Under Pressure: Investigating the Effectiveness of the Apple Pencil as a Biometric Authentication Tool

Richard Deamicis
UC Irvine

Zane Karl
UC Irvine

Elina van Kempen
UC Irvine

Abstract

Biometric authentication systems, such as fingerprint scanning or facial recognition, are now commonplace and available on the majority of new smartphones and laptops. With the development of tablet-digital pen systems, the deployment of handwriting authentication is to be considered.

In this paper, we evaluate the viability of using the dynamic properties of handwriting, provided by the Apple Pencil, to distinguish and authenticate individuals. Following the data collection phase involving 25 participants, we examined the accuracy of time-series classification models on different inputs and on text-independent against text-dependent authentication, and we analyzed the effect of handwriting forgery. Additionally, participants completed a user survey to gather insight on the public reception of handwriting authentication. While classification models proved to have high accuracy, above 99% in many cases, and participants had a globally positive view of handwriting authentication, the models were not robust against forgeries, with up to 58.7% forgery success rate.

1 Introduction

The three ways of authenticating are commonly designated as "what you know", "what you have", and "what you are". Examples of these authentication methods are passwords, tokens, and fingerprints, respectively. Each method has specific drawbacks, e.g. passwords can be forgotten, and tokens can be lost.

Biometric-based techniques have been developed as an attempt to address some of these challenges. Biometrics leverage unique physical or behavioral characteristics of individuals to provide a convenient method of authentication. Biometrics are unique to each individual, difficult to steal, and do not rely on the user's memory. We distinguish static biometrics, usually physical characteristics, and dynamic biometrics, the behavioral characteristics of an individual. Common static biometrics include fingerprint scanning and facial recognition, while dynamic biometrics include voice patterns and facial movements.

Handwriting is a type of biometrics, that includes both static and dynamic properties. The visual, written form of a handwriting sample is a static factor, and the way in which someone writes, such as the angle they hold the writing instrument and how hard they press the instrument into the writing surface, is considered a dynamic factor.

Static properties of handwriting have been used consistently, usually in the form of signatures. Signatures are used to verify users on documents such as legal contracts and financial records. However, studies have been conducted that cast doubt on the viability of static handwriting properties alone to stand up to forgery in the face of modern artificial intelligence technologies [2, 4, 5].

Dynamic properties of handwriting are often used in the field of forensics. Specialists can extract these properties by carefully analyzing writing samples. Emerging technologies, such as artificial intelligence, machine learning, and sensors, lower the barrier to the adoption of these dynamic properties in user authentication.

Possible applications of live handwriting authentication, using dynamic features, comprise credit card payment signatures, package reception, access control, and electronic signature.

Collecting dynamic data from a handwritten sample requires special hardware, such as a pressure sensor or an accelerometer. Digital pens, such as the Apple Pencil, contain several sensors and provide the sensor data to the developer. These devices can thus be used to provide handwriting authentication. Furthermore, since tablets and digital pens are commercially available, a handwriting authentication system could be very easily implemented, without requiring the design of specific and additional hardware.

Contribution

In this paper, we investigate whether the Apple Pencil can be an effective biometric authentication tool, using dynamic

handwriting authentication. We consider the following four research questions as the focus of our work:

RQ1: Is data provided by the Apple Pencil's sensors distinct enough to achieve handwriting authentication?

RQ2: Which type of input would give the best accuracy when implementing handwriting authentication?

RQ3: Is enrollment convenient and realistic for real-world use?

RQ4: Would handwriting authentication be well-received by users?

Through the use of the Apple provided API PencilKit, we were able to directly capture the following handwriting features and indirectly, i.e. calculate after-the-fact, capture the associated features. Features are shown in Table 1.

Table 1: Direct and indirect handwriting features captured by the Apple Pencil

Direct	Indirect
altitude	average force/stroke
azimuth	average force/sample
force	speed
x-coordinate	average speed/stroke
y-coordinate	average speed/sample
time offset	strokes/sample
stroke number	unique strokes
sample number	

For the purpose of data collection, we developed an iOS application. Through this application, we gathered a diverse range of input types, including the user's name and simple drawings, to compare the effectiveness of these different inputs. After the data collection phase, we conducted a user survey to gauge the opinions users had of the hardware, process, and handwriting authentication as a whole. Finally, we examined the accuracy of a time-series classification model on the handwriting authentication task.

