Embedding Tracking Codes in Additive Manufactured Parts for Product Authentication

*Fei Chen, Yuxi Luo, Nektarios Georgios Tsoutsos, Michail Maniatakos, Khaled Shahin, and Nikhil Gupta**

Additive manufacturing (AM) process chain relies heavily on cloud resources and software programs. Cybersecurity has become a major concern for such resources. AM produces physical components, which can be compromised for quality by many other means and can be reverse engineered for unauthorized reproduction. This work is focused on taking advantage of layer-by-layer manufacturing process of AM to embed codes inside the components and reading them using image acquisition methods. The example of a widely used QR code format is used, but the same scheme can be used for other formats or alphanumeric strings. The code is segmented in a large number of parts for obfuscation. The results show that segmentation and embedding the code in numerous layers help in eliminating the effect of embedded features on the mechanical properties of the part. Such embedded codes can be used for parts produced by fused filament fabrication, inkjet printing, and selective laser sintering technologies for product authentication and identification of counterfeits. Post processing methods such as heat treatments and hot isostatic pressing may remove or distort these codes; therefore, analysis of AM method and threat level is required to determine if the proposed strategy can be useful for a particular product.

1. Introduction

Additive manufacturing (AM) is one of the fastest growing industries with over 21% market size growth in 2016.[1] AM has already revolutionized design and manufacturing in many fields including aerospace, automotive, and medical by providing greater design freedom for developing highly customized components that could not be manufactured by traditional methods.[2,3] SuperDraco engine chamber by SpaceX, three-dimensional (3D) printed gas turbine blades by Siemens, and 3D printed fuel nozzle for the LEAP jet engine by CFM International are among the examples of AM parts from the aerospace industry that demonstrate tremendous possibilities presented by AM methods.[4–6] Likewise, in the automobile industry, Local Motors' Strati was one of the first 3D printed cars. AM has contributed to customization of individual parts, reducing the assembly cost and eliminating the need to maintain part inventory due to on-demand and on-site manufacturing.[7]

AM is also referred to as digital manufacturing because of a completely digital work flow in the entire process chain until the printing of the part on a 3D printer.[8] A typical AM process chain is illustrated in **Figure 1**, which includes development of a 3D computer aided design (CAD) model of the part geometry. The CAD model is converted to a standard tessellation language (STL) file. Although many file formats, including some specific to AM such as AMF, are available, STL is still the most widely used format. The STL file is reduced to 2D slices, which are converted to the G-code that defines printer head movement and processing conditions such as temperature and speed.

Commercial AM machines are now capable of providing resolution of the order of 10–100 μm. Parts manufactured on such machines are acceptable in many applications without any need for surface finishing.[9] In addition, some of the micro- and nano-fabrication methods such as electron-beam lithography, photolithography, and two-photon polymerization have been promising in making 3D structures with a resolution as low as 30 nm.[10–12] Such high resolution nanoprinting has found applications in tissue engineering, electronics manufacturing, nano-patterning, and drug delivery.[10,13,14] Researchers have investigated adding quantum dots to AM parts for identification of authentic parts.[15] Enabled by high resolution as well as a layer-by-layer building process, parts can be created with artifacts that have complex geometry and unique optical characteristics to serve as a signature.[15] The study showed that printability of the part was not significantly affected by the presence of quantum dots in mass concentrations of 0.5% or lower.[15]

Dr. N. Gupta, F. Chen, Y. Luo
Composite Materials and Mechanics Laboratory
Mechanical and Aerospace Engineering Department
New York University
Tandon School of Engineering
6 MetroTech Center, Brooklyn, NY 11201, USA
E-mail: ngupta@nyu.edu
Dr. N. G. Tsoutsos, Dr. M. Maniatakos, Dr. K. Shahin
Division of Engineering
New York University-Abu Dhabi
Saadiyat Island, United Arab Emirates
The ORCID identification number(s) for the author(s) of this article can be found under https://doi.org/10.1002/adem.201800495.

DOI: 10.1002/adem.201800495

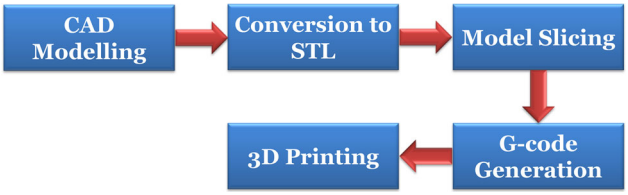

Figure 1. AM workflow from CAD solid model development to the final physical model printing stage.

The digital nature of the process chain brings several challenges that are unique to AM.[16,17] The quality of a part manufactured by traditional methods such as casting and machining is dependent on the skill of personnel involved. In contrast, the digital files are inserted in a 3D printer and the outcome is not dependent on the skill of a person, which is a major advantage for AM methods. However, such simplicity of the manufacturing step presents many security concerns in the AM process chain.[18,19] It is a possibility that stolen CAD files can be used to print a component of exactly the same quality and functionality as the original component.[16] Such unauthorized component will be very difficult to identify in a supply chain. In addition, challenges such as components made from inferior quality materials or from different composition of materials may pass some of the initial quality checks but fail over long usage time need to be addressed by developing new sampling, inspection and testing methods. Examples of supply chain contamination by counterfeit or unauthorized parts are available even from some of the perceived most secure supply chains. The crash of Partnair Flight 394 in 1989 resulted from the installation of counterfeit parts.[5] Counterfeit bolts having inferior strength were found responsible for that crash. Lawrence Livermore National Laboratory in 2001 reported that as much as $2B in unapproved parts were found on the shelves of parts distributors, airline, and repair stations.[6] A US Senate investigation in 2011 found that counterfeit parts were used on C-17 transport airplane, the CH-46 helicopter, and the Army's Theater High-Altitude Area Defense (THAAD) missile defense system.[20,21] These examples illustrate the need for developing robust authentication methods for parts manufactured by AM.

