2023 IEEE/ASME International Conference on Advanced Intelligent Mechatronics (AIM)
June 28-30, 2023. Seattle, Washington, USA

Biometric Signature Authentication with Low Cost Embedded Stylus

Divas Subedi, Digesh Chitrakar, Isabella Yung, Yicheng Zhu, Yun-Hsuan Su and Kevin Huang

***Abstract*— This paper presents an affordable stylus device with embedded inertial sensing for measuring dynamic kinematic data from handwritten signatures for the purposes of user identification. A set of spatiotemporal features are proposed for use in a simple multilayer perceptron classifier, and a brief user study is conducted for evaluation with promising results. In general, user authentication is a key component of securing digital information in cyber-physical systems. Current methods span alphanumeric passwords, multi-factor authentication, and biometric techniques, with each providing trade-offs between convenience, flexibility and security. This work presents a device that marries a kinematic trajectory unique to each person (handwritten signature) with digital authentication via a stylus type device. Handwritten signatures are ubiquitous for authenticating paperwork, credit card transactions, check deposits and ballot boxes to name a few. Oftentimes, handwritten signatures are executed and treated perfunctorily as a matter of routine with no genuine intention towards security or authentication. When authentication is requested of handwritten signatures, most often the only recourse is expert visual examination of the written pen strokes. While some methods have investigated the use of measuring temporal, inertial data from handwritten signatures as a mode of authentication, these were executed with either expensive haptic robotic devices or prototype, externally mounted sensors. This work enables dynamic inertial authentication methods of handwritten signatures in a low cost, seamless embedded stylus device.**

***Index Terms*— embedded and cyber-physical systems, biometrics, authentication, handwritten signatures, security and privacy**

I. Introduction

Modern day interactions are growing more and more reliant on technology and digital information, with many conveniences, tasks, and businesses mediated through computer devices and cloud-based storage. With this proliferation of technology in society comes a growing concern for proper and reliable security and authentication measures, as the use of technology can outpace once reliable methods for security. Alphanumeric passwords, numeric combinations or even handwritten signatures do not hold the same weight or robustness in today's cyber-connected world. Cybersecurity itself is a growing industry due to the skill and ability of adversarial attackers to steal and gain access to private, delicate or highly valuable information.

Divas Subedi, Digesh Chitrakar, Isabella Yung, Yicheng Zhu and Kevin Huang are with Trinity College, Dept. of Engineering, 300 Summit St., Hartford, CT 06106 USA {divas.subedi, digesh.chitrakar, isabella.yung, yicheng.zhu, kevin.huang}@trincoll.edu

Yun-Hsuan Su is with Mount Holyoke College, Department of Computer Science, 50 College St, South Hadley, MA 01075 USA msu@mtholyoke.edu

A. Related Work

Currently, digital user-interfaced systems typically require some method of authentication in order to verify the human user. Common methods include alphanumeric passwords, personal information numbers (PIN), one-time passwords (OTP), Multi-Factor Authentication (MFA), facial identification, and fingerprint authentication to name a few. Alphanumeric passwords and PINs are simple and easily reset, but they can be brute-force cracked. OTPs can be inconvenient, and are subject to attack without two-way authentication. Multi-factor authentication requires network connectivity and at least one additional device on-hand to complete verification. Some biometric systems can be unreliable or spoofed (e.g. face or fingerprint recognition), and are not easily reset or reconfigured. With a growing need for more unique and secure ways of user authentication, this project aims to leverage the unique kinematic data in and precedent of handwritten signatures to capture an additional digital security measure. The method is not burdensome (most people already have trained a unique handwritten signature as a formality), and sensorizing a stylus with digital inertial sensors can be achieved in a seamless, embedded fashion.

Current methods of handwriting recognition and authentication is an extremely manual and expensive undertaking. The prevailing methodology relies on "handwriting experts", who look for visual signs of feature recognition in the final handwritten signature. These handwriting experts can demand a high monetary cost for services, are hard to train, and the observed utility of their expertise over novices are not entirely confirmed [1]. Signatures are unique to every individual just like handwriting [2], [3]. The way a person holds the pen, the angle and orientation they write with, the speed and pressure used, and sizing and formation of letters is different for each unique individual. By taking advantage of these features, a classification system can be designed to authenticate its user [4], [5]. In this work, manually selected, interpretable features are developed and evaluated.