2 Related Work

Using one's handwriting as an authentication tool has been thoroughly studied, and a signature is a well-established and accepted way of authenticating a person. Most studies, either in the case of improving an authentication mechanism or in the case of forensic analysis, focus on the static analysis of a handwritten expression, i.e. analyzing the output "image" of the written content. This includes the analysis of the size and shape of the written characters, or the spacing between characters. Dynamic analysis of handwriting requires specific hardware, such as sensors and recording devices. Some features considered by dynamic analysis are the angle of the writing utensil, the amount of pressure applied to the writing surface, the speed at which the user writes, or the number of individual strokes used to create the written sample. Our work targets the dynamic analysis of handwriting on digital devices, so we will not discuss purely static analysis works.

Before the development of tablets and corresponding digital pens, custom-made digital pens were built by embedding specialized hardware such as pressure sensors and lasers into the actual pen [13, 16]. While the systems performed well, users in [18] reported discomfort in handling and manipulating the modified utensil, casting doubt that their resulting handwriting was fully representative of their standard handwriting.

Two signature datasets [15, 18] both contain data from people writing only or mainly using WACOM brand tablets and digital pens. A smaller amount of the data found in these datasets was collected using Samsung tablets with a stylus. [10, 14] evaluated their authentication models on one of the two datasets. A few studies, [3, 19], also using WACOM tablets, collected their own sample data for analysis. While high accuracy of classifiers for handwriting authentication was achieved, the availability and feasibility of deploying a handwriting authentication framework on the target devices was not reported. Previous work also fails to address the real-world usability of the devised systems.

Previous work involving Apple products and handwriting appear to be limited to [8] and [17]. The former is a analysis and exploitation, from 2021, of a side-channel attack on the Apple Pencil using its onboard magnetometer to infer what a user is writing. That is the attack seeks to observe the static output of a handwriting sample. The latter research is a paper from 1998 which details what is branded as the first automated handwriting recognition system developed for the Apple Computer Newton Message Pad. This product is no longer in commercial circulation and again focused on recognizing the static output of user handwriting. They did however employ state-of-the-art Neural Networks to their system demonstrating that the concept of applying machine learning to handwriting has a rich history.

3 Background

3.1 Apple Pencil

The Apple Pencil is a digital pen designed to work with Apple iPads. Available since 2015, the Apple Pencil 1 is listed at $99 while the Apple Pencil 2, available since 2018, costs $129. In this work, we used the Apple Pencil 2 only. It weighs 20.7 g and has length and diameter of 166 mm and 8.9 mm, respectively [1]. The Apple Pencil 2 charges by magnetically attaching it to a compatible iPad. In the second quarter of 2023, until April 1st 2023, Apple reported 6.67 million dollars in iPad sales [9]. Apple considers the Apple Pencil as an "accessory", so individual sales of the Apple Pencil are not

Figure 1: A screenshot of the interface of the iPad application for data collection.

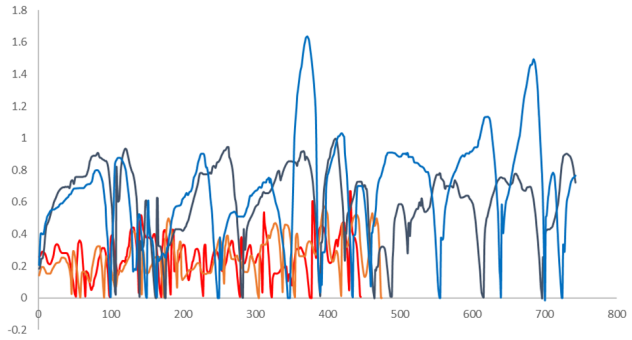

Figure 2: Force readings for individual 0, in red and orange, and individual 9, in light and dark blue. Two samples for each individual writing all ten digits.

recorded.

The Apple Pencil 2 provides pressure and tilt sensitivity to the user [1]. Through the UIKit framework, developers can access azimuth, altitude and force data from the Apple Pencil, sent with a 60-240Hz frequency. UIKit also provides the x and y position of the tip of the Apple Pencil on the screen [7].