The present work is focused on taking advantage of layer by layer manufacturing method to embed tracking codes inside an AM part. Widely used QR code is taken as the example in this work but the same scheme can be applied to any other tracking code such as a bar code, an alpha-numeric string, or uniquely designed identification marks. It is assumed that the part is not subjected to any post-processing that will distort or eliminate the code such as hot isotatic pressing. An important challenge in embedding a code in a part is that it may compromize the mechanical properties and performance, which is undesired and the developed scheme should not result in such outcomes as the side effects. Such consideration is addressed in the present work.

It should be noted that no security and product authentication approach is applicable to all AM technologies, product geometries, or application conditions. While the proposed scheme can be applied to fused filament fabrication, inkjet printing, and selective laser sintering, among others, the embedded codes can be lost or distorted by post processing steps such as hot isostatic pressing, heat treatment, or plastic deformation. Therefore, carefully selected situations that are amenable to embedding such codes may be selected. It is also noted that one of the main focus areas for future development of AM methods is to build components that do not need any post-process and can be directly put into service. Such possibility increases the likelihood for use of embedded codes.

2. Threat Models and Taxonomy

As 3D printers continue to disrupt traditional manufacturing, a global supply chain emerges: manufacturing moves to a more decentralized model and different steps of the AM process can be implemented by dedicated teams. This globalized model raises new concerns about the integrity of the process, given that the different teams can be located in different parts of the world and may be mutually distrustful. Moreover, since 3D printers use digital design files that can be copied or stolen by malicious entities (such as disgruntled insiders), the risk of unauthorized counterfeits keeps increasing. Likewise, collaborative CAD platforms, which facilitate sharing digital files across teams using cloud computing, are lucrative targets for IP theft and reverse engineering attacks. Nevertheless, in critical applications such as aerospace and automotive, these risks are certainly unacceptable and there is an increasing need to authenticate the origin of high-value 3D printed components.

The applicability of 3D printing attacks has recently been demonstrated in the academic literature. In particular, Yampolskiy et al. have demonstrated a cyber-physical attack to the AM of propellers for unmanned aerial vehicles (drones).[22] The attack entails an adversary that gains unauthorized access to the propeller CAD files and introduces vulnerabilities in the designs in the form of cavities. The unsuspicious user 3D prints the modified propeller and installs it to the drone so that it will fail mid-air due to reduced strength of the blades. Depending on the application, maliciously modified components may cause catastrophic damage to vehicles and cyber-physical systems, monetary loss due to IP theft, as well as damage to the 3D printing equipment.[16]

Detecting counterfeit or maliciously modified 3D printed parts can be very challenging using non-destructive evaluation methods for quality assessment. For example, ultrasonic imaging, X-ray radiography and computational tomography can provide increased confidence regarding the integrity of a 3D printed component, but these techniques are not always suitable for large volume mass production environments due to high cost and time involved. In addition, simple non-destructive tests such as weighing a component are only useful in non-adversarial setting where only random defects are assumed, as an attacker may remove internal material from a critical location and replace it elsewhere to maintain the same weight, without any externally-visible evidence.

Since counterfeiting has the potential to cause an adverse impact to the global economy,[23] the need for sophisticated mitigation methods becomes more urgent. One way to authenticate manufactured components is via security tags that are based on special texture patterns and inks that are embedded under the surface of each part. Likewise, unclonable security tags

can be implemented using 1) advanced optics that create watermarks and holograms, 2) special chemicals that allow tag validation using spectroscopic readers, 3) distinctive material morphology using nanocrystals or metal threads, as well as 4) electromagnetic tags (such as RFIDs) transmitting a unique signature for each part.[24] Of particular interest are passive authentication tags that are based on barcode or quick-response (QR) codes; for example, counterfeit parts can be detected using nanomaterial barcodes,[25] as well as gold nano-particle contrast agents.[26] Beyond security tags, 3D printed parts can also be authenticated by monitoring the integrity of the manufacturing process itself: State-of-the-art methods validate printer head movements using the acoustic signatures,[26–28] as well as power consumption and thermal side-channels.[29]

Nevertheless, one major drawback of the aforementioned authentication methods is their non-negligible impact to the structural integrity of the manufactured object. In addition, since these existing techniques offer limited complexity, they could be bypassed via traditional reverse engineering. Specifically, our threat model assumes globalized adversaries with reverse engineering capabilities and unlimited access to genuine copies of a manufactured part. In many scenarios, the reverse engineered products cannot be detected easily in a process chain and need a method to track and authenticate a part in the supply chain. We further assume that our adversaries are rational and economically motivated to manufacture 3D printed counterfeits of genuine parts; however, we do not consider attacks where the cost of reverse-engineering a genuine part exceeds the expected profit from manufacturing undetectable counterfeit parts. Consistent with our threat model against counterfeiting, our primary objective is to develop a method for embedding unique tags for authenticating genuine parts, without compromising the strength of the part or any other performance parameter.

