Evaluating Machine Learning Models for Handwriting Recognition-based Systems under Local Differential Privacy

Abdur R. Shahid
Department of Computer and Information Systems
Robert Morris University, USA
ashahid@ieee.org

Sajedul Talukder
School of Computing
Southern Illinois University, USA
sajedul.talukder@siu.edu

***Abstract*—Handwriting recognition, a pervasive assistive technology for a variety of consumer electronics and Internet of Things (IoT) systems does not provide meaningful privacy guarantees. Hacking of a device, malware, and compromise of handwriting recognition-enabled application's cloud service can lead to leakage of sensitive personal information with serious consequences. In this paper, we propose an algorithm to deform a user's original handwriting by adding adjustable statistical noise before sharing it with a specific application to achieve local differential privacy (LDP). To assess and quantify the algorithm's impact on recognition, we generate a shape-deformed test set by applying the algorithm to the MNIST dataset and implement a visualization tool to demonstrate the impact of the proposed algorithm. Then, we train a convolutional neural network, Naïve Bayes, random forest, support vector machine, and decision tree classifiers on the MNIST dataset and evaluate them with the privatized test set. Our experiment reveals that without tuning the CNN for privatized images, it is possible to achieve around 80% accuracy in local differential privacy settings, which lays the ground for further research in this direction.**

***Index Terms*—Machine Learning, Deep Learning, Differential Privacy, Assistive Technology, Handwriting.**

I. Introduction

Handwriting recognition is a well-known problem in Artificial Intelligence (AI). Numerous academic papers have been written on this topic, proposing different approaches utilizing traditional machine learning methods to deep neural networks to achieve near-perfect accuracy. The handwritten text carries a rich amount of information on its writer, capable of playing a vital role in security, healthcare, and consumer electronics. The efforts to utilize such information have led to the exploration of exciting systems and applications. For example, some automakers adapted handwriting recognition for in-vehicle infotainment control [16]. Such a feature in the vehicle is helpful to its passengers in various situations, such as noisy surroundings, keeping quiet is necessary, and there is a risk of eavesdropping with voice input [19]. Handwriting recognition systems have found interesting and useful applications in healthcare [5], [25], [24]. For instance, it can be used as an assistive technology for physical, visual, or cognitive disabilities [25]. Another example can be the utilization of handwriting to examine handwriting in the context of frailty [5]. It can also be an essential feature for small display devices in Internet of Things (IoT), such as a smartwatch, on which typing is prone to high error [15]. While earlier research and development focused on touchable surfaces for digital handwriting, recently, several approaches have been proposed which utilize hand movement to handwriting[20], [32]. One such example is SHOW [20], which utilizes an accelerometer and gyroscope to capture user input on a horizontal surface and transform it to English text and numbers. The concept of the air-writing is also getting attention this days [6], [7], [31]. The air-writing approaches allow users to write on the air using some form of smart devices (e.g., smart-bands [31]) to capture the movements of writing tool (e.g., fingers), detect handwriting using a trained Machine Learning (ML) model, and perform feature extraction to recognize handwriting [6], [7].

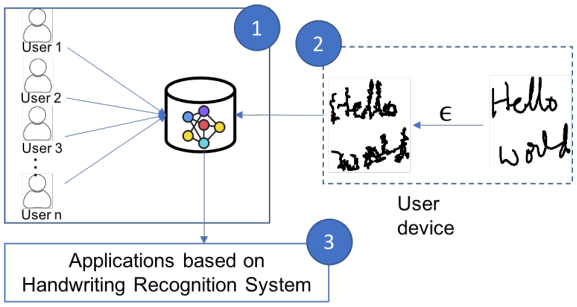


Fig. 1. Proposed system model: 1) A model is trained using original handwriting from users and deployed on the cloud, 2) A user's original handwriting is deformed using the proposed local-differentially private algorithm. Then, it is shared with the cloud, and 3) based on the recognized text, the user uses applications to perform certain tasks.

