

Sign H3re: Symbol and X-Mark Writer Identification Using Audio and Motion Data from a Digital Pen

Maximilian Schrapel
HCI Group, Leibniz University
Hannover
Hannover, Germany
schrapel@hci.uni-hannover.de

Dennis Grannemann
HCI Group, Leibniz University
Hannover
Hannover, Germany

Michael Rohs
HCI Group, Leibniz University
Hannover
Hannover, Germany
rohs@hci.uni-hannover.de

ABSTRACT

Although in many cases contracts can be made or ended digitally, laws require handwritten signatures in certain cases. Forgeries are a major challenge with digital contracts, as their validity is not always immediately apparent without forensic methods. Illiteracy or disabilities may result in a person being unable to write their full name. In this case x-mark signatures are used, which require a witness for validity. In cases of suspected fraud, the relationship of the witnesses must be questioned, which involves a great amount of effort. In this paper we use audio and motion data from a digital pen to identify users via handwritten symbols. We evaluated the performance our approach for 19 symbols in a study with 30 participants. We found that x-marks offer fewer individual features than other symbols like arrows or circles. By training on three samples and averaging three predictions we reach a mean F1-score of $F1 = 0.87$, using statistical and spectral features fed into SVMs.

CCS CONCEPTS

• **Human-centered computing** → **Accessibility technologies; Gestural input.**

KEYWORDS

digital pens, signature authentication, signing documents, pattern recognition, handwriting recognition, motor impairments, accessibility

ACM Reference Format:

Maximilian Schrapel, Dennis Grannemann, and Michael Rohs. 2022. Sign H3re: Symbol and X-Mark Writer Identification Using Audio and Motion Data from a Digital Pen. In *Mensch und Computer 2022 (MuC '22)*, September 4–7, 2022, Darmstadt, Germany. ACM, New York, NY, USA, Article 111, 10 pages. <https://doi.org/10.1145/3543758.3543764>

1 INTRODUCTION

Even today, handwritten signatures are an important means of identifying a person. Although electronic signatures offer a digital alternative [20], the legal situation defines several cases in which a physical handwritten signature with a pen on paper is necessary. According to the National Telecommunications and Information

Administration (NITA), cases include, for example, wills and testamentary dispositions, family law cases (e.g. divorce or adoption), insurance policy cancellations, products with significant health risks, all documents for the transport of hazardous materials and utility cancellations [87]. German law requires that every document in which rights are exercised must be signed. However, unless otherwise specified (e.g. testamentary dispositions [28]), documents can be signed digitally [27]. In addition, the finance and business sectors remain subject to physical signature requirements. Even today, businessmen travel around the world for notarized signatures in order to conclude valid contracts. In the financial sector, paper checks and debit cards require signatures for validity. Decentralized finance (DeFi) aims to offer a future alternative [22]. For instance, in contrast to banks, smart contracts on the Ethereum blockchain are not subject to human involvement. They can be seen as a type of account in the network with a balance and functions defined by code. Other accounts can irreversibly submit transactions to execute these functions [23]. Smart contracts offer various advantages, including anonymity, efficiency, transparency, and providing financial services to people without access to bank accounts [22]. However, legal enforceability is still unclear [29], implying that signatures are likely to remain important. Handwriting is unique because it is influenced by training, physiology, and further behavioral factors over a lifetime [26, 83]. Verifying the validity of a signature poses a major challenge. The mismatch of signatures on mail ballots with signatures on file led to the rejection of thousands of votes in the past 2012 and 2016 U.S. presidential elections [80]. In the same time period cases of signature fraud in Canada tripled between 2014 and 2016 [21].

These examples demonstrate the need for security precautions due to legal requirements and the risk of forged signatures. The verification of x-mark signatures in particular, which must be witnessed for legal validity, presents a major challenge. Illiteracy or disabilities may result in an individual not being able to write his or her full name. The witness of a x-mark signature serves to verify and confirm the identity of the writer. Hence, x-mark signatures do not provide sufficient security and validity for online signed contracts when no witness is involved. In cases of suspected fraud, witnesses of an x-mark signature must be investigated. Forensic methods on the x-mark handwriting are limited to stroke features like length, direction, orientation and connection as well as features related to pen and paper, such as line quality and the crossing point position [39, 43, 63].

In this paper, we present an approach to measure the individuality of handwritten symbols with predefined writing instructions for user identification. Recorded data of a digital pen when signing



This work is licensed under a Creative Commons Attribution International 4.0 License.

MuC '22, September 4–7, 2022, Darmstadt, Germany
© 2022 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-9690-5/22/09.
<https://doi.org/10.1145/3543758.3543764>

a contract can support in cases of suspected fraud to identify the writer. We use measured motion data and scratching sounds from a digital pen [78]. We conducted a user study with 30 participants as a proof-of-concept and to collect a dataset of 19 different symbols for authentication. On this dataset different feature sets, which are fed into SVMs, are analyzed for their applicability for writer identification. In our tests, we focus on small training sample sizes, as it would be inconvenient for a person to write his or her x-mark signature several times before the proposed system is able to identify the handwriting. We show that by combining audio data – of the scratching sound that the pen tip makes when it moves across the paper – with 3D acceleration and gyroscope data of the pen, just three training samples of a symbol are sufficient to reach an average F1-score of over 87 % on writing three test symbols. In addition, alternative symbols were identified that are easy to draw and, with our approach, reach higher F1-scores than commonly used x-marks.

2 RELATED WORK

Signature verification can be divided into offline [84] and online approaches [12]. Offline verification usually requires signature image analysis for proving one’s identity [37, 57]. Therefore, it only relies on features from the signature image. Skilled forgers imitate the style of a signature to claim a person’s identity. Online approaches use data recordings of the writing process to identify user-specific features. The larger number of features compared to offline approaches usually results in higher accuracies [45] and makes it more difficult for forgers to mimic a signature. As digital pens usually implement online-verification [89], we here briefly review online approaches related to digital devices and handwriting as well as digital pens.

Smartphones are plausible candidates for e-signatures. Beside their integrated authentication features, signatures drawn with the finger on the display have been proposed as a feasible alternative [76]. In addition to the visual representation, features such as sound and vibration can also be measured via the embedded motion sensors on the input device [92, 93]. Several classification methods have been applied on pictorial and force-related features including Dynamic Time Warping (DTW) [24, 70, 95], Hidden Markov Models (HMM) [25, 47, 66], Neural Networks [3, 46, 53, 81] as well as Support Vector Machines (SVM) [10, 34, 35] and Random Forests (RF) [64]. More recently, smartwatches gained attention for authentication purposes. For instance, drawing gestures [58] or signatures in the air [5, 14, 36, 56, 61, 65, 68, 86] can offer an unobtrusive authentication method [13]. The motion of a pen can also be tracked by wrist-worn devices for authentication [33, 60] and for recognizing text [75] or gestures [11]. In addition, other smartwatch measurements, such as blood volume changes, can increase the reliability of a signature belonging to a certain person [73]. The bending of fingers contains user-specific features [2] as well as arm movements [74], hand gestures [99] and even simple button presses can differentiate users [72]. In the vicinity of the pen, the scratching sound that the pen tip makes when it moves across the paper can serve as a distinguishing feature [19, 59, 100]. Via inaudible sound signals from a smartphone, vertical movement variations of the pen can be estimated from the reflected sounds [15]. However, it should

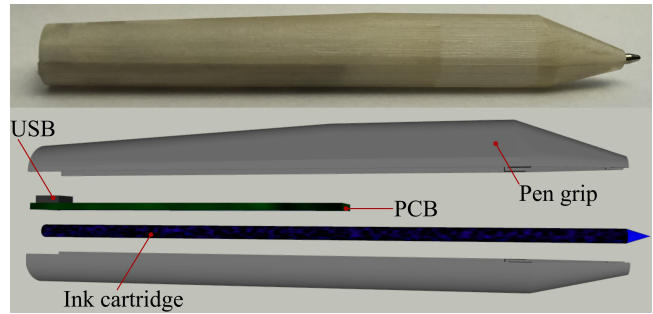


Figure 1: The 3D-printed pen prototype ($w = 12\text{cm} \times d = 1.5\text{cm}$) based on [78] with improved case (added a pen grip).

be mentioned that audio alone is not secured against replay attacks [93] and sensor data alone are not sufficient for a valid signature according to the legal situation [18].