3.2 MiniRocket

MiniRocket, [6], is the successor of Rocket, one of the fastest and most accurate time series classifier. Rocket's main contribution was an improvement in computational complexity by transforming input time series data using random convolutional kernels and then using the output of that to train a linear classifier. MiniRocket is able to improve on the speed of Rocket by up to 75 times while maintaining a comparable level of accuracy to the original Rocket.

4 Methodology

4.1 Data Collection

We used 3 Apple iPad Air devices and corresponding Apple Pencil 2 to collect data. To collect the data efficiently, we developed an application compatible with iPadOs 16.3.1, which communicates directly with a Google Sheets spreadsheet. The application prompts the user to write or draw some input, and sends the information to the spreadsheet. Figure 1 shows a screenshot of the application interface.

Each participant provided 21 unique inputs. The input values included both text and drawings. Examples include the participants name, the 10 digits, short words like "vegetarian" and "handwriting", and short phrases like "hello world". For the single word and short phrase inputs, we had the participants record them using all lowercase letters, and all uppercase letters. We also had each participant write the phrase "the quick brown fox jumps over the lazy dog." This sentence includes every character in the English language. Finally, we had the particiapnts draw an image of a cat, a fish, and a bird.

Each input was repeated five times, totalling 105 samples per participant. This led to an average of roughly 50,000 unique data points recorded from the apple pencil per participant. The number of data points had a fairly large range. The maximum number of data points collected from a single participant was over 87,000, while the minimum number was under 27,000. We attribute the large discrepancy to the writing speed and the letter size at which participants recorded their writing samples. With 25 individual users included in our dataset, we obtained a total of 2,625 writing samples.

After data collection, we asked users about their experience, satisfaction and concerns in a user survey. The user survey was conducted online via a Google Form, immediately after the participant completed recording all 105 samples.

4.2 Classification

The data provided by the Apple Pencil and UIKit framework consists of a series of points that make up multiple strokes. The iPad receives data from the Apple Pencil every 0.017 to 0.0042 seconds approximately [7].

Using sktime [11] and scikit-learn [12], we wrote several Python scripts to perform time-series data classification. Specifically, we used miniRocket [6] and RidgeClassifierCV.

For each model, 3 out of the 5 samples for each input were selected for training and 2 for testing. Figure 2 shows the force readings of two individuals (two sample readings per individual).

4.3 Forgery

We consider the threat model of skilled forgeries: the attacker has access to the handwritten content needed by the application, previously produced by the victim. The attacker can practice before trying to authenticate as the victim.

We obtained skilled forgeries attacking two participants, participant 0 and participant 1, with three data samples for every input. The forgers were different individuals for each forgery attack, so evaluation may also depend on the dexterity and experience of each attacker.

5 Evaluation

5.1 Classification Accuracy

Input comparison

For each input, a classification model decides the label of a test sample within 25 different labels, i.e. decides between all participants who most likely wrote the sample. To train the model, we selected three samples per participant and input, while two samples were reserved for testing purposes. We computed the accuracy and equal error rate (EER) for each model. These metrics assess the model's performance across inputs, showcasing differences in the model's behavior between separate inputs.

Table 2 summarizes the accuracy and equal error rate for each different input.

All the models had an accuracy above 92%, with the worst performing model, the classification using the bird drawing, having an EER of 0.397%. Perfect accuracy and null EER were observed in ten of the inputs.

A handwriting authentication system requesting each person to write a word 3 times only during the enrollment process would be able to achieve high accuracy.

Regarding the classification on simple drawings, it was surprising that the model using the fish drawing as input had a higher accuracy than the cat drawing model, since the cat drawing is the most detailed drawing chosen for this experiment.

We did expect the model trained on the bird drawing to be the least accurate, since it is the simplest, a one-stroke drawing.