While handwriting recognition systems are exciting and extremely helpful, they have serious privacy drawbacks. Privacy leakage can occur in different stages of the recognition systems, including, 1) data collection for training, 2) model training, 3) output generation of the model, and 4) use of the model on the user end. Against this backdrop, in this paper, we present a local-differentially private algorithm to deform the shape of original handwriting to preserve the privacy of its writer. This raises a critical question: **what is the accuracy of a model, trained on non-private handwriting images,**

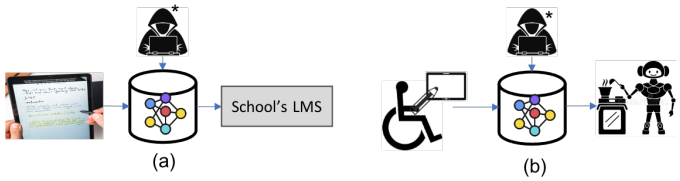


Fig. 2. Examples of privacy leakage in handwriting-based (a) Learning Management Systems (LMS), and (b) Assistive systems.

on the deformed input? To answer this question, we first train five (5) machine learning and deep learning models on the popular MNIST dataset [9]. Then, we apply our proposed local differentially private randomized algorithm on the test set of the MNIST dataset to generated a privatized test set. After that, we evaluate the trained models with the privatized test set (see Figure 1 for the proposed system model). We show through our experiment that the accuracy of the traditional ML models drops significantly ($< 30\%$) as we add more noise to the differentially private data set. However, Convolutional Neural Network (CNN) achieves around 80% accuracy under considerable privacy level ($\epsilon > 3$). In summary, we introduce the following contributions:

- **Handwriting recognition vulnerabilities**. We focus on the privacy vulnerabilities for handwriting recognition by presenting two scenarios where the recognition model is trained and deployed on the cloud using the user sent data. In both examples, the cloud can be compromised by malicious entities that can lead to leakage of sensitive personal information with serious consequences.
- **Local-differentially private algorithm**. We present a local differentially private algorithm to add statistical noise, drawn from the Laplace mechanism, to a handwriting image to achieve ϵ-LDP. We also prove our theorem that the proposed algorithm is differentially private.
- **Experimental results**. Through our experiment, we train different ML models on the popular MNIST dataset using Tensorflow in Google Colab [4] and generate local differentially private dataset using our proposed algorithm. For each value of ϵ, we then compute the accuracy of the trained models on the privatized test set and show that deep learning models can achieve a relatively better accuracy under considerable privacy level.
- **Open-source visualization tool**. We implement a visualization tool using python 3.7. (open source upon publication) to demonstrate the impact of the proposed algorithm on handwriting text by highlighting the relationship between the accuracy and privacy level. We aim to further integrate the research outcome to this tool to develop a standalone open source software for research and education.

II. Motivation

In this paper, we focus on the privacy issue for the following scenario. Imagine, a recognition model is trained and deployed on the cloud. Users send their handwriting data to the cloud, the cloud performs the recognition tasks on behalf of the user, and does the intended operation. Figure 2 depicts two examples of privacy leakage. In figure 2(a), a student writing on a digital device, and the handwriting is uploaded to the cloud. The cloud performs the recognition task, generates the text of the handwriting, and sends it to a school's Learning Management Systems (LMS). In figure 2(b), a disabled person writes on a digital device to command a home robot to perform some specific task. His/her handwriting is uploaded to the cloud. The cloud performs the handwriting recognition task and sends the command to the robot. In both examples, the cloud can be compromised by malicious entities (marked with $*$) and its users' original handwriting can be leaked to the malicious entities. Hence, to protect a user's original handwriting, some sort of measures should be taken. It is easily understandable that such measures should be taken on the user's side before it leaves the user's device.

III. Background

A. Differential Privacy

Differential privacy, presented by Dwork et al. in 2006 [11], ensures that the same conclusions will be reached for a query on a dataset, regardless the presence of an individual in the dataset [13]. A randomized algorithm $\mathcal{M}$ satisfied ϵ-differential privacy if for any two datasets D and D' (differing only in one record) and any output $S \in Range(\mathcal{M})$, satisfies:

$$e^{-\epsilon} \leq \frac{\Pr[\mathcal{M} \in S]}{\Pr[\mathcal{M} \in S']} \leq e^{\epsilon} \tag{1}$$

