Securing Cyber-Physical Additive Manufacturing Systems by *In-situ* Process Authentication using Streamline Video Analysis

Abdullah Al Mamun[a], Chenang Liu[b], Chen Kan[c], and Wenmeng Tian[a,1,2]

[a]*Department of Industrial & Systems Engineering, Mississippi State University, Mississippi State, MS, USA*

[b]*The School of Industrial Engineering & Management, Oklahoma State University, Stillwater, OK, USA*

[c]*Department of Industrial, Manufacturing, & Systems Engineering, The University of Texas at Arlington, Arlington, TX, USA*

Abstract

In cyber-physical systems (CPS) of additive manufacturing (AM), cyber-attacks may significantly alter the design of the AM part, compromising its mechanical properties and functionalities. *In-situ* process authentication may assure that the AM part is fabricated as intended. Most cyber-physical attacks towards AM processes can be manifested as printing path alterations, and an *in-situ* optical imaging system can detect alteration in printing path. This will prevent catastrophic geometric changes and mechanical property compromises in the AM parts, ultimately improving the AM process security. In this paper, a novel process authentication methodology is proposed based on image texture analysis of the layer-wise *in-situ* videos. The layer-wise distribution of the segmented textures' geometric features is characterized as the layer-wise texture descriptor tensor (LTDT). Given the high dimensionality and sparsity of the extracted LTDTs, the multilinear principal component analysis (MPCA) algorithm is used for dimension reduction. Subsequently, the Hotelling T^2 control charting technique is adopted for alteration detection based on the

[1] Corresponding author. tel.: +1-662-325-7625; fax: +1-662-325-7618.
E-*mail address:* tian@ise.msstate.edu

[2] This manuscript is an extended work of the previous conference paper entitled "Real-time Process Authentication for Additive Manufacturing Processes based on *In-situ* Video Analysis", published in Procedia Manufacturing (DOI: https://doi.org/10.1016/j.promfg.2021.06.068).

extracted low-dimensional layer-wise features. Case studies based on a fused filament fabrication (FFF) process were conducted to evaluate and validate the proposed framework. The proposed method can achieve over 95% of accuracy, which illustrates that the proposed method can accurately detect process alterations due to printing path changes. In addition, the proposed method significantly outperforms the benchmark method. The computation time for both the proposed and benchmark method is also compared.

Keywords: Additive manufacturing; cyber-physical security; image processing; process authentication; texture analysis; tensor decomposition; video-based monitoring

1 Introduction

1.1 Motivation and challenges

The increased interconnectedness in the cyber-physical systems (CPS) has greatly enhanced the automation and productivity for modern manufacturing systems [1], in which cyber-physical security is of utmost importance for both quality and safety assurance. Malicious attacks can significantly affect a manufacturing system, altering machine parameters and product design, ultimately resulting in compromised products [2]. For example, the cyber-physical attack in the German steel mill in 2014 resulted in loss of control for the regulation of crucial parameters, leading to a massive blast of a furnace and even deaths of two workers [3]. Such catastrophic incidences of cyber-physical attacks show an urgent need in protecting manufacturing systems, identifying cyber threats, and detecting cyber-physical attacks as soon as they occur. In the area of additive manufacturing (AM), the CPS provides unique opportunities for cost-effective production planning and control and enables new methods of collaboration [4], [5], where all the AM machines can be operated and controlled remotely without human operator intervention [4]. The digital threads not only facilitate effective digital file sharing for design iteration, but also create significant risks of malicious cyber-physical attacks, which are considered as a growing concern in AM systems. Malicious alterations in the design files and process parameters could significantly affect final part's geometry, structural stability, mechanical performance, and functionality. What's worse, the layer-by-layer fashion of

the AM processes dramatically expands the victim space for potential alteration, leading to significantly changed structural compromises which are very challenging to detect [6]. For example, internal structure changes, such as infill percentage, infill pattern, and unintended void addition, cannot be easily detected in the traditional Geometric Dimensioning and Tolerancing (GD&T) framework unless X-ray inspection is used, which is costly and very time-consuming [7].

The AM process in a typical CPS is comprised of design (i.e., CAD design and STL file generation), slicing (i.e., G-codes generation), manufacturing (i.e., AM fabrication), and inspection [4], [6]. Figure 1 illustrates the major steps of AM processes in a typical CPS, with ***red*** arrows illustrating the data/information transfer and ***green*** arrows showing the material flow. In general, cyber-physical attacks may target on all the phases which involve data or information transfer, and typical attacks include inserting additional undesirable features in the original CAD design [8], altering slicing parameters in generating the g-code [9], and injecting fake process data to mislead quality control decision making [10]. It is worth noting that most of the above-mentioned process alterations which involve AM process changes can be manifested by the change in the printing path of the AM processes. For instance, adding undesirable features lead to interruptions in the printing path, and altering slicing parameters (such as layer thickness and extrusion width) changes the geometry of the printing path.

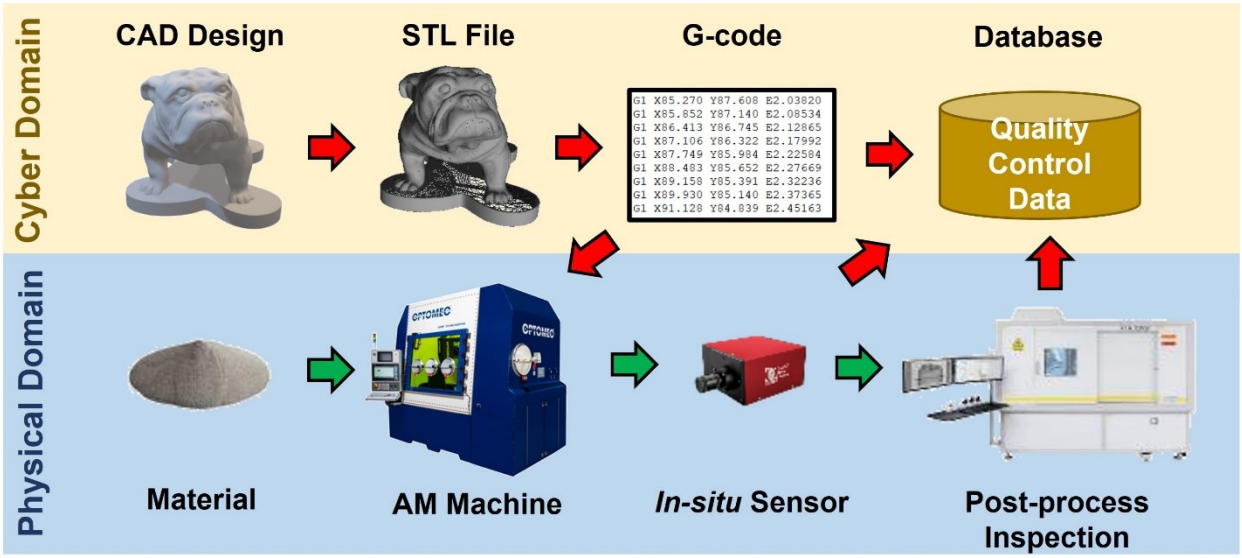

Figure 1: Material and information flow in the CPS of AM

Various types of sensors, including thermal couples, infrared (IR) imaging, accelerometers, microphones, power meters, can be potentially used to detect printing path alteration in AM processes [6], [11]–[13]. However, the anomaly detection results are generally difficult to interpret since those process variables are indirect measures of printing path changes. In addition, *in-situ* AM process authentication can be facilitated through optical imaging during the AM build. For example, in Figure 2, the images in the top row provide the slicing results of a square-shaped cross-sectional layer using different infill orientation angles, and the images in the bottom row illustrate their corresponding distribution of the texture orientation angles. It is observed that the layer-wise texture geometric feature distribution is largely determined by the printing path of the layer, and thus can be used as an informative and interpretable feature to detect printing path alteration. It is also noteworthy that the *in-situ* optical imaging can be used for process authentication for most AM processes as long as the AM printing path plays a critical role in the structural properties of the completed part [14], with a few exceptions including stereolithography and laminated-object manufacturing processes.

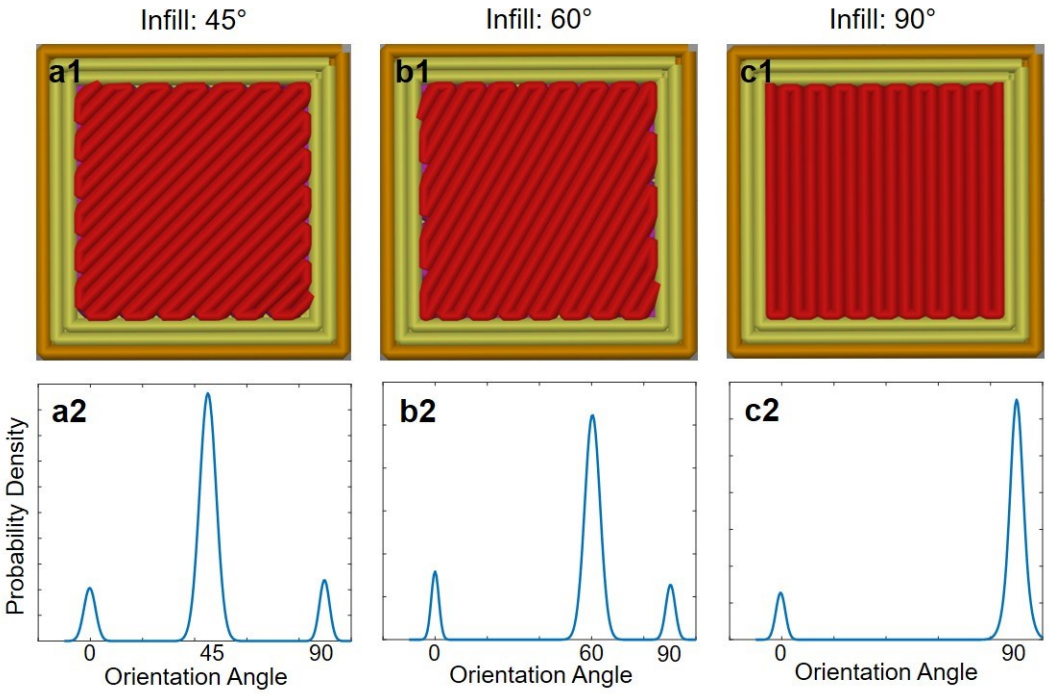

Figure 2: Different geometric feature distributions due to printing path alterations.