Table 2: Accuracy and EER for each input

Input	***Accuracy (%)***	***EER (%)***
name	100.0	0
digits	98.0	0
carnivorous	98.0	0.099
CARNIVOROUS	100.0	0
vegetarian	98.0	0.099
VEGETARIAN	98.0	0
pineapple	96.0	0.198
PINEAPPLE	100.0	0
handwriting	100.0	0
HANDWRITING	98.0	0.099
security	100.0	0
SECURITY	98.0	0.099
computer	100.0	0
COMPUTER	98.0	0
hello world	94.0	0.298
HELLO WORLD	100.0	0
a short sentence	100.0	0
The quick brown fox [...]	100.0	0
cat drawing	96.0	0
bird drawing	92.0	0.397
fish drawing	100.0	0

Lowercase vs. uppercase

After splitting lowercase and uppercase words data, we compared the accuracy of classifying on lowercase and uppercase words. The selected words are "carnivorous", "vegetarian", "pineapple", "handwriting", "security", "computer" and "hello world".

With one model built to classify lowercase words, and one to classify uppercase words, for each word and each person, 3 samples were picked for training data and 2 for testing.

Table 3 displays the accuracy and EER for both lowercase and uppercase models. The lowercase-trained classification model had an accuracy of 98.9% and an EER of 0.064%, and the uppercase-trained model had an accuracy of 99.1% and an EER of 0.047%

The uppercase classification performs slightly better than lowercase. We hypothesize that since people write with bigger letters when writing in uppercase, this may lead to the collection of more data points in each sample, which could increase accuracy.

Table 3: Accuracy and EER for lowercase and uppercase input classification

	Accuracy (%)	**EER (%)**
Lowercase	98.9	0.064
Uppercase	99.1	0.047

Global vs. individual models

We define a "global model" a model that predicts between the 25 classification labels, i.e. one label per participant. An "individual model" is associated with one participant i and is binary: it should predict 1 if the sample was written by i, and 0 otherwise. Thus, one global model is sufficient for classification, and 25 individual models are needed to assess model performance for all participants.

First with a global model, we included all word samples in our evaluation, both lower and uppercase. We did not include sentences, names, digits, or drawings. The accuracy of the model was 99.2% and the EER 0.040%.

With individual models, the average accuracy was 99.5%

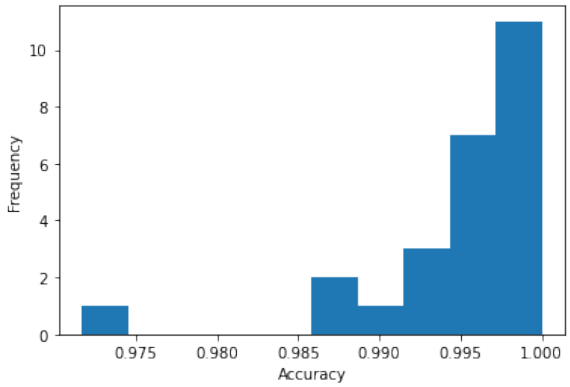

Figure 3: Accuracy of 25 binary models.

and the EER 0.021%. Figure 3 displays the distribution of the accuracy of individual models. We observe that 18 out of the 25 models have an accuracy above 99.5%.

The amount of storage needed for the individual models is similar to the one needed by the global mode: the global model was 2,000,402 bytes, and each individual model 80,882 bytes, for a total of 2,022,050 bytes for all 25 individual models.

Text-dependent vs. text-independent

Text-dependent classification indicates that the same text is used for both training and testing of the model, while text-independent classification seeks to predict on text that is different than the text available for training. Text-independent classification may be useful in some applications, e.g. continuous authentication.

In this experiment, we allowed models to train on 4 lowercase words, "carnivorous", "vegetarian", "pineapple", and "handwriting", and tested on 3: "security", "computer", and "hello world". We repeated this analysis on the same words, in uppercase.

Table 4 displays the accuracy and the EER for each model, including using both a global model, and individual models. The global model performed worse, with an accuracy of 84.5%, and an EER of 0.414% for lowercase, and an accuracy of 84.8% and an EER of 0.461% for uppercase. On the other hand, individual models had a higher average accuracy, with an average accuracy of 98.1% and 98.2%, and an EER of 0.267% and 0.167% for lowercase and uppercase, respectively.

In general, text-dependent classification models, presented in previous sections of this paper, were more accurate than text-independent classification models. To perform text-independent classification, using individual models can lead to higher accuracy.