Here, ϵ denotes the privacy level of $\mathcal{M}$. Generally, differential privacy can be achieved by adding noise, drawn from a probability distribution, to the results of the query function. A popular way of guaranteeing differential privacy is Laplace mechanism [12]. By definition, for a query function $f : D \rightarrow \mathcal{R}$, a randomized algorithm $\mathcal{M}$ satisfies ϵ-differential privacy if

$$\mathcal{M}(D) = f(D) + Lap\Big(\frac{\mathcal{S}(f)}{\epsilon}\Big) \tag{2}$$

Here, $\mathcal{S}(f)$ is the sensitivity of f and $Lap(\frac{\mathcal{S}(f)}{\epsilon})$ is the amount of noise from Laplace distribution with center 0 and scaling $\frac{\mathcal{S}(f)}{\epsilon}$ [17]. The sensitivity $\mathcal{S}(f)$ of a query f is defined as $\max_{\text{adjacent}D,D'} |f(D) - f(D')|$.

B. Local Differential Privacy

A major problem with the standard notion of differential privacy is that it assumes the presence of a trusted central entity. That is, the data curator performs the data privatization using a ϵ-DP method while releasing information from a dataset. Such a notion does not provide a strong privacy to the original generator of the data, that is, the users. Such a limitation led to the introduction of the concept of Local Differential Privacy (LDP)[10]. We can say that an algorithm π satisfies ϵ-Local Differential Privacy where ϵ ¿ 0 if and only if for any input v and v',

$$\forall y \in Range(\pi) : \frac{Pr[\pi(v) = y]}{Pr[\pi(v') = y]} \leq e^{\epsilon} \tag{3}$$

where $Range(\pi)$ denotes every possible output of the algorithm π. In an LDP settings, the noise, drawn from a probability distribution, is added to the private data before it leaves an individual's device [13]. One way to satisfy the condition (3) is to apply the Laplace mechanism locally. If an 1-d data value v is within the range $[m, M]$ with the $d = M - m$, then it can be proved that the Laplace mechanism $y = v + Lap(\frac{d}{\epsilon})$ [8]. Differentially private algorithms satisfy various composition properties, including parallel composition and postprocessing [21].

Theorem III.1. *Let $\mathcal{M}_1(.)$ and $\mathcal{M}_2(.)$ be ϵ_1- and ϵ_2-differentially private algorithms [27]. Then,*

- Parallel composition: If $D_1 \cap D_2 = \emptyset$, then Releasing $\mathcal{M}_1(D_1)$ and $\mathcal{M}_2(D_2)$ satisfies $max(\epsilon_1, \epsilon_2)$-differential privacy.
- Postprocessing: Application of a postprocessing algorithm, $\mathcal{M}$, on the output of $\mathcal{M}_1(D_1)$-is still ϵ_1 differentially private.

IV. Related Work

Due to its simplicity and robustness, the recognition of digits, a subfield of character recognition, is the subject of much attention since the first years of research in the field of handwriting recognition. In 1992, Xu et al. [30] proposed methods to combine several classifiers for recognizing totally unconstrained handwritten numerals. The same year, Hansen et al. [18] applied neural network ensembles to handwritten digit recognition. Subsequently, Gunter and Bunke (Gunter, 2003) applied several different methods such as bagging, boosting, random subspace, and architecture variation to generate ensembles of classifiers in the context of handwritten word recognition. Zhang et al. [33] proposed a novel cascade ensemble classifier system using three parallel artificial neural networks (ANNs) with a high recognition performance on handwritten digits. Adankon et al. [2] proposed to tune the least-squares SVM (LS-SVM) hyperparameters using the empirical error criterion in the cross-validation procedure. Darmatasia et al. [14] proposed a workflow and a machine learning model based on Convolutional Neural Network (CNN) as a powerful feature extraction and Support Vector Machines (SVM) as a high-end classifier for recognizing handwritten characters on form document. Very recently, Sharma et al. [26] presented a fully convolution-based deep network architecture for cursive handwriting recognition from line-level images.