The texture of each layer can be observed by an optical camera which captures streamline videos during

the printing process. The advantages of the optical cameras include their cost-effectiveness and enhanced interpretability compared to other sensing technologies (such as acoustic emission and acceleration) [15], [16]. However, capturing a layer-wise image after fabricating each layer like the ones in the first row of Figure 2 may introduce significant interruptions in the fabrication, resulting in extended printing time. In addition, capturing a top-view image after the fabrication of every layer requires a careful trade-off between the field of view and the spatial resolution of the image. For parts that have layers with significantly different dimensions, the focus and magnification of the camera need to be adjusted multiple times during one build. This not only further complicates the data collection process, but also is prone to additional human errors. On the contrary, layer-wise real-time video captures detailed information with the unified imaging and focus conditions for the microscope camera, which extends opportunities for process authentication of highly diversified part designs [17].

Therefore, an optical microscope attached to the extruder of the 3D printer can be used as an alternative solution to continuously capture streamline videos without process interruptions [18]. Nevertheless, there are several challenges in information extraction from the streamline videos captured by the optical camera. First, the streamline video data are highly noisy since a large portion of the pixels demonstrate low resolution due to the inevitable vibration of the microscope attached to the extruder during the printing process. Secondly, the field of view (FoV) of the camera is changing since the camera is attached to the moving extruder, resulting in unstable lighting conditions, and thus varying image contrast over time and space due to dynamic light conditions. Third, the streamline videos are in high dimension and large volume [17]. In summary, the *in-situ* streamline video data are high-volume but low-quality. Therefore, how to extract low-dimensional informative layer-wise features from the streamline video with low signal-to-noise ratio (SNR) is an open challenge for effective AM process authentication.

1.2 Technical contributions of this paper

In this paper, a new AM process authentication method is proposed to extract critical features from the high-volume, low-quality streamline videos collected from the camera attached to the printing head. The overall framework of the proposed methodology has three major phases: 1) Image-level texture feature

extraction, which applies adaptive image filtering to retain the segmented regions (SRs) that demonstrate high contrast and are relevant to the printing path; 2) Layer-wise feature extraction based on the geometric feature distribution of SRs, which constructs the layer-wise texture descriptor tensor (LTDT) to characterize the layer-wise texture distribution; and 3) Dimension reduction for the LTDTs based on multilinear principal component analysis (MPCA) [17], which extracts low-dimensional features from the LTDTs to develop a Hotelling T^2 control chart for alteration detection. The effectiveness of the proposed method is evaluated by comparing with the benchmark method, which leverages the gray-level cooccurrence matrix (GLCM) to extract multivariate textural features [18] and the autoencoder technique to compress the high dimensional features.

The rest of the paper is organized as follows. The relevant research is reviewed, and the research gaps are summarized in Section 2. Section 3 introduces the proposed methodology in detail. A case study based on the fused filament fabrication (FFF) process is demonstrated and the effectiveness of the proposed method is validated in Section 4. The conclusion and future work are summarized in Section 5.

2 Literature review

To achieve AM process authentication, traditional quality control methodologies can be leveraged, including post-process quality inspection and *in-situ* process monitoring, which are summarized in Section 2.1. Moreover, the state-of-the-art studies on AM process security are summarized in Section 2.2.

2.1 Relevant quality assurance methods for authentication

The quality assurance methods for AM processes can be briefly categorized as post-process quality inspection (section 2.1.1) and *in-situ* monitoring and anomaly detection (section 2.1.2).

2.1.1 Post-process quality inspection

In general, AM post-process quality inspection methods fall into two major categories: destructive and non-destructive testing (NDT) techniques. In the destructive methods, AM built parts are destroyed during either testing or sample preparation for material qualification. The most widely practiced destructive testing of AM fabricated parts includes tensile strengths (i.e., Young's modulus, yield strength, ultimate tensile strength, and elongation), ductility test, and fatigue cycle performance [19]. In addition, material

qualification/certification methods can be applied to evaluate the material properties (i.e., morphology, crystallography, and crack growth) of the AM parts [19], [20].

NDT techniques include visual inspection, eddy current and electromagnetic testing, liquid penetrant testing, ultrasonic testing, and X-ray radiography and computed tomography (CT) [20]–[24]. The advanced visual inspection techniques use optical metrological techniques in the geometry assessment of AM final parts [25], [26]. Moreover, the eddy current and electromagnetic techniques involve in detecting changes in dielectric and electronic properties of electrically conductive materials, and is therefore useful for detecting variations in capacitance due to presence of crack, porosity, and associated defects in AM-built parts [24], [27]. Regarding material characterization and inspection, ultrasonic techniques are widely used for the purpose of material testing and evaluation [23]. In addition, piezoelectric impedance-based measurements can be used as another NDE of AM part's dimensional alterations, positional changes, and internal porosity [28], [29]. With its higher resolution and accuracy compared to the forementioned NDT methods, X-ray Computed tomography (CT) is regarded as one of the most reliable part certification methods, especially used in internal structure certification (i.e., porosity, crack growth, etc.) [7][30]. However, several practical challenges will limit the broader application of the X-ray CT techniques in AM part authentication. Firstly, the size of the X-ray CT machine chamber enforces a strict constraint in the dimension of the inspected parts. Therefore, it becomes infeasible to assess large-scale AM parts [28]. Secondly, X-ray CT scanning is a time-consuming procedure and the equipment is also rather costly that limits its broad industrial applications [7]. Thirdly, as a post-manufacturing quality inspection method, the X-ray CT scans only detect the alteration after the entire part is completely fabricated, which will significantly extend the lead time for AM part delivery once there is a part alteration detected.

2.1.2 *In-situ* monitoring and anomaly detection

In-situ monitoring systems can be used in AM part/process authentication by fusing heterogeneous sensing data. ASTM technical committee (F42) approved a complete list of AM process terminology regarding process monitoring and quality control of AM [31]. Based on multiple review studies, heterogenous sensing technologies have been extensively implemented in real-time process monitoring and

control for metal-based AM processes, including acoustic emission, vibration, power consumption, temperature, and images [32]–[34].

The advanced sensing technologies generate high volume of data with various formats, including time series signals/curves, images, and point clouds. Univariate/multivariate time series are usually integrated for AM process monitoring and anomaly detection by leveraging various data fusion techniques, such as physics-based regression modeling [35], generative adversarial networks [36], and the Bayesian Dirichlet process (DP) mixture model [37].

Image streams include both optical and thermal image streams, which have been widely leveraged for *in-situ* defect detection. Due to the high volume and low signal-to-noise ratio in the image stream data, various dimension reduction methods are needed for data compression, including principal component analysis (PCA) [34], manifold learning [38], Deep Neural Networks (DNNs) based feature extraction [39], and the image series modeling based feature extraction [40]. In the laser-based AM process, *in-situ* process porosity can be detected through correlating the pyrometer images and porosity occurrence using a convolutional neural network (CNN) based data fusion technique [41]. In addition, a real-time layer-wise porosity prediction technique was also proposed by obtaining melt pool images, reducing the dimension of captured melt pool images with tensor decomposition, and incorporating an SVM classifier for predicting layer-wise quality [42]. In addition, in laser powder bed fusion (LPBF) AM, a computer vision algorithm is applied to detect anomalies during the powder spreading phase, and an unsupervised machine learning algorithm is used to classify those anomalies [43]. Moreover, a closed-loop proportional-integral-derivative (PID) feedback control scheme has been integrated for printing defect mitigation based on image data [18]. Furthermore, Cheng *et al.* [44] investigated surface patterns by leveraging the image intensity information, where the surface defects are categorized into random defects and assignable defects due to specific process parameter shifts.

3D point clouds data characterizes the surface topology of AM parts for anomaly detection. For example, the deep forest machine learning methods have been used for *in-situ* layer-wise process shift detection [45], [46]. A high-speed CMOS (complementary metal-oxide-semiconductor) camera has been

used for real-time process monitoring for the layer-wise laser melting process [47]. Moreover, various optical sensors, including a structured-light scanner [45] and a 3D digital image correlation (DIC) camera [48], have been used to collect 3D point clouds of printed parts for anomaly detection. In summary, the state-of-the-art process monitoring and anomaly detection methods usually focus on detecting process changes/shifts due to unstable fabrication. However, malicious attack induced process alterations, in general, do not lead to unstable processes, and thus cannot be easily detected by traditional process monitoring methods.

2.2 AM process security

Cyber-physical attacks in AM may occur in the designing, slicing, and manufacturing phases, and numerous studies have focused on the cyber-physical security of AM processes [49]. The literature on AM process security has been summarized through two aspects: 1) AM attack models; and 2) AM attack detection, which are introduced in subsections 2.2.1 and 2.2.2, respectively.

2.2.1 AM attack models

There are plenty of AM attack models that have been investigated in the literature. Bridges *et al*. [50] summarizes the vulnerabilities in the entire AM process chain. Potential attacks to AM processes can target the digital files during all the phases in the AM processes. Firstly, quite a few studies attempted to alter the STL files in the design phase. For example, additional features, such as internal voids, can be inserted into the STL file of the AM part, leading to compromised mechanical properties and catastrophic failures in the final product [2], [4], [48]. Moreover, embedded defects can also be included by jetting a different material, leading to nonhomogeneous material properties in the final AM build [51]. Secondly, the slicing operations can be altered by AM attacks, generating an altered g-code file. The implemented alterations cover the whole set of slicing parameters, including printing direction [9], layer thickness [6], [44], infill path and/or infill percentage [9]. In addition, AM attacks can also be directly applied to modify the g-code files [48–50]. For example, Moore *et al.* [52] applied an attack on a firmware linked to the 3D printer to alter the g-codes by implementing the printing command in an altered order. Thirdly, AM attacks can also aim to alter

AM process parameters, such as printing speed and fan cooling [11], extruding temperature, which can significantly affect the final part quality and reliability [10], [38].

2.2.2 Real-time AM attack detection

Side-channel analysis and monitoring have been widely used to detect AM part/process alteration by leveraging *in-situ* process measurements, such as acoustic emission, vibration, power consumption signals, and videos [13], [44], [45]. With the help of the above-mentioned techniques, a baseline of the signals is firstly established by AM parts which are verified to be normal, and then compared with a potentially altered part for alteration detection [9]. It is worth noting that even though some sensors used for side-channel analysis are also widely used in process anomaly detection, the purposes of using those sensors are no longer assuring process quality but focusing on authenticating the process to its design intent. For example, Belikovetsky *et al.* [53] conducted a side-channel authentication procedure to detect atomic modification (e.g., insertion, deletion, and modification of g-code commands) by analyzing the digital audio signatures in real time. Yu *et al.* [54] incorporated machine learning methods with the multi-modal side-channels for system state estimation for process authentication. Shi *et al.* [55] leveraged the autoencoder method to compress the multi-stream acceleration signals to detect AM part/process alteration. Most of the side-channel monitoring studies are purely data-driven methods and thus heavily rely on a sufficiently large benchmark (or training) dataset which have already been verified to be unaltered. However, the uniqueness of AM processes in producing in high variety and low quantity makes it challenging to collect such a big dataset to train the detection models.