Table 4: Accuracy and EER for text-independent models, for both a global model and averaged values for individual models.

		Accuracy(%)	**EER(%)**
Global model	Lowercase	84.5	0.414
	Uppercase	84.8	0.461
Individual models	Lowercase	98.1	0.267
	Uppercase	98.2	0.167

Table 5: Fraction of successful forgeries

	Model	**% of successful forgeries**
Forgery of 0	Global	4.76%
	Individual	58.70%
Forgery of 1	Global	4.76%
	Individual	34.90%

5.2 Forgery

In this section, we studied the effect of skilled forgery on classification. A skilled forgery is defined in opposition to random forgery: a skilled forger has access to the victim's handwriting samples and can practice, while a random forger just guesses a person's handwriting.

We obtained two forgeries, one for participant 0 and the second for participant 1. Each forgery was performed by a different forger. Each forger had 3 tries per input, resulting in 63 data samples per forgery.

Table 5 presents the average percentage of successful forgeries for each writing input, out of all 63 data samples for both forgeries. We evaluated forgery success for both the global model and the victim's individual model. We consider a forgery "successful" if the predicted label corresponded to the victim when predicting on forged data.

Using the global model, forgeries were successful in 4.76% of the tries for both victims. With individual models, forgeries were successful 58.7% and 34.9% of the time, for participants 0 and 1 respectively.

The forgeries had a high rate of success in all cases, highlighting the need to train models to be robust against forgeries.

5.3 User study

In this section, we report participants' answers to the user survey, which they completed after data collection.

Initial questions aimed to assess the participants' opinions on the Apple Pencil device. First, participants shared their satisfaction with using the Apple Pencil, rating the following statements:

- "The Apple Pencil was easy to use."
- "I experienced no physical discomfort or strain when using the Apple Pencil."

Participants' answers are shown in Figure 4. The majority of users considered the Apple Pencil easy to use, with only 2 of the 25 participants that did not find the device simple to control. Note that 7 of the 25 participants had never tried an Apple Pencil before, and 6 had only tried it a few times only. Out of these 13 participants, only 1 found the Apple Pencil hard to handle. One participant commented that the digital pen "flowed really well, felt like a regular pencil". However, 4 participants did experience some physical discomfort or strain when using the Apple Pencil, which may be due to the prolonged and constant use during data collection, as well as the tiredness due to writing the same text multiple times. Specifically, users commented that "it is heavier than the usual pen", and "hand started to cramp".

We then asked participants which input type was their favorite, in a situation where they would use handwriting authentication. Figure 5 displays participants' answers, with the majority of participants preferring words or doodles. A participant that enjoyed using words as input better expressed that "doodles were too hard, sentences made my hand cramp", while another with doodles as the preferred input type stated that "they were more fun".

Later questions focused on the perception of usefulness of handwriting authentication. 17 participants agreed or strongly agreed that they would use handwriting authentication in their daily life, if given the opportunity. Two participants wrote that handwriting authentication would be "great for large purchases", and that they would use handwriting authentication "if implemented in software like DocuSign". On the other hand, one participant commented "No secure. I don't trust it".

Participants then rated the usefulness of handwriting authentication for specific applications: electronic document signatures, credit card payment signatures, package reception, essay writing, art, and access control. Figure 6 displays the results, and shows that using handwriting authentication for signatures, both for electronic documents and credit card payments, was identified as useful by 21 and 23 out of 25 participants, respectively. Implementing handwriting authentication for essay writing did not seem useful for 11 of the 25 participants.

Finally, we asked participants about any security concerns they had if handwriting authentication were to become available. Participants first commented that using handwriting authentication was more secure than using written signatures only, writing that "it is like normal writing but with more data to authenticate" and "no one looks at traditional handwriting". Meanwhile, when asked if they had any privacy or security concerns regarding the use of handwriting authentication, many participants answered positively. We list below participants' answers to the question "Do you have any privacy or security concerns regarding the use of handwriting authentication technology?":

- "Don't want my identity stolen"
- "I would like to have professionals evaluate the security and show the results."
- "Yes, how easy to forge is it?"
- "I do not have anything specific but I feel like there might be some problems."
- "Yes, handwriting can be forged"
- "Yes" (twice)
- "Some privacy concerns"
- "Hacking"
- "Ppl's handwriting change from time to time"
- "Handwriting may change "
- "My concerns are whether the technology would accurately get my signature from a forger"

Still, 13 of the 25 participants did not report any privacy or security concern.