In local differential privacy, users' input's are randomly perturbed to provide plausible deniability of their data while the ensuring building of accurate models and predictors. Oftentimes, this is done by adding a randomization layer before data leave the data owners' devices and reach a potentially untrusted machine learning service. Ren et al. [23] developed a local differentially private high-dimensional data publication algorithm (LoPub) to ensure privacy in high-dimensional crowdsourced data. Nguyên et al. [22] propose Harmony, a practical, accurate, and efficient system for collecting and analyzing data from smart device users while satisfying LDP. Several researchers aimed to develop new algorithmic techniques for learning and refined analysis of privacy costs within the framework of local differential privacy [3], [1], [28], [29]. However, to the best of our knowledge, this paper is the first approach to evaluate machine learning models for handwriting recognition-based systems under local differential privacy.

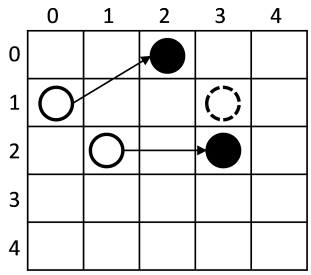


Fig. 3. Privatizing pen positions using the proposed algorithm.

Algorithm 1: Privatizing Handwriting

Data: M, N, privacy level ϵ
Result: Privatized positions of pen, $Positions$

List of privatized positions, $Positions \leftarrow \emptyset$
Previous position of pen, $(x_{prev}, y_{prev}) \leftarrow \emptyset$
while *Writing* **do**
  $(x, y) \leftarrow$ Current position of pen
  Compute (x', y') from (x_0, y_0) according to eq. 4
  if $(x_{prev}, y_{prev}) \neq \emptyset$ **then**
    Get all the positions on the straight line between (x_{prev}, y_{prev}) and (x', y') through interpolation from the grid and append them to $Positions$
  end
  Append (x', y') to $Positions$
  $(x_{prev}, y_{prev}) \leftarrow (x', y')$
end
Return $Positions$

V. Proposed Approach

A. Proposed Local Differentially Private Algorithm

In this section, we present our proposed method to add statistical noise, drawn from the Laplace mechanism, to a handwriting image to achieve ϵ-LDP. Let us consider the canvas is a $M \times N$ grid, starting at index $(0, 0)$. Then, the ranges of the indices on the X and Y axis are $[0, M)$ and $[0, N)$, respectively. let us consider a monochrome canvas on which a user writes using a writing tool, pen. One straightforward way to achieve ϵ-LDP on a 2-D or higher dimensional handwriting image is to add the same amount of noise to the image in the pixel domain. That is, first, generate the noise, and add it each (x, y) position of pen. However, it is similar to image translation which cannot provide privacy in reality. It is required to deform the shape of the handwriting. Hence, it is required to perform the translation of each position independently different amount of noise.

TABLE I
DESCRIPTION OF THE DIFFERENT TRAINED MODELS

Model	Description
CNN	Layer / Output Shape: Conv2D (None,24,24,32); MaxPooling2D (None,12,12,32); Dropout (None,12,12,32); Flatten (None,4608); Dense (None,128); Dense (None,10). Total params: 592,074. Trainable params: 592,074
Random Forest	Number of estimators = 100
Decision Tree	maximum depth = 10
SVM	Kernel = "Poly", C = 1
Naive Bayes	Default values in sklearn

Assume the pen's current position is index (x, y). If user's privacy level is ϵ, the local differential private index (x', y') for (x, y) can be achieved as follows,

$$x_0 = x + Lap(\frac{M-1}{\epsilon})$$
$$y_0 = y + Lap(\frac{N-1}{\epsilon})$$
$$x' = \begin{cases} 0, x_0 < 0 \\ \lfloor x_0 \rceil, 0 \leq x_0 < M-1 \\ M-1, x_0 \geq M \end{cases} \quad (4)$$
$$y' = \begin{cases} 0, y_0 < 0 \\ \lfloor y_0 \rceil, 0 \leq y_0 < N-1 \\ N-1, y_0 \geq N \end{cases}$$

The detailed process of privatizing handwriting with local differential privacy is presented in algorithm 1. Based on the user privacy level ϵ, the dimension of the canvas M and N, the algorithm first generates a random position (x', y') by adding Laplace noise to the original pen position (x, y) (lines 4 and 5). Then, through interpolation, we generate all the positions on the straight line between the previous randomized position (x_{prev}, y_{prev}) and current randomized position (x', y'). An example of the working principle of the proposed algorithm is depicted in figure 3. Let, the pen's two consecutive original positions were $(1, 0)$ and $(2, 1)$. After adding Laplace noise, these two positions became $(0, 2)$ and $(2, 3)$, respectively. After interpolation, the position $(1, 3)$ also became a part of the handwriting.