In a similar work, tablet devices were used to digitize the final written output to intelligently automate handwriting quality feedback [6]. While the resultant signature was digitized, the method did not incorporate the kinematics of the stylus in its feature space, and authentication was not implemented. Other groups, also motivated by handwriting development, sensorized the stylus to quantify performance [7]. The way a person holds a stylus device has been investigated for use in teleoperated systems [8], [9]. Using hand-

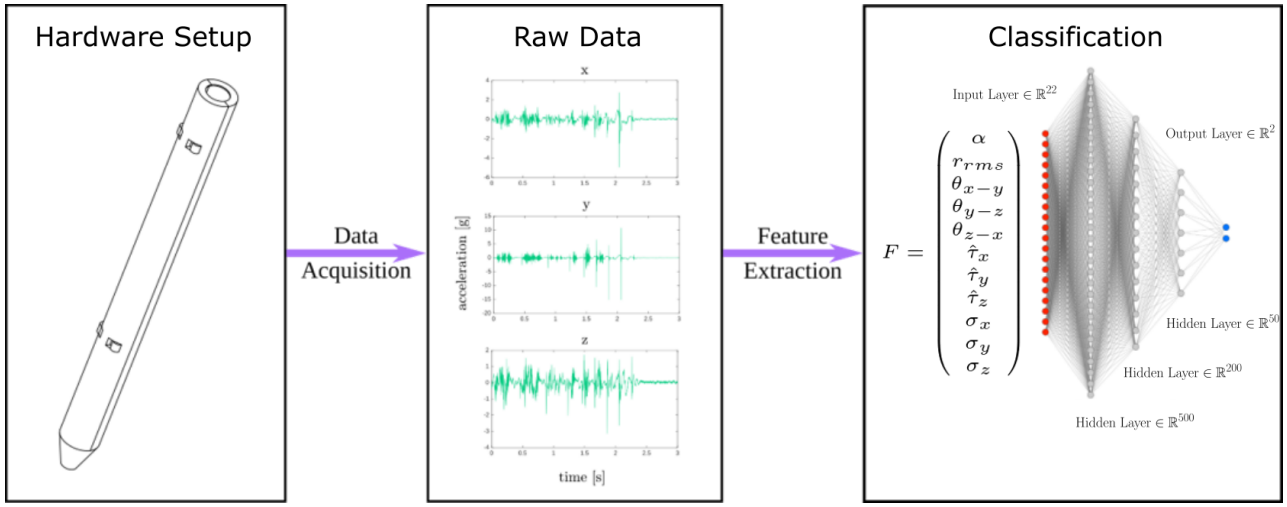


Fig. 1: Simple overview of stylus device with embedded IMU sensor authentication. Surface mount IMU devices are conspicuously implanted axially along the center of the writing stylus, which are used to collect kinematic data. Manual features are then extracted and used for both training and classification of user via a multilayer perceptron network.

writing stylus kinematics has also been applied to detection of Alzheimer's and Parkinson's disease [10]–[13], user-input devices for written character recognition [14], [15], and robot training [16]. Intelligent handwriting verification methods have been explored for post-processing of handwriting using image processing and comparison algorithms [17]. Sae et al. analyzed the dynamics of finger-written signatures on a touch screen mobile devices [18]. Early methods of classification included simple match-making algorithms [19], and more recent methods incorporate hidden markov models and recurrent networks [20]. Kurowski et al. used an embedded pen and tablet system with a single inertial measurement unit (IMU) with acceleration and angular velocity, signature shape capture, and pen pressure [5]. A neural network was then used to train classification via a triplet loss function.

B. Contributions

To the best of the authors' knowledge, this work is the first to introduce simultaneously a single, low-cost embedded biometric handwritten signature stylus device that:

- incorporates dual accelerometers to measure kinematic information at two points along the center axis of the pen;
- implements an automated coordinate frame registration to accommodate grip symmetry of cylindrical stylus;
- introduces novel interpretable features for signature classification based on accelerometer data alone;
- evaluates via a preliminary user study the validity of the low-cost system and selected features for authentication.