When asked about their fear of getting their handwriting forged, only 5 out of 25 participants were not concerned that someone would forge their handwriting. Since forgery seems to be a common concern, and implementation of handwriting authentication should benchmark robustness against forgery.

6 Discussion and limitations

In this section, we discuss some limitations in our approach and limitations to handwriting authentication, and also discuss the deployability of handwriting authentication using an Apple Pencil.

While the accuracy of handwriting authentication proved to have high accuracy, several factors may impact our results. First, during the data collection phase, users often reported fatigue and boredom, because of the repetitiveness of the task. Because of this, they may start writing faster or with less precision towards the end of the data collection process. Additionally, for users that may not have used an Apple Pencil or similar digital pen before, they may have been slower at the beginning of the data collection. Some users also paused for several seconds in the middle of writing a sentence.

The number of participants in our dataset may also influence accuracy of the models, as a bigger dataset may lead to lower accuracy.

6.1 Limitations to handwriting authentication

Obvious physical limitations to handwriting authentication are injuries and disabilities, e.g. a person may have a broken wrist or arm and be unable to write for some short or long period of time, or have a permanent disability preventing them from having a distinct handwriting.

Additionally, some people do not know how to write, and will be unable to auhtenticate in this way.

A person's handwriting may also change with time, requiring regular re-enrollment. This is especially true for children whose handwriting changes as they acquire more dexterity.

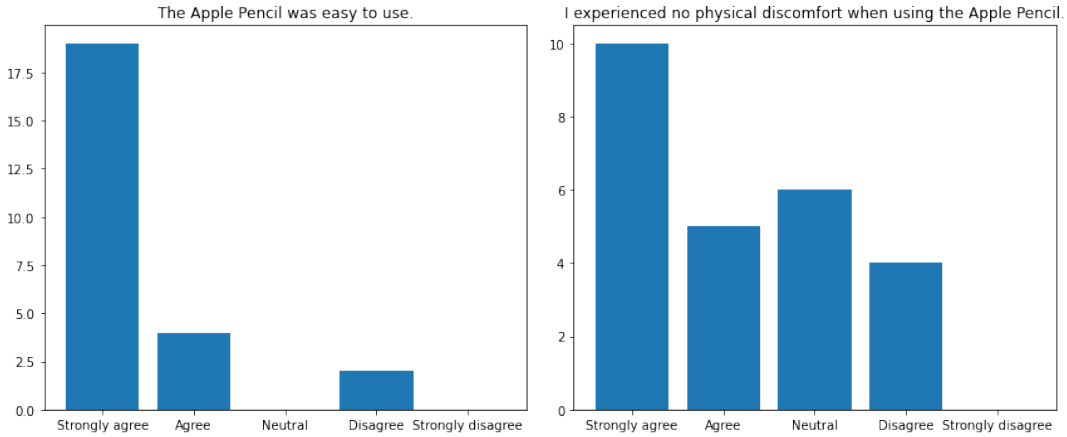

Figure 4: User satisfaction concerning the use of the Apple Pencil.

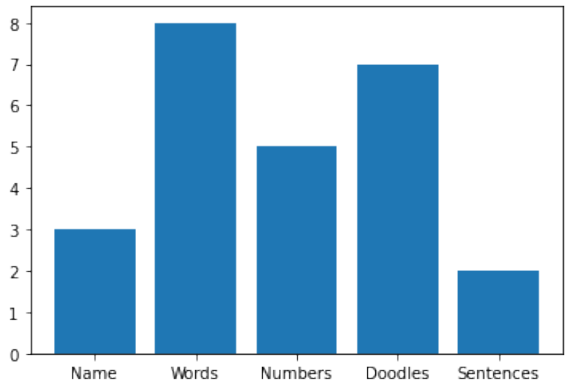

Figure 5: Answers to: "Which type of input did you prefer when writing?"