Theorem V.1. *The proposed algorithm is differentially private.*

Proof. To prove that the algorithm is differentially private, it is necessary to prove that 1) privatized position of pen, (x', y'), from its original position (x, y) is differentially private, and 2) the positions selected through the interpolation are also differentially private. According to the definition of differential privacy, x_0 and y_0 are ϵ-differentially private and their calculations are done in parallel. The generation of x' and y' also follows the postprocessing properties of the differential privacy. Hence, the mechanism of calculating (x', y') position is differentially private. Consequently, the interpolation of the positions between two ϵ-differentially private positions follows the postprocessing property of differential privacy. □

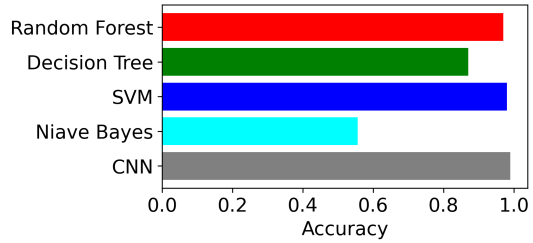


Fig. 4. Accuracy of the different models on non-private test set.

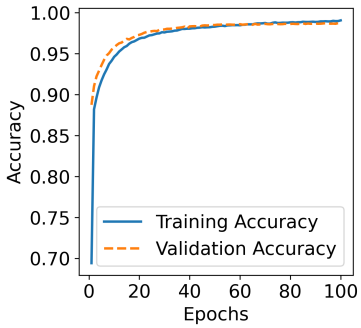


Fig. 5. Training and validation accuracys of CNN.

B. Machine Learning Models

Well, we have a local differentially private algorithm to add random noise to the handwriting before it is released to a remote application/data curator. Now we must seek the answer to the question of how good a handwriting recognition model for such a noisy input. While the answer to this question is not straightforward, we know that many of the traditional machine learning models (e.g. support vector machine (SVM)), are highly susceptible to noise, compare to deep learning models. To validate such hypothesis of our problem, we train the following traditional machine learning and deep learning algorithms.

- **Convolutional neural network (CNN)**
- **Random Forest**
- **Decision Tree**
- **Support Vector Machine (SVM)**
- **Naive Bayes**

The detail of the trained models is presented in table I.

VI. EXPERIMENTAL ANALYSIS

Our experiment design includes training different models, privatized datasets generation using the proposed algorithm, the evaluation of the different models against the privatized datasets, and the development of a visualization tool with the implementation of the proposed algorithm. We carry out model training and testing using Tensorflow in Google Colab. We implement the visualization tool using python 3.7.

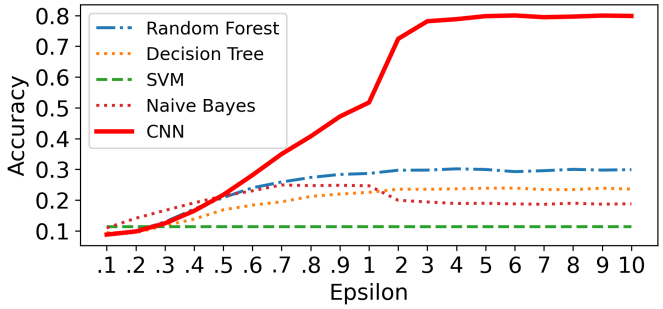


Fig. 6. Accuracy of the different models on the nineteen (19) ϵ-private test sets.