II. Design

Previous work investigated the use of attaching commodity IMU sensors to existing writing utensils [4]. This work seeks to incorporate inertial sensing into a streamlined form factor writing stylus, and the overall workflow is depicted in Fig. 1. The device enclosure is prototyped with readily available rapid prototyping (extrusion 3D printing). To accommodate rotational symmetry, an orientation normalization procedure is performed. Additionally, manual features are extracted and used to train and validate the authentication via a user study.

A. Stylus Enclosure Specifications

The prototype enclosure consisted of two halves split down the length of the stylus, as shown in Fig. 2, and both halves were printed with polylactic acid filament and polyvinyl alcohol supports using the Ultimaker S5 printer. The stylus is 151 mm in length and 13 mm in diameter (to accommodate the profile of the surface mount IMU sensors while maintaining structural integrity).

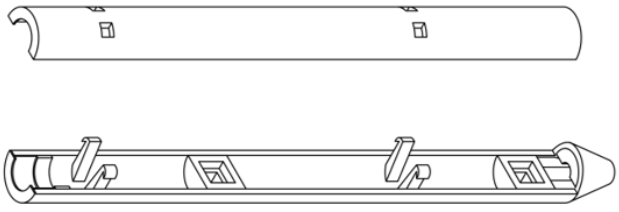


Fig. 2: Stylus enclosure prototype consisted of two halves. Spring clips are designed to easily secure the two halves together and disassemble when needed.

The print was completed using 1.2 mm layer height, 220°C print temperature, and print speed of 50 mm per second. Note that in addition to clips for securing the two halves together, the design incorporates sections for securing a truncated pen refill at the tip, two wells to hold the surface mount IMUs, and a terminal end pin connector slot to output inertial signals. The pin connector used was a standard MD-90 connector. The dimensions of these components are detailed in Fig. 3.

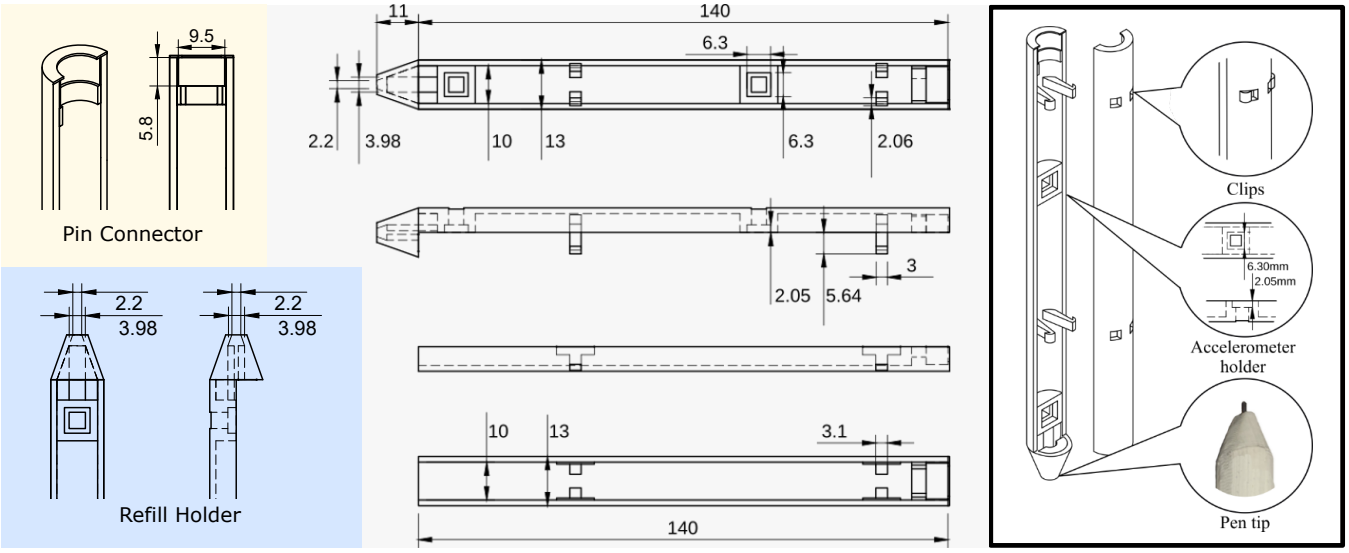


Fig. 3: Dimensions of stylus enclosure. Spatial dimensions for callouts are in millimeters.

