [30]–[32] Suzuki *et al.* [33]–[35]	Internal watermarking	+	○	○○	×	×	○○	×	×	Require additional devices for detection
Wee *et al.* [36], [37]	Geomatric watermarking during printing proces	−	×	×	×	×	○○	○	○	Require additional devices for detection
Williams *et al.* [18], Misfeldt *et al.* [38]	Watermarking based on distinguishable material	++	×	×	×	×	○○	×	×	Require additional devices for insertion and detection
Wee *et al.* [36], [37], Voris *et al.* [20]	Electrical device based (RFID)	++	×	×	×	×	○○	×	×	Require additional devices for insertion and detection
Elliott *et al.* [39], [40]	Quantum dot based	++	×	×	×	×	○○	×	×	Require additional devices for insertion and detection
Sharon *et al.* [41]–[43]	Chemical material based	++	×	×	×	×	○○	×	×	Require additional devices for insertion and detection

Notes: [1] ++: does not affect object's quality, +: induces small distortions, −: visible mark(s) or distortion(s)
[2] ○○: applicable for this scenario, ○: applicable in limited setting, ×: inoperative

chemical material based techniques [42] are only applicable to metal material based printing.

Digital watermarking [23], [24] can provide copyright protection for low cost 3D printing methods, such as laminated object manufacturing (LOM) and fused deposition modeling (FDM). However, the methods cannot be used for higher end printers because they provide very high printing resolution, making it difficult to capture printing artifacts using general scanners [24]. In the future, 3D printing and scanning technology will provide very accurate, almost perfect, copies of 3D objects. Watermarking system degrees of freedom are expected to increase for situations with high DA and AD conversion accuracy. Therefore, future research directions must consider entirely new security techniques or watermarking technologies robust to DA-AD conversion rather than focusing on printing process noise part of DA conversion.

The main advantage of digital watermarking technologies introduced here is that there is no need to change 3D printing technology or device to insert copyright information, i.e., the digital watermark can be printed directly on a typical 3D printer without any special equipment. In contrast, several other techniques require additional devices and printing technology modifications. Internal watermarking [30]–[32] needs special devices only for detection, e.g. infrared or thermographic camera, x-ray machine, etc. Some protection techniques require additional devices for both insertion and detection. Distinguishable material techniques [18], [38] require printing equipment modification, and quantum dot [39], [40] and chemical material [41]–[43] technologies need very sophisticated techniques and equipment.

Unfortunately, none of the current techniques completely cover all scenarios. Future research is essential to develop methods and technologies to solve these copyright issues. However, reasonable copyright protection can be achieved immediately by performance improvements and optimization of current technologies. Since each technique has advantages and disadvantages, combining various technologies could significantly improve protection coverage. For example, digital watermarking on the object surface [24] and inside the printed model [30] complement each other to some extent. Thus, until new approaches are developed, content providers need to focus on the limited requirements for their specific applications.

B. OTHER COPYRIGHT ISSUES

There are a wide variety of copyright infringement scenarios in addition to the scenarios described in this paper. Although we focused on copyright issues and security technologies for digital content, creating digital 3D content can also raise copyright infringement problems. For example, the iron throne that appears in the TV show Game of Thrones, or a video game tank design are intellectual property, since they are someone's creative product.

In 2013, a 3D printing technology startup created a smartphone charging cradle inspired by the iron throne (see Fig. 13(a) and Fig.13(b)). The startup registered the 3D printed steel throne design for $50 USD on a website for 3D content sharing, but sales were blocked by HBO, the TV channel that owns Game of Thrones copyright. This copyright infringement is beyond the scope

(a) (b)

FIGURE 13. Creating digital 3D content can raise copyright infringement. For example: (a) the 'Iron throne' from the popular TV drama 'Game of Thrones', and (b) a subsequent smartphone charging cradle 3D printer output.

considered in this paper. The startup did not digitally copy an existing object (either digitally or by 3D scanning), but designed their model based on the TV images. Continuous monitoring of 3D content sharing and sales platforms is required to actively prevent such infringement cases. Thus, an effective monitoring system incorporating image based 3D model retrieval [45], [46] or 3D object retrieval [47], [48] is required.

