Approaches to Maintaining Provenance throughout the Additive Manufacturing Process

Nawfal F. Fadhel
ECS, University of Southampton
UK
nff1g08@ecs.soton.ac.uk

Richard M. Crowder
ECS, University of Southampton
UK
rmc@ecs.soton.ac.uk

Gary B. Wills
ECS, University of Southampton
UK
gbw@ecs.soton.ac.uk

Abstract— The development of 3D printers has resulted in significant Intellectual Property Right issues. This work presents a model for signing printable 3D objects. The paper initially reviews the security principles of signing of objects in both digital or physical form, and the metrics for assessing signatures. 3D designs are not just a file, but actual physical objects and should be treated identically, to digital documents that have associated intellectual property rights and copyright protection. In this paper we propose a signing methodology intended to resolve issues with the adaptation of rapid prototyping and 3D printing by users both in engineering and the humanities. The proposed digital signing methodology is based on physical signing principles that follow archival principles to maintain accurate records. The new model allows the transition of provenance between digital and physical form.

Index Terms—Digital Signing; 3D printing; 3D objects; provenance.

I. INTRODUCTION

Additive manufacturing as a process has been used within engineering development since the late 1970's [1]. However it is only very recently that the technology has been widely available at reasonable cost. Currently a 3D printer can be purchased from approximately $600 (£400). The relatively low cost of this technology has raised a number of challenges, in particular how can the provenance of the printed object be proven and guaranteed. In day-to-day activities of architects, designers and engineers, valuable intellectual property is created; including the 3D designs used during the process of rapid prototyping a product. These objects are frequently used to illustrate and share designs or ideas. The problems associated with breaches of copyright etc., are as acute in the humanities as in engineering, for this reason, the paper will look across both domains. The digital document from which the object is printed is either acquired through digital capture devices or produced by a CAD system. Some of these 3D designs (digital documents) are secured by publishing them under Creative Commons Licenses[1] or making them available only to certain individuals. The paper explores the possibility of securely signing printable 3D objects using additive manufacturing. The paper reviews a number of attempts to solve the issue of secure signing either directly or indirectly; such as the covering it under the definition of a secure system as in ISO7498 standard for trusted hardware [1], or using digital watermarking [2].

The aim of the paper is to present a framework for sharing information about 3D objects securely using signing methods such that when the object is printed, the following attributes are also transferred to the printed object:

- Authentication: we need to authenticate an object with a trusted party.
- Integrity: we need to track visible changes and ensures the object has not been tampered with.
- Non-Repudiation: we need to prove that the object belongs to a certain party within reasonable doubt.

It is clear that using additive manufacturing as described later in Section II raises significant questions related to intellectual property and copyright. In the development of this new model we have to consider a number of related areas in digital security, however we first consider the underlying principles of digital signing (and the

[1] http://creativecommons.org

signature) in Section III. In order to achieve this we consider Semantics (Section IV), the cataloging and archiving processes (Section V), compliance (Section VI) and ownership (Section VII). Once these have been considered we present the proposed model in Section VIII. Finally we discuss digital identity and provenance of 3D objects in Section IX, which we aim to maintain through out the transition process of the object from its digital state to the resultant physical state. The paper concludes with comments in Section X.

II. ADDITIVE MANUFACTURING

The additive manufacturing process can be effectively considered to consist of two distinct phases, firstly the digitization of an object and then its manufacture by 3D printing, as summarized in Figure 1.

A. *Digitization principles*

The initial step is to acquire a three dimensional model, which depending on the application domain can exist in a number of formats. If we are considering engineering, the component will in all probability exist as either a 3D CAD model or as engineering drawings. The first step is acquiring or creating the 3D data from a singular source or multiple such is the case in reconstruction projects [3]. However if we are considering the humanities, in particular archeology, we have a number of viewpoints, either the actual physical objects or a description or artistic visualization of an object as described in texts etc. This lead to a number of options depending on the application for which additive manufacturing is being used:

- **Replica:** is a digital copy of an object with exact measurement taken using a digital tool such as 3D scanner [3].
- **Reconstructed Replica:** is a digital copy of an object with reconstructed design that is based on fragments and document description of the missing areas of the original object [3].
- **Dictated realization of a design:** is a digital copy of an artistic presentation based on description of an object that was measured and documented in the archaeological record. For example the Bayman Buddha in Afghanistan that were destroyed by the Taliban [4].
- **Inspired realization of a design:** is a digital copy of an artistic presentation based on description of an object that was mentioned in historical record in poems and inscriptions. For example the artistic depiction of the Colossus of Rhodes [5].