B. Kinematic Sensor and Interface

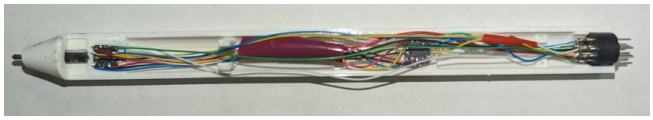
An IMU is a combination of multiple inertial measurement devices such as gyroscopes and accelerometers. These devices can also equip magnetometers, providing much more detail in orientation sensing. Gyroscopes measure orientation and angular acceleration, and can be found in navigation and guidance systems. Smaller form factor via microelectromechanical systems (MEMs) gyroscopes are also found in commercial devices like smartphones. However, reliable gyroscopes can be expensive or otherwise prohibitively large, which contradict the low-cost and seamless goal of this work.

In contrast, commodity low-profile surface mount accelerometers can be obtained off-the-shelf at low cost. The 3-axis MEMs based ADXL-357 was chosen for its slim profile (14-LCC package, 6 mm $\times$ 5.6 mm $\times$ 2.2 mm footprint) and affordability. The sensor can measure linear acceleration, and requires minimal external circuitry to implement. Key specifications for the ADXL-357 are summarized in Table I.

Acceleration Range	±10g, ±20g, ±40g
Sensitivity	12800 (±10g) ~51200 (±40g)
Bandwidth	1Hz ~1kHz
Output Type	I^2C, SPI
Features	Adjustable Bandwidth, Selectable Scale

TABLE I: Key Specifications for ADXL-357

Electrical connections to the accelerometers, pin connectors and discrete surface mount capacitors were made via soldering and 30 gauge solid wire. All internal electronics fit within the enclosure, and data and power are tethered to a Raspberry Pi microcontroller. Data transmission was established using Serial Peripheral Interface at a sampling rate of 1kHz. The simple sensor suite is embedded in the enclosure and easily assembled, as shown in Fig. 4.



a) electrical connections, opened

b) enclosed and tethered

Fig. 4: Sensorized stylus with electrical components shown.

Figure 5 shows typical compensated 3-axis accelerometer data from a handwritten signature.

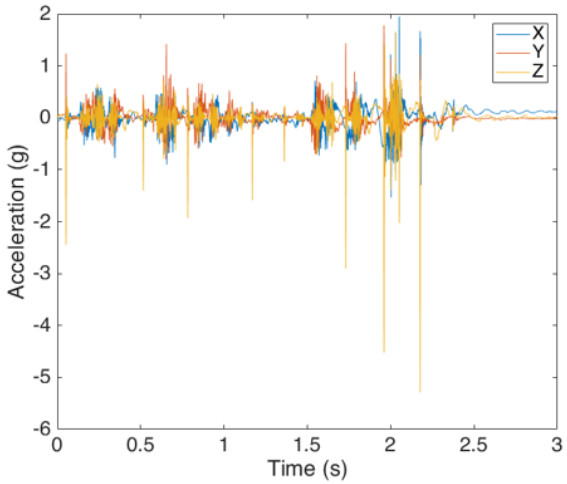


Fig. 5: Compensated 3-axis accelerometer data from pen-tip captured from a handwritten signature that lasted just under three seconds. Since two accelerometers are embedded in the device, a total of six traces are captured per signature.

III. Methods

A. Orientation Normalization

Since the stylus exhibits rotational symmetry about the length of the device, no standard coordinate frame is guaranteed between or within users. In order to ascertain a standard frame, the direction of acceleration due to gravity was used ($\mathbf{g}$). After kinematic data of a signature is acquired, the dynamic acceleration data were compensated such that the mean 3DOF acceleration over the time series was assigned as an approximation of $\mathbf{g}$. In order to perform this normalization, the rotation matrix ($\mathbf{U}$) was computed for each captured signature and mean acceleration ($\hat{\mathbf{a}}$).

$$\boldsymbol{\nu} = -\frac{\hat{\mathbf{a}}_{\perp \mathbf{g}}}{\|\hat{\mathbf{a}}_{\perp \mathbf{g}}\|} \tag{1}$$

$$\mathbf{G} = \begin{bmatrix} \hat{\mathbf{a}} \cdot \mathbf{g} & -\|\boldsymbol{\nu}_1 \mathbf{g}\| & 0 \\ \|\hat{\mathbf{a}} \times \mathbf{g}\| & \hat{\mathbf{a}} \cdot \mathbf{g} & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{2}$$

$$\mathbf{F} = \begin{bmatrix} \hat{\mathbf{a}} & \boldsymbol{\nu} & \mathbf{g} \times \hat{\mathbf{a}} \end{bmatrix} \tag{3}$$

$$\mathbf{U} = \mathbf{F} \cdot \mathbf{G} \cdot \mathbf{F}^{-1} \tag{4}$$

This methods assumes that a person's grip local to the stylus does not change during any single signature, as well as relative within-user kinematic consistency of signature.