In addition, derivative work of digital 3D object can cause another type of digital copyright infringement issues [49]. For example, a creator can use a 3D editing program to change the figure's posture, or insert a mark or signature to increase its value. Also, a method of editing parts of different models and combining them in one form can be used. Security technologies for this issue include digital watermarking based protections [50], [51], and feature points based 3D object retrieval system [52], [53]. In addition, distinguishable material based watermarking techniques [18], [38] are useful to cope with editing of a 3D printed model.

VII. CONCLUSIONS

This paper reviewed intellectual property infringement issues and protection technologies for 3D printing environments. We introduced various digital content copyright infringement scenarios that occur in the 3D printing environment, summarized requirements not currently defined in the literature, and defined new technology scenarios and requirements. We analyzed current copyright security technology coverage according to the introduced scenarios and various aspects and discussed the pros and cons of each technology and future research directions.

This paper suggests that research on protection technology for 3D printing environment is expanding due to the many applications that could benefit. Copyright protection is essential to develop a number of related markets. Most companies and individuals interested in 3D printing are aware that intellectual property protection is a major current issue and will only become more important in the near future. Thus, a reliable technology to protect 3D printing intellectual property (copyright and other aspects) will provide great advantages for society, industry, and academia.

REFERENCES

[1] A. Zaleski, "Here's why 2016 could be 3D printing's breakout year," Tech. Rep., 2015.
[2] V. Niess and S. Wende, "Intellectual property and product liability challenges in three-dimensional printing [IP corner]," *IEEE Consum. Electron. Mag.*, vol. 6, no. 4, pp. 128–163, Oct. 2017.
[3] R. Stern, "Napster: A walking copyright infringement?" *IEEE Micro*, vol. 20, no. 6, pp. 4–5, 95, Nov. 2000.
[4] E. Diehl and T. Furon, "Watermark: Closing the analog hole," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jun. 2003, pp. 52–53.
[5] R. Jiang, R. Kleer, and F. T. Piller, "Predicting the future of additive manufacturing: A Delphi study on economic and societal implications of 3D printing for 2030," *Technol. Forecasting Social Change*, vol. 117, pp. 84–97, Apr. 2017.
[6] P. Kulkarni and D. Dutta, "An accurate slicing procedure for layered manufacturing," *Comput. Aided Des.*, vol. 28, no. 9, pp. 683–697, 1996.
[7] D. Ahn, H. Kim, and S. Lee, "Fabrication direction optimization to minimize post-machining in layered manufacturing," *Int. J. Mach. Tools Manuf.*, vol. 47, nos. 3–4, pp. 593–606, 2007.
[8] B. Redwood. (2018). *Additive Manufacturing Technologies: An Overview*. [Online]. Available: http://www.3Dhubs.com