A. Dataset Preparation, Training and Testing Models

To evaluate the accuracy of the ML and DL algorithms we utilize the popular MNIST dataset as follows. First, we split the dataset into two sets: train and test (non-private). Next, we apply the proposed algorithm to the test test for each values of $\epsilon \in \{.1, .2, .3, .4, .5, .6, .7, .8, .9, 1, 2, 3, 4, 5{,}6, 7, 8, 9, 10\}$ and generate nineteen (19) different differentially private test tests. Therefore, in the experiment, we have 1 training set and twenty (20) test sets. Using these datasets, first, we train the models on the MNIST dataset using the training set. Then, we test their accuracy on the non-private test set. Next, we test the accuracy of these models on the nineteen differentially private test tests.

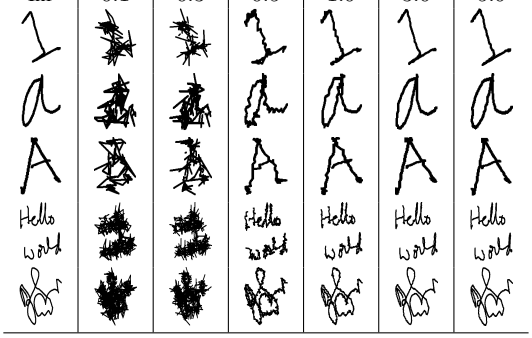
B. Evaluation of the Models with a Non-Private Test Set

Handwriting recognition using the MNIST dataset and the evaluation results of the trained models with a non-private test set is well-known to many of us. Many traditional ML and deep learning models achieved tremendous accuracy for this problem. Our experimental results in figure 4 also exhibit a similar trend. With the traditional ML models, random forest, decision tree, and SVM, we achieve very high accuracy($> 90\%$). On the other hand, with a CNN model, we are able to achieve near-perfect accuracy ($\approx 97\%$). Figure 5 details the training and validation accuracy of CNN. It shows a negligible overfitting after 60 epochs.

C. Evaluation of the Models with Different Deferentially Private Test Sets

While the trained models show incredible performance on a non-private test set, the bigger question is how well they perform against a test set with handwriting images deformed using the proposed algorithm. To find the answer, we test the models using the nineteen privatized test sets and present the result in figure 6. The first observation we can make from this result is that under a test set, comprising images with very high noise, all the models perform very poorly. For example, when the value of ϵ is 0.1, their accuracy drops to 0.1. The second observation is, with the decrease in the privacy level, the traditional ML models do not show much improvement. In fact, their accuracy eventually flattens at some point. For instance, Random Forest, which is the best model among the traditional ML models, has its accuracy frozen at ≈ 0.3 after $\epsilon = 2$. The third observation, which is completely aligned with the recent year's development in deep learning, is that CNN outperforms the traditional ML models for privatized test sets. To illustrate, CNN can achieve $\approx 80\%$ accuracy for a test set privatized with ϵ's value is greater than 4. The final observation that we can make is that this correlation between CNN's accuracy and the value of ϵ can be used to develop a privacy settings recommendation system where users can tune the trade-off between privacy and visibility of their handwriting. Furthermore, this correlation can help a handwriting recognition system to implement a adjustable privacy on their system.

TABLE II
EXAMPLES OF THE LOCAL DIFFERENTIAL PRIVACY ON DIFFERENT HANDWRITTEN TEXTS.

Privacy level, ϵ						
Inf	0.1	0.3	0.5	1.0	3.0	5.0
						

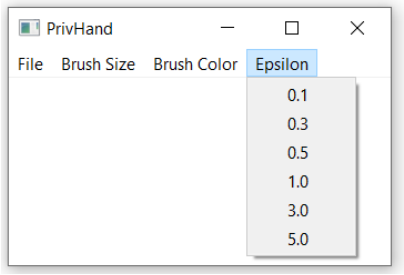


Fig. 7. $PrivHand$: Software tool to generate privacy-preserving handwriting using the proposed algorithm.

D. Visualization of the Proposed Algorithm

We implement a visualization tool, called $PrivHand$, to demonstrate the impact of the proposed algorithm on handwriting text. The long-term goal is to further integrate the research outcome to $PrivHand$ to develop a standalone open-source software for research and education. While the results in figure 6 show that the accuracy of the different algorithms, most importantly CNN's, increases with the increase in the value of ϵ, $PrivHand$ further highlights the relationship between the accuracy and privacy level. Figure7 demonstrate the UI of $privHand$. In its current version, it allows a user to select a privacy level (ϵ) to make his/her handwriting privacy-preserving. Table II demonstrates examples of privacy-preserving handwriting for different ϵ values, generated using $privHand$.