B. Feature Selection

Interpretable features of authentication were sought. While standard spectral features were considered (popular in speaker-recognition, surface texture recognition, and contact localization [21]–[23]), time-series kinetic features afford more direct interpretability. 11 manual features were designed to characterize orientation, energy distribution in different spatial axes, and energy distribution temporally for each accelerometer

$$\mathbf{F} = \begin{pmatrix} \alpha \\ r_{rms} \\ \theta_{x-y} \\ \theta_{y-z} \\ \theta_{z-x} \\ \hat{\tau}_x \\ \hat{\tau}_y \\ \hat{\tau}_z \\ \sigma_x \\ \sigma_y \\ \sigma_z \end{pmatrix} \tag{5}$$

with parameters defined as

$$\alpha = \arccos\left(\hat{\mathbf{a}} \cdot \mathbf{g}\right) \tag{6}$$

$$r_{rms} = \sqrt{\frac{1}{N}\sum_t a_x^2(t) + a_y^2(t) + a_z^2(t)} \tag{7}$$

$$\theta_{i-j} = \arctan\left(\frac{a_{i_{rms}}}{a_{j_{rms}}}\right) \tag{8}$$

$$\hat{\tau}_i = \frac{1}{N_\tau}\sum_t E_i(t)t \tag{9}$$

$$\sigma_i = \frac{1}{N_\tau}\sum_t E_i(t)t^2 - \hat{\tau}_i \tag{10}$$

Here, N is number of data points in the time-series of sample acceleration. N_τ is the normalization factor, namely $N_\tau = \sum_t E_i(t)$. $E_i(t)$ is a measure of energy, where $E_i(t) = a_i^2(t)$.

With two accelerometers embedded and 11 features each, the total feature vector for any time instant is length 22. These features are based on kinematic and kinetic characteristics of the handwritten signature. The α feature describes the pen kinematic orientation. Mechanical energy measured is also of interest, and r_{rms} encodes a measure of energy at the two accelerometer locations, while θ_{i-j} describes the relative ratios distributed along the spatial axes. Finally, $\hat{\tau}_i$ describe the mean temporal distribution of energy, while σ_i is a measure of the variance of energy in time.

C. Classification

A multilayer perceptron neural network was trained with three hidden layer with 500, 200, and 50 perceptrons in each layer respectively. This model optimized the log-loss function using Limited-memory Broyden–Fletcher–Goldfarb–Shanno. Prior to classification, the data were pre-processed and normalized along all feature dimensions via Z-score normalization of the signature data.

IV. Experimental Procedure

All studies with human subjects were approved by the Trinity College Institutional Review Board. A total of 10 voluntary subjects were recruited via word of mouth.

A. Authentic Signatures

In this preliminary user study, two separate users' signatures served as authentication targets. The two subjects were designated Subject 0 and Subject 1, were right-handed and 22 years old. Both were instructed to complete their handwritten signature a total of 212 times with the embedded stylus, with kinematic data from each signature being logged per the aforementioned methods. Signatures were filled in a tabular form to ensure consistent physical scale. The users were allowed to take breaks in between signatures as they saw fit to avoid fatigue. Over the course of the 212 authentic signatures, Subject 0's signature duration was consistently just under three seconds, while Subject 1's signature was completed repeatably in just under five seconds. Figure 6 shows the graphical output of the two target authentication signatures.

(a) Subject 0 (b) Subject 1

Fig. 6: Graphical output of (a) Subject 0 and (b) Subject 1 handwritten signature using the stylus device. The signature duration was consistently about three and five seconds for Subject 0 and Subject 1 respectively.

B. Forged Signatures

To complete the dataset, the remaining eight volunteers were tasked with forging the signatures of Subject 0 and Subject 1. The subjects were all right-handed and between the ages of 18 and 23 years old. The subjects were informed that they could stop the experiment at any time. A brief introduction to the forgery task included:

- an introduction to the embedded device whose user model is similar to tethered ballpoint pens at post offices and banks;
- for each signature class, a copy (to scale) of the authentic signature graphical output (see Fig. 6);
- a description of the time duration the authentic signature (about three seconds for Subject 0, and about five seconds for Subject 1);
- time for the forger to practice with the pen to forge the target signature (20 minutes or whenever satisfied, whichever came first).

In all cases, the subjects were satisfied with training prior to the 20 minute practice threshold.

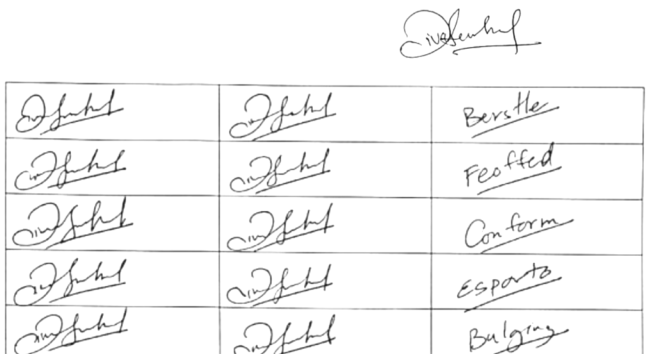


Fig. 7: Above the tabular forgery space, the authentic signature is displayed. Each row corresponds to a three word sequence of two forgeries followed by a random word.

After training, the eight forgery subjects were asked to create forged data by completing, for both Subject 0 and Subject 1 signatures, handwritten forgeries as well as random words in a sequence of two forgery attempts followed by a random word of their choosing - the random words were requested to expand the training space for negatives. Subjects were allowed to take a break or end the experiment whenever they wished. This sequence was repeated 15 times for each forger per signature. Figure 7 shows a glimpse of the forgery task.

For both Subject 0 and Subject 1 signatures, a database is collected that includes accelerometer time series for

i) 212 handwritten positive (authentic) signatures;
ii) 343 handwritten negative (forged) signatures, consisting of:
   - 238 forged replicas of authentic signature;
   - 105 random words.

Each class of signature thus includes a total of 555 collected signatures as a dataset.

C. Training and Evaluation

To train and evaluate the authentication method, an 80-20 split was heuristically determined. For each signature, the dataset of 555 samples was partitioned randomly into five disjoint folds (110 samples in the first four, 115 in the fifth). A uniform distribution of each class within each fold was attempted (42 authentic, 47 forged, and 21 random words for the first four folds, 44, 50 and 21 respectively for the fifth).

In each of five trials per signature, a single fold was used as the testing set while the remaining folds were utilized for training the network. Each of the five folds served as the testing set once in the evaluation. In this way, no test data were used for training the model on which that data were evaluated, yet all data could be tested. The same fold partitioning technique was applied to both Subject 0 and Subject 1 signatures in all evaluations and experiments.

V. Results

Figure 8 shows confusion matrices that summarizes the cumulative binary classification results from the user study across all five folds. Furthermore, receiver operating characteristic curves for both signatures and for each fold are shown in Fig. 9, with areas-under-the-curve (AUC) for each fold shown in Table II.

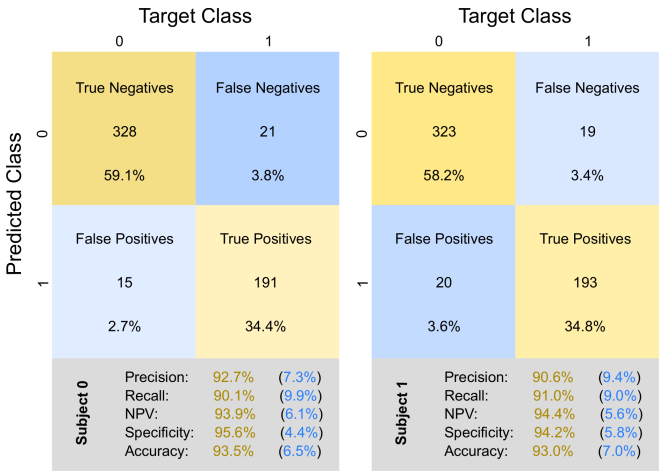
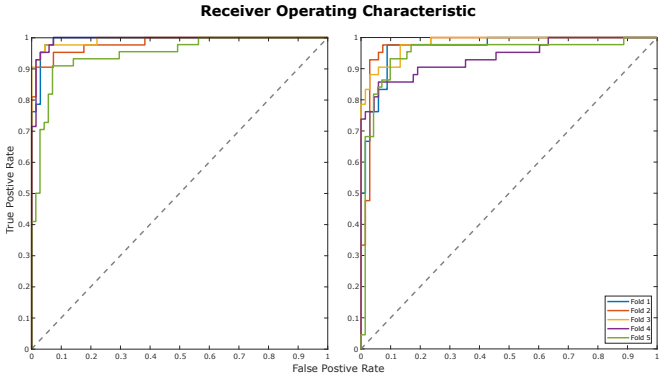