The following sections describe the process of embedding an identifying tracking code to the original CAD model for authentication security purposes. The hypothesis is that in the presence of these intentionally introduced patterns, the model is now created with unique signature for its identity authentication. Usage of different material selection, layer resolutions, and printing techniques are presented and discussed to evaluate realization of this security approach. Some of the examples presented here are simple geometries for illustrative purposes. However, many industrial component designs are complex and disguising the security features is possible without easy detection.

3. Experimental Section

SolidWorks 2015 is used for solid modeling in this work. The parts are printed using four well-developed 3D printing technologies in: 1) acrylonitrile butadiene styrene (ABS) thermoplastic using an fused deposition modeling (FDM) printer Stratasys Dimension Elite with a water soluble support material SR-10™/P400SR™ acrylic copolymer, 2) VeroClear photopolymer resin using a Stratasys Object30 Pro printer, 3) VeroWhite and VeroBlack photopolymer resins using a Stratasys J750 Polyjet, and 4) AlSi10Mg alloy using a direct metal laser sintering (DMLS) printer. Each of these printers has different resolution and capability as given in **Table 1**. The codes will be 3D printed to determine the QR code line width that can be scanned using a QR code reader.

Table 1. Specifications for 3D printers used in this study and QR code 3D printing results.

	Minimum layer thickness [mm]	Material used	Smallest QR code printed [mm^2]
FDM (Stratasys Dimension Elite)	0.178	ABS filament	42×42
PolyJet (Stratasys Objet30 Pro)	0.016	VeroClear resin	4.54×4.54
PolyJet (Stratasys J750)	0.014	VeroWhite, VeroBlack resins	3.8×3.8
DMLS (EOS M270)	0.020	AlSi10Mg powder	7.7×7.7

CatalystEX slicing software is used for toolpath generation and encoder file preparation. The "solid" model interior is chosen for all models processed in CatalystEX in this work. Further, a micro-computed tomography (micro-CT) scanner (SkyScan 1171, Bruker) is used to scan the printed objects.

4. Results and Discussion

The two-dimensional QR code encodes data in a surface pattern, which can be assessed by capturing the image with a camera and processing with a QR code reader. Here, a 2D static QR code is generated as shown in **Figure 2** as an example of identifying code while the transition into adapting the dynamic QR code is implementable. Compared to static QR code that refers to a fixed permanent address, dynamic QR code allows users to change the address and automatically redirects to newer content. Different schemes of embedding the QR code in a solid model are presented and mechanically tested to validate its manufacturability and security functions.

4.1. 3D Printing of the QR Code

For FDM 3D printing, the CAD models are prepared with QR code extruded on top of a rectangular plate for preliminary study

Figure 2. An example of a static QR code (the code points to the website link http://engineering.nyu.edu/composites/).

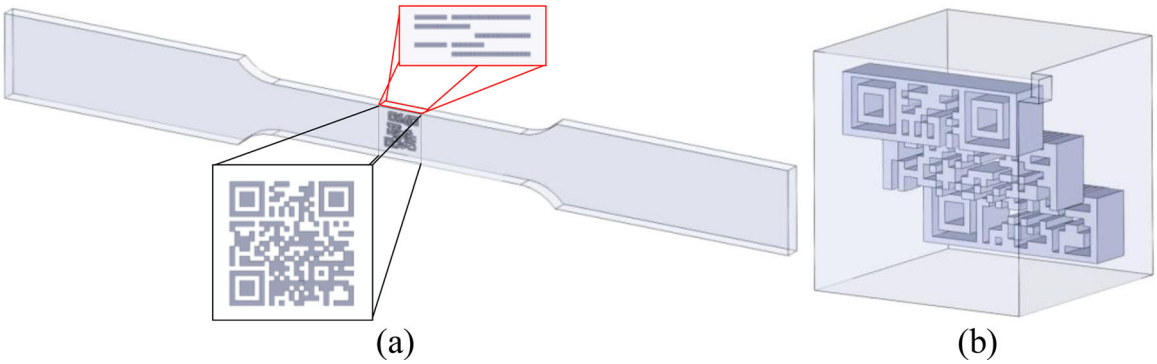

Figure 3. a) A QR code is segmented in 5 parts and embedded at different depths in a tensile test specimen. Insets show two orghogonal views of the code in the specimen. Only the front view shows a complete scannable code (the complete QR code dimensions are $7.7 \times 7.7\ mm^2$, and the thickness is 0.2 mm). b) A QR code is segmented in three parts and embedded at different depths in a solid cube ($10 \times 10 \times 10\ mm^3$). The QR code length and width are 7.7 mm each and the thickness is 2 mm.

or readability of 3D printed codes. All other techniques use CAD model prepared with QR code embedded inside a solid cube. Resin printed parts and metallic parts have finer resolution as listed in Table 1 and show better promise of miniaturization.

4.2. Embedding the Segmented QR Code in Different Layers

Figure 3a shows an example of a QR code embedded in a standard tensile test specimen. The front view of the specimen shows the complete code that can be scanned but other views show that the code is actually broken in 5 parts and each part is embedded at a different depth in the specimen. It can be visualized in Figure 3a that imaging this code from any other angle except for the front side will not provide a scannable code. This is important because industrial components are often complex in shape and unsuspecting people may not be able to easily figure out the correct orientation to image an embedded code. The tensile test specimens designed with and without embedded codes are printed and mechanically tested to determine the effect of the presence of these codes on the tensile strength and modulus of the specimen. A second simplified model is created to study the segmentation scheme and the miniaturization limit, where a 2D QR code is segmented into 3 sections and embedded at different depths for 3D printing within the same solid cube as shown in Figure 3b.