3 Proposed methodology

In this section, subsection 3.1 firstly introduces the layer-wise texture descriptor tensor (LTDT), and subsection 3.2 describes the procedure of constructing the LTDT using the *in-situ* layer-wise video. Subsequently, subsection 3.3 introduces the dimension reduction for the LTDTs using multilinear principal component analysis (MPCA) and real-time monitoring based on the Hotelling T^2 control charting technique. The overall proposed methodology is illustrated in Figure 3.

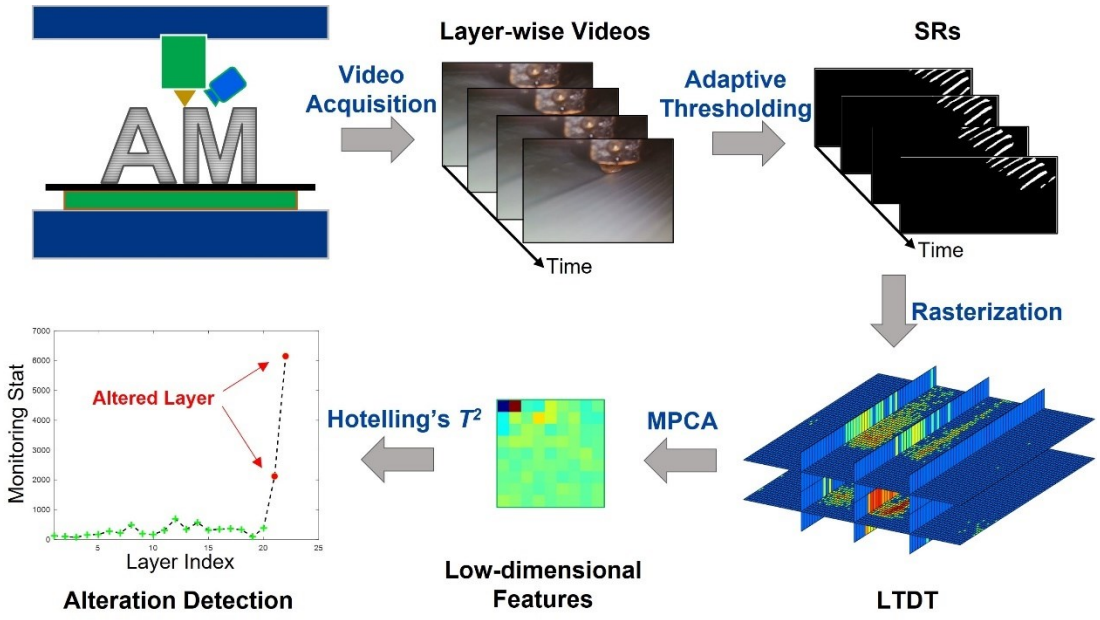

Figure 3: An overview of AM process authentication based on *in-situ* video analysis.

3.1 Layer-wise texture descriptor tensor

In CPS, most attacks aim to change the AM parts' internal structures, including infill pattern, infill percentage, and other structural features, since they are difficult to detect by traditional process monitoring methods without additional process interruptions. All the features of the internal structures are determined by the layer-wise AM printing path, which can be captured by the textures observed from the *in-situ* videos. The layer-wise texture distribution contains critical information for the AM printing paths, and thus can be extracted to authenticate AM processes. Therefore, a novel layer-wise texture descriptor tensor is proposed in this section to characterize the distribution of the geometric features of the segmented texture.

Definition 1: Layer-wise texture descriptor tensor (LTDT). An R-th order LTDT of the l-th layer, denoted as $\mathcal{Z}_l \in \mathbb{N}_0^{D_1 \times \ldots \times D_R}$, is constructed with each mode representing the r-th geometric feature of the segmented textures obtained from the layer-wise imaging ($r = 1, 2, \ldots, R$), where $\mathbb{N}_0$ denotes the non-negative integer lattice in the Euclidean space $\mathbb{R}$. The LTDT contains the multivariate geometric feature distribution of the textures in the layer-wise image(s).

It is worth noting that the LTDTs extracted from the same printing path design are assumed to be independently and identically distributed (i.i.d.) for the following reasons. First, the distribution of the

LTDTs can be uniquely determined by the layer-wise printing path, as illustrated in Figure 2, and therefore, given the same printing path, the LTDTs should come from the same distribution. Second, the correlation between the consecutive layers can be regarded negligible if the microscopic camera is focused on the proximity of the printing nozzle. In this case, the observed printed texture in the area of interest will be mainly affected by the printing path of the current layer, instead of its previous layer.

3.2 Proposed procedure for LTDT construction

Without losing generality, this paper introduces the proposed approach for constructing the LTDT when $R = 3$. However, the proposed method can be naturally extended to cases with $R > 3$.

3.2.1 Image-level texture extraction and characterization

Each image frame in the video captured is firstly cropped to obtain the region of interest (ROI), which only retains the printed layer surface in the ROIs. Subsequently, adaptive image thresholding methods are used to adaptively segment the texture in the ROIs based on the local intensity in the neighbourhood of each pixel [56]. The locally adaptive algorithm automatically adjusts for varying background intensity levels due to spatially and temporally varying lighting conditions. As a result, it automatically discards the low contrast areas in the ROIs, which significantly reduces the data volume. The image pixels are segmented into two groups of regions: one group (labelled as "zero") represents the background, and the other (labelled as "one") represents segmented texture, which characterize the printing paths.

Definition 2: Segmented region (SR). A segmented region is defined as a *continuous* region in the images that is labelled as "one" resulted from the adaptive image thresholding. The k-th SR captured from the l-th layer is denoted as SR_k^l, where $k = 1,2,\dots,K_l$ and K_l denotes the number of SRs in the l-th layer.

For SR_k^l $(k = 1,2,\dots,K_l)$, four geometric features are calculated by approximating its shape using the ellipse that has the same second moment, as listed below.

1) The orientation of SR_k^l is defined as the angle between the major axis of the SR's approximating ellipse and the horizontal axis, as illustrated in Figure 4. It approximates the printing path direction. The orientation of SR_k^l is denoted as o_k^l, where $-90° < o_k^l \leq 90°$ $(k = 1,2,\dots,K_l)$, where K_l denotes the

number of SRs in the l-th layer.

2) The major axis length of SR_k^l is defined as the length of the major axis of the approximating ellipse of the SR. It approximates the observed length of the printing path. The major axis length of SR_k^l is denoted as m_k^l $(k = 1,2, \dots, K_l)$. The unit of m_k^l can be the number of pixels in the captured image.

3) The minor axis length of SR_k^l describes the length of the minor axis of estimating the ellipse of SR_k^l. It approximates the width of the printing path, and n_k^l $(k = 1,2, \dots, K_l)$ is used to denote the minor axis length of SR_k^l. The unit of n_k^l can be the number of pixels in the captured image.

4) The eccentricity of SR_k^l describes the shape of SR_k^l. It is defined as the ratio of the distance between the foci and major axis length of the ellipse with the same second moment as SR_k^l, and denoted as ec_k^l $(k = 1,2, \dots, K_l)$ with $0 < ec_k^l < 1$. The smaller the ec_k^l value gets, the closer SR_k^l is to a circle. It is worth noting that the texture resulted from the printing path should demonstrate a large eccentricity value.

The reason for selecting those features is that their distribution over the entire layer provides critical information for the printing path of various AM processes. An illustration example of the geometric features of an SR is shown in Figure 4, where one SR is included as the white continuous region (labelled as "one") on the black background (labelled as "zero"), the approximating ellipse is denoted as the golden ellipse, and the other relevant features, i.e., orientation, major and minor axis length of the SR, are also illustrated.

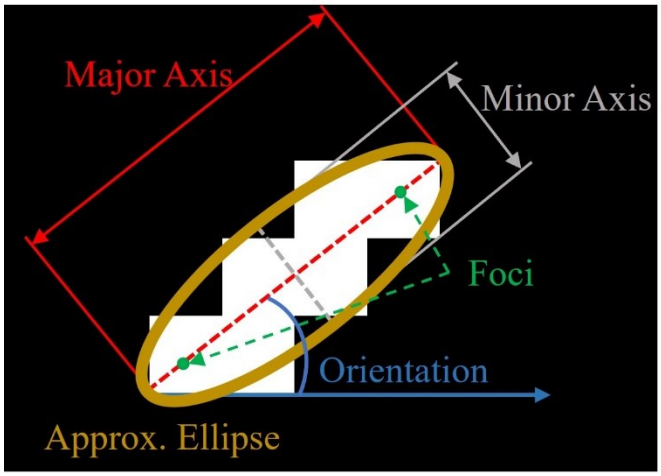

Figure 4: Illustration of the extracted geometric features where the white region represents an SR segmented from the ROI.

In the proposed framework, the eccentricity is used to remove the irrelevant SRs which have a small eccentricity value, which are probably irrelevant to the printing path. This is based on the premise that the printing paths related SRs are generally long segments with a large length-to-diameter (L/D) ratio. The threshold for this region filtering can be determined based on the nominal printing path. For example, for parts with infill patterns resulting in long printing paths like the rectilinear pattern, the filtering threshold should be set higher. In general, a larger threshold value for eccentricity will result in fewer filtered SRs.

3.2.2 Layer-wise geometric feature distribution characterization

To construct the LTDT, the distribution of SRs' geometric features is characterized using a rasterization algorithm. A set of regions are retained in the l-th layer after filtering, denoted as $\{(o_k^l, m_k^l, n_k^l) | ec_k^l \geq T_{ec}\}$, where o_k^l, m_k^l, n_k^l, and ec_k^l represents the orientation, major and minor axis length, and eccentricity of SR_k^l, respectively, and T_{ec} represents the threshold value of the eccentricity in the region filtering. Given a predefined bin size, i.e., (s_O, s_M, s_N), and ranges of these three features, i.e., (l_O, u_O), (l_M, u_M) and (l_N, u_N), the observed number of SRs in each bin can be calculated, where l_O, l_M, and l_N represent the lower bounds of the ranges and u_O, u_M, and u_N represent the upper bounds of the ranges, respectively.

Without losing generality, The rasterization algorithm to generate the LTDTs is illustrated in Figure 5.