A timeline for periodic re-enrollment would need to be estimated.

Finally, attacks against handwriting authentication using digital pens would need to be thoroughly studied.

6.2 Deployability

The potential for deployability depends on the ease of enrollment, familiarity of users with the system and ease of use, and hardware availability and price.

We found that 68% of the participants owned a digital pen and used it at least occasionally. Note that this study took place in a college setting and this number may not be representative of the overall population. Most participants had only ever tried the Apple Pencil, only 3 used a different brand of digital pen, e.g. HP Pen and Microsoft Surface Pen. The same fraction of participants found writing a few words to be fast, indicating that writing authentication would not be an overbearing burden on users.

Besides, the time needed to transform and classify 600 data samples was 7.61 seconds, giving an average of 12.68 milliseconds per data sample.

However, the classification accuracy may decrease as the number of users in the dataset increase, limiting applications or requiring extra techniques for accurate authentication. Similarly, the size of the classification model increases as a function of the number of users, increasing the storage needs for large datasets.

Lastly, the price of the Apple Pencil, along with the required iPad, can be a factor that would prevent some individuals or organizations from deciding to use handwriting authentication.

7 Conclusion and Future Work

While handwriting authentication can demonstrate high accuracy of identification, further evaluation of the models' robustness against forgeries is necessary before deploying any handwriting authentication system. Furthermore, both topics of forgery by AI or deep learning models and adversarial attacks on handwriting authentication models need more research.

Future work will aim at expanding our dataset and making it publicly available, to allow additional contributions. We expect future research in this area to work toward improving the handwriting classifying models by performing feature extraction and selection.

Inspired by handwriting authentication, we intend to explore the possibility of authenticating digital art using the Apple Pencil's properties. An entire artistic project will likely provide distinguishing features corresponding to the given artist. In this way, digital art might be "signed" by virtue of its style and method.

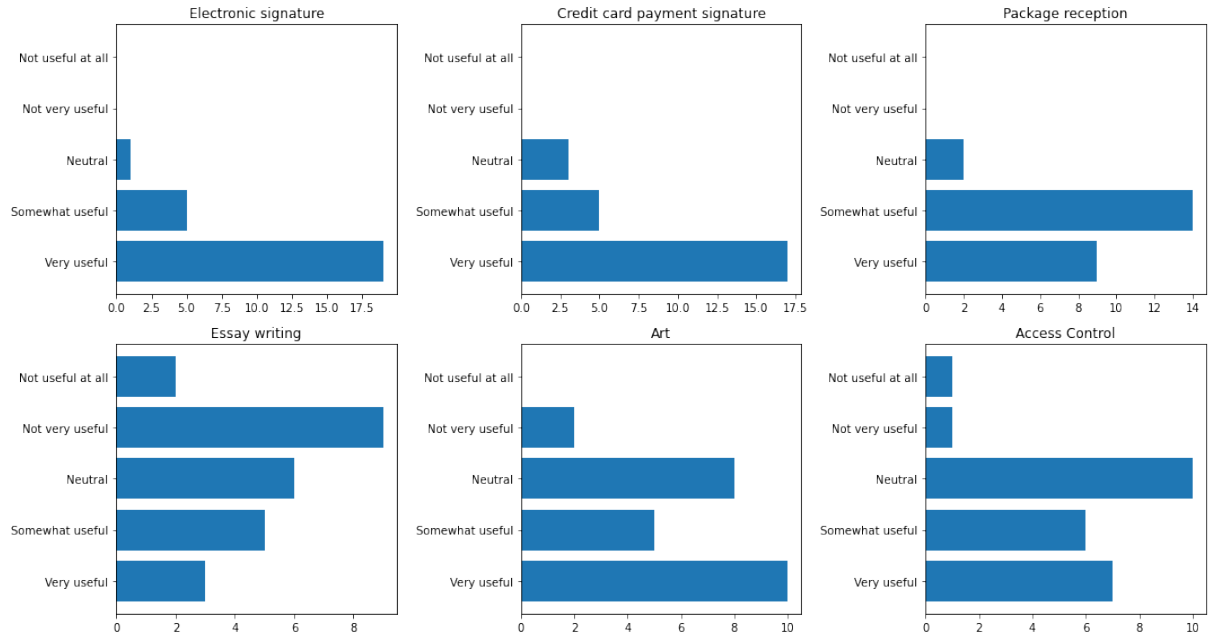

Figure 6: Answers to: "For the following applications, rate how useful handwriting authentication would be."