VII. Conclusion

This paper revisits the problem of handwriting recognition from a privacy perspective. The first defense mechanism against any privacy-invading attack is to privatize a user's data before it leaves the user's device. We show through our experiment that the accuracy of the traditional ML models drops significantly as we add more noise to the differentially private data set. On the other hand, deep learning models like CNN can achieve a relatively better accuracy under a considerable privacy level. Our findings suggest that focusing on deep learning models, rather than traditional ML algorithms is the way to go to develop a more robust model for privacy-preserving handwriting recognition. Future direction should aim to find the optimal privacy amount, and model tuning to improve the accuracy.

References

[1] Martin Abadi, Andy Chu, Ian Goodfellow, H Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. Deep learning with differential privacy. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 308–318, 2016.

[2] Mathias M Adankon and Mohamed Cheriet. Model selection for the ls-svm. application to handwriting recognition. *Pattern Recognition*, 42(12):3264–3270, 2009.

[3] Pathum Chamikara Mahawaga Arachchige, Peter Bertok, Ibrahim Khalil, Dongxi Liu, Seyit Camtepe, and Mohammed Atiquzzaman. Local differential privacy for deep learning. *IEEE Internet of Things Journal*, 7(7):5827–5842, 2019.

[4] Ekaba Bisong. Google colaboratory. In *Building Machine Learning and Deep Learning Models on Google Cloud Platform*, pages 59–64. Springer, 2019.

[5] Richard Camicioli, Seymour Mizrahi, Jacques Spagnoli, Christophe Büla, Jean-Francois Demonet, François Vingerhoets, Armin von Gunten, and Brigitte Santos-Eggimann. Handwriting and pre-frailty in the lausanne cohort 65+(lc65+) study. *Archives of gerontology and geriatrics*, 61(1):8–13, 2015.

[6] Mingyu Chen, Ghassan AlRegib, and Biing-Hwang Juang. Air-writing recognition—part i: Modeling and recognition of characters, words, and connecting motions. *IEEE Transactions on Human-Machine Systems*, 46(3):403–413, 2015.

[7] Mingyu Chen, Ghassan AlRegib, and Biing-Hwang Juang. Air-writing recognition—part ii: Detection and recognition of writing activity in continuous stream of motion data. *IEEE Transactions on Human-Machine Systems*, 46(3):436–444, 2015.

[8] Woo-Seok Choi, Matthew Tomei, Jose Rodrigo Sanchez Vicarte, Pavan Kumar Hanumolu, and Rakesh Kumar. Guaranteeing local differential privacy on ultra-low-power systems. In *2018 ACM/IEEE 45th Annual International Symposium on Computer Architecture (ISCA)*, pages 561–574, 2018.

[9] Li Deng. The mnist database of handwritten digit images for machine learning research [best of the web]. *IEEE Signal Processing Magazine*, 29(6):141–142, 2012.

[10] John C. Duchi, Michael I. Jordan, and Martin J. Wainwright. Local privacy and statistical minimax rates. In *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, pages 429–438, 2013.

[11] Cynthia Dwork. Differential privacy. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Automata, Languages and Programming*, pages 1–12, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[12] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of cryptography conference*, pages 265–284. Springer, 2006.

[13] Cynthia Dwork, Aaron Roth, et al. The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science*, 9(3-4):211–407, 2014.

[14] Mohamad Ivan Fanany et al. Handwriting recognition on form document using convolutional neural network and support vector machines (cnn-svm). In *2017 5th international conference on information and communication technology (ICoIC7)*, pages 1–6. IEEE, 2017.

[15] Liming Fang, Hongwei Zhu, Boqing Lv, Zhe Liu, Weizhi Meng, Yu Yu, Shouling Ji, and Zehong Cao. Handitext: handwriting recognition based on dynamic characteristics with incremental lstm. *ACM Transactions on Data Science*, 1(4):1–18, 2020.