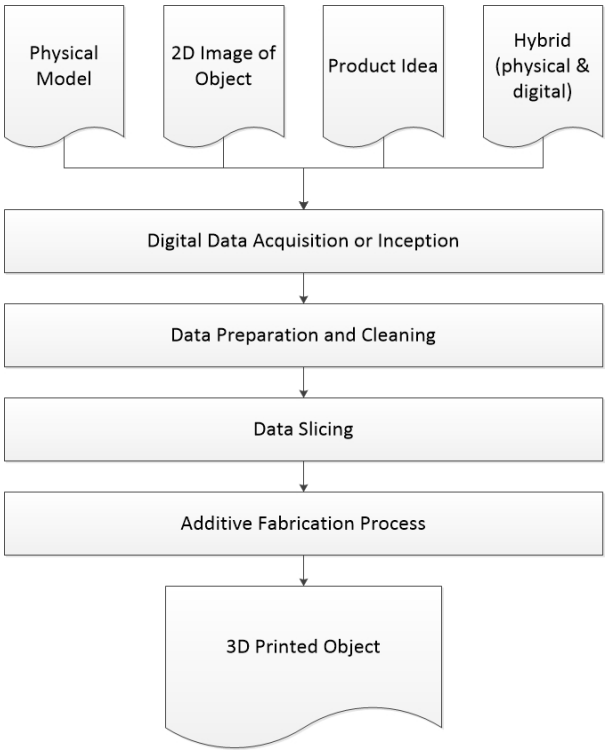

Figure 1 – The Digitization process for Additive Manufacturing objects from concepts or existing product to fabricated objects or replicas

Figure 1 shows the steps required to convert a digital design to a digital object, and can be considered to require four steps:

- A digital representation of the object is firstly generated from a number of sources, ranging from scanning a model to a CAD drawing.
- The digital representation is cleaned by removing all the undesirable data and noise. The design is allocated physical data storage and the 3D object is stored in a digital state.
- The digital representation of the 3D object is fed into a slicing program that

separate the object into layers, in preparation for fabrication.

- The fabrication process using an additive manufacturing machine to print out the object.

B. 3D printing

Once the digital information has been processed into slices, the artifact can be can be constructed by the use of additive manufacturing system. An additive manufacturing or 3D printing builds an artifact using incremental layers of material typically 0.1mm in thickness. The process is available in number of technologies including molten polymer deposition, granular material binding and photo-polymerization. These techniques allow the artifact to be manufactured in a number of materials including plastic, metal and ceramic. The final production quality of 3D printed artifact is dependent on the resolution capability of the printer used, the material used, and the method of printing. In addition the complexity of the end product and whether it will have movable parts within the artifact is also a factor. The technology selected depends on the function and usage of the fabricated object, and the required color [6]. It is important to note that a 3D printed artifact do not have an identity or method of tracking; after the digital object is printed as it loses all of its digital security identifiers, and hence is effectively impossible to validate it authenticity, particular given the rapidly improving quality of the 3D printer [7]. Hence the concern in both engineering (e.g. manufacture of out of specification components), or humanities (illegal copying of an object of significant historical content [8]).

III. DIGITAL SIGING PRINCIPLES

The principles for digital signing have not change since its introduction required by the exchange of electronic documents. Digital signing provides the authenticity of electronic mail to verify it the message is genuine by providing evidence that the message has not changed and the sender is identified. [9].

As a result of the introduction of new digital file formats (e.g STL or STereoLithography) used in additive manufacturing to reproduce an object, the digital signing process needs to be reconsidered. The objective being to allow for the capability of proving the legitimately of any 3D object whether it is in a digital or physical state. In the physical state the security requirements can be summarized as confidentiality, integrity and availability.