References

[1] Apple. Buy apple pencil 2. https://www.apple.com/shop/product/MU8F2AM/A/apple-pencil-2nd-generation.

[2] Lucas Ballard, Daniel Lopresti, and Fabian Monrose. Evaluating the security of handwriting biometrics. In *Tenth International Workshop on Frontiers in Handwriting Recognition*. Suvisoft, 2006.

[3] Muzaffar Bashir and Florian Kempf. Advanced Biometric Pen System for Recording and Analyzing Handwriting. *Journal of Signal Processing Systems*, 68(1):75–81, 7 2012.

[4] Ameur Bensefia and Hatem Tamimi. Validity of handwriting in biometric systems. PRAI 2018, page 5–10, New York, NY, USA, 2018. Association for Computing Machinery.

[5] Jin Chen. Handwritten biometric systems and their robustness evaluation: a survey. In *Technical Report*. Citeseer, 2012.

[6] Angus Dempster, Daniel F. Schmidt, and Geoffrey I. Webb. Minirocket: A very fast (almost) deterministic transform for time series classification. In Feida Zhu, Beng Chin Ooi, and Chunyan Miao, editors, *KDD '21: The 27th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, Virtual Event, Singapore, August 14-18, 2021*, pages 248–257. ACM, 2021.

[7] Apple Developer Documentation. Handling input from apple pencil. https://developer.apple.com/documentation/uikit/pencil_interactions/handling_input_from_apple_pencil.

[8] Habiba Farrukh, Tinghan Yang, Hanwen Xu, Yuxuan Yin, David Simchi-Levi, and Z. Berkay Celik. S3. *Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies*, 5(1):1–25, 3 2021.

[9] Apple Inc. Condensed consolidated statements of operations. https://www.apple.com/newsroom/pdfs/FY23_Q2_Consolidated_Financial_Statements.pdf, May 2023.

[10] Azhar Ahmad Jaini, Ghazali Sulong, and Amjad Rehman. Improved dynamic time warping (DTW) approach for online signature verification. *CoRR*, abs/1904.00786, 2019.

[11] Markus Löning, Anthony J. Bagnall, Sajaysurya Ganesh, Viktor Kazakov, Jason Lines, and Franz J. Király. sktime: A unified interface for machine learning with time series. *CoRR*, abs/1909.07872, 2019.

[12] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay. Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research*, 12:2825–2830, 2011.

[13] R. Renuka, V. Suganya, and B. Arun Kumar. Online handwritten character recognition using digital pen for static authentication. In *2014 International Conference on Computer Communication and Informatics*, pages 1–5, Coimbatore, 2014.

[14] Mohammad Saleem and Bence Kovári. K-nearest neighbour and dynamic time warping for online signature verification. *CoRR*, abs/2111.14438, 2021.

[15] Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, and Javier Ortega-Garcia. Deepsign: Deep on-line signature verification. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 3(2):229–239, 2021.

[16] J. Wang and F. Chuang. An accelerometer-based digital pen with a trajectory recognition algorithm for handwritten digit and gesture recognition. *IEEE Transactions on Industrial Electronics*, 59(7):2998–3007, 2012.

[17] Larry Yaeger, Brandyn Webb, and Richard Lyon. Combining neural networks and context-driven search for on-line, printed handwriting recognition in the newton. *AI Magazine*, 19(1):27–45, Spring 1998.

[18] Dit-Yan Yeung, Hsu-Yung Chang, Yun Xiong, Sebastian E. George, Richard S. Kashi, Tsutomu Matsumoto, and Gerhard Rigoll. SVC2004: First international signature verification competition. In *Lecture Notes in Computer Science*, pages 16–22. Springer Science+Business Media, 2004.

[19] Farhana Javed Zareen and Suraiya Jabin. Authentic mobile-biometric signature verification system. *IET Biometrics*, 5(1):13–19, 2 2016.