[16] Peter Gareffa. Automakers adopt handwriting recognition for control of infotainment systems, May 2014.

[17] Maoguo Gong, Yu Xie, Ke Pan, Kaiyuan Feng, and Alex Kai Qin. A survey on differentially private machine learning. *IEEE Computational Intelligence Magazine*, 15(2):49–64, 2020.

[18] Lars Kai Hansen, Christian Liisberg, and Peter Salamon. Ensemble methods for handwritten digit recognition. In *Neural Networks for Signal Processing II Proceedings of the 1992 IEEE Workshop*, pages 333–342. IEEE, 1992.

[19] Hao Jiang. Motion eavesdropper: Smartwatch-based handwriting recognition using deep learning. In *2019 International Conference on Multimodal Interaction*, pages 145–153, 2019.

[20] Xinye Lin, Yixin Chen, Xiao-Wen Chang, Xue Liu, and Xiaodong Wang. Show: Smart handwriting on watches. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 1(4):1–23, 2018.

[21] Frank McSherry and Kunal Talwar. Mechanism design via differential privacy. In *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*, pages 94–103. IEEE, 2007.

[22] Thông T Nguyên, Xiaokui Xiao, Yin Yang, Siu Cheung Hui, Hyejin Shin, and Junbum Shin. Collecting and analyzing data from smart device users with local differential privacy. *arXiv preprint arXiv:1606.05053*, 2016.

[23] Xuebin Ren, Chia-Mu Yu, Weiren Yu, Shusen Yang, Xinyu Yang, Julie A McCann, and S Yu Philip. LoPub: High-Dimensional Crowdsourced Data Publication with Local Differential Privacy. *IEEE Transactions on Information Forensics and Security*, 13(9):2151–2166, 2018.

[24] Sara Rosenblum, Batya Engel-Yeger, and Yael Fogel. Age-related changes in executive control and their relationships with activity performance in handwriting. *Human Movement Science*, 32(2):363–376, 2013.

[25] Mary Jane C Samonte, Allyssa Raven I Garcia, Bianca Janine D Valencia, and Michael Jae S Ocampo. Using online handwritten character recognition in assistive tool for students with hearing and speech impairment. In *Proceedings of the 2020 11th International Conference on E-Education, E-Business, E-Management, and E-Learning*, pages 189–194, 2020.

[26] Annapurna Sharma and Dinesh Babu Jayagopi. Towards efficient unconstrained handwriting recognition using dilated temporal convolution network. *Expert Systems with Applications*, 164:114004, 2021.

[27] Ben Stoddard, Yan Chen, and Ashwin Machanavajjhala. Differentially private algorithms for empirical machine learning. *arXiv preprint arXiv:1411.5428*, 2014.

[28] Lichao Sun, Jianwei Qian, Xun Chen, and Philip S Yu. Ldp-fl: Practical private aggregation in federated learning with local differential privacy. *arXiv preprint arXiv:2007.15789*, 2020.

[29] Ning Wang, Xiaokui Xiao, Yin Yang, Jun Zhao, Siu Cheung Hui, Hyejin Shin, Junbum Shin, and Ge Yu. Collecting and analyzing multidimensional data with local differential privacy. In *2019 IEEE 35th International Conference on Data Engineering (ICDE)*, pages 638–649. IEEE, 2019.

[30] Lei Xu, Adam Krzyzak, and Ching Y Suen. Methods of combining multiple classifiers and their applications to handwriting recognition. *IEEE transactions on systems, man, and cybernetics*, 22(3):418–435, 1992.

[31] Tomer Yanay and Erez Shmueli. Air-writing recognition using smart-bands. *Pervasive and Mobile Computing*, 66:101183, 2020.

[32] Jian Zhang, Hongliang Bi, Yanjiao Chen, Mingyu Wang, Liming Han, and Ligan Cai. Smarthandwriting: Handwritten chinese character recognition with smartwatch. *IEEE Internet of Things Journal*, 7(2):960–970, 2019.

[33] Ping Zhang, Tien D Bui, and Ching Y Suen. A novel cascade ensemble classifier system with a high recognition performance on handwritten digits. *Pattern Recognition*, 40(12):3415–3429, 2007.