[9] I. J. Cox and G. Doërr, and T. Furon, "Watermarking is not cryptography," in *Digital Watermarking*. Berlin, Germany: Springer-Verlag, 2006, pp. 1–15.
[10] Q. Liu, R. Safavi-Naini, and N. P. Sheppard, "Digital rights management for content distribution," in *Proc. Australas. Inf. Secur. Workshop Conf. ACSW Frontiers*, vol. 21, 2003, pp. 49–58.
[11] S. Haber, B. Horne, J. Pato, T. Sander, and R. E. Tarjan, "If piracy is the problem, is DRM the answer?" in *Digital Rights Management*. Berlin, Germany: Springer-Verlag, 2003, pp. 224–233.
[12] S. P. Mohanty, A. Sengupta, P. Guturu, and E. Kougianos, "Everything you want to know about watermarking: From paper marks to hardware protection: From paper marks to hardware protection," *IEEE Consum. Electron. Mag.*, vol. 6, no. 3, pp. 83–91, Jul. 2017.
[13] A. Sengupta and S. Bhadauria, "Exploring low cost optimal watermark for reusable IP cores during high level synthesis," *IEEE Access*, vol. 4, pp. 2198–2215, 2016.
[14] A. Sengupta, D. Roy, and S. P. Mohanty, "Triple-phase watermarking for reusable IP core protection during architecture synthesis," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 37, no. 4, pp. 742–755, Apr. 2018.
[15] M. Steinebach, A. Lang, J. Dittmann, and C. Neubauer, "Audio watermarking quality evaluation: Robustness to DA/AD processes," in *Proc. Int. Conf. Inf. Technol., Coding Comput.*, Apr. 2002, pp. 100–103.
[16] J.-U. Hou, J.-S. Park, D.-G. Kim, S.-H. Nam, and H.-K. Lee, "Robust video watermarking for MPEG compression and DA-AD conversion," in *Proc. 1st Int. Workshop Inf. Hiding Criteria Eval.*, 2014, pp. 2–8.
[17] K. Wang, G. Lavoue, F. Denis, and A. Baskurt, "A comprehensive survey on three-dimensional mesh watermarking," *IEEE Trans. Multimedia*, vol. 10, no. 8, pp. 1513–1527, Dec. 2008.
[18] R. V. Williams, R. H. Curtis, Jr., G. R. G. Bargoud, and R. Hershko, "Three-dimensional scanning watermark," U.S. Patent 14 317 516, Dec. 31, 2015.
[19] K. R. Liu, W. Trappe, J. Z. Wang, M. Wu, and H. Zhao, *Multimedia Fingerprinting Forensics for Traitor Tracing*, vol. 4. Cairo, Egypt: Hindawi Publishing Corporation, 2005.
[20] J. Voris, B. F. Christen, J. Alted, and D. W. Crawford, "Three dimensional (3D) printed objects with embedded identification (ID) elements," U.S. Patent 9 656 428, May 23 2017.
[21] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*. San Mateo, CA, USA: Morgan Kaufmann, 2007.
[22] S. Yamazaki, S. Kagami, and M. Mochimaru, "Extracting watermark from 3D prints," in *Proc. Int. Conf. Pattern Recognit.*, Aug. 2014, pp. 4576–4581.
[23] J.-U. Hou, D.-G. Kim, S. Choi, and H.-K. Lee, "3D print-scan resilient watermarking using a histogram-based circular shift coding structure," in *Proc. 3rd ACM Workshop Inf. Hiding Multimedia Secur.*, 2015, pp. 115–121.
[24] J.-U. Hou, D.-G. Kim, and H.-K. Lee, "Blind 3D mesh watermarking for 3D printed model by analyzing layering artifact," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2712–2725, Nov. 2017.
[25] G. N. Pham, S.-H. Lee, O.-H. Kwon, and K.-R. Kwon, "A watermarking method for 3D printing based on Menger curvature and K-mean clustering," *Symmetry*, vol. 10, no. 4, p. 97, 2018.