4.3. Scanning and Reading QR Code

A program is written to automate the process of code digitization and reading based on contrast between the featured and non-featured space in the code. The program first improves the image contrast and discriminates noise to facilitate the QR code reading process, and then compares the processed micro-CT image of 3D printed QR code to the original QR code image. The comparison between the original and scanned code provides the authentication information.

4.3.1. Scanning

A micro-CT scanner is used to image and reconstruct the embedded codes. A 3D printed resin specimen with QR code area $3.8 \times 3.8 \times 0.5\ mm^3$ is shown in **Figure 4**a with preliminary micro-CT results in Figure 4b. For the human eye, this scanned code seems well resolved but it cannot be scanned directly from the QR code reader due to poor resolution in areas where lines are closely spaced. The overlay of original code to determine deviation from that image is a promising scheme to determine the genuineness of codes and will be discussed in later sections.

To validate the segmentation scheme as discussed earlier, an embedded QR code (3-layer) block is 3D printed, as shown in **Figure 5**a. After micro-CT data acquisition and image reconstruction, two slices of the embedded code are shown in Figure 5b and c, where the image contrast is relatively low. This is

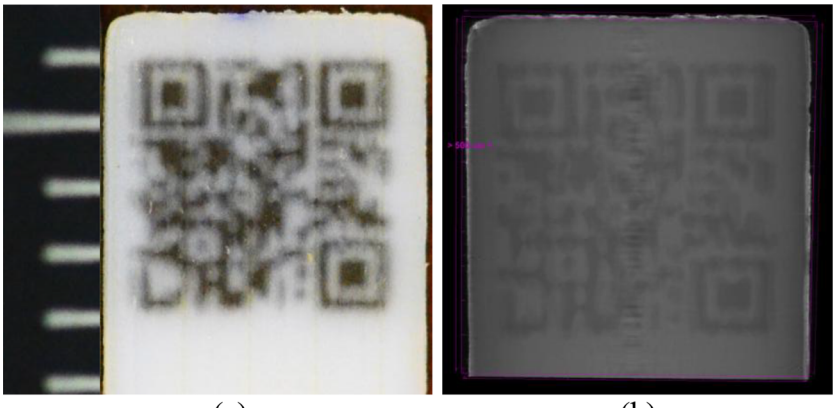

Figure 4. a) A 3D printed resin (VeroWhite and VeroBlack) QR (1-layer) code part ($3.8 \times 3.8\ mm^2$, thickness 0.5 mm) and b) cross-sectional micro-CT image after reconstruction.

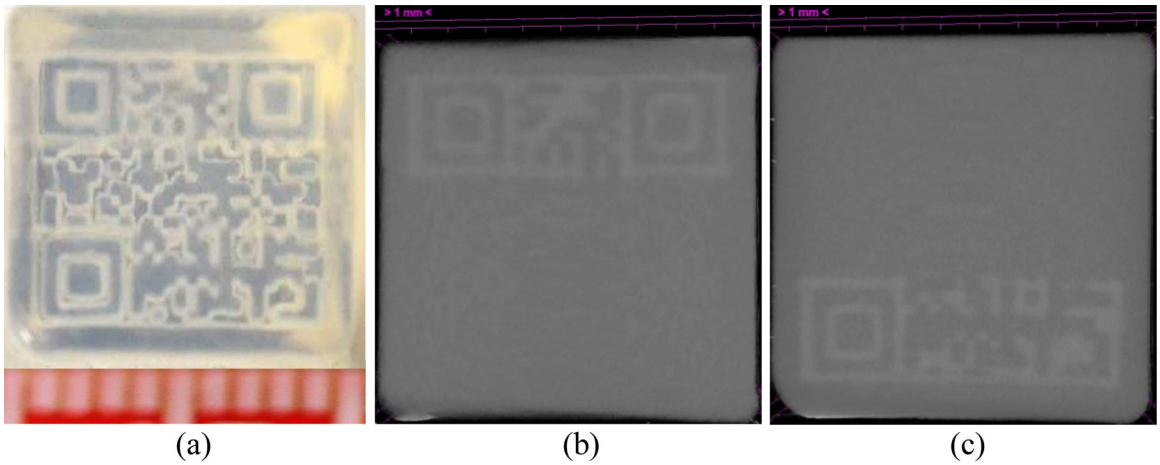

Figure 5. a) A 3D printed resin (VeroClear) cube ($10 \times 10 \times 10\,mm^3$) with embedded QR (3-layer) code part ($7.7 \times 7.7\,mm^2$) and b) and c) are cross-sectional micro-CT images of two layers of code after reconstruction.

due to the small density difference between the cured VeroClear photosensitive polymer and its support material SUP706, which is also in the photopolymer family. This effect is minimized when printing with metallic material due to the larger density difference between the metallic model material and air present in the unsintered QR code areas, as shown in **Figure 6**. The distinct outline observed in metallic codes results in greater accuracy in image processing results. The images obtained from various model depths are knitted together to produce the complete QR code image.