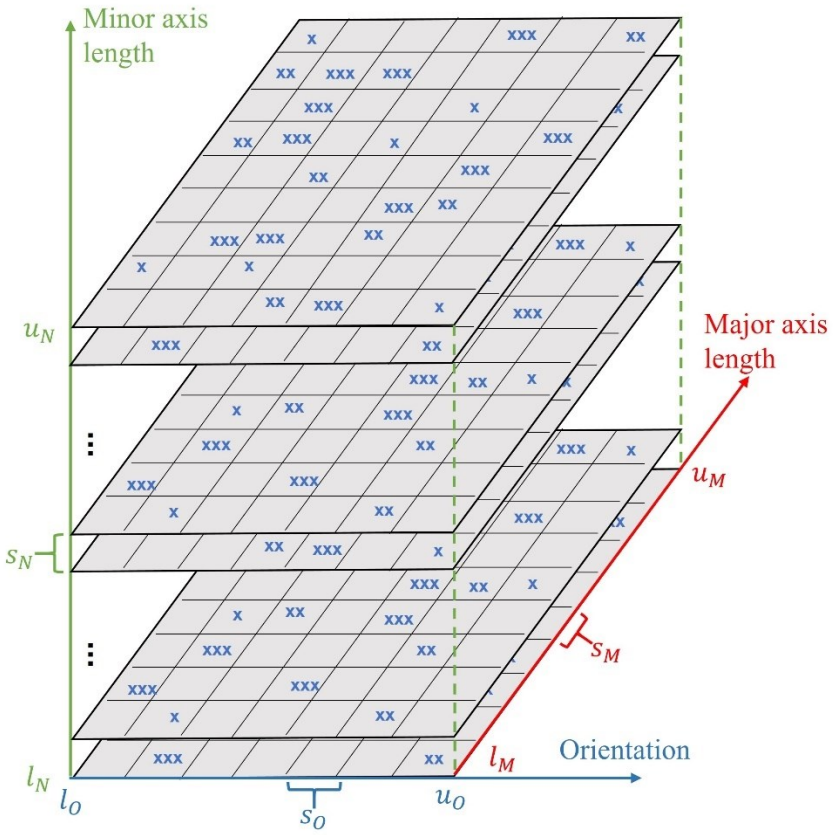

Figure 5: Rasterization to generate the LTDTs where the number of points in each raster is used as the corresponding element in the tensor.

As a result, the LTDT is represented as a 3rd-order tensor $\mathcal{Z}_l \in \mathbb{N}_0^{D_O \times D_M \times D_N}$, where $D_O = \left\lceil \frac{u_O - l_O}{s_O} \right\rceil$, $D_M = \left\lceil \frac{u_M - l_M}{s_M} \right\rceil$, and $D_N = \left\lceil \frac{u_N - l_N}{s_N} \right\rceil$. In addition, each element in $\mathcal{Z}_l$ can be calculated in Eq. (1),

$$\mathcal{Z}_l(o,m,n) = \sum_{k=1}^{K_l} \left[\begin{pmatrix} l_O + (o-1)s_O \\ l_M + (m-1)s_M \\ l_N + (n-1)s_N \end{pmatrix} \leq \begin{pmatrix} o_k^l \\ m_k^l \\ n_k^l \end{pmatrix} < \begin{pmatrix} l_O + os_O \\ l_M + ms_M \\ l_N + ns_N \end{pmatrix} \right] \tag{1}$$

where $[\cdot]$ refers to the Iverson bracket, i.e.,

$$[Q] = \begin{cases} 1, \text{if } Q \text{ is true} \\ 0, \text{if } Q \text{ is false} \end{cases}$$

where $1 \leq o \leq D_O,\ 1 \leq m \leq D_M$ and $1 \leq n \leq D_N$, and K_l represents the total number of SRs in the l-th layer.

Due to the sparsity and high dimensionality of $\mathcal{Z}_l$, it is necessary to further extract the key information from $\mathcal{Z}_l$ for monitoring. Given its effectiveness in reducing the dimensionality of high-dimensional tensors [39, 44, 58], MPCA is used in dimension reduction of the LTDTs for process alteration detection.

3.3 Dimension reduction from geometric feature distribution

The LTDT, denoted as $\mathcal{Z}_l \in \mathbb{N}_0^{D_O \times D_M \times D_N}$, is a 3rd-order tensor with the following properties: 1) all the elements in the tensor are non-negative integers and the distribution of those elements is right skewed; 2) the LTDTs are of high dimension and the elements in the tensor are highly correlated; and 3) The LTDTs are sparse tensors, which means there are a lot of zeros in the tensor. Therefore, dimension reduction methods are needed to compress the LTDTs and extract critical features for effective process authentication.

To avoid numerical issues in tensor decomposition, a log-link function is used to transfer the original elements in the LTDTs to reduce its skewness. In addition, to retain the same lower bound (i.e., zero) and sparsity of the tensor after transformation, each element in $\mathcal{Z}_l$ is shifted by 1, as illustrated in Eq. (2).

$$\mathcal{X}_l = \log\left(\mathcal{Z}_l + 1\right) \tag{2}$$

Based on the standard multilinear algebra, the tensor $\mathcal{X}_l$ can be expressed as in Eq. (3),

$$\mathcal{X}_l = \mathcal{G}_l \times_1 \mathbf{U}_O \times_2 \mathbf{U}_M \times_3 \mathbf{U}_N \tag{3}$$

where $\mathcal{G}_l = \mathcal{X}_l \times_1 \mathbf{U}_O{}^T \times_2 \mathbf{U}_M{}^T \times_3 \mathbf{U}_N{}^T$, and $\mathbf{U}_O$, $\mathbf{U}_M$ and $\mathbf{U}_N$ are orthogonal projection matrices corresponding to the mode of the orientation, major and minor axis length, respectively. $\mathcal{G}_l$ represents the core tensor with reduced dimension $d_O \times d_M \times d_N$, where $0 < d_O < D_O$, $0 < d_M < D_M$ and $0 < d_N < D_N$, and $\mathcal{G}_l$ can be used as the extracted features.

Since the LTDTs are usually high-dimensional and sparse, tensor decomposition can be used to extract low dimensional features for alteration detection. Multilinear principal component analysis (MPCA) determines a multilinear projection that captures most variations in the original LTDTs. The objective of MPCA is to find the projection matrices, i.e., $\mathbf{U}_O$, $\mathbf{U}_M$ and $\mathbf{U}_N$, which maximize the total tensor scatter in

$\mathcal{G}_l$, denoted by $\psi_{\mathcal{G}}$, as illustrated in Eq. (4),

$$\{\mathbf{U}_O, \mathbf{U}_M, \mathbf{U}_N\} = \arg\max_{\mathbf{U}_O, \mathbf{U}_M, \mathbf{U}_N} \psi_{\mathcal{G}} \tag{4}$$

To solve the optimization problem in Eq. (4), the problem is decomposed into a series of projection subproblems, where the projection matrices are iteratively updated. Figure 6 illustrates the pseudocode for implementing the MPCA algorithm, which is adapted from [58], [57].

Input: A set of nominal layers' geometric features distribution $\{\mathcal{Z}_l \in \mathbb{R}^{D_O \times D_M \times D_N}, l = 1,2,\dots,L_{tr}\}$

Output: Low dimensional features $\mathcal{G}_l$ and projection matrices $\widetilde{\mathbf{U}}_O \in \mathbb{R}^{D_O \times d_O}$, $\widetilde{\mathbf{U}}_M \in \mathbb{R}^{D_M \times d_M}$ and $\widetilde{\mathbf{U}}_N \in \mathbb{R}^{D_N \times d_N}$

Algorithm:

Step 1 (Element-wise Transferring and Centering):

1.1 Transfer the original tensor as $\{\mathcal{X}_l = \log(\mathcal{Z}_l + 1)\}$

1.2 Center the benchmark samples as $\{\widetilde{\mathcal{X}}_l = \mathcal{X}_l - \overline{\mathcal{X}}, l = 1,2,\dots,L_{tr}\}$, where $\overline{\mathcal{X}} = \frac{1}{L_{tr}}\sum_{l=1}^{L_{tr}} \mathcal{X}_l$.

Step 2 (Initialization):

2.1 Calculate the eigen-decomposition of $\mathbf{\Phi}^{(j)*} = \sum_{l=1}^{L_{tr}} \widetilde{\mathbf{X}}_{l(j)} \widetilde{\mathbf{X}}_{l(j)}^T$ $(j = 1,2,3)$ and set $\widetilde{\mathbf{U}}_O$, $\widetilde{\mathbf{U}}_M$ and $\widetilde{\mathbf{U}}_N$ to consist of the eigenvectors corresponding to the most significant d_O, d_M and d_N eigenvalues, respectively. Here $\widetilde{\mathbf{X}}_{l(j)}$ represents the unfolded matrix of $\widetilde{\mathcal{X}}_l$ along the j-th mode.

2.2 Calculate $\{\tilde{\mathcal{G}}_l = \widetilde{\mathcal{X}}_l \times_1 \widetilde{\mathbf{U}}_O{}^T \times_2 \widetilde{\mathbf{U}}_M{}^T \times_3 \widetilde{\mathbf{U}}_N{}^T, l = 1,2,3\dots,L_{tr}\}$,

2.3 Calculate $\psi_{\mathcal{G}_0} = \sum_{l=1}^{L_{tr}} \left\|\tilde{\mathcal{G}}_l\right\|_F^2$

Step 3 (Optimization):

For $p = 1{:}P$

Update $\widetilde{\mathbf{U}}_O$: Set the matrix $\widetilde{\mathbf{U}}_O$ to consist of the d_O eigenvectors of the matrix $\mathbf{\Phi}^{(1)} = \sum_{l=1}^{L_{tr}} \widetilde{\mathbf{X}}_{l(1)} \cdot \widetilde{\mathbf{U}}_O \cdot \widetilde{\mathbf{U}}_O{}^T \cdot \widetilde{\mathbf{X}}_{l(1)}^T$, corresponding to the largest d_O eigenvalues.

Update $\widetilde{\mathbf{U}}_M$: Set the matrix $\widetilde{\mathbf{U}}_M$ to consist of the d_M eigenvectors of the matrix $\mathbf{\Phi}^{(2)} = \sum_{l=1}^{L_{tr}} \widetilde{\mathbf{X}}_{l(2)} \cdot \widetilde{\mathbf{U}}_M \cdot \widetilde{\mathbf{U}}_M{}^T \cdot \widetilde{\mathbf{X}}_{l(2)}^T$, corresponding to the largest d_M eigenvalues.

Update $\widetilde{\mathbf{U}}_N$: Set the matrix $\widetilde{\mathbf{U}}_N$ to consist of the d_N eigenvectors of the matrix $\mathbf{\Phi}^{(3)} = \sum_{l=1}^{L_{tr}} \widetilde{\mathbf{X}}_{l(3)} \cdot \widetilde{\mathbf{U}}_N \cdot \widetilde{\mathbf{U}}_N{}^T \cdot \widetilde{\mathbf{X}}_{l(3)}^T$, corresponding to the largest d_N eigenvalues.

Calculate $\{\tilde{\mathcal{G}}_l, l = 1,2,3\dots,L_{tr}\}$ and $\psi_{\mathcal{G}_p}$.

If $\psi_{\mathcal{G}_p} - \psi_{\mathcal{G}_{p-1}} < \varepsilon$, break and output projection matrices, $\widetilde{\mathbf{U}}_O$, $\widetilde{\mathbf{U}}_M$ and $\widetilde{\mathbf{U}}_N$.

Step 4 (Projection): For any newly collected layer, the low-dimensional features are calculated as $\{\mathcal{G}_l = (\mathcal{X}_l - \overline{\mathcal{X}}) \times_1 \widetilde{\mathbf{U}}_O{}^T \times_2 \widetilde{\mathbf{U}}_M{}^T \times_3 \widetilde{\mathbf{U}}_N{}^T, l = 1,2,3\dots,L_{tr}\}$.

Figure 6: The MPCA algorithm for projection matrix estimation.

Given training data set with several verified healthy layers, the projection matrices can be estimated

based on the algorithm in Figure 6, and low-dimensional features can be extracted to describe the major variability in the LTDTs. Subsequently, the Hotelling T^2 control charting scheme can be applied to the extracted multivariate features [59]. Based on the features extracted from the training set, the covariance matrix (denoted as $S_{\mathcal{G}}$) can be estimated. When a new part is fabricated and the streamline video data collected, the Hotelling T^2 monitoring statistics of the l-th layer is calculated in Eq. (5),

$$T_l^2 = \text{vec}(\mathcal{G}_l)^T \left(S_{\mathcal{G}}\right)^{-1} \text{vec}(\mathcal{G}_l) \tag{5}$$

where $\text{vec}(\cdot)$ denotes the function to vectorize the resulting low dimensional tensor, and $\mathcal{G}_l$ denotes the low-dimensional features extracted based on the projection matrices obtained from the training data. The upper control limit (UCL) of the control chart can be determined as the empirical $100 \times (1-\alpha)\%$ quantile of the monitoring statistics based on the Phase I data, where α is the pre-determined Type I error rate.

The alarm rule of the proposed process authentication is that whenever the monitoring statistic T_l^2 exceeds the pre-determined UCL, the printing path of the l-th layer of the tested build is altered, and the printing process should be terminated for further investigation.

4 Case study

This section investigates the performance of the proposed methodology based on a fused filament fabrication (FFF) process which is equipped with a microscope camera to capture streamline videos. The experimental setup and data collection are described in Sec. 4.1, and the results are summarized and discussed in Sec. 4.2.

4.1 Experimental setup and data collection

An FFF-based 3D printer (Prusa i3 MK3S) was used for data collection. A Teslong Portable MS 100 USB microscope was attached to the extruder head and focused on the nozzle tip while continuously capturing streamline videos from the fabricated surface. The camera's frame rate is 25 Hz, and the resulting resolution of each frame is 480×640. Figure 7a) and b) illustrate the experimental setup with the real-time video shown on the screen of the laptop. In addition, Figure 7 c) shows five example frames captured

from the fabrication of one layer with solid infill of the rectilinear pattern; and Figure 7 d) shows example image frames captured from the fabrication of one layer with a square shaped hollow feature included. It can be observed that the image contrast varies significantly within the same image and among multiple images.

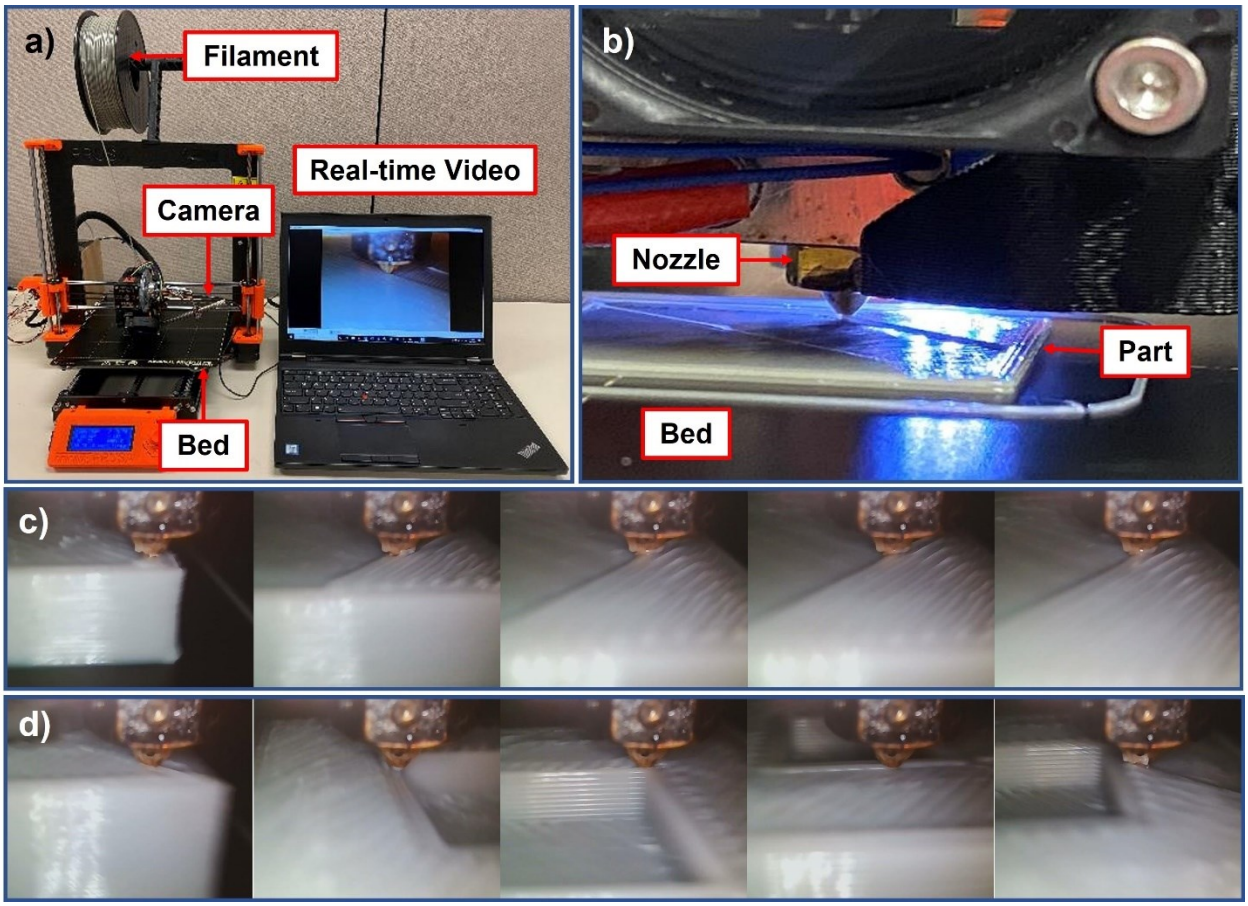

Figure 7: Demonstration of the experimental setup (a and b) and representative sample images (c and d).

This case study intends to simulate two scenarios of the cyber-physical attacks, i.e., varying the infill orientation (Group B) and altering the STL files (Group C). As illustrated in Figure 8, both cyber-attack scenarios considered result in changes the printing path, and thus alter the entire AM chain starting from the slicing phase. Three different groups of parts were fabricated, in which Group A is the nominal part, and Group B and C are altered parts with printing path rotated and undesired feature added, respectively. Table 1 summarizes the part dimension and infill orientation of the three groups. The feedstock material used was the filament of polylactic acid (PLA) with a cross-sectional diameter of 1.75 mm. The printing parameters used for all the parts are summarized in

Table 2, which remain the same and therefore excluded from the analysis in this study. Four parts in total were fabricated, among which two parts belong to Group A, and the other two are from Group B and C, respectively. Figure 9 illustrates the cross sections of the three printed parts which belong to Group A,

B, and C, respectively.

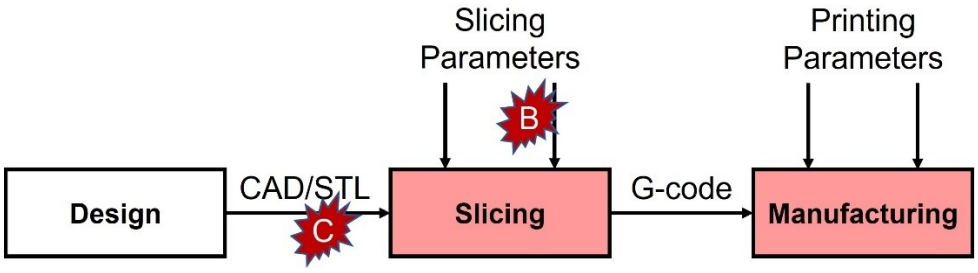

Figure 8: Cyber-attack scenarios simulated in the case study, where B and C denote the corresponding locations where the attacks are applied, and the shaded phases (i.e., slicing and manufacturing) denote the phases with altered information.

Figure 9: Illustration of three groups of parts.

Table 1: Model dimensions and infill parameters.

Part Group	A (Nominal)	B (Altered)	C (Altered)
Dimensions (L × W × H) (mm)	30 × 30 × 10		
Undesired feature (L× W × H) (mm)	NA	NA	10 × 10 × 5
Infill orientation (degree)	45	90	45
Build time (second)	3,761	3,812	3,550

Table 2: Printing parameters shared by all the three groups.

Parameter	Value	Parameter	Value
Infill (%)	100	Printing speed (mm/s)	20
Extrusion width (mm)	0.5	Nozzle temperature (°C)	200

First layer thickness (mm)	0.4	Bed temperature (°C)	65
Layer thickness (mm)	0.3	Number of layers	33

4.2 Results and discussion

4.2.1 Benchmark method selection

The image-based monitoring and control method for the FFF process proposed in Liu *et al.* [18] was adopted as the benchmark method for alteration detection, because it is the most recent study on anomaly detection by leveraging texture analysis of real-time optical images. In the benchmark method, a variety of textural statistics were extracted based on the gray-level co-occurrence matrix (GLCM), and the multivariate statistics are compressed using the autoencoder technique [60], which has been demonstrated as an effective data compression method in [61]. This method is mainly focused on the defect detection and its effectiveness has been validated in [18] through the comparison between the conventional machine learning approaches. It is worth noting that the benchmark method is proposed for *image-wise* anomaly detection. Therefore, to achieve *layer-wise* alteration detection, the arithmetic mean of the image-wise monitoring statistics across each entire layer was used as the layer-wise monitoring statistic.

Another potential benchmark method is proposed by Bui and Apley [62], which proposed a stochastic textured surface modelling approach for high-dimensional images. Although this method has demonstrated its effectiveness and great potential in textile applications, the method is not applicable to the problem in this paper, because their modelling approach requires to establish a benchmark textured surface for monitoring and anomaly detection. In the streamline video captured from the 3D printing process, it will be quite cumbersome to find the unique benchmark textured surface for all the images due to dynamic nature of the ROIs captured. Therefore, this method is not adopted as a second benchmark method to compare with the proposed approach.

4.2.2 Model settings and parameter estimation for both methods

For both methods, image pre-processing was implemented. For the proposed method, the ROI was cropped by removing the region above the nozzle tip, resulting in the ROIs of size 315×637. For the benchmark method, the ROI cropping suggested in [18], resulting in the ROIs of size 80×80. All the 33

layers of each part except for the first layer were used since the textural information in the first layer is not comparable with any of the subsequent layers.

For the proposed method, each layer-wise video constructed the LTDTs with the dimension of $181 \times 140 \times 15$, which is a high-dimensional tensor. To examine the sparsity of the LTDTs, the proportions of the zero elements in Part 1 is illustrated in Figure 10. It can be observed that the constructed LTDT tensors are very sparse tensors with over 94% of the elements that are zero.

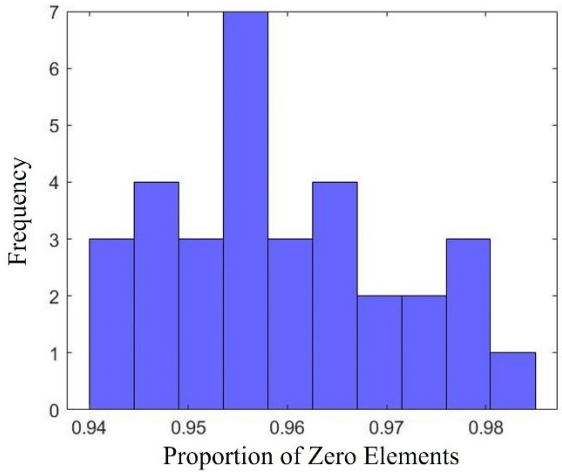

Figure 10: Histogram of proportion of zero elements in the 32 layers of Part 1 of Group A.

For both methods, all the layers of the first part in Group A were used as the training data set for necessary parameter estimation. This includes projection matrices estimation in MPCA and covariance matrix estimation for the T^2 monitoring statistics for the proposed method, and the training of autoencoder for the benchmark method. Furthermore, randomly selected 75% layers of the second part in Group A were used as Phase I data for control limit determination. The remaining 25% layers of the second part of Group A and all the layers of Group B and C were used as the Phase II data to evaluate the performance. The random split between Phase I and Phase II data was repeated for 100 times, and the average performance was summarized. It is also worth noting that, for the proposed method, the parameter estimation and UCL determination for the odd and even number of layers need to be separated, because the texture distributions of the odd and even number of layers in Group A are different. In Phase II, whenever the monitoring statistic exceeds the pre-determined UCL, the control chart will signal and that corresponding layer is detected as

an altered layer; otherwise, the layer is regarded as unaltered. A test run example is illustrated in Figure 11.

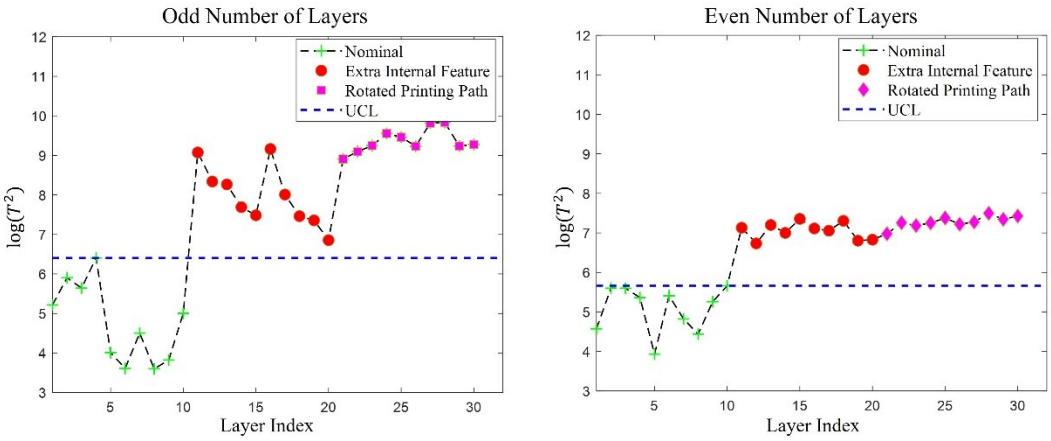

Figure 11: Examples of control charts for odd number and even number of layers.

4.2.3 Results comparison and discussion

The performance metrics used to evaluate the proposed and benchmark methods include precision, recall, Fscore, and overall accuracy, which are defined below based on the elements in the confusion matrix.

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{6}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{7}$$

$$\text{Fscore} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{8}$$

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{9}$$

where true positive (TP) denotes the number of altered layers which are predicted accurately as altered, whereas true negative (TN) represents the unaltered layers which are accurately predicted as unaltered. In addition, false-negative (FN) denotes inaccurate prediction of altered layers as unaltered, while false positive (FP) represents inaccurate prediction of the layers which are unaltered but predicted as altered. Fscore is the harmonic mean of precision and recall, and the overall accuracy is the percentage of accurately classified layers within all the evaluated Phase II layers. To assess the feasibility for real-time analysis, the computational efficiency of the proposed and benchmark methods is also evaluated and compared.

There are two tuning parameters used in the proposed method: 1) the threshold value of eccentricity used in the SR filtering, denoted as T_{ec}; and 2) the number of MPCs retained in the monitoring statistics, denoted as d_{pc}. To test the robustness of the proposed method, both tuning parameters are varied, and the performance of the proposed method is summarized in Table 3. It can be observed that the proposed method outperforms the benchmark method within the wide range of the tuning parameters for all the performance metrics evaluated. In addition, the average rates of each entry in the confusion matrix have been summarized in Table 4 in the Appendix.

Even though the proposed method demonstrates good performance in all the combinations of tuning parameters tested, some trends are still visible in Table 3. Based on the Fscore values, the best performing rows within each given T_{ec} value have been bolded in Table 3. It can be observed that when the T_{ec} value is small to medium (i.e., 0.85, and 0.9), the proposed method performs best using relatively large d_{pc} values (i.e., 10). When the T_{ec} value is medium to large (i.e., 0.95 and 0.98), the proposed method performs best using relatively small d_{pc} values (i.e., 5). The reason behind this observation is that smaller (larger) T_{ec} values, in general, lead to more SRs retained and less sparse LTDTs. Therefore, more (fewer) MPCs are potentially needed to capture the major variations in the extracted LTDTs for effective alteration detection.

The major reason for the inferior performance of the benchmark method is that their method works under the underlying premise that the GLCM based features can fully characterize the textured surfaces captured. However, in the real-world AM fabrication, the lighting condition and image contrast are varying significantly over time due to the high printing speed, making the GLCM features limited in characterizing these complex stochastic textured surfaces.

Table 3: Results summary of the proposed and benchmark methods

T_{ec}	d_{pc}	Accuracy	Precision	Recall	Fscore
0.85	2	95.8%	95.5%	98.4%	96.9%
	5	86.1%	87.9%	91.8%	89.8%
	8	95.0%	93.1%	100.0%	96.4%
	10	**97.8%**	**96.8%**	**100.0%**	**98.4%**

	12	84.3%	91.3%	84.6%	87.8%
0.9	2	92.6%	93.0%	96.3%	94.6%
	5	89.4%	87.7%	97.9%	92.5%
	8	94.3%	92.2%	100.0%	95.9%
	10	**96.4%**	**94.9%**	**100.0%**	**97.4%**
	12	93.5%	91.2%	100.0%	95.4%
0.95	2	90.8%	87.8%	100.0%	93.5%
	5	**95.0%**	**96.0%**	**96.8%**	**96.3%**
	8	86.5%	95.4%	83.9%	89.3%
	10	82.7%	90.0%	83.4%	86.5%
	12	84.4%	90.3%	86.0%	88.0%
0.98	2	84.2%	96.2%	79.8%	87.1%
	5	**93.0%**	**90.6%**	**100.0%**	**95.0%**
	8	90.7%	93.7%	92.4%	93.0%
	10	88.1%	91.8%	90.4%	91.0%
	12	84.3%	91.2%	84.7%	87.8%
Benchmark		72.5%	84.0%	62.0%	71.0%

To evaluate the computational efficiency of the proposed method, the computation time distribution is illustrated as boxplots in Figure 12. To better illustrate the variability of the distributions under different scenarios, the computation time distributions are plotted in the log scale. Since the different d_{pc} values ranging from 2 to 12 do not significantly affect the computation time, the computation time is only compared based on different T_{ec} values (Intel® Core™ Processor i7-7700 CPU @ 3.60GHz). It can be observed that even though the proposed method is less efficient compared with the benchmark method, both are significantly shorter than the layer-wise build time. Within different tuning parameters used in the proposed method, it is also observed that when the T_{ec} value is small, the variation of computation time is higher than when the T_{ec} value is medium or large. Furthermore, the average computation time decreases slightly as the T_{ec} increases, because the number of retained SRs will decrease given a higher threshold value of T_{ec}. In addition, it is also worth noting that given the same camera, the layer-wise computation time of the proposed method is determined by the size of the video, which is proportional to the layer-wise build time. For the proposed method, the computation time stays between 25.0% and 28.3% of the layer-wise build time, depending on the tuning parameter used.

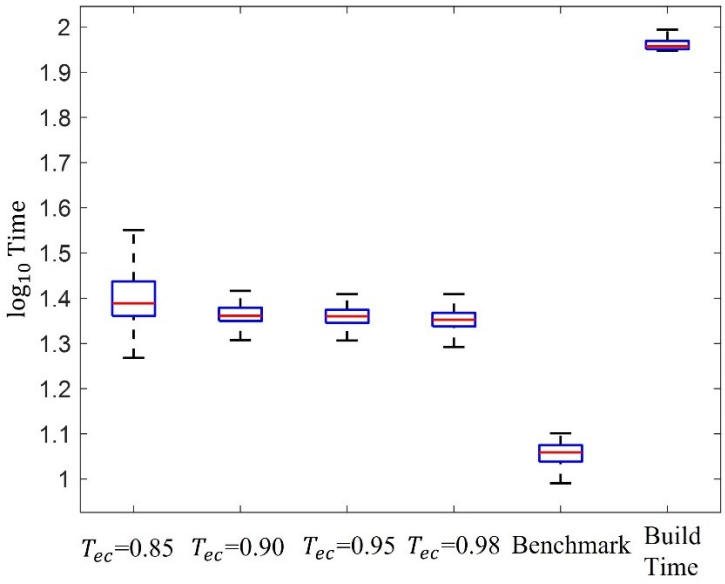

Figure 12: Average layer-wise computation time (second) comparison in the log scale.

5 Conclusion and future work

Cyber-manufacturing systems accelerate the communication, prototyping, and sharing of digital files to optimize productivity in different categories of AM process. The layer-by-layer fashion of fused filament fabrication AM process significantly makes a large variety of process/part alterations possible and therefore extensively enlarge the vulnerability space. Most cyber-physical attacks focus on altering the printing path, so that the internal structure of the product can be changed. This will lead to deteriorated mechanical properties and compromised product functionality for mission-critical structures. What's worse, it may even cause catastrophic accidents for the operators for functional AM components. This paper proposes a new real-time AM process authentication based on layer-wise streamline video data. By integrating adaptive image thresholding, the multivariate distribution of texture geometric features is extracted. In addition, a novel layer-wise AM process descriptor, i.e., the layer-wise texture descriptor tensor (LTDT), is constructed for process authentication. MPCA is used to extract low-dimensional features from those high-dimensional and sparse LTDTs. To evaluate the effectiveness of the proposed methodology, a case study based on an FFF process is used. The proposed method outperforms the benchmark method in terms of alteration

detection accuracy, while the computational efficiency remains satisfactory for real-time alteration detection.

This study can be potentially extended in the following four directions. First, the sensitivity of the alteration detection will be further quantified for major part alteration categories, such as undesired feature added and rotated printing orientation. Second, under the proposed framework, AM parts with diversified geometric features, including different shapes, infill patterns, and infill percentages, will be considered, and their performance will be evaluated. Third, a machine learning scheme can be used to categorize different types of printing path alterations for fault diagnosis and impact assessment of the cyber-physical attacks. Last but not the least, the proposed framework will be adapted to other AM processes with printing path being critical to the structural properties, such as direct laser deposition, and selected laser melting processes.

6 Acknowledgment

This research has been partially supported by the National Science Foundation under Grant No. 2046515. In addition, the authors would like to thank Mr. Durant Fullington for his help with the fused filament fabrication based experimental setup in the case study.

7 Appendix: Average Rates of Confusion Matrix Entries in the Case Study

In Table 4, the average rates of the confusion matrix entries of the case study are summarized for both the proposed method with various tuning parameters and the benchmark method.

Table 4: Average rates of confusion matrix entries in the case study

T_{ec}	d_{pc}	TP Rate	TN Rate	FP Rate	FN Rate
0.85	2	65.6%	30.2%	3.2%	1.1%
	5	61.2%	24.9%	8.5%	5.4%
	8	66.7%	28.4%	5.0%	0.0%
	10	66.7%	31.1%	2.2%	0.0%
	12	56.4%	27.9%	5.5%	10.3%

0.9	2	64.2%	28.4%	4.9%	2.5%
	5	65.3%	24.1%	9.2%	1.4%
	8	66.7%	27.6%	5.7%	0.0%
	10	66.7%	29.8%	3.6%	0.0%
	12	66.7%	26.8%	6.5%	0.0%
0.95	2	66.7%	24.1%	9.3%	0.0%
	5	64.5%	30.5%	2.8%	2.2%
	8	55.9%	30.6%	2.7%	10.8%
	10	55.6%	27.1%	6.3%	11.1%
	12	57.3%	27.0%	6.3%	9.3%
0.98	2	53.2%	31.1%	2.3%	13.5%
	5	66.7%	26.3%	7.0%	0.0%
	8	61.6%	29.1%	4.2%	5.1%
	10	60.3%	27.9%	5.5%	6.4%
	12	56.5%	27.8%	5.5%	10.2%
Benchmark		34%	33.8%	38.6%	20.7%

8 References

[1] V. Gunes, S. Peter, T. Givargis, and F. Vahid, "A survey on concepts, applications, and challenges in cyber-physical systems," *KSII Trans. Internet Inf. Syst.*, vol. 8, no. 12, pp. 4242–4268, 2014, doi: 10.3837/tiis.2014.12.001.

[2] H. Turner, J. White, J. A. Camelio, C. Williams, B. Amos, and R. Parker, "Bad Parts: Are Our Manufacturing Systems at Risk of Silent Cyberattacks?," *IEEE Secur. Priv.*, vol. 13, no. 3, pp. 40–47, 2015, doi: 10.1109/MSP.2015.60.

[3] R. M. Lee, M. J. Assante, and T. Conway, "ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – German Steel Mill Cyber Attack," *SANS, Ind. Control Syst.*, p. 15, 2014.

[4] L. D. Sturm, C. B. Williams, J. A. Camelio, J. White, and R. Parker, "Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the.STL file with human subjects," *J. Manuf. Syst.*, vol. 44, pp. 154–164, 2017, doi: 10.1016/j.jmsy.2017.05.007.

[5] S. Rokka Chhetri and M. A. Al Faruque, "Side Channels of Cyber-Physical Systems: Case Study in Additive Manufacturing," *IEEE Des. Test*, vol. 34, no. 4, pp. 18–25, 2017, doi:

10.1109/MDAT.2017.2682225.

[6] H. Vincent, L. Wells, P. Tarazaga, and J. Camelio, “Trojan Detection and Side-channel Analyses for Cyber-security in Cyber-physical Manufacturing Systems,” *Procedia Manuf.*, vol. 1, pp. 77–85, 2015, doi: 10.1016/j.promfg.2015.09.065.

[7] A. Thompson, I. Maskery, and R. K. Leach, “X-ray computed tomography for additive manufacturing : a review,” *Meas. Sci. Technol.*, vol. 072001, p. 72001, doi: 10.1088/0957-0233/27/7/072001.

[8] Z. Shi, C. Kan, W. Tian, and C. Liu, “A Blockchain-based G-code Protection Approach for Cyber-Physical Security in Additive Manufacturing,” *J. Comput. Inf. Sci. Eng.*, vol. 21, no. 4, p. 041007, 2021.

[9] J. Brandman, L. Sturm, J. White, and C. Williams, “A physical hash for preventing and detecting cyber-physical attacks in additive manufacturing systems,” *J. Manuf. Syst.*, vol. 56, pp. 202–212, 2020.

[10] C. J. Bayens, “Physical signal-based intrusion detection for cyber physical systems.” Georgia Institute of Technology, 2017.

[11] Y. Gao, W. Wang, W. Xu, C. Zhou, Z. Jin, and B. Li, “Watching and Safeguarding Your 3D Printer: Online Process Monitoring Against Cyber-Physical Attacks,” *Proc. ACM Interactive, Mobile, Wearable Ubiquitous Technol.*, vol. 2, no. 3, p. 108, 2018.

[12] J. Gatlin, S. Belikovetsky, S. B. Moore, Y. Solewicz, Y. Elovici, and M. Yampolskiy, “Detecting sabotage attacks in additive manufacturing using actuator power signatures,” *IEEE Access*, vol. 7, pp. 133421–133432, 2019, doi: 10.1109/ACCESS.2019.2928005.

[13] D. Genkin, M. Pattani, R. Schuster, and E. Tromer, “Synesthesia: Detecting screen content via remote acoustic side channels,” *Proc. - IEEE Symp. Secur. Priv.*, vol. 2019-May, pp. 853–869, 2019, doi: 10.1109/SP.2019.00074.

[14] C. Liu, R. Wang, Z. Kong, S. Babu, C. Joslin, and J. Ferguson, “Real-time 3D surface measurement in additive manufacturing using deep learning,” 2019.

[15] S. Nuchitprasitchai, M. Roggemann, and J. M. Pearce, “Factors effecting real-time optical monitoring of fused filament 3D printing,” *Prog. Addit. Manuf.*, vol. 2, no. 3, pp. 133–149, 2017, doi: 10.1007/s40964-017-0027-x.

[16] S. Kleszczynski and T. Jan, “Error Detection in Laser Beam Melting Systems by High Resolution Imaging,” no. August, 2012.

[17] H. Yan, K. Paynabar, and J. Shi, “Image-based process monitoring using low-rank tensor decomposition,” *IEEE Trans. Autom. Sci. Eng.*, vol. 12, no. 1, pp. 216–227, 2015, doi: 10.1109/TASE.2014.2327029.

[18] C. Liu, A. C. C. Law, D. Roberson, and Z. (James) Kong, “Image analysis-based closed loop quality control for additive manufacturing with fused filament fabrication,” *J. Manuf. Syst.*, vol. 51, no. April, pp. 75–86, 2019, doi: 10.1016/j.jmsy.2019.04.002.

[19] H. Gong, K. Rafi, H. Gu, G. D. Janaki Ram, T. Starr, and B. Stucker, “Influence of defects on mechanical properties of Ti-6Al-4V components produced by selective laser melting and electron beam melting,” *Mater. Des.*, vol. 86, pp. 545–554, 2015, doi: 10.1016/j.matdes.2015.07.147.

[20] M. Seifi, A. Salem, J. Beuth, O. L. A. Harrysson, and J. J. Lewandowski, “Overview of Materials Qualification Needs for Metal Additive Manufacturing,” vol. 68, no. 3, 2016, doi: 10.1007/s11837-015-1810-0.

[21] M. Seifi *et al.*, “Progress Towards Metal Additive Manufacturing Standardization to Support Qualification and Certification,” *JOM*, vol. 69, no. 3, 2017, doi: 10.1007/s11837-017-2265-2.

[22] J. M. Waller, B. H. Parker, K. L. Hodges, E. R. Burke, J. L. Walker, and E. R. Generazio, “Nondestructive evaluation of additive manufacturing,” *Natl. Aeronaut. Sp. Adm.*, 2014.

[23] S. Everton *et al.*, “Evaluation of laser ultrasonic testing for inspection of metal additive manufacturing,” vol. 9353, pp. 1–8, 2015, doi: 10.1117/12.2078768.

[24] A. Toma, R. Condruz, R. Carlanescu, and I. Daniel, “A mini-review on non-destructive techniques for additive manufactured metal parts,” *AIP Conf. Proc.*, vol. 2302, no. December, 2020, doi: 10.1063/5.0033732.

[25] X. Zhang *et al.*, “Correlation approach for quality assurance of additive manufactured parts based on optical metrology,” *J. Manuf. Process.*, vol. 53, no. May 2019, pp. 310–317, 2020, doi: 10.1016/j.jmapro.2020.02.037.

[26] P. I. Stavroulakis and R. K. Leach, “Invited Review Article: Review of post-process optical form metrology for industrial-grade metal additive manufactured parts,” *Rev. Sci. Instrum.*, vol. 87, no. 4, pp. 1–15, 2016, doi: 10.1063/1.4944983.

[27] W. Du, Q. Bai, Y. Wang, and B. Zhang, “Eddy current detection of subsurface defects for additive/subtractive hybrid manufacturing,” *Int. J. Adv. Manuf. Technol.*, vol. 95, no. 9–12, pp. 3185–3195, 2018, doi: 10.1007/s00170-017-1354-2.

[28] M. I. Albakri, L. D. Sturm, C. B. Williams, and P. A. Tarazaga, “Impedance-based non-destructive evaluation of additively manufactured parts,” *Rapid Prototyp. J.*, vol. 23, no. 3, pp. 589–601, Jan. 2017, doi: 10.1108/RPJ-03-2016-0046.

[29] G. Park, H. Sohn, C. R. Farrar, and D. J. Inman, “Overview of Piezoelectric Impedance-Based Health Monitoring and Path Forward,” vol. 35, no. 6, pp. 451–463, 2003.

[30] M. Pavan, T. Craeghs, R. Verhelst, O. Ducatteeuw, J. Kruth, and W. Dewulf, “Case Studies in Nondestructive Testing and Evaluation CT-based quality control of Laser Sintering of Polymers,” *Case Stud. Nondestruct. Test. Eval.*, vol. 1, pp. 1–7, 2016, doi: 10.1016/j.csndt.2016.04.004.

[31] L. Koester, H. Taheri, L. J. Bond, D. Barnard, and J. Gray, “Additive manufacturing metrology: State of the art and needs assessment,” *AIP Conf. Proc.*, vol. 1706, 2016, doi: 10.1063/1.4940604.

[32] G. Tapia and A. Elwany, “A Review on Process Monitoring and Control in Metal-Based Additive Manufacturing,” *J. Manuf. Sci. Eng. Trans. ASME*, vol. 136, no. 6, pp. 1–10, 2014, doi: 10.1115/1.4028540.

[33] K. Zeng, D. Pal, and B. Stucker, “A review of thermal analysis methods in Laser Sintering and Selective Laser Melting Kai Zeng, Deepankar Pal, Brent Stucker Department of Industrial Engineering, University of Louisville, Louisville, KY 40292,” pp. 796–814.

[34] E. Rodriguez *et al.*, “Integration of a thermal imaging feedback control system in electron beam

melting," *23rd Annu. Int. Solid Free. Fabr. Symp. - An Addit. Manuf. Conf. SFF 2012*, no. Figure 1, pp. 945–961, 2012.

[35] W. Tian, R. Jin, T. Huang, and J. A. Camelio, "Statistical process control for multistage processes with non-repeating cyclic profiles," *IISE Trans.*, vol. 49, no. 3, pp. 320–331, 2017.

[36] Y. Li, Z. Shi, C. Liu, W. Tian, Z. Kong, and C. B. Williams, "Augmented Time Regularized Generative Adversarial Network (ATR-GAN) for Data Augmentation in Online Process Anomaly Detection," *IEEE Trans. Autom. Sci. Eng.*, 2021.

[37] P. K. Rao, J. Liu, D. Roberson, Z. Kong, and C. Williams, "Online Real-Time Quality Monitoring in Additive Manufacturing Processes Using Heterogeneous Sensors," *J. Manuf. Sci. Eng. Trans. ASME*, vol. 137, no. 6, pp. 1–12, 2015, doi: 10.1115/1.4029823.

[38] C. Liu, Z. Kong, S. Babu, C. Joslin, and J. Ferguson, "An integrated manifold learning approach for high-dimensional data feature extractions and its applications to online process monitoring of additive manufacturing," *IISE Trans.*, vol. 53, no. 11, pp. 1215–1230, 2021.

[39] F. Imani, R. Chen, E. Diewald, E. Reutzel, and H. Yang, "Deep learning of variant geometry in layerwise imaging profiles for additive manufacturing quality control," *J. Manuf. Sci. Eng. Trans. ASME*, vol. 141, no. 11, 2019, doi: 10.1115/1.4044420.

[40] M. N. Esfahani, W. Tian, and L. Bian, "In-situ layer-wise quality monitoring for laser-based additive manufacturing using image series analysis.," *Annu. Int. Solid Free. Fabr. Symp. (SFF), Austin, Texas.*, 2019.

[41] Q. Tian, S. Guo, E. Melder, L. Bian, and W. Guo, "Deep learning-based data fusion method for in situ porosity detection in laser-based additive manufacturing," *J. Manuf. Sci. Eng. Trans. ASME*, vol. 143, no. 4, pp. 1–14, 2021, doi: 10.1115/1.4048957.

[42] S. H. Seifi, W. Tian, H. Doude, M. A. Tschopp, and L. Bian, "Layer-Wise Modeling and Anomaly Detection for Laser-Based Additive Manufacturing," *J. Manuf. Sci. Eng. Trans. ASME*, vol. 141, no. 8, pp. 1–12, 2019, doi: 10.1115/1.4043898.

[43] L. Scime and J. Beuth, "Anomaly detection and classification in a laser powder bed additive

manufacturing process using a trained computer vision algorithm," *Addit. Manuf.*, vol. 19, pp. 114–126, 2018, doi: 10.1016/j.addma.2017.11.009.

[44] Y. Cheng and M. A. Jafari, "Vision-based online process control in manufacturing applications," *IEEE Trans. Autom. Sci. Eng.*, vol. 5, no. 1, pp. 140–153, 2008, doi: 10.1109/TASE.2007.912058.

[45] Z. Ye, C. Liu, W. Tian, and C. Kan, "A Deep Learning Approach for the Identification of Small Process Shifts in Additive Manufacturing using 3D Point Clouds," *Procedia Manuf.*, vol. 48, pp. 770–775, 2020.

[46] Z. Ye, C. Liu, W. Tian, and C. Kan, "In-situ point cloud fusion for layer-wise monitoring of additive manufacturing," *J. Manuf. Syst.*, vol. 61, pp. 210–222, 2021.

[47] T. Craeghs, S. Clijsters, J. P. Kruth, F. Bechmann, and M. C. Ebert, "Detection of Process Failures in Layerwise Laser Melting with Optical Process Monitoring," *Phys. Procedia*, vol. 39, pp. 753–759, 2012, doi: 10.1016/j.phpro.2012.10.097.

[48] O. Holzmond and X. Li, "In situ real time defect detection of 3D printed parts," *Addit. Manuf.*, vol. 17, pp. 135–142, 2017, doi: 10.1016/j.addma.2017.08.003.

[49] M. Yampolskiy *et al.*, "Security of additive manufacturing: Attack taxonomy and survey," *Addit. Manuf.*, vol. 21, pp. 431–457, 2018, doi: 10.1016/j.addma.2018.03.015.

[50] S. M. Bridges, K. Keiser, N. Sissom, and S. J. Graves, "Cyber security for additive manufacturing," *ACM Int. Conf. Proceeding Ser.*, vol. 06-08-Apri, pp. 1–3, 2015, doi: 10.1145/2746266.2746280.

[51] S. E. Zeltmann, N. Gupta, N. G. Tsoutsos, M. Maniatakos, J. Rajendran, and R. Karri, "Manufacturing and Security Challenges in 3D Printing," *Jom*, vol. 68, no. 7, pp. 1872–1881, 2016, doi: 10.1007/s11837-016-1937-7.

[52] S. B. Moore, W. B. Glisson, and M. Yampolskiy, "Implications of malicious 3D printer firmware," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 2017-Janua, pp. 6089–6098, 2017, doi: 10.24251/hicss.2017.735.

[53] S. Belikovetsky, Y. Solewicz, M. Yampolskiy, J. Toh, and Y. Elovici, "Digital Audio Signature

for 3D Printing Integrity," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 5, pp. 1127–1141, 2018, doi: 10.1109/TIFS.2018.2851584.

[54] S. Yu and S. Member, "Sabotage Attack Detection for Additive Manufacturing Systems," vol. 8, 2020.

[55] Z. Shi, A. Al Mamun, C. Kan, W. Tian, and C. Liu, "An LSTM-Autoencoder Based Online Side Channel Monitoring Approach for Cyber-Physical Attack Detection in Additive Manufacturing," *J. Intell. Manuf.*, 2021.

[56] D. Bradley and G. Roth, "Adaptive thresholding using the integral image," *J. Graph. tools*, vol. 12, no. 2, pp. 13–21, 2007.

[57] H. Lu, K. N. Plataniotis, and A. N. Venetsanopoulos, "MPCA: Multilinear principal component analysis of tensor objects," *IEEE Trans. Neural Networks*, 2008, doi: 10.1109/TNN.2007.901277.

[58] M. Khanzadeh, W. Tian, A. Yadollahi, H. R. Doude, M. A. Tschopp, and L. Bian, "Dual process monitoring of metal-based additive manufacturing using tensor decomposition of thermal image streams," *Addit. Manuf.*, vol. 23, no. July, pp. 443–456, 2018, doi: 10.1016/j.addma.2018.08.014.

[59] C. A. Lowry and D. C. Montgomery, "A review of multivariate control charts," *IIE Trans.*, vol. 27, no. 6, pp. 800–810, 1995.

[60] B. A. Olshausen and D. J. Field, "Sparse coding with an overcomplete basis set: A strategy employed by V1?," *Vision Res.*, vol. 37, no. 23, pp. 3311–3325, 1997.

[61] C. Liu, C. Kan, and W. Tian, "An Online Side Channel Monitoring Approach for Cyber-physical Attack Detection of Additive Manufacturing," 2020.

[62] A. T. Bui and D. W. Apley, "Monitoring for changes in the nature of stochastic textured surfaces," *J. Qual. Technol.*, vol. 50, no. 4, pp. 363–378, 2018.