It is widely recognized that cryptographers resolve the requirements for digital signing roles using three underlying principles; authentication, integrity and non-repudiation. It is our view that for the provenance of physical objects, we can use semantics in an identical mechanism to that used for the signing of the digital document. The semantics can include the author of a document, acknowledgment of the reception of a document by a second party, witnessing the document signature and lastly agreement that the document is genuine. For scholarly publication and the identity of data sets prior to digital publishing [10], it was noted that "*authorship has multiple functions in the sciences. We can describe these as follows: 1) attributing credit for discoveries to a person or group of people; 2) assigning ownership to this person or persons; and 3) enabling the accrual of reputation.*"

In the process we are considering in this paper, we are looking at the transition of the identity of an object from the state where its claim of identity is proven in digital state to proving its claim of identity in an artifact after is has been 3D printed, by achieving the same three criteria; confidentiality, integrity and availability, which also makes our framework agnostic.

IV. SEMANTICS IN DESCRIBING PHYSICAL AND 3D PRINTED OBJECTS

The public key infrastructure and the information used in the signing process as constructed by cryptographic community currently can falls short in describing a 3D objects from a archival prospective. It has been suggested that cryptographers disregarded semantics about the object's origin and background and focus more on the security between participating partners in a transaction; Bantin [11] notes while archivist would have liked more semantics that describe the object to assist the archivist in proving

maintenance of records, archaeologists practice a similar attitude as they study of materials. It can be concluded that by considering the material culture of a relic would benefit from using semantics when describing an object. Within artistic communities, artists place proving provenance of an artistic work is given the highest priority, taking precedence in the digitization process of artifacts or sharing a digital designs more widely [8].

V. CATALOGING AND ARCHIVING IN THE PUBLIC DOMAIN

In the field of archiving, it is common for archivist to use metrics such as Kipling's approach known as the 5W's and the H of journalism which are; *when* the record was appraised, *what* was appraised, *why* is was appraised, *how* were records appraised. *Who* and *where* are not mentioned but are implied. The requirements mentioned by Bantin [11], described the archiving of electronic records using Kipling method, which align with *authentication, integrity* and *non-repudiation,* used by the Internet Engineering Task Force requirements for secure digital signing. The provenance of a 3D objects is becoming a significant issue, whether the native state of the object was native digital or natively physical it remains in the hands of the creator of the object. For example, according to the aims of London charter [12], where the digitization of cultural heritage artifacts is preformed only when required, as result we are establishing two objects and one identity.

VI. COMPLIANCE WITH SECURE SYSTEM ARCHITECTURE

If we consider the metrics for a digital signature we will start by defining authentication, integrity and non-repudiation as defined in [1]. The terms are defined as follows:

- Authentication is used in conjunction with integrity, which is defined as "a property in which the data has not been altered or destroyed in unauthorized procedure" [13].
- Data integrity is defined as the process where data is maintained to achieve a high level of accuracy and consistency over its life cycle [18].
- Non-repudiation is a state where the entity involved in a communication with other entities is unable to deny involvement in the communication between parties [1].

Based on these definitions and our understanding of the problem we can combine the digital signing principle described above with the physical provenance methods, which are confidentiality, integrity and availability as discussed by Bishop [15]. If the object was created in digital state then it can be recreated in a physical state via 3D printing and if the object is in physical state it can be digital scanned and becomes a digital object. The framework (see Figure 2) is tailored to enable the transition of properties from the digital object to the physical 3D printed object.

VII. OWNERSHIP AND DIGITAL RIGHTS OF A 3D OBJECT (PROVENANCE)

Attempts in the commercial sector and academic circles regarding ownership are complex and can be considered at two levels. The first, the users have the right to print the object but not own it and the object can either be viewed remotely via secure streaming like the attempt describe by [16]. Currently it is unknown if this method would be widely adopted because of similar cases where Amazon deleted content from users Kindles claiming the users only had the right to rent them but not own [17]. The second approach is you can posses the object but in order to secure it, it is provided with a watermark or similar feature that has to be incorporated. The watermarking procedure removes, modify or change a part of the object, and therefor can impinge on the purpose or quality of the object. Related to this we need to consider the Berne Convention for the protection of literary and artistic works (WIPO)[2] which states

[2] "Berne Convention for the Protection of Literary and Artistic Works", WIPO

(http://www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html (accessed 25 March 2010)).

the copying procedure of artistic and literary works must be "...substantial copied..." to infringe its copyrights. In other words if forgers or illegal copyholders of 3D objects watermarks an object and removes part of it, the clam of ownership from the original author will be harder to prove because a substantial copying must occur and removing part of the object will only make it harder. This definition is somewhat different from the protection a patent or the implementation of a trade secret that can be invoked in the case of manufacturing. It can be concluded that watermarking a 3D object by the holder or creator of the original to protect it's intended purpose, which is to provide intellectual copyright but in reality the resulted object ceases to be a replica if the watermarking substantially the quality or form of the copy. In adding a signature to the 3D copy of object instead of subtracting or changing the information of a copy as in the case of watermarking.