[26] (2018). *3D Slicer*. [Online]. Available: https://www.slicer.org/
[27] G. N. Pham, S.-H. Lee, O.-H. Kwon, and K.-R. Kwon, "A 3D printing model watermarking algorithm based on 3D slicing and feature points," *Electronics*, vol. 7, no. 2, p. 23, 2018.
[28] G. N. Pham, S.-H. Lee, and K.-R. Kwon, "Interpolating spline curve-based perceptual encryption for 3D printing models," *Appl. Sci.*, vol. 8, no. 2, p. 242, 2018.
[29] A. Kumar, N. P. Goel, and M. Hemani, "Method and apparatus for storing and retrieving data embedded into the surface of a 3D printed object," U.S. Patent 9 400 910, Jul. 26, 2016.
[30] A. Okada, P. Silapasuphakornwong, M. Suzuki, H. Torii, Y. Takashima, and K. Uehira, "Non-destructively reading out information embedded inside real objects by using far-infrared light," *Proc. SPIE*, vol. 9599, p. 95992V, Sep. 2015.
[31] P. Silapasuphakornwong, M. Suzuki, H. Unno, H. Torii, K. Uehira, and Y. Takashima, "Nondestructive readout of copyright information embedded in objects fabricated with 3-D printers," in *Proc. Int. Workshop Digit. Watermarking*. Cham, Switzerland: Springer, 2015, pp. 232–238.
[32] K. Uehira, M. Suzuki, P. Silapasuphakornwong, H. Torii, and Y. Takashima, "Copyright protection for 3D printing by embedding information inside 3D-printed objects," in *Proc. Int. Workshop Digit. Watermarking*. Cham, Switzerland: Springer, 2016, pp. 370–378.
[33] M. Suzuki, P. Silapasuphakornwong, Y. Takashima, H. Torii, and K. Uehira, "Number of detectable gradations in X-ray photographs of cavities inside 3-D printed objects," *IEICE Trans. Inf. Syst.*, vol. E100-D, no. 6, pp. 1364–1367, 2017.
[34] M. Suzuki, P. Silapasuphakornwong, Y. Takashima, H. Torii, H. Unno, and K. Uehira, "Technique for protecting copyrights of digital data for 3-D printing, and its application to low infill density objects," in *Proc. 8th Int. Conf. Adv. Multimedia*, 2016, pp. 56–59.
[35] M. Suzuki, P. Dechrueng, S. Techavichian, P. Silapasuphakornwong, H. Torii, and K. Uehira, "Embedding information into objects fabricated with 3-D printers by forming fine cavities inside them," *Electron. Imag.*, vol. 2017, no. 7, pp. 6–9, 2017.
[36] J. Y. S. Wee, C. I. Byatte, A. D. G. Rhoades, and D. L. McNeight, "Product authentication," U.S. Patent 14 250 533, Sep. 3, 2015.
[37] J. Y. S. Wee, C. I. Byatte, A. D. G. Rhoades, and D. L. McNeight, "Objets de vertu," U.S. Patent 14 485 880, Dec. 10, 2015.
[38] E. D. Misfeldt, M. T. Allott, and S. J. Pierz, "Component and watermark formed by additive manufacturing," U.S. Patent 9 826 115, Nov. 21, 2017.
[39] O. Ivanova, A. Elliott, T. Campbell, and C. B. Williams, "Unclonable security features for additive manufacturing," *Additive Manuf.*, vols. 1–4, pp. 24–31, Oct. 2014.
[40] A. M. Elliott, "The effects of quantum dot nanoparticles on the polyjet direct 3D printing process," Ph.D. dissertation, Dept. Mech. Eng., Virginia Tech, Blacksburg, VA, USA, 2014.
[41] S. Flank, G. E. Ritchie, and R. Maksimovic, "Anticounterfeiting options for three-dimensional printing," *3D Printing Additive Manuf.*, vol. 2, no. 4, pp. 180–189, 2015.
[42] S. Flank, A. R. Nassar, T. W. Simpson, N. Valentine, and E. Elburn, "Fast authentication of metal additive manufacturing," *3D Printing Additive Manuf.*, vol. 4, no. 3, pp. 143–148, 2017.
[43] S. Flank, "3D fakes: Chemical fingerprinting in additive manufacturing, from pharmaceuticals to engines," in *Proc. NIP, Digit. Fabr. Conf.*, vol. 1. Springfield, VA, USA: Society for Imaging Science and Technology, 2017, pp. 187–190.
[44] A. Earls and V. Baya. (2016). *The Road Ahead for 3-D Printers*. [Online]. Available: http://www.pwc.com/us/
[45] M. Aubry, D. Maturana, A. A. Efros, B. C. Russell, and J. Sivic, "Seeing 3D chairs: Exemplar part-based 2D-3D alignment using a large dataset of CAD models," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2014, pp. 3762–3769.
[46] F. Massa, B. C. Russell, and M. Aubry, "Deep exemplar 2D-3D detection by adapting from real to rendered views," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2016, pp. 6024–6033.
[47] B. Li *et al.*, "A comparison of 3D shape retrieval methods based on a large-scale benchmark supporting multimodal queries," *Comput. Vis. Image Understand.*, vol. 131, pp. 1–27, Feb. 2015.
[48] T. Furuya and R. Ohbuchi, "Deep aggregation of local 3D geometric features for 3D model retrieval," in *Proc. BMVC*, 2016, pp. 121.1–121.12
[49] M. J. Meurer, "Price discrimination, personal use and piracy: Copyright protection of digital works," *Buffalo Law Rev.*, vol. 45, p. 845, Dec. 1997.
[50] H.-U. Jang *et al.*, "Cropping-resilient 3D mesh watermarking based on consistent segmentation and mesh steganalysis," *Multimedia Tools Appl.*, vol. 77, no. 5, pp. 5685–5712, 2018.
[51] H.-Y. Choi, H.-U. Jang, J. Son, and H.-K. Lee, "Blind 3D mesh watermarking based on cropping-resilient synchronization," *Multimedia Tools Appl.*, vol. 76, no. 24, pp. 26695–26721, 2017.
[52] J. W. Tangelder and R. C. Veltkamp, "A survey of content based 3D shape retrieval methods," in *Proc. Shape Modeling Appl.*, Jun. 2004, pp. 145–156.
[53] A. Mian, M. Bennamoun, and R. Owens, "On the repeatability and quality of keypoints for local feature-based 3D object retrieval from cluttered scenes," *Int. J. Comput. Vis.*, vol. 89, nos. 2–3, pp. 348–361, 2010.