4.3.2. Image Processing and Discrepancy Calculation

Representative micro-CT images in Figure 6 are combined into one image using Adobe Photoshop CS6 and further subjected to the image processing flow, as shown in **Figure 7**.

Original combined micro-CT image is in low contrast with small range of grayscale values in the intensity histogram. This is improved by applying the contrast limited adaptive histogram equalization (CLAHE) algorithm in OpenCV Python library to provide a more balanced and equalized histogram, preserve enough image details, and avoid over-exposure during the image processing. The Otsu's method[30] is applied to choose the optimal threshold value with minimum variance over the entire grayscale histogram from 0 to 255. The selected optimal threshold value is automatically applied to the original combined micro-CT image to return the binary image. This QR code binary image is compared to the original QR code pattern, that is, first gridded into many small tiles, within which the average of grayscale value for every pixel is calculated. The tile is converted to entire white color if the average grayscale value is larger than 50% and black color if smaller than or equal to 50%. Here, the grid size plays an important role to determine the proper use and comparison between the processed image and original QR image. Therefore, discrepancy is calculated for grid sizes from 1 to 24 which return the optimal grid size with minimum discrepancy 0.2028 to be 12. To better facilitate the identification process, these discrepancy areas between the standard QR code and processed gridded image are highlighted in colors. Green areas represent discrepancy between originally white but processed to be black areas, while the blue areas indicate

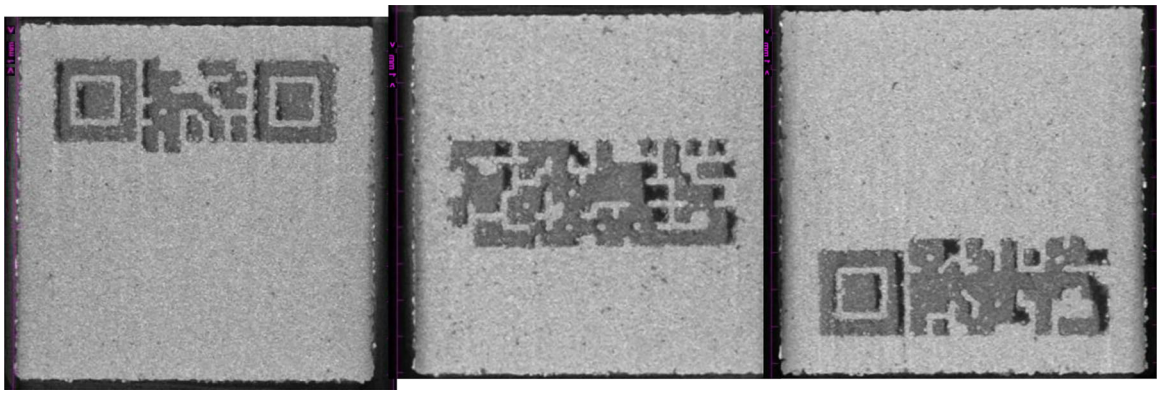

Figure 6. Cross-sectional micro-CT images of a 3D printed metal (AlSi10Mg) cube ($10 \times 10 \times 10\,mm^3$) with embedded QR (3-layer) code part ($7.7 \times 7.7\,mm^2$).

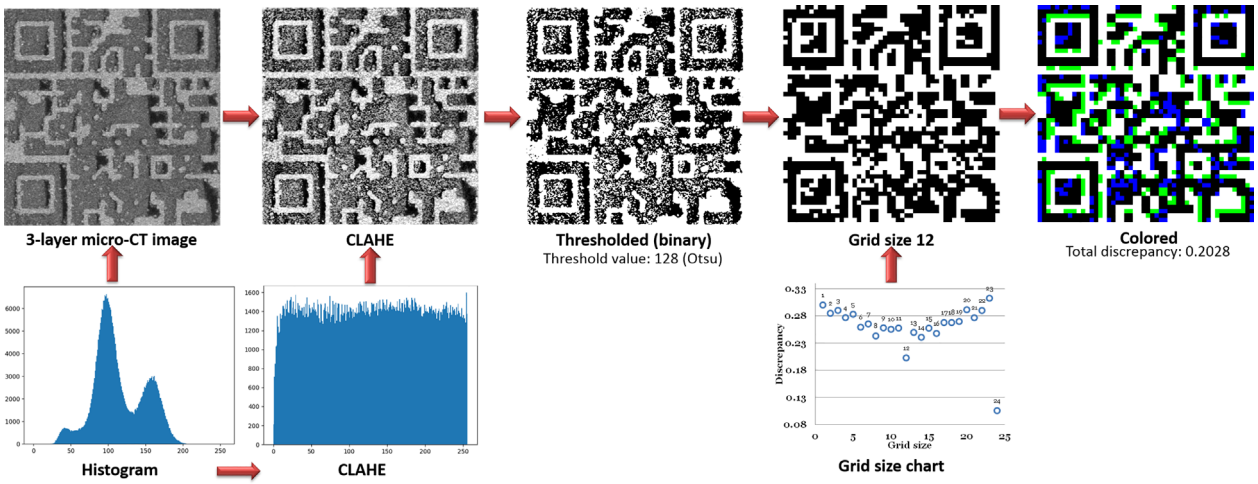

Figure 7. Image processing flow chart and results.

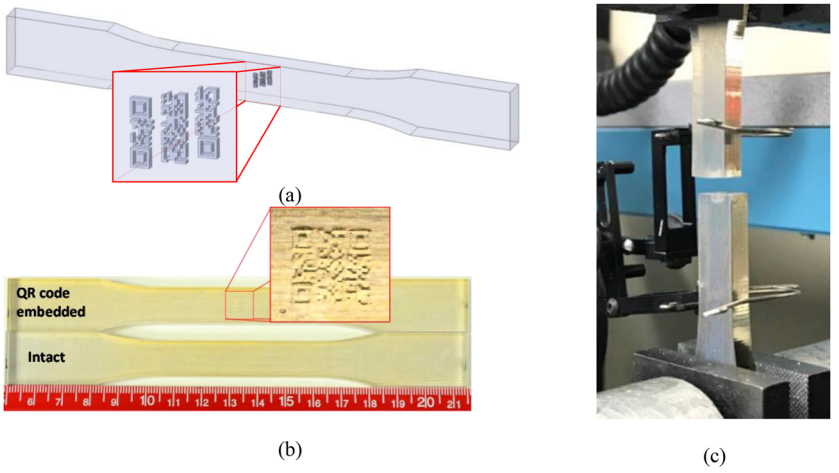

Figure 8. a) ASTM D638 type I tensile bar with three segmented QR codes embedded at different depths CAD model. (QR code dimensions 4.5 × 4.5 mm^2, each segment is 0.5 mm in thickness). b) 3D printed resin (VeroClear) tensile bars with and without embedded QR code, and c) the specimen with embedded QR code subjected to tensile testing.

originally black areas, as on the standard QR code image. Many other image processing algorithms are available in the literature that can be used for image enhancement for improved scanning using standard QR code readers. It is also noted that the embedded codes may be of other formats, including alpha-numeric strings, which can be processed in a similar manner.

4.4. Mechanical Testing of Specimens with Embedded Codes

Adopting the segmentation details shown in Figure 5a, the 3-layer QR code is embedded at different depths in a standard tensile bar CAD model as shown in **Figure 8**a. The tensile bars with embedded codes are printed using VeroClear photopolymer resin as shown in Figure 8b.[31] Coupons without embedded codes are also printed and tested to obtain baseline properties. Standard tensile tests are performed on all tensile bars at the strain rate $1.67 \times 10^{-3}\,s^{-1}$ in accordance with ASTM D638 using the Instron 4469 test system with 30 kN load cell. The specimens fracture within the gauge length, as shown in Figure 8c. As summarized in **Table 2**, the averaged ultimate tensile strength and modulus show around 2% and 0.4% difference, respectively, between the intact bars and QR code embedded bars. Such difference is insignificant because it is within the standard deviation range. The measured weight of the specimens with and without QR code is close to each other with only 0.05% difference. These results indicate that embedding identifying codes to a CAD model can serve as an authentication signature to the final product without compromising product quality. Further work on code miniaturization and multi-segmentation can be used to enhance structural integrity and facilitate the use of these security codes.

There are limitations of different methods such as SLM, FDM and SLA, for example, porosity present in SLM specimens or directionality in the FDM specimens, are expected to interfere with the QR code and also with the experimental results.

Table 2. Properties for 3D printed resin (VeroClear) standard tensile bars.

	Intact bars	QR code embedded bars
Ultimate tensile strength (MPa)	57.07 ± 0.44	55.92 ± 0.98
Modulus (GPa)	2.57 ± 0.12	2.56 ± 0.11
Weight (grams)	21.80 ± 0.02	21.79 ± 0.02

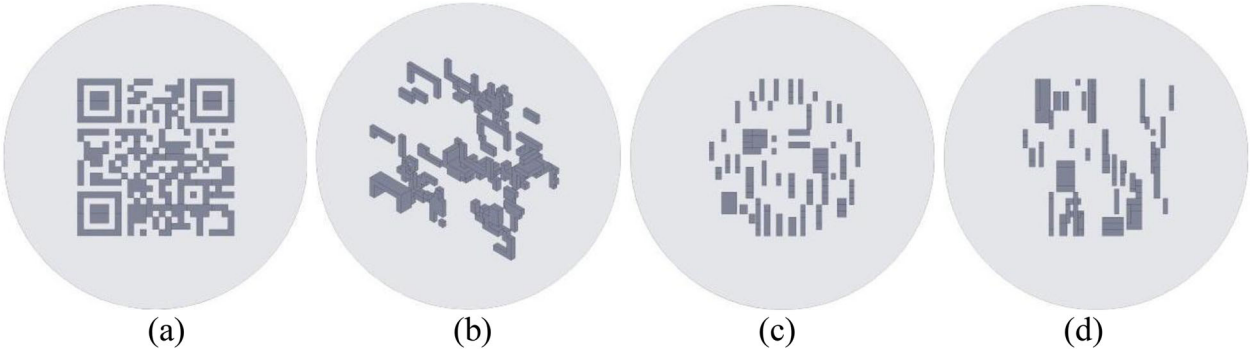

Figure 9. QR code divided into 44 segments and embedded at multiple locations shown in a) complete code, b) isometric view of the code, c), and d) two orghogonal views of the code (Sphere diameter 10 mm, QR code dimensions $5.15 \times 5.15\ mm^2$, varying thickness from 0.15 to 0.7 mm for each segment).

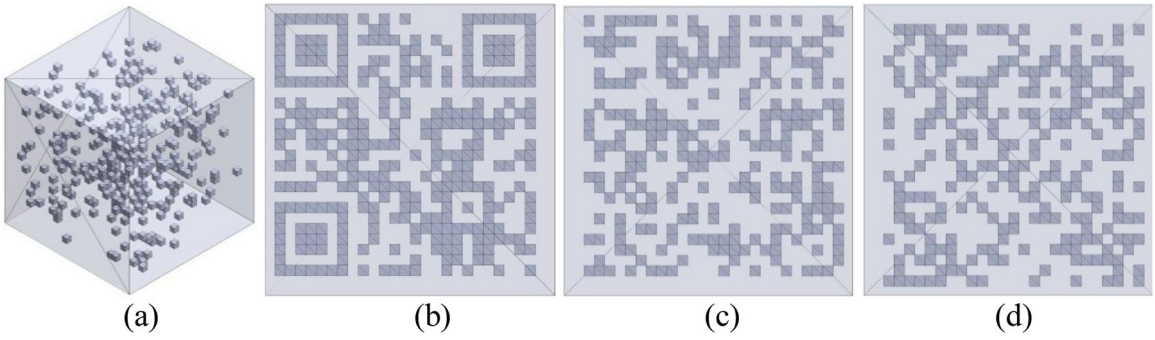

Figure 10. CAD of a cube with embedded QR code segmented into 320 small cubes in a) isometric view. b–d) show three views normal to each other. Only b) will give the correct reading orientation (large cube is $10 \times 10 \times 10\ mm^3$ and 320 small cubes are $0.36 \times 0.36 \times 0.36\ mm^3$ each).

However, testing multiple specimens and conducting non-destructive imaging will help in reducing the uncertainty in the reading of code.

4.5. Code Obfuscation

To increase the complexity of visualization against external attackers, the tracking code segmentation is not limited to the five layers example but can be further divided into numerous segments and embedded at different depths and locations. The example given in **Figure 9** shows a QR code segmented into 44 sections and embedded at different depths. When the code is spread out in an enclosed volume such as a sphere, it is more challenging to recognize a single correct orientation for viewing the code. Another possible variant of code obfuscation is presented in **Figure 10**, where the code is segmented in 320 parts and each part has enough thickness to develop an image (not the correct QR code) from multiple sides. It can be observed that by slightly varying the viewing angle, the resulting code pattern looks different from the correct code, making it challenging to figure out the encoded information. Advancements in the printing technologies to provide finer print resolution will make it possible to further miniaturize the codes and obfuscate them in the parts to enable identification of authentic parts.

5. Conclusions

The digital manufacturing chain of additive manufacturing (AM) presents many challenges for security of digital files and makes it easier to produce unauthorized parts. This work demonstrates the possibility of embedding identification codes inside 3D printed parts without compromising the mechanical properties of parts. The codes are segmented into a number of fractions, which minimizes their effect on mechanical properties as well as helps in obfuscation. The codes can be read correctly only from a specific viewing orientation. The scheme of embedding codes can be implemented in combination of carefully selected segmentation parameters and layer thickness to develop a more restrictive set of parameters that will result in the embedded code. Like any security and authentication method, the approach of embedded codes is not suitable for all AM products. Factors such as post-processing methods, build material, AM technology and usage environment should be considered while deciding about using this approach. As the AM technologies develop further to the level where as-fabricated components are directly put into service without the need for any post-processing operations, use of such methods will become easier. Such schemes can be implemented at the design level and can be used in addition to traditional cybersecurity methods such as network protection, encryption of files, and access control.

Acknowledgements

NYU Global Seed Grant for Collaborative Research to Drs. Nikhil Gupta and Khaled Shahin is acknowledged. Parts of this work are supported by the Office of Naval Research grant N00014-10-1-0988. Steven E. Zeltmann is thanked for useful technical discussions. The views and conclusions contained in this work are those of the authors and should not be interpreted as presenting the official policies or position, either expressed or implied, of the ONR or the U.S. Government unless so designated by other authorized documents.

Conflict of Interest

The authors declare no conflict of interest.

Keywords

additive manufacturing, computer aided design, product authentication, security, 3D printing

Received: May 7, 2018
Revised: May 26, 2018
Published online: July 10, 2018

[1] T. T. Wohlers, *Wohlers Report 2016: 3D Printing and Additive Manufacturing State of the Industry*, Wohlers Associates, Fort Collins, Colorado, USA **2016**.
[2] J. P. Kruth, M. C. Leu, T. Nakagawa, *CIRP Ann*. **1998**, *47*, 525.
[3] A. L. Jardini, M. A. Larosa, R. M. Filho, C. A. D. C. Zavaglia, L. F. Bernardes, C. S. Lambert, D. R. Calderoni, P. Kharmandayan, *J. Cranio-Maxillof Surg*. **2014**, *42*, 1877.
[4] M. Molitch-Hou, First jet engines with 3d-printed nozzles delivered to Airbus, https://www.engineering.com/AdvancedManufacturing/ArticleID/11948/First-Jet-Engines-with-3D-Printed-Nozzles-Delivered-to-Airbus.aspx, (accessed March 9th **2018**).
[5] SpaceX News launches 3d-printed part to space, creates printed engine chamber, http://www.spacex.com/news/2014/07/31/spacex-launches-3d-printed-part-space-creates-printed-engine-chamber-crewed, (accessed March 9, **2018**).
[6] M. Siebert, Breakthrough with 3d printed gas turbine blades, https://www.siemens.com/innovation/en/home/pictures-of-the-future/industry-and-automation/additive-manufacturing-3d-printed-gas-turbine-blades.html, (accessed March 9th, **2018)**.
[7] E. Atzeni, A. Salmi, *Int. J. Adv. Manuf. Technol*. **2012**, *62*, 1147.
[8] L. Yang, K. Hsu, B. Baughman, D. Godfrey, F. Medina, M. Menon and S. Wiener, in *Additive Manufacturing of Metals: The Technology, Materials, Design and Production*, Springer Series in Advanced Manufacturing, Springer, Cham **2017**, p. 33.
[9] M. Vaezi, H. Seitz, S. Yang, *Int. J. Adv. Manuf. Technol*. **2013**, *67*, 1721.
[10] M. Mao, J. He, X. Li, B. Zhang, Q. Lei, Y. Liu, D. Li, *Micromachines* **2017**, *8*, 113.
[11] B. H. Cumpston, S. P. Ananthavel, S. Barlow, D. L. Dyer, *Nature* **1999**, *398*, 51.
[12] F. P. W. Melchels, M. A. N. Domingos, T. J. Klein, J. Malda, P. J. Bartolo, D. W. Hutmacher, *Prog. Polym. Sci*. **2012**, *37*, 1079.
[13] J. W. Lee, *J. Nanomater*. **2015**, *2015*, 4.
[14] C. Ru, J. Luo, S. Xie, Y. Sun, *J. Micromech. Microeng*. **2014**, *24*, 053001.
[15] A. Elliott, O. Ivanova, C. Williams, T. Campbell, *An investigation of the effects of quantum dot nanoparticles on photopolymer resin for use in polyjet direct 3D printing. in Proceedings of the 2012 Solid Freeform Fabrication Symposium*. August 6-8, **2012**. Austin, Texas. The PDF can be access at http://sffsymposium.engr.utexas.edu/Manuscripts/2012/2012-75-Elliott.pdf, through http://sffsymposium.engr.utexas.edu/2012TOC
[16] F. Chen, G. Mac, N. Gupta, *Mater. Des*. **2017**, *128*, 182.
[17] W. Gao, Y. Zhang, D. Ramanujan, K. Ramani, Y. Chen, C. B. Williams, C. C. L. Wang, Y. C. Shin, S. Zhang, P. D. Zavattieri, *Comput.-Aid. Des*. **2015**, *69*, 65.
[18] M. Yampolskiy, W. E. King, J. Gatlin, S. Belikovetsky, A. Brown, A. Skjellum, Y. Elovici, *Addit. Manuf*. **2018**, *21*, 431. DOI: https://doi.org/10.1016/j.addma.2018.03.015.
[19] S. E. Zeltmann, N. Gupta, N. G. Tsoutsos, M. Maniatakos, J. Rajendran, R. Karri, *JOM* **2016**, *68*, 1872.
[20] Lawmakers: Counterfeit electronics flood Pentagon supply, https://usatoday30.usatoday.com/news/washington/story/2011-11-07/pentagon-counterfeit-electronics/51112630/1?csp=34news), (accessed July 3rd, 2018).
[21] Agence France-Presse, Chinese fake parts 'flood' us military: Report, http://www.military.com/daily-news/2012/05/22/chinese-fake-parts-flood-us-military-report.html), (accessed July 3rd, 2018)
[22] S. Belikovetsky, M. Yampolskiy, J. Toh, J. Gatlin, Y. Elovici, presented in *part at the 11th USENIX Workshop on Offensive Technologies (WOOT 17)*, Vancouver, BC, Canada, August 14–15, **2017**.
[23] A. F. Smith, S. E. Skrabalak, *J. Mater. Chem. C*. **2017**, *5*, 3207.
[24] J. Gooch, B. Daniel, V. Abbate, N. Frascione, *Trends Anal. Chem*. **2016**, *83*, 49.
[25] M. Wang, B. Duong, H. Fenniri, M. Su, *Nanoscale* **2015**, *7*, 11240.
[26] C. Bayens, T. Le, L. Garcia, R. Beyah, M. Javanmard, S. Zonouz, presented in *part at the Proceedings of the 26th USENIX Security Symposium*, Vancouver, BC, Canada, August 16–*18*, **2017**.
[27] M. A. Al Faruque, S. R. Chhetri, A. Canedo, J. Wan, presented in *part at the Proceedings of the 7th International Conference on Cyber-Physical Systems*, IEEE Press Piscataway, NJ, USA **2016**.
[28] S. R. Chhetri, A. Canedo, M. A. Al Faruque, presented in *part at the Proceedings of the 35th International Conference on Computer-Aided Design*, ACM, New York, NY, USA **2016**.
[29] S. R. Chhetri, S. Faezi, A. Canedo, M. A. Al Faruque, presented in *part at the Proceedings of the 7th International Conference on Cyber-Physical Systems*, IEEE Press Piscataway, NJ, USA **2016**.
[30] N. Otsu, *IEEE Trans. Syst. Man Cybernet*. **1979**, *9*, 62.
[31] ASTM International, in ISO/ASTM52921-13, Standard Terminology for Additive Manufacturing - Coordinate Systems and Test Methodologies, ISO/ASTM International, West Conshohocken, PA **2013**.