Digital pens emit ink on the paper for legally valid contracts and measure related handwriting features, mostly related to the motion of the pen [32, 42, 69, 90]. Companies like Anoto [1], Wacom [16], and Stabilo [30] offer digital pens for education and industrial applications. In addition, 3D Systems introduced a haptic pen input device that can be utilized to write signatures in the air [17]. Modular concepts for digital pens have been proposed to allow users to create their own applications [88] with different input and output modalities [52, 55, 91, 97]. Integrating fingerprint sensors [85] provides additional security mechanisms, e.g. for biometric authentication in pharmaceutical digital audits [1]. The pressure on the pen grip is another source for individual handwriting features [7, 9, 40, 51] and also pressure applied to the surface is a relevant feature [8, 67]. Pictorial features can not only be obtained from cameras [82] but also via magnet tracking, which has been used for sketching on the back of the hand [77] and signatures [49, 50]. Combinations of audio and motion data have been applied for pen-based handwritten digit recognition [78].

In contrast to related work, we explore the applicability of simple and easy to draw symbols for user authentication. Along with predefined writing trajectories, authentication becomes particularly challenging, because forgers do not have to fully learn another person’s handwriting. Furthermore, as few samples as possible should be used for training in order not to stress users who are only able to produce simple x-mark signatures. As previously applied for handwritten digit recognition [78], we combine audio and motion of a digital pen for our approach.

3 PROTOTYPE

Our prototype is based on Pentelligence by Schrapel et al. [78]. Data is transmitted via USB to the PC for further analysis. The integrated contact microphone samples audio data at a rate of 7.1 kHz and 3D accelerometer as well as 3D gyroscope measurements at a rate of 800 Hz. Ambient noise is attenuated by the housing, thus mainly scratching sounds are measured during writing. Symbols and strokes are separated by detecting when the pen tip touches the writing surface. For this purpose, a pin is soldered on the spring, which is connected to electrical ground on the PCB. When the pen

tip touches a surface, the pin on the spring of the ink cartridge closes a contact to the PCB for identifying writing.

In contrast to the earlier prototype of Schrapel et al. [78] we improved the case by adding a pen grip to constrain the ways the pen can be held. This reduces one source of intra-user variability and helps to capture the way the pen is held in the motion data. Figure 1 shows the prototype printed with a Keyence AGILISTA and the corresponding 3D model with the position of the internal PCB.

4 USER STUDY

We conducted a study to collect a dataset of various easy to draw symbols. In order to adhere to a skilled forgery setup, we gave instructions regarding the order and direction of the strokes of each gesture. Figure 2 on the right, shows our gesture set with predefined writing instructions. Each of our selected symbols just consists of a few strokes and taps, since we aimed to analyze the individuality of symbols that are comparable in complexity to x-mark signatures. For x-marks we use the most frequently occurring writing trajectory in signing tasks [63]. In addition, common gestures from related work [38, 42, 48, 62] were selected to analyze their applicability for writer identification. In total 19 gestures were selected for our study.

We invited 30 volunteers aged 18 to 56 years ($M = 25.6$ years, $SD = 10.3$ years) including 5 female and 25 male individuals. Two of the male participants were left-handed writers. All participants reported feeling well and rested, which is important because fatigue affects handwriting [4]. Our study procedure was adapted from Schrapel et al. [78]. The study was conducted in a quiet office environment to avoid interfering the internal audio measurements and to allow the participants to focus on their tasks. We began by introducing our prototype and the study procedure. We stated that we intended to collect and analyze gestures with the digital pen. The participants were instructed to repeatedly write a symbol on a 21.0×29.7 cm white squared paper with a box size of 11×14 mm and 15 boxes per row. The symbol and its writing instruction was displayed on a nearby screen. To simplify the selection of individual symbols, the writing of a symbol was confirmed with a short beep and the current count was displayed with a green background. Symbols were cropped in time from the data stream by storing the data from 20 ms before to 20 ms after the pen tip touched the paper. Between two strokes more than 500 ms had to elapse to be recognized as two different symbols. Figure 2, left, shows a participant during the study procedure. All 19 symbols were collected in random order. After writing a symbol 20 times, another symbol was displayed until all symbols were written. When a participant accidentally wrote a symbol before hearing the soft beep sound, used the wrong writing instruction or wrote a wrong symbol, the samples were discarded and repeated. This ensured that a clean and balanced data set was created.

5 RESULTS

We analyzed the collected dataset in order to investigate the individuality of the handwritten symbols. Here, we focus on the use of a small number of training samples with SVM classifiers, as it would be inconvenient, e.g. in the case of signing contracts, to give one’s own (symbol-) signature many times before an identification

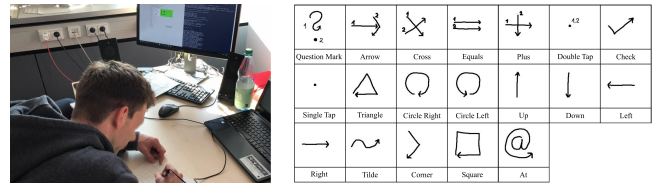


Figure 2: Study setup and gestures. The photo shows a participant writing symbols on squared paper. The screen displayed symbols with writing instructions. The set of symbols is visualized on the right. The arrows and numbers represent the writing direction and stroke sequence, respectively.

system can be used. Our total dataset consists of 11,400 samples including 380 samples per user with 20 samples for each of the 19 symbols.

5.1 Feature Creation

For our analysis, we decided to evaluate different preprocessing steps in the frequency domain for keeping the length of the resulting feature vector constant among the cropped samples [54, 98]. To create the feature vector, we first convert the audio signal of each sample into spectral components using a Fast Fourier Transformation (FFT). This is done by splitting the signal of the symbol into one, two, or three equal parts and then applying the FFT to each part. By splitting the data stream, a time component is integrated into the feature vector which may contains additional information about the time depended writing speed and scratching sounds. After normalizing each resulting set of amplitudes by the maximum value and adding the array to the feature vector, statistics are calculated from the raw audio signal. We use the mean and median value as well as standard deviation, and variance of the signal, normalized in the interval [0,1]. In addition, we count the number at which the normalized signal reaches the maximum and minimum value. The time interval between two peaks is also counted. From the counted numbers we calculate the previously applied statistical metrics, normalized by the signal length. This integrates general features of a handwriting into the feature vectors. Then, the same procedure is repeated for the motion data by first summing up the accelerometer

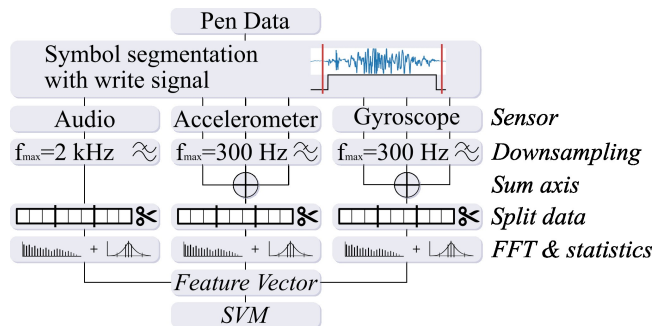


Figure 3: The block diagram depicts the algorithm for calculating a feature vector. Each sensor data is processed separately and then concatenated to a feature vector.

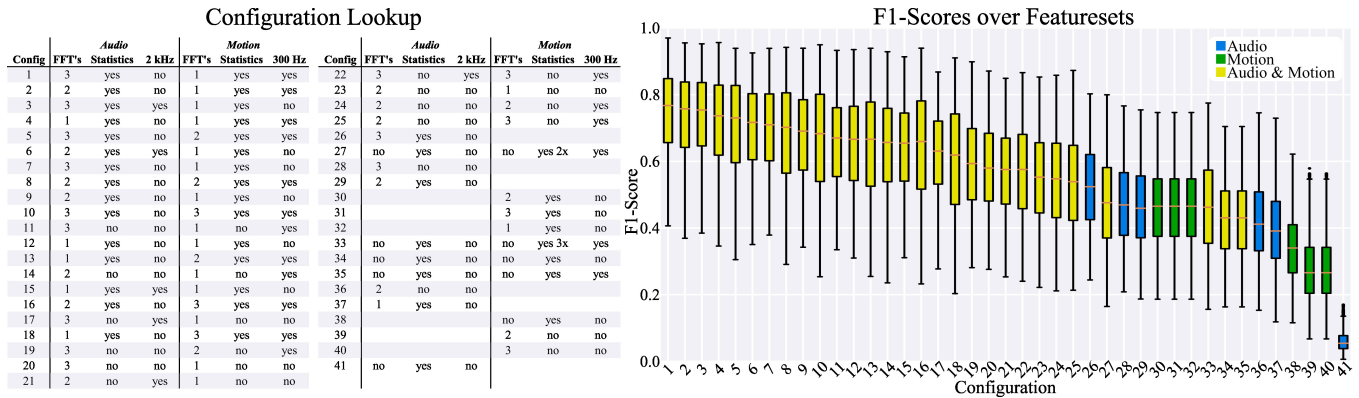


Figure 4: F1-score analysis of different feature sets. The tables on the left show the analyzed feature vector generation methods for the visualization on the right. The box plots visualize the F1-scores of different feature vectors including signal splitting, FFTs, statistical features, and downsampling.

axes and gyroscope axes separately. For each summed sensor signal FFTs and statistical features are calculated using the same methods as for audios. The most relevant feature components for audio in handwriting recognition are located below 1 kHz [78]. To correctly measure the relevant features, the signal must be sampled with at least twice this cutoff frequency [79, 94]. Thus, we also added the downsampled audio signal to 2 kHz to the analyzed feature set. For motion we downsampled the signal to 300 Hz. Downsampling attenuates high-frequency noise and can may support a classifier to focus on user-specific features. Figure 3 visualizes the process of generating the feature vector sets.

5.2 Feature Analysis

To analyze the symbols on their suitability for writer identification, we first optimize the SVM parameters and then continue by cross validating on each given feature vector set. The SVM hyperparameters *kernel* (linear or *rbf*) and cost *C* (1, 10, 100, 100) are optimized via grid search [71]. The goal of this initial grid search process is to recognize the 30 writers on all symbols as accurately as possible for each previously calculated feature set. Using the established SVM parameters on a given preprocessed dataset, we randomly split the data of each writer into 70 % for training and 30 % for testing. Hence, for each training iteration the training set consists of 266 samples per writer. The SVM is then trained using in total randomly picked 7980 samples to identify the 30 users. We repeat the training and test procedure for 25 times on each corresponding feature set and note down the resulting metrics, i.e. accuracy, precision, recall, and F1-score. As proposed by Levy et al. [57], for each feature set we use the same set of random seeds to obtain comparable results. We performed the procedure on 41 different feature sets resulting in a total of 1,025 tests (41 feature sets × 25 training and testing).

Figure 4 on the right shows the results of our feature vector tests sorted by the maximum average F1-score. We obtained an average (macro) F1-score of $F1 = 0.78$ ($SD = 0.05$) with comparable recall ($R = 0.78$; $SD = 0.12$) and precision ($P = 0.79$; $SD = 0.12$) on the best performing feature set. Stating the average AUC score of $AUC = 0.96$ ($SD = 0.03$) and equal error rate $EER = 0.09$ ($SD = 0.04$) is misleadingly high in our case, because for each of the 30 classes

(writers) there exist 114 positive and 3,306 negative test samples. Thus, we will continue reporting F1-scores. In general we derive from the tests that the statistical features have a substantial contribution to the distinguishability of users, and by splitting the audio signal into three parts further improvements are achieved. Combining audio and motion measurements from pens for user identification ($\overline{F1} = 0.74$; $SD = 0.12$) clearly outperforms audio alone ($\overline{F1} = 0.53$; $SD = 0.12$) and motion alone ($\overline{F1} = 0.46$; $SD = 0.11$). On all our 41 SVM hyperparameter optimizations, linear kernels showed better results than Gaussian kernels (*rbf*). In 31 cases a cost parameter of $C = 10$ was selected, followed by five cases using $C = 1000$ (selected by the SVMs trained exclusively on statistical features) and three cases using $C = 100$. A larger C value corresponds to a smaller margin hyperplane and defines how strongly a sample is penalized inside the margin. The best performance is achieved when the raw audio of the samples is splitted into three equal parts where of each statistical features and FFTs are added to the feature vector. Data of accelerometer axes and gyroscope axes are downsampled to 300 Hz and summed up respectively. The FFT and statistical metrics are calculated from each of the two summed signals and added to the feature vector. Splitting of the summed motion signals is not applied. The grid search on this best performing feature set resulted in using a *linear kernel* with a *cost C = 1* for the trained SVMs. For the best performing feature set we repeated the grid search test on three, four, and five-degree polynomial kernels and a sigmoid kernel, again obtaining the best results with a linear kernel with a $C = 1$.

5.3 Symbol Analysis

We now analyze symbols with respect to their suitability for writer identification by using the best-performing feature set and corresponding SVM hyperparameters. The cross validation test is repeated by using one, three, five, and ten training samples. For each training size on each symbol we perform 25 tests by using a fixed set of random seeds to pick training and test samples. In total 1,900 multi-class SVMs were trained and tested (4 training sizes × 19

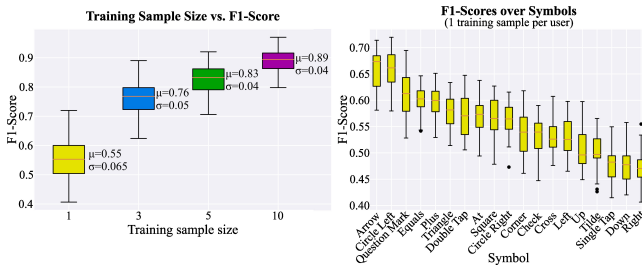


Figure 5: Training size and symbol analysis. The left plot depicts the impact of training sample count on the average F1-score over all symbols. The right plot compares the F1-scores of each symbol with one training sample. We use the best performing SVM hyperparameters and feature set for the results. One training example was chosen to illustrate the most challenging use case.

symbols \times 25 tests). We analyze the influence of the training set size on the F1-score of the classifiers for each symbol.

In Figure 5 on the right, the symbols are displayed sorted by the highest average F1-score with one training sample. On average, we obtain an F1-score of $F1 = 0.55$ ($SD = 0.065$). *Arrow* achieves the highest F1-score ($F1 = 0.66$; $SD = 0.035$), followed by *Circle Left* ($F1 = 0.658$; $SD = 0.035$). *Cross* showed an average performance within the overall confidence interval ($F1 = 0.57$; $SD = 0.029$). *Right* had the worst performance ($F1 = 0.47$; $SD = 0.035$). A one-way ANOVA revealed a statistically significant difference of the F1-scores between at least two symbols ($F(19, 25) = 61.02, p << 0.001$). Hence, we performed a post-hoc Tukey test to identify which symbol pairs have a significantly different F1-score. *Cross* shows a significantly different F1-score to twelve of the symbols including: *Arrow*, *At*, *Circle Left*, *Double Tap*, *Down*, *Equals*, *Plus*, *Question Mark*, *Right*, *Single Tap*, *Square*, *Triangle*. The symbol with the best performance, *Arrow*, showed only no statistically significant difference to *Circle Left* ($p = 0.9 \gg 0.05$).

Figure 5 on the left, depicts the impact of the number of training samples on the F1-score. With increasing training sample size we obtain more accurate results. A one-way ANOVA revealed a statistically significant difference of the F1-scores between at least two training sizes ($F(4, 475) = 3940.85, p < 0.001$). A subsequent post-hoc Tukey test showed a statistical significant difference of the F1-scores between all group pairs meaning that a larger training set significantly improved the classifier’s performance, as one would expect. In addition, we wanted to find out whether the precision and recall measures have comparable performances. A one-way ANOVA indicated statistically significant differences between both measures ($F(8, 475) = 3125.71, p < 0.001$). A subsequent post-hoc Tukey test found no significant difference between recall and precision when ten training samples are used ($p = 0.1 > 0.05$). On average the precision is slightly higher by $\Delta = 1.2\%$ ($SD = 0.38\%$), which still indicates an acceptable tradeoff between the two measures.

Ideally, the classifier would reject all other writers and only accept true samples of an individual. A higher precision means that the SVM is more accurately rejecting other writers. While a

higher recall results in a more accurate identification of the writer. Therefore, precision is more important in authentication tasks. The F1-score is the harmonic mean of both measures and reaches in an ideal case a value of 1.

5.4 Majority Voting

As contracts might require a person to sign a document several times, we analyze the impact of averaging classification results. For this purpose, we used the predicted results of the previous tests and average all possible combinations without duplicates by the formula: $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. Where n is the number of predictions and k is the number of voting samples. Using each previous training sample sizes $t = [1, 3, 5, 10]$ and the corresponding test sample sizes $n = [19, 17, 15, 10]$, we analyzed $k = [1, 3, 5, 7, 9]$ voting test samples. The user is then determined in a voting result based on the maximum occurring class.

In Figure 6, left, the impact of majority voting on the F1-score and training sample size is plotted. The lines are the determined mean values of the F1-scores for each training sample size. The colored shades indicate the standard deviation around the mean values. For each training size a one-way ANOVA revealed significant differences between at least two groups of majority voting F1-scores ($F(5, 475) = [727.5, 1805.9, 2405.0, 2263.5], p < 0.001$). A subsequent Tukey test found significant differences for each training size between all corresponding numbers of voting samples. There was no significant difference between 7 and 9 voting samples using 10 training samples ($p = 0.127$). However, this result can be related to the limited amount of 20 samples per symbol and user. To exemplify the impact of majority voting, Figure 6, right, depicts voting results on the symbols *Arrow*, *Cross* and *Right*. On average three voting samples increase the F1-score by $\Delta = 8.9\%$ ($SD = 3.3\%$). We derive that majority voting positively effects writer identification and that signing a contract with three symbols allows a more reliable user identification than with just one symbol. Symbols such as *Arrow* were found to have a significantly higher potential of accurately identifying users than *Cross* with our approach.

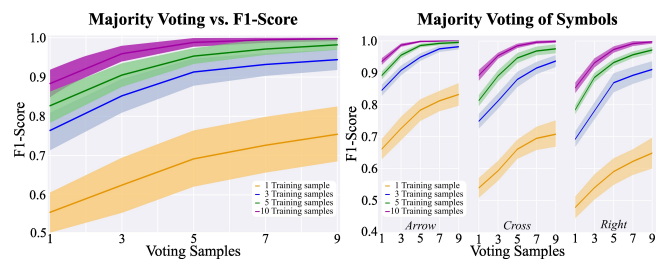


Figure 6: Majority voting analysis. The left plot shows the average impact of the number of voting samples on the F1-score across all symbols. The plots on the right depict the impact of the number of voting samples on the symbols *Arrow*, *Cross* and *Right*.

6 DISCUSSION

Identifying writers by handwritten symbols is a major challenge in cases of suspected fraud. So far, the focus has been on ordinary

signatures, but in cases of illiteracy or disabilities, a writer may be limited to signing with x-marks or similar easy to draw symbols. At least three people have to be involved in the process of a valid x-mark signature [18]. This includes the writer, the contractor, and a witness. Cases of suspected fraud are associated with a high financial expense, as the signatures have to be analyzed using forensic methods and the relationships of witnesses have to be investigated. Additional security mechanisms can contribute to identify forgeries. One challenge in collecting samples of handwritten symbols is that writers of x-mark signatures may tire faster. Thus, a classifier must be able to reliably distinguish writers with as few samples as possible.

Our results show that combining audio and motion data of digital pens can more reliably identify writers by handwritten symbols than single sensors. This confirms the finding by Schrapel et al. [78] that both sensors contain relevant and specific features of a symbol signature. In addition, this is in agreement with the results of Muramatsu et al. that combined sensor approaches increase the reliability of online verification approaches [67]. Splitting the incoming data stream is advantageous for scratching sounds in order to integrate a time component into the features. In contrast, higher recognition rates were achieved when motion data of a symbol were not splitted. In addition, downsampling the measurements to 300 Hz was beneficial on motion data, while using the raw audio signal at 7.1 kHz resulted in higher scores. Compared to previous approaches that used spectral analysis [54, 98], our results show the importance of the time component in signature verification tasks. Additional statistical features of both sensors can further increase the accuracy of the classifier. Hence, the time component of the signals is more important for audio measurements, while the high-frequency components of motion data contain less information. This can be attributed to the writing speed. Vibrations on the paper are more likely to occur at lower frequencies (up to 150 Hz). Produced scratching sounds are modulated by the writing speed [59]. Small irregularities of the paper surface act as a carrier that influence the pitch of the produced scratching sounds. In addition, the volume is influenced by the pressure on the paper [44]. Together with loop-back sounds that propagate via the bones of the hand, resonance properties of the writing surface and the way the pen is held, unique features are produced. This allows relatively accurate identification of a writer with just a few training samples.

Our analysis of the individual symbols shows that certain symbols include a higher diversity of individual characteristics for our participants. This can be attributed to the individual writing style and the way of holding the pen. While the x-marks achieved a uniform performance over the analyzed symbols, the F1-scores of the three best performing symbols *Arrow*, *Circle Left*, *Question Mark* exhibit a significantly higher reliability in identifying writers. However, arrows on contracts are commonly used to indicate signing fields and question marks may also be misinterpreted. In addition, according to the legal situation in Germany, a contract must be signed with three crosses for validity [18]. With three crosses as a training set, the F1-Score already increases to about 75 % in comparison to 55 % with only one training cross. In the case of suspected fraud, it would be required to write at least three crosses again and select a user based on majority voting. With this approach the F1-Score increased to over 80 %. The more training

and test samples are given for majority voting, the more reliably the 30 users were identified. With 7 test majority samples, we already reached an F1-score of over 90 % on x-marks by using three training samples. It should be noted that x-mark signatures are particularly challenging due to their structural simplicity. A skilled forger can easily learn the trajectories of a symbol [39, 43, 63]. However, the scratching sounds that propagate via the loop-back channel over the hand bones contain individual features that make forgeries more challenging.

Compared to previous research on handwritten digit recognition with audio and motion data [78], we showed that combining both sensors allows identifying writers. Since these features are writer specific, generalization of handwriting recognition classifiers is challenging. Schrapel et al. circumvent this problem by retraining their neural networks on samples of the writer. This assumes that the current writer is known and individualized classifiers already exist. However, it could not be determined whether the current writer is already known to the system. Our research has closed this gap and shown that the writer can be detected by individual symbols. This detection allows automatic selection of a user-specific classifier and support for multiple users of a pen. In addition, the presented approach opens up new application scenarios.

We will now discuss the components and challenges of such a possible future x-mark signature verification application. In this context, our prototype may serve as an additional security element in cases of suspected fraud. The system components involved are illustrated in Figure 7. A full implementation would have to be integrated into a suitable public-key and document archive infrastructure. When signing a contract the pen would encrypt and cryptographically sign the measured data along with a unique pen hardware identifier and timestamps. The date and time on the physical contract allows assigning a digital timestamp of the pen to a signing event. Furthermore, the metadata of the contract can serve to enable unique identification. To additionally prevent subsequent modification of the stored pen data, each signing event could be irreversibly stored in a blockchain or on a trusted, secured server. Although both a blockchain and a server structure would be possible on the backend [96], there is a major challenge in making the stored data immutable with a central solution. An attacker could try to delete or modify the data to prevent later verification.

When signing a contract, only the person authorized to sign with crosses uses the digital pen. In case of suspected fraud, all persons involved (e.g. contractor, witnesses and writer) would write at least 3 samples of the symbol, e.g. the x-mark, with the digital pen that was used when signing the contract. These samples are used to verify the signature on the contract. As shown in Figure 6, the more samples are written, the more reliably a person can be identified by majority voting. To prevent the writing of invalid samples during this observation, another neutral person (investigator) monitors the process. The neutral person ensures that all writers give samples of the symbol with the same writing instructions as found on the physical contract in the same environment, or at least with comparably low ambient noise level in a similar environment. While the pen is not in use, the ambient noise level may be measured so that comparable conditions can be created later. Likewise, signatures could be automatically rejected in noisy environments. In order to verify a symbol signature, data previously stored in the blockchain

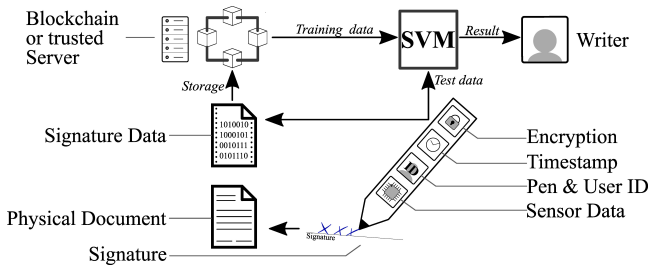


Figure 7: Proposed application scenario: The encrypted measured motion and audio data of a signature is stored in the blockchain or on a trusted server and can be retrieved for subsequent writer identifications. The data is encrypted and used for training an SVM. Additional signatures or symbols are then tested on the trained SVM.

or on a trusted server is used to train an SVM. This allows to later determine a probability that the signature on the contract belongs to a specific person in question. The more contracts were previously signed with our digital pen by an individual, the more reliable the identification system becomes. Since audio modulates the scratching sounds on the surface and by propagating through the hand, the signal includes individual characteristics. However, in case of intermediate hand surgeries or diseases those characteristics might change. Thus we do not consider such cases. In addition, it may happen that a writer merely claims not to have signed a document. In these cases, the person would try to fool the system by, for example, holding the pen differently or pressing the pen tip harder on the sheet of paper. It is likely that the resulting x-mark signatures differ from other previous contracts of the writer. Differences could also be determined by forensic analysis. Furthermore, stored signatures may already exist in the backend from other valid contracts that can be used for analysis. Since the handwriting changes in the course of life [26, 83] a time limit of used signatures for training an SVM would be necessary. Besides this application scenario, an additional security mechanism could be implemented, e.g. for biometric authentication in pharmaceutical digital audits [1]. In addition to the fingerprint sensor [85], our approach would recognize x-marks while filling out forms. Since fingerprint sensors in mobile devices can be easily fooled by fake fingers, e.g., made of silicone [31], our mechanism could provide additional confidence that the pen is held by an authorized user.

The results of our study and the example application scenario show limitations of the presented prototype. First, the acoustic signals might also include sounds from the environment. Even though the scratching sounds are considerably louder than environmental noises while writing, our approach is limited to quiet office environments. The influence of environmental noise has to be further investigated in future studies. In addition, the paper used for signing a contract can have an influence on the measured scratching sounds. Therefore, scratching sounds on different surfaces and papers should be further investigated. Furthermore, our approach must be limited to small numbers of writers. In our use case, all contract partners are known and therefore a classifier can more easily identify individual features of the writers. We assume that

in a usage scenario with a significantly larger number of writers, there may be more false positive classifications. Hence, we limit our approach to contracts which are likely to involve a limited number of contract partners. To further increase the reliability with a significant higher number of users the pen could be extended to measure the force of holding the pen in the hand [6, 41] and a fingerprint sensor [85].

7 CONCLUSION

This paper presented an approach to identify users via handwritten symbols using a digital pen that measures audio and motion data. A study with 30 participants was conducted to evaluate the approach on 19 candidate symbols. The collected dataset consists of 11,400 samples resulting from 380 samples per user with 20 samples for each of the 19 symbols. The proposed method has three main contributions: (1) a preprocessing algorithm for combining audio and motion data from digital pens in the frequency domain to identify writers via handwritten symbols, (2) an analysis of different feature sets fed into SVMs on their suitability for writer identification, and (3) an examination of various symbols including x-marks on their ability to identify writers based on small training sets in an online-verification task.

We found that combining scratching sounds of a pen tip when moving on a sheet of paper with the motion of a pen outperforms single sensor approaches to identify writers via handwritten symbols. Signal representations in the frequency domain were fed into SVMs to establish our results. To the best of our knowledge, we are the first to unite audio and motion data for writer identification via handwritten symbols. The approach achieves an average F1-Score of 76 % when using only three training samples and 17 test samples per user and symbol. Applying majority voting on three test samples increases the average F1 score to 87 %. We were able to show that certain symbols have more distinctive features despite having similar writing trajectories. The symbol *Arrow* achieved the highest F1-Score of about 91 % with three training samples and applying majority voting on three test samples. X-mark signatures reached significantly lower F1-Scores of about 82 % in the same configuration.

The proposed system may be used as an additional security mechanism for illiterate persons or persons with motor disabilities to support investigators in cases of suspected fraud. In this application scenario, the challenges of writer identification are particularly high. As few symbol samples as possible must suffice to identify the writer. In the ideal case, the signature on the contract should be sufficient to train a classifier. The presented approach allows this, but is limited to low-noise environments, such as offices. Therefore, further research is required in the future on how external noises can be suppressed. A long-term study is also required to investigate the change of handwritten x-mark signatures of single persons as handwriting changes in the course of life.

REFERENCES

- [1] Anoto AB. 2022. Anoto. Digital pen and paper technology. <http://www.anoto.com>.
- [2] Sraddhanjali Acharya and Abdul Serwadda. 2021. On Finger Stretching and Bending Dynamics as a Biometric Modality. In *2021 International Conference on Smart Applications, Communications and Networking (SmartNets)*. IEEE, 1–8. <https://doi.org/10.1109/SmartNets50376.2021.9555429>

- [3] Eman Alajrami, Belal AM Ashqar, Bassem S Abu-Nasser, Ahmed J Khalil, Musleh M Musleh, Alaa M Barhoom, and Samy S Abu-Naser. 2020. Handwritten signature verification using deep learning. *International Journal of Academic Multidisciplinary Research (IJAMR)* 3, 12 (2020), 39–44.
- [4] Hiroki Asai and Hayato Yamana. 2013. Detecting Student Frustration Based on Handwriting Behavior. In *Proceedings of the Adjunct Publication of the 26th Annual ACM Symposium on User Interface Software and Technology* (St. Andrews, Scotland, United Kingdom) (UIST '13 Adjunct). ACM, New York, NY, USA, 77–78. <https://doi.org/10.1145/2508468.2514718>
- [5] Gonzalo Bailador, Carmen Sanchez-Avila, Javier Guerra-Casanova, and Alberto de Santos Sierra. 2011. Analysis of pattern recognition techniques for in-air signature biometrics. *Pattern Recognition* 44, 10 (2011), 2468–2478. <https://doi.org/10.1016/j.patcog.2011.04.010> Semi-Supervised Learning for Visual Content Analysis and Understanding.
- [6] Muzaffar Bashir and Florian Kempf. 2012. Advanced biometric pen system for recording and analyzing handwriting. *Journal of Signal Processing Systems* 68, 1 (2012), 75–81. <https://doi.org/10.1007/s11265-011-0576-z>
- [7] Muzaffar Bashir and Jürgen Kempf. 2008. Reduced Dynamic Time Warping for Handwriting Recognition Based on Multidimensional Time Series of a Novel Pen Device. *International Journal of Electrical and Computer Engineering* 2 (2008), 1839–1845.
- [8] Muzaffar Bashir, Jürgen Kempf, G Schickhuber, and Georg Scharfenberg. 2009. Online person authentication using dynamic signature on a novel tactile and pressure sensitive pad. In *17th Telecommunication forum, TELFOR Belgrade, Serbia*.
- [9] Muzaffar Bashir, Georg Scharfenberg, and Jürgen Kempf. 2011. Person Authentication by Handwriting in air using a Biometric Smart Pen Device. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft für Informatik (GI)* 191, 219–226.
- [10] Faiza Eba Batool, Muhammad Attique, Muhammad Sharif, Kashif Javed, Muhammad Nazir, Aaqif Afzaal Abbasi, Zeshan Iqbal, and Naveed Riaz. 2020. Offline signature verification system: a novel technique of fusion of GLCM and geometric features using SVM. *Multimedia Tools and Applications* (2020), 1–20. <https://doi.org/10.1007/s11042-020-08851-4>
- [11] Vincent Becker, Linus Fessler, and Gábor Sörös. 2019. GestEar: Combining Audio and Motion Sensing for Gesture Recognition on Smartwatches. In *Proceedings of the 23rd International Symposium on Wearable Computers* (London, United Kingdom) (ISWC '19). Association for Computing Machinery, New York, NY, USA, 10–19. <https://doi.org/10.1145/3341163.3347735>
- [12] Kiran Bibi, Saeeda Naz, and Arshia Rehman. 2020. Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities. *Multimedia Tools and Applications* 79, 1 (2020), 289–340. <https://doi.org/10.1007/s11042-019-08022-0>
- [13] Attaullah Buriro, Bruno Crispo, Mojtaba Eskandri, Sandeep Gupta, Athar Mahboob, and Rutger Van Acker. 2018. SnapAuth: A Gesture-Based Unobtrusive Smartwatch User Authentication Scheme. In *Emerging Technologies for Authorization and Authentication*, Andrea Saracino and Paolo Mori (Eds.). Springer International Publishing, Cham, 30–37.
- [14] Attaullah Buriro, Rutger Van Acker, Bruno Crispo, and Athar Mahboob. 2018. Airsign: A gesture-based smartwatch user authentication. *2018 International Carnahan Conference on Security Technology (ICCSST)* (2018), 1–5. <https://doi.org/10.1109/CCST.2018.8585571>
- [15] Mengqi Chen, Jiawei Lin, Yongpan Zou, Rukhsana Ruby, and Kaishun Wu. 2020. SilentSign: Device-free Handwritten Signature Verification through Acoustic Sensing. In *2020 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. 1–10. <https://doi.org/10.1109/PerCom54595.2020.9127372>
- [16] Wacom Company. 2022. Wacom InKling. <http://inkling.wacom.eu>.
- [17] Luca De Luisa, Gabriel Emile Hine, Emanuele Maiorana, and Patrizio Campisi. 2021. In-Air 3D Dynamic Signature Recognition using Haptic Devices. In *2021 IEEE International Workshop on Biometrics and Forensics (IWBF)*. IEEE, 1–6. <https://doi.org/10.1109/IWBF50991.2021.9465089>
- [18] dejure.org. 2022. Beurkundungsgesetz BeurkG §39 Einfache Zeugnisse. <https://dejure.org/gesetze/BeurkG/39.html>. Accessed: 2022-01-03.
- [19] Feng Ding, Dong Wang, Qian Zhang, and Run Zhao. 2019. ASSV: Handwritten Signature Verification Using Acoustic Signals. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 3, 3, Article 80 (sep 2019), 22 pages. <https://doi.org/10.1145/3351238>
- [20] DocuSign. 2021. Are Electronic Signatures Legal? <https://www.docusign.com/blog/are-electronic-signatures-legal>. Accessed: 2022-01-03.
- [21] CBC News Erica Johnson. 2017. Document forgery in financial industry more common than you'd think, past employees say. <https://www.cbc.ca/news/business/financial-industry-employees-forge-documents-more-often-than-you-d-think-1.4138212>. Accessed: 2022-01-03.
- [22] Ethereum.org. 2021. Decentralized finance (DeFi) - What is DeFi? <https://ethereum.org/en/defi/>. Accessed: 2022-01-03.
- [23] Paul Wackerow Ethereum.org. 2021. Introduction to smart contracts. <https://ethereum.org/en/developers/docs/smart-contracts/>. Accessed: 2022-01-03.
- [24] Ping Fang, ZhongCheng Wu, Fei Shen, YunJian Ge, and Bing Fang. 2005. Improved DTW Algorithm for Online Signature Verification Based on Writing Forces. In *Proceedings of the 2005 International Conference on Advances in Intelligent Computing - Volume Part I* (Hefei, China) (ICIC '05). Springer-Verlag, Berlin, Heidelberg, 631–640. https://doi.org/10.1007/11538059_66
- [25] Julian Fierrez, Javier Ortega-Garcia, Daniel Ramos, and Joaquin Gonzalez-Rodriguez. 2007. HMM-based on-line signature verification: Feature extraction and signature modeling. *Pattern Recognition Letters* 28 (12 2007), 2325–2334. <https://doi.org/10.1016/j.patrec.2007.07.012>
- [26] DJ Gamble. 1980. The handwriting of identical twins. *Canadian Society of Forensic Science Journal* 13, 1 (1980), 11–30.
- [27] gesetzte-im internet.de. 2022. Bürgerliches Gesetzbuch (BGB) §126 Schriftform. http://www.gesetze-im-internet.de/bgb/_126.html. Accessed: 2022-06-14.
- [28] gesetzte-im internet.de. 2022. Bürgerliches Gesetzbuch (BGB) §2247 Eigenhändiges Testament. https://www.gesetze-im-internet.de/bgb/_2247.html. Accessed: 2022-06-14.
- [29] Mark Giancaspro. 2017. Is a smart contract really a smart idea? Insights from a legal perspective. *Computer Law & Security Review* 33, 6 (2017), 825–835. <https://doi.org/10.1016/j.clsr.2017.05.007>
- [30] STABLO International GmbH. 2022. DigiVision. <https://stabilodigital.com/>.
- [31] Ines Goicoechea-Telleria, Raul Sanchez-Reillo, Judith Liu-Jimenez, and Ramon Blanco-Gonzalo. 2018. Attack potential evaluation in desktop and smartphone fingerprint sensors: can they be attacked by anyone? *Wireless Communications and Mobile Computing* 2018 (2018), 1–16. <https://doi.org/10.1155/2018/5609195>
- [32] Erika Griechisch, M Imran Malik, and Marcus Liwicki. 2013. Online signature verification using accelerometer and gyroscope. *International Graphonomics Society* (01 2013), 143–146.
- [33] Isaac Griswold-Steiner, Richard Matovu, and Abdul Serwadda. 2017. Handwriting watcher: A mechanism for smartwatch-driven handwriting authentication. In *2017 IEEE International Joint Conference on Biometrics (IJCB)*. IEEE, 216–224. <https://doi.org/10.1109/BTAS.2017.8272701>
- [34] Christian Gruber, Thiemo Gruber, Sebastian Krininger, and Bernhard Sick. 2009. Online signature verification with support vector machines based on LCSS kernel functions. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)* 40, 4 (2009), 1088–1100. <https://doi.org/10.1109/TSMCB.2009.2034382>
- [35] Yasmine Guerbai, Youcef Chibani, and Bilal Hadjadji. 2015. The effective use of the one-class SVM classifier for handwritten signature verification based on writer-independent parameters. *Pattern Recognition* 48, 1 (2015), 103–113. <https://doi.org/10.1016/j.patcog.2014.07.016>
- [36] Elyoanai Guerra-Segura, Aysse Ortega-Pérez, and Carlos M Travieso. 2021. In-air signature verification system using Leap Motion. *Expert Systems with Applications* 165 (2021), 113797. <https://doi.org/10.1016/j.eswa.2020.113797>
- [37] Luiz G Hafemann, Robert Sabourin, and Luiz S Oliveira. 2017. Offline handwritten signature verification - literature review. In *2017 seventh international conference on image processing theory, tools and applications (IPTA)*. IEEE, 1–8. <https://doi.org/10.1109/IPTA.2017.8310112>
- [38] Chris Harrison and Scott E. Hudson. 2008. Scratch Input: Creating Large, Inexpensive, Unpowered and Mobile Finger Input Surfaces. In *Proceedings of the 21st Annual ACM Symposium on User Interface Software and Technology* (Monterey, CA, USA) (UIST '08). ACM, New York, NY, USA, 205–208. <https://doi.org/10.1145/1449715.1449747>
- [39] Ordway Hilton. 1992. *Scientific examination of questioned documents*. CRC press.
- [40] Christian Hook, Juergen Kempf, and Georg Scharfenberg. 2003. New Pen Device for Biometrical 3D Pressure Analysis of Handwritten Characters, Words and Signatures. In *Proceedings of the 2003 ACM SIGMM Workshop on Biometrics Methods and Applications* (Berkley, California) (WBMA '03). Association for Computing Machinery, New York, NY, USA, 38–44. <https://doi.org/10.1145/982507.982515>
- [41] Christian Hook, Juergen Kempf, and Georg Scharfenberg. 2004. A Novel Digitizing Pen for the Analysis of Pen Pressure and Inclination in Handwriting Biometrics. In *Biometric Authentication*, Davide Maltoni and Anil K. Jain (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 283–294.
- [42] Yu-Liang Hsu, Cheng-Ling Chu, Yi-Ju Tsai, and Jeen-Shing Wang. 2015. An Inertial Pen With Dynamic Time Warping Recognizer for Handwriting and Gesture Recognition. *IEEE Sensors Journal* 15, 1 (2015), 154–163. <https://doi.org/10.1109/JSEN.2014.2339843>
- [43] Roy A Huber and Alfred M Headrick. 1999. *Handwriting identification: facts and fundamentals*. CRC press.
- [44] Sungjae Hwang, Andrea Bianchi, and Kwangyun Wohn. 2012. MicPen: Pressure-Sensitive Pen Interaction Using Microphone with Standard Touchscreen. In *CHI '12 Extended Abstracts on Human Factors in Computing Systems* (Austin, Texas, USA) (CHI EA '12). Association for Computing Machinery, New York, NY, USA, 1847–1852. <https://doi.org/10.1145/2212776.2223717>
- [45] Donato Impedovo and Giuseppe Pirlo. 2008. Automatic Signature Verification: The State of the Art. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 38, 5 (2008), 609–635. <https://doi.org/10.1109/>