JONG-UK HOU received the B.S. degree in information and computer engineering from Ajou University, South Korea, in 2012, and the M.S. degree in Web science and technology from the Korea Advanced Institute of Science and Technology, South Korea, in 2014, where he is currently pursuing the Ph.D. degree with the Multimedia Computing Laboratory, School of Computing. His major interests include various aspects of information hiding, point cloud processing, computer vision, machine learning, and multimedia signal processing. He was a recipient of the Global Ph.D. Fellowship from the National Research Foundation of Korea in 2015. He has been a Reviewer of many international journals, including the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY and the IEEE TRANSACTIONS ON IMAGE PROCESSING.

DONGKYU KIM received the B.S. degree in electronics and communications engineering from Hanyang University, Seoul, South Korea, in 2013, and the M.S. degree in electrical engineering from the Korea Advanced Institute of Science and Technology, Daejeon, South Korea, in 2015, where he is currently pursuing the Ph.D. degree with the School of Computing. His research interests include various aspects of information hiding, digital image forensics, machine learning, and deep learning.

WON-HYUK AHN received the B.S. degree in software and computer engineering from Ajou University, South Korea, in 2016. He is currently pursuing the Ph.D. degree with the School of Computing, Korea Advanced Institute of Science and Technology. His research interests include multimedia forensics, computer vision, and machine learning.

HEUNG-KYU LEE received the B.S. degree in electronics engineering from Seoul National University, Seoul, South Korea, in 1978, and the M.S. and Ph.D. degrees in computer science from the Korea Advanced Institute of Science and Technology (KAIST), South Korea, in 1981 and 1984, respectively. Since 1986, he has been a Professor with the School of Computing, KAIST. He has authored/co-authored over 200 international journal and conference papers. His major interests are digital watermarking, digital fingerprinting, and digital rights management. He has been a Reviewer of many international journals, including the *Journal of Electronic Imaging*, *Real-Time Imaging*, and the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY.