Adaptive Thermal History Deidentification for Privacy-preserving Data Sharing of Directed Energy Deposition Processes

Mahathir Mohammad Bappy [a], Durant Fullington [a], Linkan Bian [a,b], and Wenmeng Tian [a,b]

[a] Department of Industrial and Systems Engineering, Mississippi State University, Mississippi State, MS 39762, United States

[b] Center for Advanced Vehicular Systems (CAVS), Mississippi State University, MS 39762, United States

Abstract

In collaborative additive manufacturing (AM), sharing process data across multiple users can provide small to medium-sized manufacturers (SMMs) with enlarged training data for part certification, facilitating accelerated adoption of metal-based AM technologies. The aggregated data can be used to develop a process-defect model that is more precise, reliable, and adaptable. However, the AM process data often contains printing path trajectory information that can significantly jeopardize intellectual property (IP) protection when shared among different users. In this study, a new adaptive AM data deidentification method is proposed that aims to mask the printing trajectory information in the AM process data in the form of melt pool images. This approach integrates stochastic image augmentation (SIA) and adaptive surrogate image generation (ASIG) via tracking melt pool geometric changes to achieve a tradeoff between AM process data privacy and utility. As a result, surrogate melt pool images are generated with perturbed printing directions. In addition, a convolutional neural network (CNN) classifier is used to evaluate the proposed method regarding privacy gain (i.e., changes in the accuracy of identifying printing orientations) and utility loss (i.e., changes in the ability of detecting process anomalies). The proposed method is validated using data collected from two cylindrical specimens using the directed energy deposition (DED) process. The case study results show that the deidentified dataset

significantly improved privacy preservation while sacrificing little data utility, once shared on the cloud-based AM system for collaborative process-defect modeling.

Keywords: Additive manufacturing, cloud manufacturing, deidentification, intellectual property, process-defect modeling, privacy-preserving data sharing.

1 Introduction

Additive manufacturing (AM) technologies have demonstrated their unprecedented capacity and flexibility in new product prototyping, component repair, and product fabrication [1]. Unfortunately, process uncertainty is still a major challenge in AM adoption, and various machine learning-based process-defect modeling methods have been developed for process monitoring and anomaly detection [2], [3]. Due to the high complexity and large variety of part designs and process parameters, a large amount of training data is usually needed to develop reliable machine learning models for anomaly detection [4]–[6]. Nevertheless, it is prohibitively expensive for a lot of AM users, especially small-to-medium manufacturers (SMMs), to gather a large dataset to train the machine learning algorithms [7]–[9], which is especially true for metal-based AM processes (e.g., directed energy deposition (DED)).

A collaborative manufacturing platform poses an unprecedented opportunity for connecting multiple AM resources with various AM users, which will naturally promote training data availability [10]. This platform integrates multiple physical AM machines and their AM process data to meet the needs of demographically diverse AM users for component fabrication and *in-situ* process monitoring and part certification. This is accomplished by the cloud technology which allows for AM data sharing, storage, and modeling [11], [12]. As illustrated in Figure 1, a cloud-based AM platform may provide AM machine access to all users [7],[13]. More specifically, users may send their component designs and g-codes to the networked machines for fabrication, with process data being collected and aggregated for process-defect modeling [10], [14]. The aggregated data and the resulting models can be subsequently shared, providing anomaly detection solutions to all AM users, especially ones with limited data availability and AM process knowledge [4], [5].

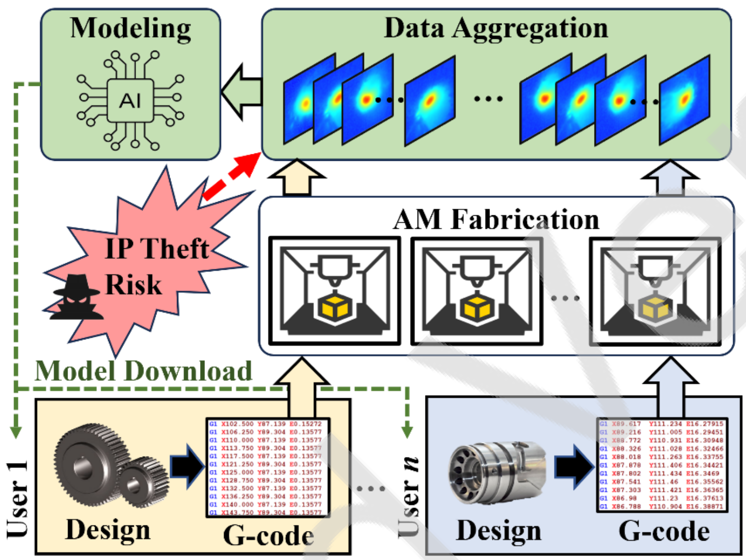


Figure 1: Overview of AM data sharing for collaborative modeling

However, some AM process data (such as thermal imaging data) also contains critical product design information [8], that must be carefully protected when shared on the data-sharing platform. Otherwise, as demonstrated in Figure 1, malicious attackers or users can extract confidential information related to the product intellectual property (IP) from AM process data, leading to severe consequences for both manufacturers and their clients [15]–[17]. Two prime examples of cyber-attacks which may occur during the AM data sharing include: (i) *Privacy breaches:* a reidentification attack [18], [19] targeting process data may lead to severe privacy breaches [20], [21], allowing unauthorized access to the product IP information, including manufacturing parameters and design specifics. Such breaches pose a significant risk, potentially compromising proprietary processes and unique manufacturing techniques; (ii) *Insider threats:* malicious insiders with access to the process data may intentionally disclose product IP or design information for personal gain or sabotage [22]. To address these risks, it is essential to develop a tool for privacy-preserving AM process data sharing to facilitate knowledge exchange while masking product design information in the shared data [23]. To be more specific, data privacy and utility are defined as follows in the context of AM process data:

AM Process Data Privacy refers to the capability in masking the printing trajectory information in the thermal image data shared with external collaborators, and thus preventing the re-identification of product design. It can be measured by the accuracy of a machine learning model in identifying the printing path orientation, conditioned on a specific type of machine learning models. The higher the accuracy is, the lower the data privacy will be.

AM Process Data Utility denotes the overall usability of the dataset for specific modeling purposes (e.g., process-defect modelling) once shared and aggregated. It is assessed by a machine learning model's ability to accurately detect anomalies using the process data, conditioned on a specific type of machine learning models. The higher the accuracy is, the higher the data utility will be.

It is important to note that the outcomes of data privacy and data utility are dependent on the specific machine learning model used for evaluating the AM datasets. Once the process data are processed to achieve a balanced level of privacy and utility, the combined dataset can be shared and utilized for collaborative process-defect modeling. In addition, the data heterogeneity caused by different original equipment manufacturers (OEMs) and other AM system specifications may be addressed by transfer learning techniques, which are widely used in learning across various yet relevant domains [8].

The objective of this study is to deidentify the product design information (manifested as the printing path orientation) in the AM thermal history, while simultaneously retaining the attributes for process-defect modelling. An adaptive AM data deidentification methodology is proposed to achieve this goal. The proposed method will generate surrogate thermal images to secure the sensitive printing path orientation information in AM thermal history data, and thus facilitate privacy-preserving and utility-aware process-defect modelling on the collaborative AM platform.

It is worth noting that a commonly used approach of protecting sensitive data and improving data privacy is the use of a *multi-layered* protection framework, where a variety of complimentary protection techniques are integrated to provide more robust protections against data privacy breaches and IP theft [24]–[26]. Our research specifically aims to develop one layer of protection focused on using deidentification for enhanced IP protections in AM process data sharing. This topic is relatively underrepresented in current literature focused on IP protections, and it provides a potential way to remove confidential design information from AM process data while simultaneously working to ensure that the data is still usable for quality control purposes.

The *technical contribution* of this paper is developing a novel, adaptive AM thermal process data deidentification algorithm. The proposed method can adaptively enhance the privacy of the dataset by deidentifying thermal images while maintaining the utility of the AM process data for anomaly detection. This can be achieved through two iterative steps: stochastic image augmentation (SIA) and adaptive surrogate image generation (ASIG). SIA involves random rotations of melt pool images to obscure the printing path trajectory and sensitive design information based on the validated premise that melt pool orientation is key to inferring AM process directions. ASIG then generates a surrogate image by averaging the SIA-generated images, with adaptiveness enabled by monitoring changes in melt pool geometric features (such as melt pool area) compared to the original image. These geometric features are crucial for anomaly detection, allowing the surrogate images to retain the necessary utility for process-defect modeling. By dynamically tailoring the deidentification process to the sensitivity of the melt pool image's geometric features, the method ensures that critical attributes essential for anomaly detection are preserved while simultaneously enhancing privacy. The *impacts* of the proposed method are two-fold. For the AM quality control area, this method opens the venue for privacy-preserving data sharing for AM process-defect modelling. For industrial practices, using shared process data facilitates the development of cross-system *in-situ* process-defect models. As a result, the enhanced *in-situ* quality control tools can promote optimized resource allocation for post-manufacturing inspection, which is usually very costly and sometimes cumbersome for AM components [27], [28]. These will collectively lead to accelerated adoption of AM technologies in various industrial practices.

The remainder of the paper is organized as follows. In section 2, the relevant state-of-the-art studies are summarized, and the research gaps are identified. In section 3, the proposed adaptive deidentification methodology is introduced, and in section 4, a case study based on the directed energy deposition (DED) process is used to evaluate the effectiveness of the proposed methodology. Finally, the conclusion and future work are introduced in section 5.

2 Literature Review

This section summarizes the complexities of data privacy and IP protection within AM. Section 2.1 highlights the state-of-the-art strategies and remaining challenges in protecting confidential information in AM. The specific IP protection needs in AM data are analyzed in Section 2.2. Advancements in image data deidentification for enhancing privacy in AM data sharing are discussed in Section 2.3. Finally, through a research gap analysis (Section 2.4), opportunities for further investigation and development are identified to advance knowledge and practices in data privacy in the field of AM.

2.1 Current Solutions and Challenges of Data Privacy and IP Protection in AM

The data security and privacy preservation in cloud-based manufacturing systems is becoming increasingly important for individual users who are participating and sharing information in these frameworks. In terms of data privacy, IP is a closely related aspect [29], especially within AM applications. When sharing AM process data (e.g., thermal history), IP theft can occur through re-identification and reverse engineering attacks, where critical design related information is embedded into the process data. From there, the sequential print trajectories and layer-wise patterns can be directly leveraged to extract the product design geometry [9]. The connection between the AM process data (especially thermal process data) and printing path trajectories has been highlighted in several recent works [9], [30], [31]. These works have highlighted this critical vulnerability, emphasizing the need to review and develop IP protections for AM process data. These protections must be tailored to the unique needs of AM applications. Both data-level and model-level strategies have been used for IP protection.

Various data-level operations used in IP artifacts protection include *watermarking, access control, cryptography-based methods,* and *anonymization.* For these four commonly used methods, their characteristics, working mechanisms and corresponding limitations are summarized below. *Firstly,* watermarking and access control measures are indirect approaches of IP protection [32]–[35]. For example, watermarking generally embeds a unique mark on the digital or physical artifact that identifies the source and ownership of the product IP [33], [35]. This ensures that ownership of the design and information is clearly identifiable; however, this method does not prevent the information from being accessed or used in a malicious manner. In addition, access control aims to prevent unauthorized access to the data by controlling access and managing the storage of sensitive data [36]. However, access control does not add any direct protection to the data. Several limitations and challenges for access control include compromised credentials, malicious insiders, and even human errors [37], [38]. *Secondly*, cryptography- and anonymization-based approaches aim to provide data-level protection by directly manipulating the data in an either reversible or irreversible manner. For example, cryptography-based methods, most employed as encryption methods, cover a family of different approaches aimed at obscuring information into an unrecognizable state using an encryption key. After encryption, the intended party is able to access the original information only if they have the corresponding decryption key [39]–[42]. This allows the data to be transformed into a protected state, where it can be difficult for someone to maliciously access the data and re-identify IP embedded in the data. Despite of the increasing popularity of encryption methods, such as homomorphic encryption [43], they demonstrate a few notable limitations. Firstly, the use of encryption and decryption keys presents an added security vulnerability to the system [44], [45]. If the right decryption key is obtained through an attack, such as a brute-force attack [46], [47], the protected data can be directly accessed and the IP information stolen. Furthermore, encryption algorithms can be highly complex, which requires a large pool of resources, and can also potentially limit computational capabilities on the encrypted data [48].

An alternative method for enhancing IP protections is anonymization, also referred to as *deidentification*. The objective of anonymization is to remove or obscure the confidential information contained within the dataset in a non-reversible manner [49], [50]. This approach has been leveraged in a wide range of privacy-related applications, including in healthcare and facial image anonymization [51], [52]; however, it also provides a strong potential to provide direct IP protections for AM data sharing applications. Through anonymization, the sensitive information is obscured so that the availability of sensitive, IP-related information is severely limited, while simultaneously maintaining the original structure and usability of the data [52]. In general, there are two key limitations to the use of anonymization, including (1) the balance and tradeoff between improved protections and decreased data usability, where anonymization can lead to potentially degraded performance of the data in downstream tasks [53], [54], and (2) the threat of re-identification attacks [55], [56], which can potentially identify compromising data post-anonymization.

In addition to the data-level approaches, there are also model-level techniques to ensure data privacy and IP protection, including federated learning (FL) and differential privacy (DP). FL methods offer additional layers of security by enabling collaborative learning without sharing raw data [57], [58]. Specifically, FL allows multiple entities to collaboratively train a model without sharing raw data, significantly reducing the risk of data breaches and maintaining privacy by keeping data decentralized [57], [59]. However, FL can be challenged by the heterogeneity of data across different entities, leading to potential biases and discrepancies in model performance. Additionally, the communication overhead between entities can be significant, affecting the efficiency and scalability of the approach [60], [61] .

On the other hand, DP introduces noise to the data or the learning process to prevent the extraction of sensitive information from the outputs [62]. This technique ensures that individual data points cannot be distinguished from aggregate data, providing strong privacy guarantees even if the model outputs are accessed [63], [64]. DP, while providing strong privacy guarantees, can impact the accuracy of the ML models due to the added noise, making it critical to balance privacy and utility effectively [65],[64].

2.2 IP Protection Needs in AM Data

There are diversified data streams generated in the AM production. Properly categorizing these data according to their relevance to the product IP information is essential for effective data management and IP protection in AM [9], [66]. The key AM data can be categorized into three different types of attributes, as summarized in Table 1. More information regarding this categorization of the AM attributes can be found in [9].

Table 1: Key categorizations for AM attributes

Attribute	Description	Example AM Features
Sensitive Attribute	Attributes that directly relate to compromising design data and pose a significant risk of IP disclosure.	• Design Files (CAD) • G-code Files • Print Trajectory Information • Complete Thermal History
Quasi-identifier	Attributes that do not pose a significant IP disclosure risk, but compromise product IP information when used with other attributes.	• Single Thermal Images • Individual Pixels • Layer Location • Image Index
Insensitive Attribute	Attributes that do not relate to the design information in any capacity.	• Quality Control Labels • Extracted Descriptive Features

Given this categorization, the complete thermal history is considered as a sensitive attribute and thus needs to be protected before sharing with other users. Otherwise, the product IP can be disclosed to external users. For instance, during part fabrication using DED process, the *in-situ* thermal history can be collected in the form of thermal images for process monitoring and anomaly detection [27], [28]. As shown in Figure 2, the sensitive attributes of thermal history data include the printing trajectory that can be extracted from the images, as this information can be used to reversely decipher the global print path and part design. This is similar to the idea of side-channel attacks in AM, which can be used to infer critical design and process information, leading to significantly compromised IP [46], [67]. As thermal history data are highly informative for defect detection and process monitoring, there is an urgent need in effective masking and deidentification of the thermal history data before sharing for modelling purposes [68]–[70]. Moreover, during the deidentification to mask the IP information, it is important to note that there is usually a tradeoff between data privacy and the resulting data utility [71]. This tradeoff is very important, as thermal history plays a significant role in metal-based AM process monitoring. In general, applying a naïve or too obstructive deidentification method, such as pixilation or blurring, can result in a drastic loss in AM process data utility for anomaly detection [72], [73]. Therefore, there is a critical need to ensure a balance between AM process data privacy and AM process data utility during deidentification.

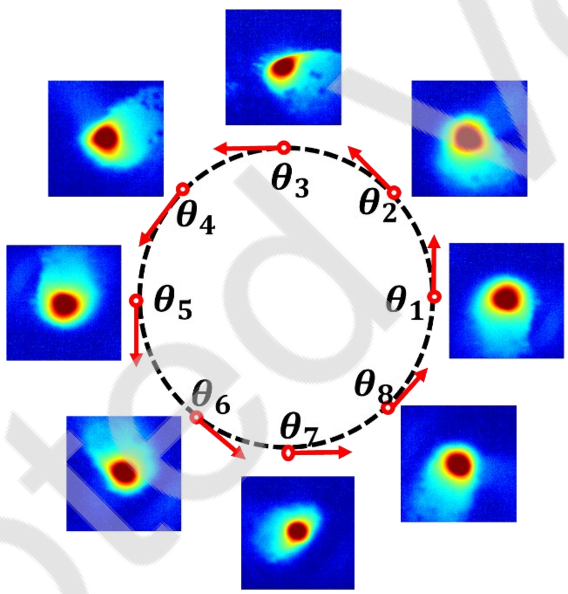


Figure 2: Printing path trajectories that can be derived from the melt pool images, where θ_t represents the instantaneous printing direction inferred from each image ($t = 1,2,\dots,8$).

2.3 Image Data Deidentification for Privacy-preserving Data Sharing in AM

The deidentification, commonly known as anonymization, is an attractive solution that has the potential to achieve the goal of data privacy and IP protection [74]. In general, image data anonymization methods transform the original images to remove the sensitive information while retaining the useful features of interest to preserve user data privacy [75]. It depends on the information that should be removed/anonymized, and on the information that should remain.

However, balancing utility with anonymity presents significant challenges. Considering this, to promote data privacy while maintaining data utility, various image data (i.e., face) deidentification algorithms have already been developed [50], [72], [76]–[80]. Moreover, the deidentification methods exhibit unique strengths of (i) non-reversibility in traditional applications with less impacts on data usability [79],[81]; (ii) providing data privacy without necessitating the complex structures and systems (i.e., encryption keys) [82]. Furthermore, deidentification can be strategically employed as part of a layered approach to security, alongside other traditional security measures, to enhance its effectiveness [74], [83], [84]. Ultimately, the utility-awareness and privacy-preserving nature of data deidentification makes it a compelling solution, especially in collaborative environments.

Recently, a novel adaptive design deidentification method was developed to deidentify AM process thermal images by integrating AM process knowledge to isolate and combine the most similar images to better mask the printing path trajectory while simultaneously preserving data usability [9]. This method demonstrates good performance; however, it leverages a pre-defined reference dataset to perform deidentification. Because of the use of this external reference set, the privacy gain is directly proportional to the diversity, quality and size of the reference data set [9]. Even though there has been advancement in this field, further study is required to develop effective AM process data deidentification methods, and reliable methods to incorporate them into the AM workflow in cloud-based AM systems.

2.4 Research Gap Analysis

Considering the limitations of different data privacy and IP protection techniques, applying a multi-layered approach is generally more advantageous [25], [85]. In the AM domain, most research has focused on techniques like encryption-based approaches. However, less research has been conducted to developing de-identification-based methods. Exploring de-identification for AM applications can fill this research gap and enhance IP confidentiality protections. The proposed work aims to develop de-identification-based data privacy measures, offering an additional layer of security for AM process data shared in cloud-based systems. Specifically, de-identification-based techniques are well-suited for thermal image data sharing, as they can mask sensitive IP information embedded in the dataset [63]. Despite progress, gaps remain in protecting sensitive information in AM process images, summarized as follows:

1) The dynamic properties of thermal images make implementing global de-identification methods extremely difficult.
2) Limited data availability and recurring angular identities in thermal images challenge the application of existing de-identification methods.
3) Evaluating AM-based de-identification methods is challenging due to their dependency on the quality of the reference image set.

Therefore, developing a new adaptive thermal history de-identification method that better balances data privacy and utility without requiring a reference dataset is essential. This method can ultimately enhance the privacy of printing path-related design information, reinforcing the protection of sensitive information in the AM data sharing platform.

3 Proposed Methodology

The proposed method can adaptively deidentify the instantaneous printing path from each individual image to enhance AM process data privacy, creating a surrogate melt pool image for each original image. More specifically, the generation of the surrogate melt pool image involves stochastic image augmentation (SIA) and adaptive surrogate image generation (ASIG) which are coordinated by the monitoring mechanism of the melt pool geometric feature. The ***rationale*** of the proposed method is based on the process knowledge of DED processes where the printing direction governs the melt pool orientation. Therefore, the random rotation operations in SIA directly perturb the angular orientation of each melt pool, significantly enhancing the obfuscation of the printing path trajectory. Subsequently, ASIG adaptively averages the multiple randomly perturbed melt pool images to generate the surrogate image, where the melt pool geometric features are leveraged as a stopping criterion for the perturbation. Both SIA and ASIG significantly raise the barrier for extracting sensitive design information in the original melt pool images.

Figure 3 illustrates the framework of the proposed methodology and the visualization of the results at each step. The key components of Figure 3 are summarized as follows: (a) illustrates a step-by-step workflow of the proposed method; and (b) through (f) illustrate the visualization of the results obtained at each step, respectively. In Figure 3, $\mathbf{I}^t$ and $\mathbf{X}^t$ $(t = 1,2, \dots n)$ denote the original and centered image collected at time t, respectively. $\mathbf{X}^t(\theta_m)$ denotes the rotated images with the randomly generated target orientation θ_m $(m = 1,2, \dots 9)$, and $\mathbf{S}_{(m)}^t$ denotes the surrogate thermal image. The absolute geometric feature change can be calculated as $\left|g\left(\mathbf{S}_{(0)}^t\right) - g\left(\mathbf{S}_{(m)}^t\right)\right|$ where $g(\cdot)$ denotes the function to compute the melt pool geometric feature of $\mathbf{S}_{(m)}^t$. m_t^* represents the optimal number of artificial images used for generating the surrogate image for $\mathbf{X}^t$, and the λ value is a predefined threshold that governs the maximum allowable geometric feature change, balancing privacy and utility. A larger λ improves privacy by incorporating more SIA-generated images, but excessive values can cause significant changes in melt pool geometry.

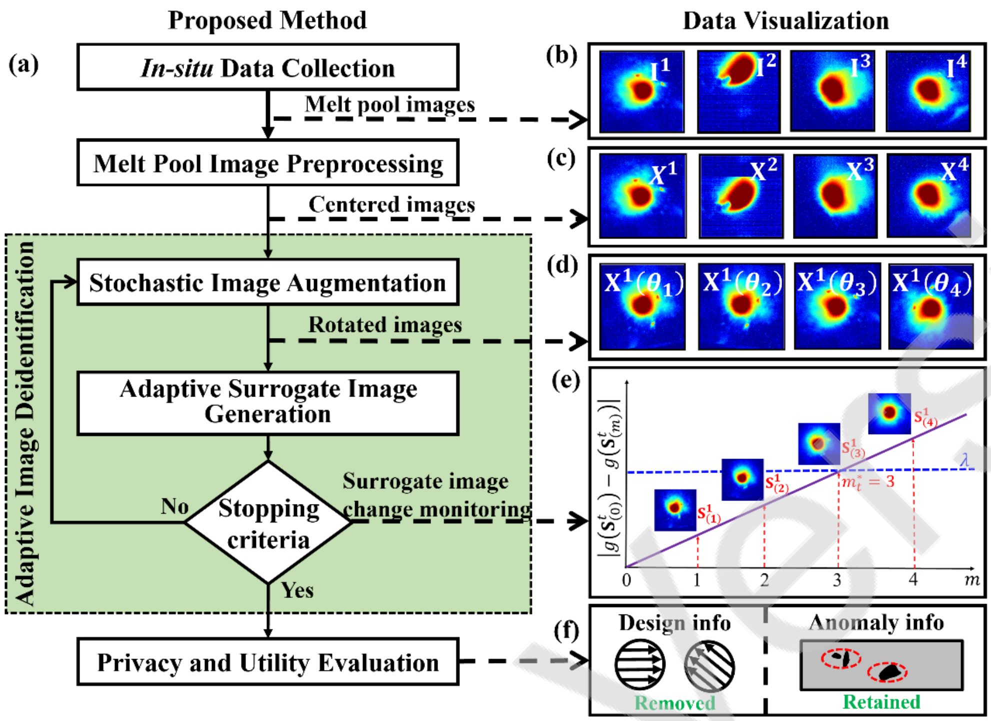


Figure 3: Overall workflow of the proposed methodology.

3.1 Preprocessing of Melt Pool Images

Let $\mathbf{I}^t \in \mathbb{R}^{r \times c}$ denote the original melt pool image captured at time t, which is an $r \times c$ dimensional matrix with the temperature measurement stored at each pixel. Each melt pool images are firstly pre-processed through the centering operation, where the melt pool of each image is shifted to the center of the field of view. Essentially, this centering operation removes the peak temperature location variability and thus reduces its impact on the geometric attributes of melt pool. In this sense, the geometric features of the surrogate images will have a shared baseline and are only determined by the adaptive image deidentification. Specifically, the centering operation is illustrated in Figure 3(c), and the resulting image (denoted as $\mathbf{X}^t$) can be obtained using the Equation (1),

$$\mathbf{X}^t = C\left(\mathbf{I}^t, \left(\left(\left\lfloor\frac{r^t}{2}\right\rfloor - p_r^t\right), \left(\left\lfloor\frac{c^t}{2}\right\rfloor - p_c^t\right)\right)\right) \quad (1)$$

where $\mathbf{X}^t \in \mathbb{R}^{r \times c}$ denotes the centered image and the function $C(\cdot,\cdot)$ denotes the image translation operation [86] with the corresponding image and translating vector of $\left(\left(\left\lfloor\frac{r^t}{2}\right\rfloor - p_r^t\right), \left(\left\lfloor\frac{c^t}{2}\right\rfloor - p_c^t\right)\right)$. Here, $\left\lfloor\frac{r^t}{2}\right\rfloor$ and $\left\lfloor\frac{c^t}{2}\right\rfloor$ denotes the row and column coordinates for center point of the field of view, which is the target coordinates that the peak temperature location of the melt pool is moved to. In addition, p_r^t and p_c^t denotes the row and column coordinates of the original peak temperature location in $\mathbf{I}^t$.

3.2 Adaptive Image Deidentification

The proposed adaptive image deidentification algorithm is accomplished by integrating two iterative steps, i.e., stochastic image augmentation (SIA) and adaptive surrogate image generation (ASIG). Specifically, SIA technique is implemented through random rotation to change the orientation of the melt pool within an image, making it difficult to identify the nominal printing path trajectory or infer any sensitive design information based on its orientation. This SIA scheme is under the premise that the melt pool orientation is the major feature to infer the instantaneous printing directions of the AM process. This premise has been validated in the literature for layer-wise thermal image time series analysis [27], [87]. Moreover, the ASIG is applied to generate a surrogate image by averaging the multiple SIA-generated images. The adaptiveness of ASIG is enabled by monitoring the melt pool geometric feature changes in the surrogate image from its original counterpart. The geometric features of melt pools, such as melt pool area, are critical process features for anomaly detection without AM design information. Therefore, monitoring the change in the geometric features for each melt pool will assure the surrogate thermal image maintain comparable utility related information for process-defect modeling.

Definition 1. **Stochastic image augmentation (SIA):** The SIA procedure is proposed to stochastically generate artificial melt pool images which share identical melt pool geometric features with the original image by the image rotation operation. This is based on the engineering knowledge that the orientation of the melt pool is the major feature that discloses the printing trajectory information in the thermal history. The formulation of SIA is illustrated in Equation (2).

$$\text{SIA:} \qquad \mathbf{X}^t(\theta_m) = R(\mathbf{X}^t, \theta_m) \qquad \theta_m \sim \mathrm{Unif}(0, 2\pi) \tag{2}$$

where $\mathbf{X}^t(\theta_m) \in \mathbb{R}^{r \times c}$ denotes the SIA generated image in the m-th iteration. The function $R(\cdot,\cdot)$ denotes the image rotation operation given the original image $\mathbf{X}^t$, and the randomly generated target orientation θ_m with $(m = 1,2, \dots 9)$, sampled from a uniform distribution ranging from 0 to 2π.

In the proposed algorithm, the ASIG is established to iteratively synthesize the SIA generated images one by one, as illustrated in Equation (3). The stopping criteria for image synthesis is based on the similarity of the melt pool geometric features of the synthesized image $\mathbf{S}^t_{(m)}$ compared with the original image $\mathbf{S}^t_{(0)}$, as illustrated in Equation (4).

$$\text{ASIG:} \qquad \mathbf{S}^t_{(m)} = \begin{cases} \mathbf{X}^t, & m = 0 \\ \frac{(m-1)\mathbf{S}^t_{(m-1)} + \mathbf{X}^t(\theta_m)}{m}, & m = 1,2,3 \dots \end{cases} \tag{3}$$

$$\text{Stopping Criteria:} \qquad m_t^* = \min\left\{ m \,\middle|\, \left| g\left(\mathbf{S}^t_{(0)}\right) - g\left(\mathbf{S}^t_{(m)}\right) \right| \geq \lambda \right\} \tag{4}$$

where $\mathbf{S}^t_{(m)} \in \mathbb{R}^{r \times c}$ represents the surrogate thermal image, which takes an average of the m SIA generated images $\mathbf{X}^t(\theta_m)$, obtained in Equation (2). As the m value increases, more diversely rotated images are averaged to generate $\mathbf{S}_{(m)}^{t}$, resulting a better masking of the original printing orientation in $\mathbf{X}^{t}$. In the meantime, an excessively high value of m may lead to a significant change in the melt pool geometry. This will affect the process data utility, since the melt pool geometric features, especially the melt pool area, are strongly correlated with the anomaly related information [8], [88], [89]. Therefore, a melt pool geometry-based stopping criterion is incorporated in Equation (4), where g(·) denotes the function to compute the melt pool geometric feature of $\mathbf{S}_{(m)}^{t}$, such as area, eccentricity, major axis length, and minor axis length. The geometric properties of melt pool images are determined through a two-step process. First, the melt pool images undergo binarization to distinguish between the two regions above and below the melting temperature of the feedstock material. This binary transformation identifies the melt pool region in the image, and the specific geometric features of the melt pool region can be calculated using methods in [90]. The flow diagram of melt pool geometric feature extraction is demonstrated in Figure 4.

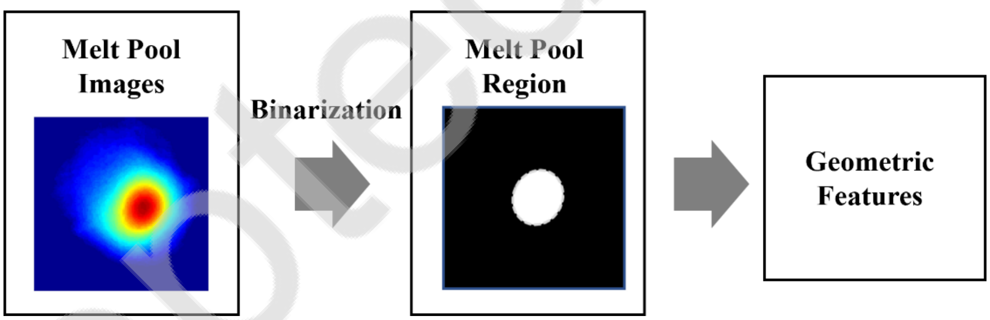


Figure 4: Flow diagram of melt pool geometric feature extraction.

Figure 3 (d) and (e) also demonstrate the workflow involved in image augmentation and surrogate image generation. The first row includes the original image (when $m = 0$), followed by SIA generated images ($m = 1, 2, 3$). During SIA, the randomly generated θ_m values change with each iteration m, altering the printing path trajectory. Subsequently, the surrogate images are generated by averaging the SIA generated image series. Combining more SIA generated images in the surrogate image can better hide the original printing trajectory, but it may also alter the geometric attributes of the melt pool from its original form, which have impact on data usability. To address this, a stopping criterion is introduced to specify the maximum allowable change in the geometric attributes of the melt pool.

Furthermore, in Equation (4), m_t^* denotes the optimal number of artificial images used to generate the surrogate image for $\mathbf{X}^t$. In addition, the λ value is a pre-defined threshold or stopping criteria that provide the maximum allowable value of the geometric feature change. Proper selection of the λ value can achieve the trade-off between AM process data privacy and utility. For a better privacy gain, a larger λ value is usually preferred, as it allows for more SIA generated images being incorporated into the surrogate image. However, a larger λ value may lead to a dramatic change in the melt pool area compared to the original melt pool, and therefore it cannot be too big in order to avoid significant change in the melt pool geometric features. In the case study, we examined the impacts of the λ value on the resulting average m_t^*.

The proposed iterative method will assure effective use of the SIA generated images, since it will guarantee that $(m_t^* - 1)$ SIA generated images are used in the final surrogate melt pool image. The ASIG method is designed under the working hypothesis that the series of the absolute geometric feature change, i.e., $\left| g\left(\mathbf{S}_{(0)}^t\right) - g\left(\mathbf{S}_{(m)}^t\right) \right|$, will be non-decreasing as m gets larger (as illustrated in Figure 3(d)). This hypothesis is realistic since the more SIA generated images involved in ASIG, the more different $\mathbf{S}_{(m)}^t$ will be from $\mathbf{X}^t$.

3.3 Surrogate Image Post-processing

The resulting surrogate images $\mathbf{S}^t(m_t^*)$ may possess some undesirable image artifacts due to the image rotation operation in SIA. Those artifacts usually present in the background of the melt pool images with lower temperature measurements. Therefore, the image thresholding technique can be employed to remove these artifacts. Therefore, the $\mathbf{S}^t(m_t^*)$ is processed with the soft thresholding operation to obtain the final deidentified surrogate images based on the Equation (5) as follows;

$$\mathbf{Z}^t = \begin{cases} \mathbf{S}^t(m_t^*) - T_0, & \text{if } \mathbf{S}^t(m_t^*) \in \mathcal{R}_u \\ 0, & \text{if } \mathbf{S}^t(m_t^*) \leq 0 \end{cases} \tag{5}$$

where $\mathbf{Z}^t \in \mathbb{R}^{r \times c}$ denotes deidentified surrogate melt pool images thresholded [27],[91] using a specified temperature range of interest $\mathcal{R}_u = [T_0, +\infty)$ with a tunable lower bound of T_0. This post-processing step can also reduce the variation in the background of the melt pool images, which will accelerate the training of machine learning algorithms for process-defect modeling.

The algorithm of the proposed methodology is illustrated in **Algorithm 1**. Each melt pool image is firstly processed through **Algorithm 1** for deidentification to generate a surrogate image, which will be shared on the platform for collaborative process-defect modeling.

Algorithm 1: SIA-ASIG Melt Pool Image Deidentification

Input: Original image set $\{\mathbf{I}^t \in \mathbb{R}^{r \times c}\}$, stopping criteria λ

Step 1: Initialization.

1.1 Center $\mathbf{I}^t$ to obtain $\mathbf{X}^t$

1.2 Set $m = 0$

Step 2: Adaptive Image Deidentification.

while $\left| g\left(\mathbf{S}_{(0)}^t\right) - g\left(\mathbf{S}_{(m)}^t\right) \right| \leq \lambda$ **do**

2.0 Set $m = m + 1$

2.1 Perform SIA to obtain $\mathbf{X}^t(\theta_m) \in \mathbb{R}^{r \times c}$ based on Equation (2).

2.2 Perform ASIG to generate $\mathbf{S}_{(m)}^t$ based on Equation (3) - (4), and

end while

Store the surrogate image $\mathbf{S}^t(m_t^*)$.

Step 3: Surrogate Image Post-processing. Post-process $\mathbf{S}^t(m_t^*)$ to obtain the deidentified image $\mathbf{Z}^t$ using Equation (5).

Output: Deidentified surrogate image set $\{\mathbf{Z}^t \in \mathbb{R}^{r \times c}\}$.

3.4 Evaluation of Deidentification Method

It is essential to examine the privacy-utility trade-off in the deidentification of AM process data. Two critical deidentification performance measures based on classification metrics are used to evaluate the design attribute deidentification performance. To assure a fair comparison, the same classifier is selected to compare the performance changes before and after the deidentification.

A convolutional neural network (CNN) is used for performance evaluation to establish the classification models for predicting anomalies and the angular identities of printing path trajectories. During evaluation, angular identities are treated as a multi-class classification problem, while anomalies are considered a binary classification task. CNN is selected for the following reasons [92]–[95]: (1) It can automatically learn spatial hierarchies of features, which is essential for capturing the intricate details in melt pool images. (2) It offers robustness to variations in image properties, such as scale and orientation. (3) CNNs can effectively handle large datasets and complex patterns, making them suitable for image analysis. (4) CNNs are capable of feature extraction and classification in a single integrated framework, simplifying the model architecture. Furthermore, CNNs have demonstrated proven success in numerous image processing applications [96], [97].

The AM data privacy performance is measured before and after deidentification using the accuracy of a CNN model in identifying the printing path orientation. Higher accuracy indicates lower data privacy. In this study, the privacy gain (PG) can be computed to evaluate the performance of deidentification by assessing the improvement in data privacy compared to the original dataset. This assessment is based on the CNN model's classification accuracy of printing orientations. Thus, the equation for AM data privacy gain can be derived as follows:

$$\mathrm{PG} = Z_{\mathrm{base}}^{\mathrm{acc}} - Z_{\mathrm{deid}}^{\mathrm{acc}} \tag{6}$$

where $Z_{\mathrm{base}}^{\mathrm{acc}}$ denotes the printing direction classification accuracy of original images and $Z_{\mathrm{Deid}}^{\mathrm{acc}}$ represents the classification accuracy after deidentification of melt pool images. In cases of PG evaluation metric, accuracy is used as the label of interests is balanced, whereas for imbalanced label information, the Fscore metric can be adopted. On the other hand, AM data utility can be defined as CNN model's ability to detect anomalies of AM process data accurately. The higher the accuracy is, the higher the data utility will be. Similarly, the utility loss (UL) can be computed to evaluate the performance of deidentification by assessing the improvement in AM data utility compared to the original dataset. The change of the anomaly classification percentage after deidentification of the melt pool images can be formulated as follows,

$$\mathrm{UL} = Z_{\mathrm{Deid}}^{\mathrm{Fscore}} - Z_{\mathrm{Base}}^{\mathrm{Fscore}} \tag{7}$$

where $Z_{\mathrm{Base}}^{\mathrm{Fscore}}$ denotes the Fscore value based on the anomaly detection results of original images and $Z_{\mathrm{Deid}}^{\mathrm{Fscore}}$ represents the Fscore percentage based on deidentified melt pool images. Here, the minimized UL is desirable to retain data utility in the surrogate melt pool images. It is worth noting that due to the imbalanced nature of the anomaly data, the Fscore metric is leveraged [9].

It is worth noting that the evaluation metrics of privacy gain and utility loss find application in various research domains beyond deidentification methods, particularly in the broader context of privacy-preserving data analysis and machine learning. In the field of differential privacy, privacy gain and utility loss serve as essential metrics for assessing the impact of privacy-preserving mechanisms on data utility[98]. Furthermore, in privacy-preserving data mining, metrics such as privacy gain and utility loss are commonly used to quantify the compromise between privacy protection and the usefulness of data for analysis [99]. Recent research also has focused on various aspects of privacy and utility trade-offs, considering the implications of different deidentification methods [8], [9], [100], [101].

4 Case Study

In this section, the proposed method is validated using the data collected from real-world experiments using the directed energy deposition (DED) process. Both the privacy gain and the data usefulness are quantified during the validation of the proposed method.

4.1 Experimental Setup and Data Description

An OPTOMEC LENS 750 machine equipped with a co-axial pyrometer camera for thermal image monitoring, as shown in Figure 5, was used to fabricate two Ti-6Al-4V cylindrical specimens. Process parameters used to fabricate the specimen are summarized in Table 2. The dimensions of the fabricated specimens are 8mm (diameter) by 90mm (length). These cylindrical specimens are commonly employed in material testing and mechanical characterization [102]. A segment of approximately 30 mm is machined and X-ray scanned for porosity analysis for each cylinder. Moreover, cylindrical specimens facilitate the exploration of diverse angular identities in the dataset which are also available in complex AM component fabrication.

The melt pool images were captured by a dual-wavelength pyrometer (Stratonics, Inc.) during part fabrication. The pyrometer has a nominal image collection rate of about 6.4 Hz. Observed thermal images are presented as matrices with each pixel recording the temperature value between 1000-2500°C. The original dimension of the thermal images is 752 by 480. To reduce the dimensions, the irrelevant regions that do not contain the melt pools were first cropped. Moreover, the g-codes of the two specimens were used to determine the instantaneous printing directions of each thermal image in both datasets. Also, because the AM thermal process data showed shifting trends with respect to the building layers, only the data after layer 20 was used to tune and test the performance of the proposed algorithm. Also, combining both datasets will result in four different angles and 2,458 images of thermal images to use for experimentation.

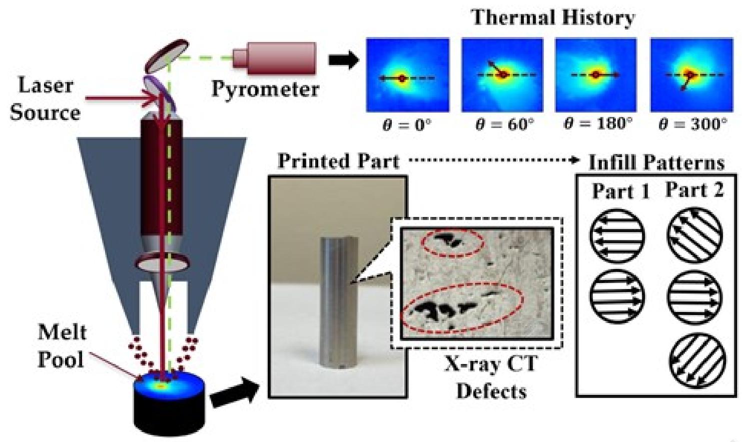


Figure 5: Experimental setup and data collected.

After the part fabrication, the specimens were inspected using a high-resolution X-ray computed tomography system (Skyscan 1172), which is capable of examining the internal structures of the AM parts with a fine resolution of 1μm. The manufactured specimens were inspected to detect any process-induced porosity. The outputs of the X-ray CT characterization were used to label the normal and abnormal melt pool images. The X-ray CT results contain the size, morphology, and location of the detected defects. It is worth noting that only Part 1, which consists of 1616 images with anomaly label information, has been inspected for internal defect detection, thus providing images for utility-related evaluation. However, both datasets combining Part 1 and Part 2, which consist of 2,458 images with angular orientation label are used to evaluate the privacy related metric.

Table 2: Process parameters used for the two parts [9].

Process Parameters	**Part 1**	**Part 2**
Scan speed	40 inch/min	50 inch/min
Powder feed rate	3 rpm	2.5 rpm
Hatch spacing	0.02 inch	0.025 inch
Power	300 W	350 W

Layer thickness	0.015 inch	0.015 inch
Number of thermal images utilized	1,616	842
Number of layers in the build	69	55
Number of anomalies	138 (6%)	N/A
Infill pattern	Unidirectional (0°/180°)	Unidirectional (60°/180/300°)

4.2 Benchmark Method Selection

In this study, two benchmark methods were considered to compare with the proposed method. Benchmark Method 1, also known as the Adaptive Design De-identification for Additive Manufacturing (ADDAM) methodology [9], incorporates AM process knowledge into an adaptive de-identification procedure. This mask the printing trajectory information in the thermal history of metal-based AM, which would otherwise reveal significant details about the printing path. The ADDAM method was selected because it has already been compared with the state-of-the-art method, which uses a global *k*-anonymization approach. This traditional approach anonymizes each sample image using a constant number of *k*-closest neighbours rather than allowing an adaptive *k* value for each image. This reflects the conventional global *k*-anonymization techniques commonly employed in past methods, particularly in *k*-same methods [9]. It is also worth noting that the ADDAM method has demonstrated better performance in both privacy gain and utility loss than the global *k*-anonymization approach. Essentially, in the ADDAM method, the application of vectorized Principal Component Analysis (vPCA) involves extracting key features from both the sample image and the reference image set. The PCA is a statistical technique widely used for dimensionality reduction, data compression, and pattern recognition [103]. In the context of image analysis, PCA helps identify the most significant patterns or features by transforming the original data into a new set of uncorrelated variables called principal components. These components capture the variance in the data, allowing for a more efficient representation. In the specific case of vPCA-based features, the technique involves vectorizing the image data, which is essentially flattening each image into a vector format. The resulting vectors are then subjected to PCA and the principal components are used as features for subsequent analysis. This process enables the extraction of key information from the images while simultaneously reducing the dimensionality of the data, making it computationally more manageable, and preserving essential patterns. Specifically, ADDAM method is developed leveraging constraints related to build layer, angular identity, and Euclidean distance [9]. These constraints are unique to their adaptive algorithm and provide two key advantages: (1) provides the ability to be tuned and incorporate user control on the trade-off of data privacy and usability. (2) works towards ensuring that the deidentification is balanced across each potential angular identity [9].

Furthermore, Benchmark Method 2, termed Thermal Image Rotation for De-identification (TIRD), centers the melt pool in the field of view of the thermal images and then rotates all images of various orientations in the same orientation. The main objective of this process is to effectively hide the original printing path trajectory information by applying one rotation operation.

For a fair comparison with the proposed method, the same image post-processing method in Section 3.3 has been applied to the surrogate images generated from both benchmark methods. After generating the surrogate images, classification techniques are applied for evaluation. The ADDAM method has been recreated using a representative grid of user-defined parameters and the same convolutional neural network (CNN) classifier framework as the proposed method to evaluate performance. Furthermore, the TIRD method applies same CNN classifier for a fair comparison with the proposed method.

4.3 Evaluation Procedure

As classification-based approach is adopted for quantification of the performance metrics of data utility and privacy, the labeling information is essential for supervised machine learning. In this case, Part 1 consists of both anomaly and printing path related label information whereas Part 2 consists of only instantaneous print orientations label. Therefore, for evaluating the data utility, the data set of Part 1 was considered whereas for privacy evaluation the combined data of Part 1 and Part 2 were leveraged. In addition, when evaluating the proposed method, the datasets of before and after deidentification were randomly split into the training (76%), tuning (10%) and testing sets (14%) in a stratified manner. Basically, the tuning dataset are leveraged to tune the λ value that is also associated with the parameter of optimal number of SIA (m_t^*). On the other hand, for the benchmark method 1 evaluation, the dataset was randomly split into the reference (30%), training (42%), tuning (14%) and testing sets (14%). In benchmark method 1, the independent reference dataset was used for the deidentification process, which basically generates the difference between the data splitting with the proposed method. While the specific data splitting may be different between the benchmark 1 and the proposed method, the evaluation metrics used to compare the performance of the methods can still be comparable. This is because the evaluation metrics are calculated based on the same percentage of the test set. Similarly, for benchmark method 2, the same data splitting is performed as in the proposed method. In addition, five replications of the evaluations for the proposed and benchmark methods were performed to assess their average performance. For clarity, the data splitting for the proposed and benchmark methods is demonstrated in Figure 6.

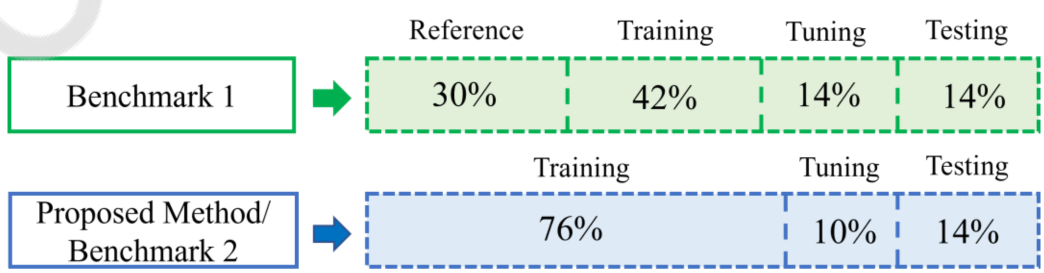


Figure 6: Data splitting for the proposed and benchmark methods [9].

The structure of the CNN is demonstrated in Figure 7. The CNN architecture for the classification of melt pool images consists of several layers designed to extract and learn hierarchical features from the input data. The network begins with an input layer, which takes in melt pool images with a size of 200 by 200. The first convolutional layer comprises 32 filters with a 3x3 kernel, followed by Batch Normalization (light blue) to normalize the activations and enhance training stability. Rectified Linear Unit (ReLU) activation (in purple) is applied to introduce non-linearity, and a subsequent Max Pooling layer with a 2x2 pool size (in green) reduces spatial dimensions, focusing on important features. The process is repeated in the second convolutional layer with 64 filters and the third with 128 filters. Each convolutional layer is followed by Batch Normalization and ReLU activation. After these convolutional layers, the network employs a Fully Connected (FC) layer depicted in light green, followed by the Softmax activation function at the output layer for multi-class classification. The input to the FC layer is obtained by flattening the output from the final convolutional or pooling layer, and the output consists of multiple neurons corresponding to the number of classes. The use of distinctive colors such as orange for convolution, light blue for Batch Normalization, purple for ReLU, green for Max Pooling, and light green for the FC layer provides a visual representation of the flow of information through the network, aiding in understanding the architecture's structure and functionality [104]. Customization of hyperparameters and layer configurations is crucial based on the specific characteristics of the melt pool image dataset and the classification task. The choice of this architecture is advantageous for several reasons. First, the use of multiple convolutional layers enables the network to hierarchically learn intricate features, promoting effective representation of melt pool patterns. Including Batch Normalization [105] enhances training stability and accelerates convergence, while ReLU introduces non-linearity crucial for capturing complex relationships. Furthermore, Max Pooling aids in retaining essential information, while reducing computational complexity. The final FC layer aggregates the high-level features for classification, and the Softmax activation function provides normalized class probabilities. This architecture aligns with the principles of effective feature extraction and hierarchical learning, making it well-suited for melt pool image classification tasks [106]. Moreover, during training phase of the CNN classifier, the random oversampling was applied both for anomaly and printing path identification, where the model learns from the augmented data and adjusts its weights to better classify the minority class of imbalanced dataset, and the Bayesian optimization technique was adopted for hyperparameter tuning [107], [108].

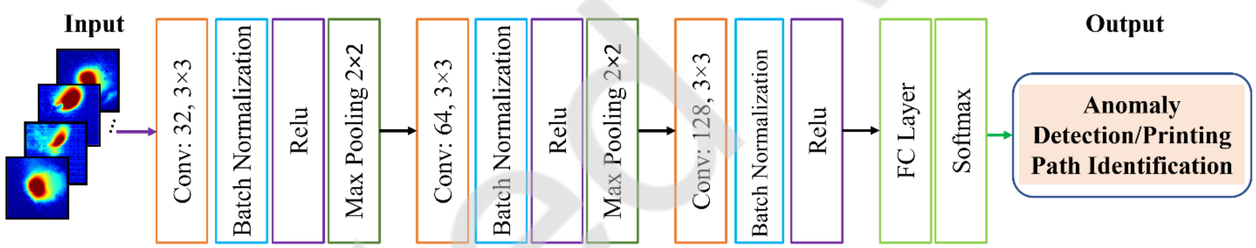


Figure 7: CNN architecture for classification.

4.4 Results and Discussion

All the evaluation used the same CNN model setup (Figure 7) for a fair comparison. Initially, the performance was determined by considering the dataset before deidentification. These results demonstrate the non-deidentified performance using the CNN classifier. Based on the non-deidentified tuning and test dataset, the results along with the standard deviation are presented in Table 3.

Table 3: Results based on non-deidentified dataset.

Method	Tuning dataset	Test dataset

	Anomaly Detection: Fscore	Printing Path Identification: Accuracy	Anomaly Detection: Fscore	Printing Path Identification: Accuracy
Proposed/ Benchmark 2	84.50 (3.67)	97.98 (0.51)	83.92 (2.64)	97.97 (0.38)
Benchmark 1	82.55 (3.73)	96.99 (0.53)	80.76 (4.53)	97.44 (0.65)

In this case study, the change in melt pool areas was leveraged to set the threshold value to obtain the deidentified images. With the change of the λ values, the optimal number of SIA (m_t^*) also changes, as depicted in Figure 8, which are then leveraged to obtain different deidentified datasets for evaluation. Specifically, Figure 8 demonstrates the average m_t^* given different threshold λ values. In addition, the error band illustrates the standard deviation of the m_t^* values for the normal and abnormal image samples, as shown in Figure 8(a) and Figure 8(b), respectively. Given the same λ values, the normal melt pool images have comparatively larger average m_t^* than the abnormal melt pool images. Here, the standard deviation values of m_t^* of the normal melt pool images are generally higher than those of the abnormal melt pool images. Moreover, the mean value and standard deviation for a normal melt pool image can increases higher than those for abnormal images due to differences in the geometric characteristics of the melt pools. In general, normal melt pools tend to have a more consistent shape and size, which leads to a larger average m_t^* with the increase of λ values. On the other hand, abnormal melt pools may exhibit more irregular shapes and sizes, which can lead to a comparatively lower mean value of m_t^* and standard deviation based on different λ values.

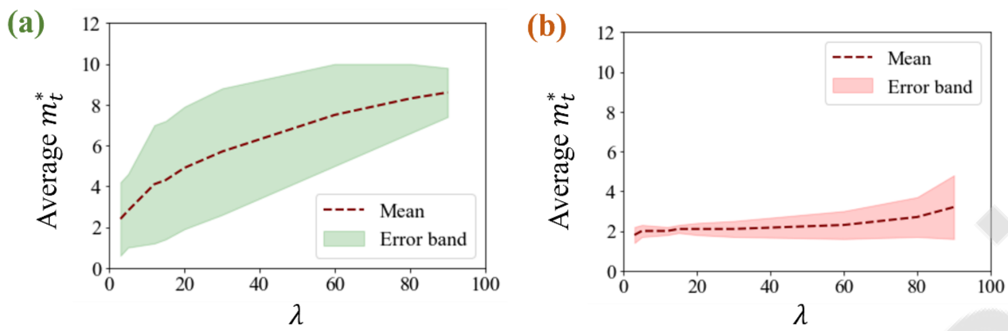


Figure 8: Illustration of the average m_t^* value over λ for samples of (a) normal and (b) abnormal thermal images.

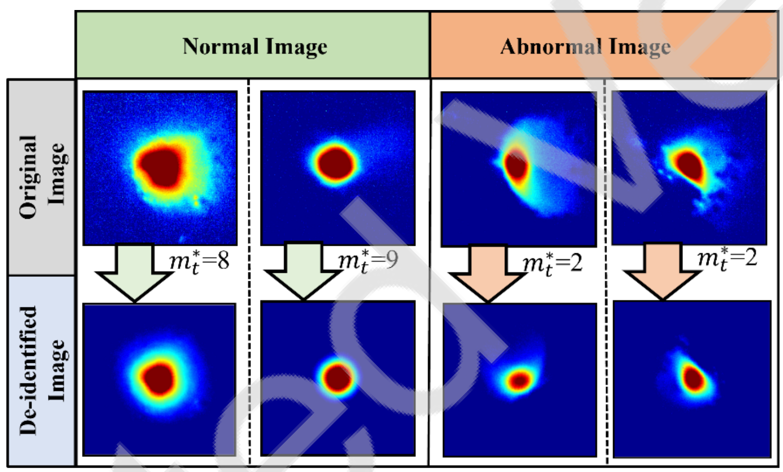
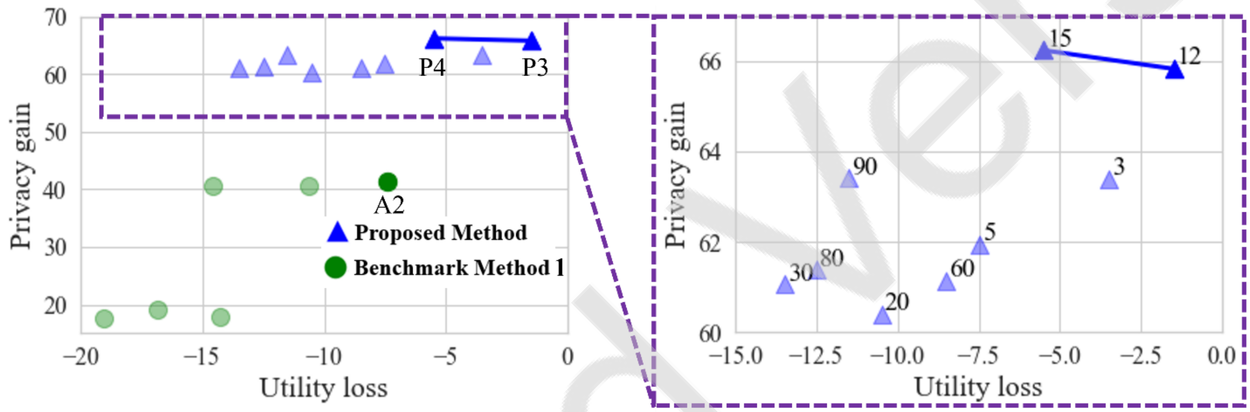


Figure 9: Surrogate images based on the proposed adaptive method.

Using the optimal value of m_t^* for each individual thermal image, the surrogate thermal images can be generated. A few example surrogate images for both normal and abnormal images are illustrated in Figure 9. It can be observed that the adaptive method alters the orientation of the melt pool as well as significantly blurs the printing path trajectory related sensitive information, which is desirable to protect data privacy. On the other hand, the geometric attributes (i.e., shape and size) of the melt pool in the deidentified images are maintained at best to preserve the utility attributes of the normal and abnormal melt pool images, which can fulfill the purpose of process defect modeling.

In this study, computing the classification accuracy and Fscore of the non-deidentified and deidentified datasets, the utility loss (UL) and privacy gain (PG) metrics were determined and demonstrated for different λ values, as illustrated in Figure 10. Regarding the proposed method, the geometric threshold, λ, plays a significant role for data deidentification and the corresponding performance metrics. Therefore, parameter tuning is very important for the performance of the proposed method. Since there are two outcomes of interest, this Pareto optimal front chart based on UL and PG was used to determine the optimal points, as depicted in Figure 10. Specifically, to generate this pareto optimal front chart, the tuning data were leveraged in the proposed algorithm to determine which parameters were optimal. As illustrated in Figure 10, each point represents a user-defined input of either λ values or M and Δl values for the proposed and benchmark method 1 [9], respectively. Thus, the points that are on the optimal front of the performance evaluation chart with a higher opacity were determined to be the Pareto optimal points. The additional points (lower opacity) are the alternative combinations of parameters that do not lie on the Pareto optimal front. These points reflect parameters that do not perform optimally when utilizing the tuning datasets and are therefore not selected to evaluate the final test performance. The specific performance and corresponding parameter values are also demonstrated in Figure 10. From these optimal points, the corresponding parameter sets were selected and then used to deidentify the testing dataset. Here, in the Figure 10, Pareto optimal front comparison is also demonstrated during the parameter tuning for the proposed method and benchmark method 1 for the different combinations of tuning parameters, which are detailed in the corresponding table. From these results, the proposed adaptive algorithm outperforms benchmark method 1 in terms of UL and PG, which are detailed in Figure 10. It is worth mentioning that benchmark method 2 does not require any user-defined parameters to be tuned. Therefore, no results need to be included in the optimal front charts for this method. Furthermore, the results in the Figure 10 demonstrate that the proposed adaptive algorithm is able to more effectively secure the sensitive design information in the process data for sharing within an AM platform. In the context of privacy preservation, the adaptive deidentification method's superior performance implies a more effective means of protecting sensitive design information while sharing thermal history data with other users.



Proposed Method				Benchmark Method 1				
#	λ	UL	PG	#	M	Δl	UL	PG
P1	3	-3.5	63.4	A1	1	1	-14.25	17.78
P2	5	-7.5	61.95	A2	1	10	-7.39	41.42
P3	12	-1.5	65.83	A3	1.1	1	-16.85	19.03
P4	15	-5.5	66.24	A4	1.1	10	-14.57	40.51
P5	20	-10.5	60.41	A5	1.25	1	-19.03	17.61
P6	30	-13.5	61.06	A6	1.25	10	-10.65	40.57
P7	60	-8.5	61.14					
P8	80	-12.5	61.38					
P9	90	-11.5	63.41					

Figure 10: Pareto optimal fronts with parameter tuning based on tuning dataset.

Based on the pareto optimal front chart, optimal points are determined. Furthermore, with the optimal geometric threshold values, the corresponding parameter sets (i.e., m_t^*) were determined for each image to deidentify the test dataset, which were used for performance evaluation. The test results are summarized in Table 4. The scale ranges from 0 to a 100 for PG and from 0 to a negative 100 for UL. It is important to note that, in the context of both PG and UL, a higher numerical value indicates a desirable outcome. Therefore, these scales provide a clear and intuitive framework for evaluating and interpreting those performance measures.

The key strength of the proposed adaptive deidentification algorithm is its ability to preserve data usability through a smaller UL with a significantly improved privacy gain (PG). The benchmark methods 1, 2, and proposed method can be compared based on the results of the test datasets, as shown in Table 4. From Table 4, it is observed that the proposed method is able to achieve a noticeable improvement in privacy gain while maintaining a comparable, and even slightly better utility loss than the benchmark method 1. Specifically, the proposed method outperforms benchmark method 1 in terms of PG while achieving comparable performance in terms of UL. Similarly, when comparing the results of the proposed method with benchmark method 2, it is observed that the proposed method significantly outperforms in terms of PG, while demonstrating comparable results in terms of UL.

Table 4: Results summary based on test dataset (standard deviation in the parentheses).

Method	Pareto optimal points	UL	PG
Proposed	P3	-2.40 (9.13)	57.51 (7.77)
	P4	-6.42 (6.79)	**61.59 (4.00)**
Benchmark 1	A2	-6.51 (5.62)	39.18 (4.63)
Benchmark 2	--	**-1.89 (2.72)**	0.70 (1.55)

The improved performance of both the UL and PG of the algorithm can be attributed to the following reasons. First, in the proposed adaptive deidentification method, each melt pool image is deidentified using the SIA generated images, which significantly blurs the printing path trajectory related sensitive information while retaining utility attributes at best. Second, the benchmark method 1 requires as a large and diverse reference set to facilitate deidentification of the thermal images. Therefore, the performance of the deidentification model is highly dependent on the diversity, size, and quality of the reference image set. In this experimentation, the reference set is sacrificed from the training data, ultimately reducing the training data set and leading to a smaller and less diverse reference set. The difference in available training data between the benchmark 1 and proposed method can also explain the variation in the results of the model, as model performance is known to be more sensitive to the amount of training data.

Similarly, from Table 4, it is observed that for benchmark method 2, there is little PG with a smaller UL, failing to fulfill the intended purpose of data deidentification. To demonstrate the potential reason for this minimal PG, Figure 11 includes images before and after deidentification. Basically, in this case, the deidentified images are rotated 90 degrees to remove the printing path trajectory, generating unified orientation images. Despite the intention to create these unified orientation images, it is evident that each class of images after deidentification retains some directional patterns with their tail and melt pool. Due to these patterns, the images can be accurately classified into their associated class labels, explaining the minimal PG for benchmark method 2.

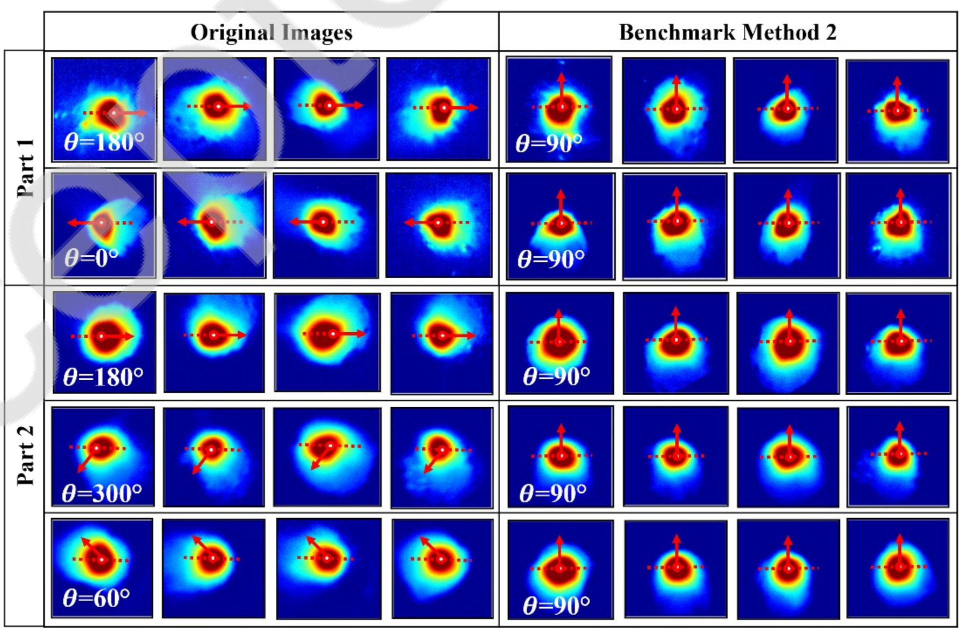


Figure 11: Demonstration of images before and after deidentification along with their angular orientations leveraging benchmark method 2 for Part 1 and Part 2 (the orientations of the images in a row are denoted in the first image).

Furthermore, leveraging the concept of Benchmark Method 2, the datasets from Part 1 and Part 2 were separately utilized to evaluate PG. The results demonstrate very little PG compared to the original images. Specifically, for Part 1, the PG is -1.59%, and for Part 2, the PG is 2.49%. Even with separate datasets, the results did not improve. One of the potential reasons for this is that, for each individual class label, the melt pool region above the melting point temperature and the tail region of the heat-affected zone exhibit specific identifiable orientations and shapes that differ for each class label, as demonstrated in Figure 11 for Part 1 and Part 2. Another potential reason is the very small number of angular classes, which limits the variability and effectiveness of the deidentification process.

It is worth noting that the design deidentification techniques for AM process data, while essential for privacy preservation, may face challenges in ensuring complete data security. Therefore, it should be emphasized on the importance of consistent integration of the proposed adaptive deidentification method into the existing cloud-based AM framework, such as [10], [109]. Specifically, this integration of the deidentification method serves as an additional layer in protecting sensitive information during AM process data sharing, leading to a more secured foundation for data sharing in the cloud-based AM platform for collaborative modeling.

5 Conclusion and Future Research Directions

In this paper, an SIA-ASIG thermal image deidentification method is proposed for design information deidentification of AM thermal process data. The resulting deidentified data can be aggregated from multiple AM users, leveraging a cloud platform for robust *in-situ* process-defect modeling. Specifically, the adaptive methodology can achieve a trade-off between privacy and utility for AM thermal process data that can be shared in a platform for privacy-preserving and utility-aware process-defect modeling. It is observed that the proposed method can substantially improve data privacy while sacrificing limited data utility. Moreover, the proposed method achieves higher privacy gain compared to the benchmark methods and demonstrates comparable utility loss, which is also associated with the design information deidentification of thermal AM process data. Overall, the proposed method provides an efficient mechanism to deidentify the design information in the AM process data, which can be leveraged for data sharing among AM users within a collaborative platform.

A few research directions are still open for future research. Firstly, incorporation of more complex printing trajectories can potentially improve the performance of the proposed adaptive method. This may involve analyzing non-unidirectional infill angles and free-formed components that can potentially improve image deidentification. These artifacts will introduce variability and complexity, requiring the deidentification algorithms to adapt and perform reliably under diverse conditions, ultimately enhancing their robustness. Secondly, with an increased diversity of angular identities in the training dataset, a potential enhancement to the evaluation method would be to use a regression-based approach for angular identity (i.e., printing trajectory) prediction. This would yield continuous-valued results, offering a more precise assessment of angular identity detection compared to discrete classification. Third, the proposed method provides melt-pool-wise data privacy while preserving data utility, and future research may provide a layer-by-layer privacy preservation mechanism to prevent re-identification threats. Furthermore, some privacy-preserving machine learning methods (i.e., differential privacy) can also be developed to reduce the risk of re-identification attacks. Lastly, while deidentification serves as a fundamental component in the wider domain of information security [110], the incorporation of supplementary security measures, like digital signatures [111] and cryptography techniques, has the potential to amplify the overall security of shared information. Therefore, in future iterations, these additional security measures should be investigated and integrated to establish a more comprehensive and robust security framework, presenting a layered defense against unauthorized tampering or alterations.

Acknowledgements

This work was partially sponsored by the National Science Foundation CMMI-2046515.

References

[1] J. J. Beaman, D. L. Bourell, C. C. Seepersad, and D. Kovar, "Additive Manufacturing Review: Early Past to Current Practice," Journal of Manufacturing Science and Engineering, Transactions of the ASME. 2020. doi: 10.1115/1.4048193.

[2] H. Kim, Y. Lin, and T. L. B. Tseng, "A review on quality control in additive manufacturing," Rapid Prototyp. J., vol. 24, no. 3, pp. 645–669, 2018, doi: 10.1108/RPJ-03-2017-0048.

[3] S. M. Thompson, L. Bian, N. Shamsaei, and A. Yadollahi, "An overview of Direct Laser Deposition for additive manufacturing; Part I: Transport phenomena, modeling and diagnostics," Addit. Manuf., vol. 8, pp. 36–62, 2015, doi: 10.1016/j.addma.2015.07.001.

[4] J. Qin, F. Hu, Y. Liu, P. Witherell, C.C. Wang, D.W. Rosen, T.W. Simpson, Y. Lu, and Q. Tang, "Research and application of machine learning for additive manufacturing," Addit. Manuf., vol. 52, no. February, 2022, doi: 10.1016/j.addma.2022.102691.

[5] C. Liu, W. Tian, and C. Kan, "When AI meets additive manufacturing: Challenges and emerging opportunities for human-centered products development," J. Manuf. Syst., vol. In press, no. May, 2022.

[6] L. Xiang and F. Tsung, "Statistical monitoring of multi-stage processes based on engineering models," IIE Trans. (Institute Ind. Eng., vol. 40, no. 10, pp. 957–970, 2008, doi: 10.1080/07408170701880845.

[7] Y. Wang, Y. Lin, R. Y. Zhong, and X. Xu, "IoT-enabled cloud-based additive manufacturing platform to support rapid product development," Int. J. Prod. Res., 2019, doi: 10.1080/00207543.2018.1516905.

[8] M. M. Bappy, D. Fullington, L. Bian, and W. Tian, "Evaluation of Design Information Disclosure through Thermal Feature Extraction in Metal based Additive Manufacturing," Manuf. Lett., vol. 36, pp. 86–90, 2023, doi: 10.1016/j.mfglet.2023.03.004.

[9] D. Fullington, L. Bian, and W. Tian, "Design De-identification of Thermal History for Collaborative Process-defect Modeling of Directed Energy Deposition Processes," J. Manuf. Sci. Eng., pp. 1–40, 2022, doi: 10.1115/1.4056488.

[10] C. Liu, L. Le Roux, C. Körner, O. Tabaste, F. Lacan, and S. Bigot, "Digital Twin-enabled Collaborative Data Management for Metal Additive Manufacturing Systems," J. Manuf. Syst., 2022, doi: 10.1016/j.jmsy.2020.05.010.

[11] Y. Lu, P. Witherell, F. Lopez, and I. Assouroko, "Digital solutions for integrated and collaborative additive manufacturing," 2016. doi: 10.1115/DETC2016-60392.

[12] L. Haghnegahdar, S. S. Joshi, and N. B. Dahotre, "From IoT-based cloud manufacturing approach to intelligent additive manufacturing: industrial Internet of Things—an overview," International Journal of Advanced Manufacturing Technology, vol. 119, no. 3–4. pp. 1461–1478, 2022. doi: 10.1007/s00170-021-08436-x.

[13] Y. Wang, Y. Lin, R. Y. Zhong, and X. Xu, "IoT-enabled cloud-based additive manufacturing platform to support rapid product development," Int. J. Prod. Res., vol. 57, no. 12, pp. 3975–3991, 2019.

[14] H. Elhoone, T. Zhang, M. Anwar, and S. Desai, "Cyber-based design for additive manufacturing using artificial neural networks for Industry 4.0," Int. J. Prod. Res., 2020, doi: 10.1080/00207543.2019.1671627.

[15] H. Zhang, B. Liu, and H. Wu, "Smart Grid Cyber-Physical Attack and Defense: A Review," IEEE Access. 2021. doi: 10.1109/ACCESS.2021.3058628.

[16] 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.

[17] M. Barrère, C. Hankin, N. Nicolaou, D. G. Eliades, and T. Parisini, "Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies," J. Inf. Secur. Appl., 2020, doi: 10.1016/j.jisa.2020.102471.

[18] X. Chen, E. Këpuska, S. Mauw, and Y. Ramírez-Cruz, "Active re-identification attacks on periodically released dynamic social graphs," 2020. doi: 10.1007/978-3-030-59013-0_10.

[19] J. Henriksen-Bulmer and S. Jeary, "Re-identification attacks—A systematic literature review," Int. J. Inf. Manage., 2016, doi: 10.1016/j.ijinfomgt.2016.08.002.

[20] G. Livraga and N. Park, "Analysis and Implications for Equifax Data Breach," WPES 2021 - Proceedings of the 20th Workshop on Privacy in the Electronic Society, co-located with CCS 2021. 2021.

[21] S. Khan, I. Kabanov, Y. Hua, and S. Madnick, “A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned,” ACM Trans. Priv. Secur., 2022, doi: 10.1145/3546068.

[22] J. Song, “Mitigating Insider Threat Risks in Cyber-physical Manufacturing Mitigating Insider Threat Risks in Cyber-physical Manufacturing Systems Systems,” 2021, [Online]. Available: https://surface.syr.edu/etd/1367

[23] J. Lu, R. Xiao, and S. Jin, “A Survey for Cloud Data Security,” Dianzi Yu Xinxi Xuebao/Journal of Electronics and Information Technology. 2021. doi: 10.11999/JEIT200158.

[24] S. H. Gill, M.A. Razzaq, M. Ahmad, F.M. Almansour, I.U. Haq, N.Z. Jhanjhi, M.Z. Alam, and M. Masud, “Security and privacy aspects of cloud computing: A smart campus case study,” Intell. Autom. Soft Comput., 2022, doi: 10.32604/IASC.2022.016597.

[25] W. A. Awadh, A. S. Alasady, and M. S. Hashim, “A multilayer model to enhance data security in cloud computing,” Indones. J. Electr. Eng. Comput. Sci., 2023, doi: 10.11591/ijeecs.v32.i2.pp1105-1114.

[26] G. Wijaya and N. Surantha, “Multi-layered security design and evaluation for cloud-based web application: Case study of human resource management system,” Adv. Sci. Technol. Eng. Syst., 2020, doi: 10.25046/AJ050583.

[27] M. M. Bappy, C. Liu, L. Bian, and W. Tian, “Morphological Dynamics-Based Anomaly Detection Towards In Situ Layer-Wise Certification for Directed Energy Deposition Processes,” J. Manuf. Sci. Eng., vol. 144, no. 11, pp. 1–11, 2022, doi: 10.1115/1.4054805.

[28] 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. August, pp. 443–456, 2018, doi: 10.1016/j.addma.2018.08.014.

[29] R. Mahesh and T. Meyyappan, “Anonymization technique through record elimination to preserve privacy of published data,” 2013. doi: 10.1109/ICPRIME.2013.6496495.

[30] J. Petrik, B. Kavas, and M. Bambach, “MeltPoolGAN: Auxiliary Classifier Generative Adversarial Network for melt pool classification and generation of laser power, scan speed and scan direction in Laser Powder Bed Fusion,” Addit. Manuf., 2023, doi: 10.1016/j.addma.2023.103868.

[31] W. Liu, Z. Wang, L. Tian, S. Lauria, and X. Liu, “Melt pool segmentation for additive manufacturing: A generative adversarial network approach,” Comput. Electr. Eng., 2021, doi: 10.1016/j.compeleceng.2021.107183.

[32] V. M. Potdar, H. Song, and C. Elizabeth, “A survey of digital image watermarking techniques,” 2005. doi: 10.1109/INDIN.2005.1560462.

[33] A. B. Kahng, J. Lach, W. H. Mangione-Smith, S. Mantik, I. L. Markov, M. Potkonjak, P. Tucker, H. Wang, and G. Wolfe, “Watermarking techniques for intellectual property protection,” 1998. doi: 10.1145/277044.277240.

[34] A. Mohanarathinam, S. Kamalraj, G. K. D. Prasanna Venkatesan, R. V. Ravi, and C. S. Manikandababu, “Digital watermarking techniques for image security: a review,” J. Ambient Intell. Humaniz. Comput., 2020, doi: 10.1007/s12652-019-01500-1.

[35] A. Dixit and R. Dixit, “A Review on Digital Image Watermarking Techniques,” Int. J. Image, Graph. Signal Process., 2017, doi: 10.5815/ijigsp.2017.04.07.

[36] Y. A. Younis, K. Kifayat, and M. Merabti, “An access control model for cloud computing,” J. Inf. Secur. Appl., 2014, doi: 10.1016/j.jisa.2014.04.003.

[37] P. S. Suryateja, “Threats and Vulnerabilities of Cloud Computing A Review,” Int. J. Comput. Sci. Eng., 2018, doi: 10.26438/ijcse/v6i3.297302.

[38] Nagesh Santosh Gund and Aniket Anant Jadhav, “Cloud Computing Security: Threats and Countermeasures,” Int. J. Adv. Res. Sci. Commun. Technol., 2023, doi: 10.48175/ijarsct-11678.

[39] M. Ogburn, C. Turner, and P. Dahal, “Homomorphic encryption,” Procedia Comput. Sci., vol. 20, pp. 502–509, 2013, doi: 10.1016/j.procs.2013.09.310.

[40] M. Agrawal and P. Mishra, “A comparative survey on symmetric key encryption techniques,” Intern. J. Comput. Sci. Eng., 2012.

[41] M. R. Shinde and R. D. Taur, “Encryption Algorithm for Data Security and Privacy in Cloud Storage,” Am. J. Comput. Sci. Eng. Surv., vol. 3, no. 1, pp. 34–39, 2015.

[42] C. Fontaine and F. Galand, “A survey of homomorphic encryption for nonspecialists,” Eurasip J. Inf. Secur., 2007, doi: 10.1155/2007/13801.

[43] C. Marcolla, V. Sucasas, M. Manzano, R. Bassoli, F. H. P. and Fitzek, N. Aaraj, “Survey on Fully Homomorphic Encryption, Theory, and Applications,” Proc. IEEE, 2022, doi: 10.1109/JPROC.2022.3205665.

[44] O. R. Arogundade, “Addressing Cloud Computing Security and Visibility Issues,” IARJSET, 2023, doi: 10.17148/iarjset.2023.10321.

[45] A. Singh and K. Chatterjee, “Cloud security issues and challenges: A survey,” Journal of Network and Computer Applications. 2017. doi: 10.1016/j.jnca.2016.11.027.

[46] J. Gatlin, S. Belikovetsky, Y. Elovici, A. Skjellum, J. Lubell, P. Witherell, and M. Yampolskiy, “Encryption is futile: Reconstructing 3D-printed models using the power side-channel,” 2021. doi: 10.1145/3471621.3471850.

[47] L. Kumar and N. Badal, “Minimizing the Effect of Brute Force Attack using Hybridization of Encryption Algorithms,” Int. J. Comput. Appl., 2019, doi: 10.5120/ijca2019919213.

[48] P. S. Munoz, N. Tran, B. Craig, B. Dezfouli, and Y. Liu, “Analyzing the Resource Utilization of AES Encryption on IoT Devices,” 2018. doi: 10.23919/APSIPA.2018.8659779.

[49] H. Y. Youm, “An overview of de-identification techniques and their standardization directions,” IEICE Trans. Inf. Syst., 2020, doi: 10.1587/transinf.2019ICI0002.

[50] E. M. Newton, L. Sweeney, and B. Malin, “Preserving privacy by de-identifying face images,” IEEE Trans. Knowl. Data Eng., vol. 17, no. 2, pp. 232–243, 2005, doi: 10.1109/TKDE.2005.32.

[51] I. E. Olatunji, J. Rauch, M. Katzensteiner, and M. Khosla, “A Review of Anonymization for Healthcare Data,” Big Data, 2022, doi: 10.1089/big.2021.0169.

[52] S. Murthy, A. Abu Bakar, F. Abdul Rahim, and R. Ramli, “A Comparative Study of Data Anonymization Techniques,” 2019. doi: 10.1109/BigDataSecurity-HPSC-IDS.2019.00063.

[53] H. Hukkelås and F. Lindseth, “Does Image Anonymization Impact Computer Vision Training?,” 2023. doi: 10.1109/CVPRW59228.2023.00019.

[54] J. H. Lee and S. J. You, “Balancing Privacy and Accuracy: Exploring the Impact of Data Anonymization on Deep Learning Models in Computer Vision,” IEEE Access, 2024, doi: 10.1109/ACCESS.2024.3352146.

[55] P. L. M. K. Bandara, H. D. Bandara, and S. Fernando, “Evaluation of Re-identification Risks in Data Anonymization Techniques Based on Population Uniqueness,” 2020. doi: 10.1109/ICITR51448.2020.9310884.

[56] H. Kikuchi, T. Yamaguchi, K. Hamada, Y. Yamaoka, H. Oguri, and J. Sakuma, “Ice and fire: Quantifying the risk of re-identification and utility in data anonymization,” 2016. doi: 10.1109/AINA.2016.151.

[57] T. H. Rafi, F. A. Noor, T. Hussain, and D. K. Chae, “Fairness and privacy preserving in federated learning: A survey,” Inf. Fusion, 2024, doi: 10.1016/j.inffus.2023.102198.

[58] X. Yin, Y. Zhu, and J. Hu, “A Comprehensive Survey of Privacy-preserving Federated Learning: A Taxonomy, Review, and Future Directions,” ACM Computing Surveys. 2021. doi: 10.1145/3460427.

[59] M. Chen, N. Shlezinger, H. Vincent Poor, Y. C. Eldar, and S. Cui, “Communication-efficient federated learning,” Proc. Natl. Acad. Sci. U. S. A., 2021, doi: 10.1073/pnas.2024789118.

[60] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, “Federated Learning: Challenges, Methods, and Future Directions,” IEEE Signal Process. Mag., 2020, doi: 10.1109/MSP.2020.2975749.

[61] D. Fullington, E. Yangue, M. M. Bappy, C. Liu, and W. Tian, “Leveraging small-scale datasets for additive manufacturing process modeling and part certification: Current practice and remaining gaps,” J. Manuf. Syst., no. April, 2024, doi: 10.1016/j.jmsy.2024.04.021.

[62] W. K. Liu, Y. Zhang, H. Yang, and Q. Meng, “A Survey on Differential Privacy for Medical Data Analysis,” Annals of Data Science. 2024. doi: 10.1007/s40745-023-00475-3.

[63] Q. Hu, R. Chen, H. Yang, and S. Kumara, “Privacy-preserving data mining for smart manufacturing,” Smart Sustain. Manuf. Syst., vol. 4, no. 2, 2020, doi: 10.1520/SSMS20190043.

[64] M. U. Hassan, M. H. Rehmani, and J. Chen, “Differential Privacy Techniques for Cyber Physical Systems: A Survey,” IEEE Communications Surveys and Tutorials. 2020. doi: 10.1109/COMST.2019.2944748.

[65] R. Xu, N. Baracaldo, and J. Joshi, “Privacy-Preserving Machine Learning: Methods, Challenges and Directions,” 2021, [Online]. Available: http://arxiv.org/abs/2108.04417

[66] M. Widmer and V. Rajan, “3D opportunity for intellectual property risk: Additive manufacturing stakes its claim,” 2016.

[67] S. R. Chhetri, A. Canedo, and M. A. Al Faruque, “Confidentiality breach through acoustic side-channel in cyber-physical additive manufacturing systems,” ACM Trans. Cyber-Physical Syst., 2018, doi: 10.1145/3078622.

[68] J. Domingo-Ferrer and V. Torra, “A critique of k-anonymity and some of its enhancements,” ARES 2008 - 3rd Int. Conf. Availability, Secur. Reliab. Proc., no. May 2014, pp. 990–993, 2008, doi: 10.1109/ARES.2008.97.

[69] K. LeFevre, D. J. DeWitt, and R. Ramakrishnan, “Mondrian multidimensional K-anonymity,” Proc. - Int. Conf. Data Eng., vol. 2006, p. 25, 2006, doi: 10.1109/ICDE.2006.101.

[70] L. Samarati, P., & Sweeney, “Generalizing data to provide anonymity when disclosing information,” Paper presented at the seventeenth ACM SIGACT-SIGMOD-SIGART symposium on Principles of database systems, Seattle, WA, 1998. doi: 10.1145/275487.275508.

[71] P. Xiong and T. Zhu, “An anonymization method based on tradeoff between utility and privacy for data publishing,” 2012. doi: 10.1109/ICMeCG.2012.14.

[72] R. Gross, E. Airoldi, B. Malin, and L. Sweeney, “Integrating utility into face de-identification,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 3856 LNCS, pp. 227–242, 2006, doi: 10.1007/11767831_15.

[73] Y. F. Yiting Cao , Yaofang Zhang , Jiahua Wu, “Multi-channel attribute preservation for face de-identification,” Multimed. Tools Appl., 2024, [Online]. Available: 10.1007/s11042-024-19308-3

[74] L. Sweeney, “k-Anonymity: A model for protecting privacy,” Ieee S&P ’02, vol. 10, no. 5, pp. 1–14, 2002, doi: 10.1142/S0218488502001648.

[75] K. N. Rao, P. Jayasree, C. V. M. Krishna, S. Prasanth, and C. S. Reddy, “Image Anonymization using Deep Convolutional Generative Adversarial Network,” J. Phys. Conf. Ser., vol. 2089, no. 1, 2021, doi: 10.1088/1742-6596/2089/1/012012.

[76] L. Du, M. Yi, E. Blasch, and H. Ling, “GARP-face: Balancing privacy protection and utility preservation in face de-identification,” IJCB 2014 - 2014 IEEE/IAPR Int. Jt. Conf. Biometrics, 2014, doi: 10.1109/BTAS.2014.6996249.

[77] A. Jourabloo, X. Yin, and X. Liu, “Attribute preserved face de-identification,” Proc. 2015 Int. Conf. Biometrics, ICB 2015, pp. 278–285, 2015, doi: 10.1109/ICB.2015.7139096.

[78] T. Li and L. Lin, “AnonymousNet: Natural face de-identification with measurable privacy,” IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Work., vol. 2019-June, pp. 56–65, 2019, doi: 10.1109/CVPRW.2019.00013.

[79] B. Meden, Z. Emersic, V. Struc, and P. Peer, “κ-Same-Net: Neural-Network-Based Face Deidentification,” 2017 Int. Work Conf. Bio-Inspired Intell. Intell. Syst. Biodivers. Conserv. IWOBI 2017 - Proc., no. September, 2017, doi: 10.1109/IWOBI.2017.7985521.

[80] H. N. Taichi Nakamura, Yuiko Sakuma, “Face-Image Anonymization as an Application of Multidimensional Data k-anonymizer,” Int. J. Netw. Comput., vol. 11, no. 1, pp. 102–119, 2021.

[81] C. Dwork and A. Roth, “The algorithmic foundations of differential privacy,” Found. Trends Theor. Comput. Sci., 2013, doi: 10.1561/0400000042.

[82] P. Ohm, “Broken promises of privacy: Responding to the surprising failure of anonymization,” UCLA Law Rev., 2010.

[83] X. Ren and D. Jiang, “A Personalized α,β,l,k -Anonymity Model of Social Network for Protecting Privacy,” Wirel. Commun. Mob. Comput., 2022, doi: 10.1155/2022/7187528.

[84] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, “A survey of IoT security based on a layered architecture of sensing and data analysis,” Sensors (Switzerland). 2020. doi: 10.3390/s20133625.

[85] S. K. Sood, “A combined approach to ensure data security in cloud computing,” J. Netw. Comput. Appl., 2012, doi: 10.1016/j.jnca.2012.07.007.

[86] Y. Pang, J. Lin, T. Qin, and Z. Chen, “Image-to-Image Translation: Methods and Applications,” IEEE Transactions on Multimedia. 2022. doi: 10.1109/TMM.2021.3109419.

[87] M. N. Esfahani, M. M. Bappy, L. Bian, and W. Tian, “In-situ layer-wise certification for direct laser deposition processes based on thermal image series analysis,” J. Manuf. Process., vol. 75, no. July 2021, pp. 895–902, 2022, doi: 10.1016/j.jmapro.2021.12.041.

[88] M. Khanzadeh, S. Chowdhury, M. Marufuzzaman, M. A. Tschopp, and L. Bian, “Porosity prediction: Supervised-learning of thermal history for direct laser deposition,” J. Manuf. Syst., vol. 47, no. April, pp. 69–82, 2018, doi: 10.1016/j.jmsy.2018.04.001.

[89] A. J. Pinkerton and L. Li, “Modelling the geometry of a moving laser melt pool and deposition track via energy and mass balances,” J. Phys. D. Appl. Phys., vol. 37, no. 14, pp. 1885–1895, 2004, doi: 10.1088/0022-3727/37/14/003.

[90] M. Castejón, E. Alegre, J. Barreiro, and L. K. Hernández, “On-line tool wear monitoring using geometric descriptors from digital images,” Int. J. Mach. Tools Manuf., 2007, doi: 10.1016/j.ijmachtools.2007.04.001.

[91] L. E. Criales, Y. M. Arısoy, B. Lane, S. Moylan, A. Donmez, and T. Özel, “Laser powder bed fusion of nickel alloy 625: Experimental investigations of effects of process parameters on melt pool size and shape with spatter analysis,” Int. J. Mach. Tools Manuf., vol. 121, no. September 2016, pp. 22–36, 2017, doi: 10.1016/j.ijmachtools.2017.03.004.

[92] Purwono, A. Ma’arif, W. Rahmaniar, H. I. K. Fathurrahman, A. Z. K. Frisky, and Q. M. U. Haq, “Understanding of Convolutional Neural Network (CNN): A Review,” Int. J. Robot. Control Syst., 2022, doi: 10.31763/ijrcs.v2i4.888.

[93] W. Xing, X. Chu, T. Lyu, C. G. Lee, Y. Zou, and Y. Rong, “Using convolutional neural networks to classify melt pools in a pulsed selective laser melting process,” J. Manuf. Process., 2022, doi: 10.1016/j.jmapro.2021.12.030.

[94] C. Xia, Z. Pan, Y. Li, J. Chen, and H. Li, “Vision-based melt pool monitoring for wire-arc additive manufacturing using deep learning method,” Int. J. Adv. Manuf. Technol., 2022, doi: 10.1007/s00170-022-08811-2.

[95] B. Zhang, S. Liu, and Y. C. Shin, “In-Process monitoring of porosity during laser additive manufacturing process,” Addit. Manuf., 2019, doi: 10.1016/j.addma.2019.05.030.

[96] A. A. M. Al-Saffar, H. Tao, and M. A. Talab, “Review of deep convolution neural network in image classification,” 2017. doi: 10.1109/ICRAMET.2017.8253139.

[97] S. S. Kadam, A. C. Adamuthe, and A. B. Patil, “CNN Model for Image Classification on MNIST and Fashion-MNIST Dataset,” J. Sci. Res., 2020, doi: 10.37398/jsr.2020.640251.

[98] M. Abadi, A. Chu, I. Goodfellow, H.B. McMahan, I. Mironov, K. Talwar, and L. Zhang, “Deep learning with differential privacy,” 2016. doi: 10.1145/2976749.2978318.

[99] R. Mendes and J. P. Vilela, “Privacy-Preserving Data Mining: Methods, Metrics, and Applications,” IEEE Access, 2017, doi: 10.1109/ACCESS.2017.2706947.

[100] H. Wang, Z. L. Jiang, Y. Zhao, S. M. Yiu, P. Yang, Z. Tan, B. Jin, S. Xu, and S. Pan “Securer and Faster Privacy-Preserving Distributed Machine Learning,” 2022, [Online]. Available: http://arxiv.org/abs/2211.09353

[101] H. Liu, C. Peng, Y. Tian, S. Long, and Z. Wu, “Balancing Privacy-Utility of Differential Privacy Mechanism: A Collaborative Perspective,” Secur. Commun. Networks, 2021, doi: 10.1155/2021/5592191.

[102] ASTM E8, “ASTM E8/E8M standard test methods for tension testing of metallic materials 1,” Annu. B. ASTM Stand. 4, no. C, pp. 1–27, 2010, doi: 10.1520/E0008.

[103] R. Bro and A. K. Smilde, “Principal component analysis,” Analytical Methods. 2014. doi: 10.1039/c3ay41907j.

[104] G. LeCun, Y., Bengio, Y., Hinton, “Deep learning. nature 521 (7553): 436,” Nature, 2015.

[105] S. Ioffe and C. Szegedy, “Batch normalization: Accelerating deep network training by reducing internal covariate shift,” 2015.

[106] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “ImageNet classification with deep convolutional neural networks,” Commun. ACM, 2017, doi: 10.1145/3065386.

[107] A. Al Mamun, M. M. Bappy, A. S. Mudiyanselage, J. Li, Z. Jiang, Z. Tian, S. Fuller, T. C. Falls, L. Bian and W. Tian, “Multi-channel sensor fusion for real-time bearing fault diagnosis by frequency-domain multilinear principal component analysis,” Int. J. Adv. Manuf. Technol., vol. 124, no. 3–4, pp. 1321–1334, 2023, doi: 10.1007/s00170-022-10525-4.

[108] J. Wu, X. Y. Chen, H. Zhang, L. D. Xiong, H. Lei, and S. H. Deng, “Hyperparameter optimization for machine learning models based on Bayesian optimization,” J. Electron. Sci. Technol., 2019, doi: 10.11989/JEST.1674-862X.80904120.

[109] Y. Wang, R. Blache, and X. Xu, "Design for additive manufacturing in the cloud platform," 2017. doi: 10.1115/MSEC2017-2708.

[110] S. Ribaric, A. Ariyaeeinia, and N. Pavesic, "De-identification for privacy protection in multimedia content: A survey," Signal Process. Image Commun., 2016, doi: 10.1016/j.image.2016.05.020.

[111] P. Jain, P. Muskara, and P. Jain, "Enhance Data Security in Cloud Computing with Digital Signature & Hybrid Cryptographic Algorithm," 2021. doi: 10.1109/SASM51857.2021.9841171.