VIII. THE PROPOSED SECURITY FRAMEWORK

Constructing a proposed framework for digital signing 3D objects requires us to place the logical semantics of signing methods in the digital domain and the claim of providence in the physical domain. We have to go back to the basics of authentication and digital signing, by examining the metrics and semantics that were used to build the digital signing models that are currently used. In Figure 2 a framework for signing additive manufacturing objects is presented where three attributes (authentication, integrity and non-repudiation) reside within the digital domain, and three attributes (confidentiality, physical integrity and availability) are placed in the physical world.

If the object was created in digital state then it can transition to a physical state via 3D printing and if the object is in physical state it can be digital scanned and becomes a digital object, hence the framework is agnostic. In Figure 2 the signing principles for the digital and physical objects the state of the object determines the signing methodology.

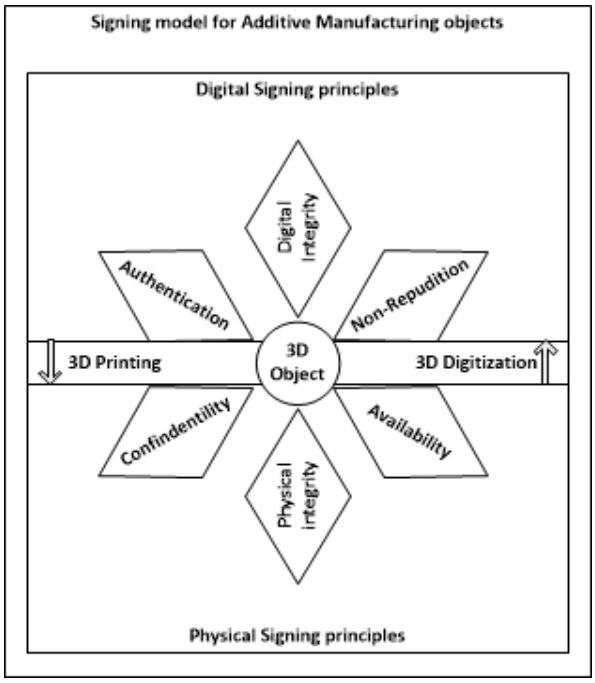

Figure 2 - Framework for Signing Additive Manufacturing objects As a realized 3D design has two states, digital and physical, these are illustrated as two domains, with the 3D object is in the middle.

In summarizing the logic and need for the new signing framework for additive manufacturing objects we need to consider five points:

- According to the definition by NSTISS security system model acknowledges information not technology [18]. BSI standard of 1989 extend to the technology to establish trust outside the OSI model, which by definition can include trusted hardware.
- Digital artifacts have significant applications, For example, as an educational and learning tool in humanities or as a product in the engineering design process [12].
- XML format of the additive manufacturing file format has room for future amendment [19].
- According the draft ISO 52915 x.2.1.6 [19] lists provisions for future copyright protection and water marking but does not mention digital signing.
- Watermarking remove part of the object this process disrupts substantial copying of original artifacts [7].

These five points illustrate valid reasons and technological ability for creating a transitional signing model where the provenance is transferable from digital to physical form.

IX. Digital Identity

There is a general acceptance for the current signing principles and roles followed in the digital and physical domain, implementation of signing principles on additive manufacturing objects or 3D objects will contribute to digital identity using the uniqueness of the signed objects. Using the framework presented in Figure 2 we can establish digital identity by assigning a unique identifier to a data set using the signing data [20]. Currently unique identification numbers are assigned to physical object such as in packaging products, we can produce uniqueness in a 3D printed object by adding to signature to the 3D design rather than removing a part like in the case of watermarking 3D objects where the least significant bit is manipulated to imbed information [2].Our model insures the integrity of a 3D object because we do not remove from the object only add to it.