- TSMCC.2008.923866
- [46] Vahab Iranmanesh, Sharifah Mumtazah Syed Ahmad, Wan Azizun Wan Adnan, Fahad Layth Malallah, and Salman Yusoff. 2013. Online signature verification using neural network and pearson correlation features. In *2013 IEEE conference on open systems (ICOS)*. IEEE, 18–21. <https://doi.org/10.1109/ICOS.2013.6735040>
- [47] Edson JR Justino, Flávio Bortolozzi, and Robert Sabourin. 2001. Off-line signature verification using HMM for random, simple and skilled forgeries. In *Proceedings of Sixth International Conference on Document Analysis and Recognition*. IEEE, 1031–1034. <https://doi.org/10.1109/ICDAR.2001.953942>
- [48] Juha Kela, Panu Korpipää, Jani Mäntyjärvi, Sanna Kallio, Giuseppe Savino, Luca Jozzo, and Di Marca. 2006. Accelerometer-Based Gesture Control for a Design Environment. *Personal Ubiquitous Comput.* 10, 5 (2006), 285–299. <https://doi.org/10.1007/s00779-005-0033-8>
- [49] Hamed Ketabdar, Peyman Moghadam, Babak Naderi, and Mehran Roshandel. 2012. Magnetic Signatures in Air for Mobile Devices. In *Proceedings of the 14th International Conference on Human-Computer Interaction with Mobile Devices and Services Companion* (San Francisco, California, USA) (*MobileHCI '12*). Association for Computing Machinery, New York, NY, USA, 185–188. <https://doi.org/10.1145/2371664.2371705>
- [50] Hamed Ketabdar, Kamel A Yüksel, Amirhossein Jahnbekam, Mehran Roshandel, and Daria Skripko. 2010. MagiSign: User Identification/Authentication. *Proc. Of UBICOMM'10* (2010).
- [51] Mariusz Kurowski, Andrzej Sroczyński, Georgis Bogdanis, and Andrzej Czyżewski. 2021. An Automated Method for Biometric Handwritten Signature Authentication Employing Neural Networks. *Electronics* 10, 4 (2021), 456. <https://doi.org/10.3390/electronics10040456>
- [52] Ki-Uk Kyung and Jun-Young Lee. 2008. WUbi-Pen: Windows Graphical User Interface Interacting with Haptic Feedback Stylus. In *ACM SIGGRAPH 2008 New Tech Demos* (Los Angeles, California) (*SIGGRAPH '08*). Association for Computing Machinery, New York, NY, USA, Article 42, 4 pages. <https://doi.org/10.1145/1401615.1401657>
- [53] Songxuan Lai, Lianwen Jin, and Weixin Yang. 2017. Online signature verification using recurrent neural network and length-normalized path signature descriptor. In *2017 14th IAPR international conference on document analysis and recognition (ICDAR)*, Vol. 1. IEEE, 400–405. <https://doi.org/10.1109/ICDAR.2017.73>
- [54] Chan F. Lam and David Kamins. 1989. Signature recognition through spectral analysis. *Pattern Recognition* 22, 1 (1989), 39–44. [https://doi.org/10.1016/0031-3203\(89\)90036-8](https://doi.org/10.1016/0031-3203(89)90036-8)
- [55] Johnny C. Lee, Paul H. Dietz, Darren Leigh, William S. Yerazunis, and Scott E. Hudson. 2004. Haptic Pen: A Tactile Feedback Stylus for Touch Screens. In *Proceedings of the 17th Annual ACM Symposium on User Interface Software and Technology* (Santa Fe, NM, USA) (*UIST '04*). Association for Computing Machinery, New York, NY, USA, 291–294. <https://doi.org/10.1145/1029632.1029682>
- [56] Shih-Hsiung Lee and Hsuan-Chih Ku. 2022. SIAR: Signing in the Air Using Finger Tracking Technology for Authentication on Embedded System. In *2022 IEEE International Conference on Consumer Electronics (ICCE)*. 1–2. <https://doi.org/10.1109/ICCE53296.2022.9730446>
- [57] Alona Levy, Ben Nassi, Yuval Elovici, and Erez Shmueli. 2018. Handwritten Signature Verification Using Wrist-Worn Devices. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 3, Article 119 (sep 2018), 26 pages. <https://doi.org/10.1145/3264929>
- [58] Antwane Lewis, Yanyan Li, and Mengjun Xie. 2016. Real time motion-based authentication for smartwatch. In *2016 IEEE Conference on Communications and Network Security (CNS)*. 380–381. <https://doi.org/10.1109/CNS.2016.7860521>
- [59] F. F. Li. 2004. Handwriting authentication by envelopes of sound signature. In *Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004.*, Vol. 1. 401–404. <https://doi.org/10.1109/ICPR.2004.1334136>
- [60] Gen Li and Hiroyuki Sato. 2020. Handwritten Signature Authentication Using Smartwatch Motion Sensors. In *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 1589–1596. <https://doi.org/10.1109/COMPSAC48688.2020.00-28>
- [61] Gen Li, Lingfeng Zhang, and Hiroyuki Sato. 2021. In-air Signature Authentication Using Smartwatch Motion Sensors. In *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 386–395. <https://doi.org/10.1109/COMPSAC51774.2021.00061>
- [62] A. Chris Long, James A. Landay, Lawrence A. Rowe, and Joseph Michiels. 2000. Visual Similarity of Pen Gestures. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (The Hague, The Netherlands) (*CHI '00*). Association for Computing Machinery, New York, NY, USA, 360–367. <https://doi.org/10.1145/332040.332458>
- [63] Raymond Marquis, Williams David Mazzella, and Tacha Hicks. 2018. X-marks: Too simple to be useful? *Nowa kodyfikacja prawa karnego* 49 (2018), 103–110.
- [64] Leetesh Meena, Vijay Kumar Chaurasiya, Neetesh Purohit, and Dhananjay Singh. 2021. Comparison of SVM and Random Forest Methods for Online Signature Verification. In *Intelligent Human Computer Interaction*, Madhusudan Singh, Dae-Ki Kang, Jong-Ha Lee, Uma Shanker Tiwary, Dhananjay Singh, and Wan-Young Chung (Eds.). Springer International Publishing, Cham, 288–299.
- [65] Han-Cheol Moon, Se-In Jang, Kangrok Oh, and Kar-Ann Toh. 2017. An In-Air Signature Verification System Using Wi-Fi Signals. In *Proceedings of the 2017 4th International Conference on Biomedical and Bioinformatics Engineering* (Seoul, Republic of Korea) (*ICBBE 2017*). Association for Computing Machinery, New York, NY, USA, 133–138. <https://doi.org/10.1145/3168776.3168799>
- [66] Daigo Muramatsu and Takashi Matsumoto. 2003. An HMM online signature verifier incorporating signature trajectories. In *Seventh International Conference on Document Analysis and Recognition, 2003. Proceedings.*, Vol. 1. IEEE, 438–442. <https://doi.org/10.1109/ICDAR.2003.1227705>
- [67] Daigo Muramatsu and Takashi Matsumoto. 2007. Effectiveness of Pen Pressure, Azimuth, and Altitude Features for Online Signature Verification. In *Advances in Biometrics*, Seong-Whan Lee and Stan Z. Li (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 503–512.
- [68] Nguyen Ngoc Diep, Cuong Pham, and Tu Minh Phuong. 2015. SigVer3D: Accelerometer Based Verification of 3-D Signatures on Mobile Devices. In *Knowledge and Systems Engineering, Viet-Ha Nguyen, Anh-Cuong Le, and Van-Nam Huynh* (Eds.). Springer International Publishing, Cham, 353–365.
- [69] Tse-Yu Pan, Chih-Hsuan Kuo, Hou-Tim Liu, and Min-Chun Hu. 2018. Handwriting trajectory reconstruction using low-cost imu. *IEEE Transactions on Emerging Topics in Computational Intelligence* 3, 3 (2018), 261–270. <https://doi.org/10.1109/TETCI.2018.2803777>
- [70] Marc Parizeau and Réjean Plamondon. 1990. A Comparative Analysis of Regional Correlation, Dynamic Time Warping, and Skeletal Tree Matching for Signature Verification. *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 12 (08 1990), 710 – 717. <https://doi.org/10.1109/34.56215>
- [71] 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. Courneau, M. Brucher, M. Perrot, and E. Duchesnay. 2011. Scikit-learn: Machine Learning in Python. *Journal of Machine Learning Research* 12 (2011), 2825–2830.
- [72] Henning Pohl, Markus Krause, and Michael Rohs. 2015. One-Button Recognizer: Exploiting Button Pressing Behavior for User Differentiation. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (Osaka, Japan) (*UbiComp '15*). Association for Computing Machinery, New York, NY, USA, 403–407. <https://doi.org/10.1145/2750858.2804270>
- [73] ABM Mohaimenur Rahman, Yetong Cao, Xinliang Wei, Pu Wang, Fan Li, and Yu Wang. 2022. On the Feasibility of Handwritten Signature Authentication Using PPG Sensor. In *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 719–720. <https://doi.org/10.1109/CCNC49033.2022.9700557>
- [74] Kumar Rajesh, Phoha Vir V, and Raina Rahul. 2016. Authenticating users through their arm movement patterns. <https://doi.org/10.48550/ARXIV.1603.02211>
- [75] Raghavendra Ramachandra, Sushma Venkatesh, Kiran Raja, and Christoph Busch. 2021. Handwritten Signature and Text based User Verification using Smartwatch. In *2020 25th International Conference on Pattern Recognition (ICPR)*. IEEE, 5099–5106. <https://doi.org/10.1109/ICPR48806.2021.9412048>
- [76] Napa Sae-Bae and Nasir Memon. 2014. Online signature verification on mobile devices. *IEEE transactions on information forensics and security* 9, 6 (2014), 933–947. <https://doi.org/10.1109/TIFS.2014.2316472>
- [77] Maximilian Schrapel, Florian Herzog, Steffen Ryll, and Michael Rohs. 2020. Watch My Painting: The Back of the Hand as a Drawing Space for Smartwatches. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) (*CHI EA '20*). Association for Computing Machinery, New York, NY, USA, 1–10. <https://doi.org/10.1145/3334480.3383040>
- [78] Maximilian Schrapel, Max-Ludwig Stadler, and Michael Rohs. 2018. *Pentelligence: Combining Pen Tip Motion and Writing Sounds for Handwritten Digit Recognition*. Association for Computing Machinery, New York, NY, USA, 1–11. <https://doi.org/10.1145/3173574.3173705>
- [79] Claude Elwood Shannon. 1949. Communication in the presence of noise. *Proceedings of the IRE* 37, 1 (1949), 10–21.
- [80] Daniel A Smith. 2018. Vote-by-mail ballots cast in florida. *ACLU of Florida*. (2018). <https://www.aclufi.org/en/press-releases/aclu-report-finds-varying-rates-rejected-vote-mail-ballots-across-florida-counties>
- [81] Elizabeth Ann Soelistio, Rafael Edwin Hananto Kusumo, Zevira Varies Martan, and Edy Irawansyah. 2021. A Review of Signature Recognition Using Machine Learning. In *2021 1st International Conference on Computer Science and Artificial Intelligence (ICCSAI)*, Vol. 1. 219–223. <https://doi.org/10.1109/ICCSAI53272.2021.9609732>
- [82] Matthias Sperber, Martin Klinkigt, Koichi Kise, Masakazu Iwamura, Benjamin Adrian, and Andreas Dengel. 2010. Handwriting reconstruction for a camera pen using random dot patterns. In *2010 12th International Conference on Frontiers in Handwriting Recognition*. IEEE, 160–165. <https://doi.org/10.1109/ICFHR.2010.32>
- [83] Sargur Srihari, Chen Huang, and Harish Srinivasan. 2008. On the discriminability of the handwriting of twins. *Journal of Forensic Sciences* 53, 2 (2008), 430–446. <https://doi.org/10.1111/j.1556-4029.2008.00682.x>
- [84] Michael Stauffer, Paul Maergner, Andreas Fischer, and Kaspar Riesen. 2021. A Survey of State of the Art Methods Employed in the Offline Signature Verification Process. In *New Trends in Business Information Systems and Technology: Digital*

- Innovation and Digital Business Transformation*, Rolf Dornberger (Ed.). Springer International Publishing, Cham, 17–30. https://doi.org/10.1007/978-3-030-48332-6_2
- [85] Jihoon Suh. 2016. Veri-Pen: A Pen-Based Identification Through Natural Biometrics Extraction. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (San Jose, California, USA) (*CHI EA '16*). Association for Computing Machinery, New York, NY, USA, 134–139. <https://doi.org/10.1145/2851581.2890379>
- [86] Ziwen Sun, Yao Wang, Gang Qu, and Zhiping Zhou. 2016. A 3-D Hand Gesture Signature Based Biometric Authentication System for Smartphones. *Security and Communication Networks* 9 (07 2016), 157–164. <https://doi.org/10.1002/sec.1422>
- [87] National Telecommunications and United States Department of Commerce Information Administration (NITA). 2002. Product Recall Exception to the Electronic Signatures in Global and National Commerce Act. https://www.ntia.doc.gov/files/ntia/publications/fr_esign_recall_020924.pdf. Accessed: 2022-01-03.
- [88] Marc Teyssier, Gilles Bailly, and Éric Lecolinet. 2017. VersaPen: Exploring Multimodal Interactions with a Programmable Modular Pen. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (Denver, Colorado, USA) (*CHI EA '17*). Association for Computing Machinery, New York, NY, USA, 377–380. <https://doi.org/10.1145/3027063.3052964>
- [89] Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, and Javier Ortega-Garcia. 2021. DeepSign: Deep on-line signature verification. *IEEE Transactions on Biometrics, Behavior, and Identity Science* 3, 2 (2021), 229–239. <https://doi.org/10.1109/TBIOM.2021.3054533>
- [90] Jeen-Shing Wang and Fang-Chen Chuang. 2012. An Accelerometer-Based Digital Pen With a Trajectory Recognition Algorithm for Handwritten Digit and Gesture Recognition. *IEEE Trans. Industrial Electronics* 59, 7 (2012), 2998–3007. <https://doi.org/10.1109/TIE.2011.2167895>
- [91] Qinglong Wang, Xiangshi Ren, Sayan Sarcar, and Xiaoying Sun. 2016. EV-Pen: Leveraging Electro-vibration Haptic Feedback in Pen Interaction. In *Proceedings of the 2016 ACM International Conference on Interactive Surfaces and Spaces* (Niagara Falls, Ontario, Canada) (*ISS '16*). Association for Computing Machinery, New York, NY, USA, 57–66. <https://doi.org/10.1145/2992154.2992161>
- [92] Zhengjie Wang, Naisheng Zhou, Fang Chen, Xiaoxue Feng, Fei Liu, Yinjing Guo, and Da Chen. 2021. Smart_Auth: User Identity Authentication Based on Smartphone Motion Sensors. In *2021 6th International Conference on Image, Vision and Computing (ICIVC)*. IEEE, 480–485. <https://doi.org/10.1109/ICIVC52351.2021.9526964>
- [93] Zhixiang Wei, Song Yang, Yadong Xie, Fan Li, and Bo Zhao. 2021. SVSV: Online handwritten signature verification based on sound and vibration. *Information Sciences* 572 (2021), 109–125. <https://doi.org/10.1016/j.ins.2021.04.099>
- [94] Edmund Taylor Whittaker. 1915. XVIII.—On the functions which are represented by the expansions of the interpolation-theory. *Proceedings of the Royal Society of Edinburgh* 35 (1915), 181–194.
- [95] B. Wirtz. 1995. Stroke-based time warping for signature verification. In *Proceedings of 3rd International Conference on Document Analysis and Recognition*, Vol. 1. 179–182 vol.1. <https://doi.org/10.1109/ICDAR.1995.598971>
- [96] Karl Wüst and Arthur Gervais. 2018. Do you need a blockchain?. In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. 45–54. <https://doi.org/10.1109/CVCBT.2018.00011>
- [97] Songlin Xu, Zhiyuan Wu, Shunhong Wang, Rui Fan, and Nan Lin. 2020. Hydro: Extending Interaction Space on the Pen through Hydraulic Sensing and Haptic Output. In *Adjunct Publication of the 33rd Annual ACM Symposium on User Interface Software and Technology* (Virtual Event, USA) (*UIST '20 Adjunct*). Association for Computing Machinery, New York, NY, USA, 43–45. <https://doi.org/10.1145/3379350.3416180>
- [98] Berrin Yanikoglu and Alisher Kholmatov. 2009. Online Signature Verification Using Fourier Descriptors. *Journal on Advances in Signal Processing* 2009, 1 (12 2009), 1687–6180. <https://doi.org/10.1155/2009/260516>
- [99] X. Yu, Z. Zhou, M. Xu, X. You, and X. Li. 2020. ThumbUp: Identification and Authentication by Smartwatch using Simple Hand Gestures. In *2020 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. IEEE Computer Society, Los Alamitos, CA, USA, 1–10. <https://doi.org/10.1109/PerCom45495.2020.9127367>
- [100] Run Zhao, Dong Wang, Qian Zhang, Xueyi Jin, and Ke Liu. 2021. Smartphone-Based Handwritten Signature Verification Using Acoustic Signals. *Proc. ACM Hum.-Comput. Interact.* 5, ISS, Article 499 (nov 2021), 26 pages. <https://doi.org/10.1145/3488544>