X. Disscussion and Conclusion

The basis for the design a signing framework that can be applied to a additive manufacturing objects has its roots in digital signature and could be further explored to incorporate semantics of 3D objects used to describe cultural heritage 3D object or printable copies of artifacts. Within the current literature attempts to enforce digital right management invariably discuses the use of watermarking, which has negative implication on the copying process. The use of digital signing introduces uniqueness to the objects, which contributes to the digital identity of additive manufacturing objects. It is our contention that we have established a need for the framework since there is no method of provenance transition between physical and digital objects. In this paper we have demonstrated that both the standard and the technology have the capability of accommodating the new model. We have explained shortcomings in the current state of proving claim of ownership in 3D printed object as also reviewed by Bradshaw [7]. We will continue apply the framework extension to copies of copies; such as scanning a finished additive manufacturing object with its signature in physical form and produce a digital model again. We will also investigate if the signatures on a 3D printed object produced using our model is transferable when captured digitally using scanning methods.

XI. References

[1] I. ISO, "7498: Information Processing Systems, Open Systems Interconnection, Basic Reference Model," *International Standards Organization, Geneva, ...*, 1984.

[2] P. Alface and B. Macq, "From 3D mesh data hiding to 3D shape blind and robust watermarking: a survey," *Transactions on data hiding and multimedia security II*, pp. 91–115, 2007.

[3] C. Neamtu and S. Popescu, "Using reverse engineering in archaeology: ceramic pottery reconstruction," *Journal of Automation ...*, vol. 6, pp. 55–59, 2012.

[4] S. Manacorda and D. Chappell, Eds., *Crime in the Art and Antiquities World*. New York, NY: Springer New York, 2011, pp. 17–48.

[5] H. Maryon, "The Colossus of Rhodes," *The Journal of Hellenic Studies*, 1956.

[6] P. Walters, D. Huson, C. Parraman, and M. Stanić, "3D printing in colour: technical evaluation and creative applications," *Proc. Impact Multidisciplinary ...*, no. September, pp. 1989–2000, 2009.

[7] S. Bradshaw, A. Bowyer, and P. Haufe, "The intellectual property implications of low-cost 3D printing," *ScriptEd*, vol. 7, no. 1, pp. 5–31, Apr. 2010.

[8] R. K. Jr, "Uniform Commercial Code Warranty Provisions and the Theory of Strict Liability in Tort as Solutions to Art Counterfeiting in Painting: A Critical Analysis, The," . *Louis ULJ*, vol. 1, 1975.

[9] D. Davies, "Applying the RSA digital signature to electronic mail," *Computer*, vol. 16, no. 2, pp. 55–62, 1983.

[10] J. Birnholtz, "What does it mean to be an author? The intersection of credit, contribution, and collaboration in science," *... of the American Society for Information Science ...*, vol. 57, no. 13, pp. 1758–1770, 2006.

[11] P. Bantin, "Strategies for managing electronic records: a new archival paradigm? An affirmation of our archival traditions?," *Archival issues*, pp. 1–22, 1998.

[12] H. Denard, "The London Charter for the computer-based visualisation of cultural heritage," no. February, pp. 1–13, 2009.

[13] C. Cullen, P. Hirtle, D. Levy, C. Lynch, and J. Rothenberg, *Authenticity in a Digital Environment.*, no. May. 2000.

[14] J. E. Boritz, "IS practitioners' views on core concepts of information integrity," *International Journal of Accounting Information Systems*, vol. 6, no. 4, pp. 260–279, Dec. 2005.

[15] M. Bishop, *Introduction to computer security*. Addison-Wesley Professional, 2004.

[16] K. Engel and O. Sommer, "Remote 3d visualization using image-streaming techniques," *ISIMADE-11 TH Internationl ...*, 1999.

[17] M. Belanger, "Amazon. com's Orwellian Gaffe: The Legal Implications of Sending E-Books Down the Memory Holy," *Seton Hall L. Rev.*, vol. 1, 2011.

[18] J. McConnell, "National Training Standard for Information Systems Security (INFOSEC) professionals," no. 4011, 1994.

[19] "Draft BS ISO DIS 52915 Additive manufacturing file format (AMF) Version 1.1," vol. 44, no. 0, 2013.

[20] L. Wynholds, "Linking to scientific data: Identity problems of unruly and poorly bounded digital objects," *International Journal of Digital Curation*, vol. 6, no. 1, pp. 214–225, 2011.