Fig. 8: Cumulative confusion matrices for binary authentication of signatures with performance metrics.



(a) Subject 0 (b) Subject 1

Fig. 9: Receiver operating characteristics for each fold in each signature authentication task.

Fold	1	2	3	4	5
Subject 0	0.9919	0.9818	0.9926	0.9930	0.9465
Subject 1	0.9678	0.9758	0.9814	0.9373	0.9481

TABLE II: Receiver Operating Characteristic Areas-Under-the-Curve

VI. Conclusion

This work presented a low cost sensorized writing stylus system to authenticate handwritten signatures. Novel, manually crafted spatiotemporal features were introduced, and a gravity compensation method was proposed to register kinematic data to the same global frame. In the user study, the proposed method showed robustness to signature variability of individual users, with over 93% accuracy and 94.2% specificity. Furthermore, the evaluation results also demonstrated an outstanding performance in receiver operating characteristic curves AUC ranging between 0.9373 and 0.9926 across subjects and folds. Compared to common password models, such as alphanumeric systems, this authentication method relies on the user's signature, which introduces complexity that is difficult to replicate or spoof, and simultaneously leverages an individual's years of practice and familiarity with their own personal handwritten signature. This work demonstrates that using inertial measurements of signature for signature authentication can be cost-effective, secure, robust, and embedded in a streamline package.

References

[1] K. A. Martire, B. Growns, and D. J. Navarro, "What do the experts know? calibration, precision, and the wisdom of crowds among forensic handwriting experts," *Psychonomic bulletin & review*, vol. 25, no. 6, pp. 2346–2355, 2018.

[2] J. Yan, K. Huang, T. Bonaci, and H. J. Chizeck, "Haptic passwords," in *2015 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. IEEE, 2015, pp. 1194–1199.

[3] K. Bibi, S. Naz, and A. Rehman, "Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities," *Multimedia Tools and Applications*, vol. 79, no. 1, pp. 289–340, 2020.

[4] D. Subedi, I. Yung, D. Chitrakar, and K. Huang, "Inertial-measurement-based biometric authentication of handwritten signature," in *2022 44th Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)*. IEEE, 2022, pp. 4320–4324.

[5] M. Kurowski, A. Sroczyński, G. Bogdanis, and A. Czyżewski, "An automated method for biometric handwritten signature authentication employing neural networks," *Electronics*, vol. 10, no. 4, p. 456, 2021.

[6] V. Kulesh, K. Schaffer, I. Sethi, and M. Schwartz, "Handwriting quality evaluation," in *International Conference on Advances in Pattern Recognition*. Springer, 2001, pp. 157–165.

[7] L. J. Serpa-Andrade, J. J. Pazos-Arias, M. López-Nores, and V. E. Robles-Bykbaev, "Sensorised low-cost pencils for developing countries: A quantitative analysis of handwriting learning progress in children with/without disabilities from a sustainable perspective," *Sustainability*, vol. 12, no. 24, p. 10682, 2020.

[8] K. Huang, D. Chitrakar, R. Mitra, D. Subedi, and Y.-H. Su, "Characterizing limits of vision-based force feedback in simulated surgical tool-tissue interaction," in *2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)*. IEEE, 2020, pp. 4903–4908.

[9] J. Yan, K. Huang, K. Lindgren, T. Bonaci, and H. J. Chizeck, "Continuous operator authentication for teleoperated systems using hidden markov models," *ACM Transactions on Cyber-Physical Systems (TCPS)*, vol. 6, no. 1, pp. 1–25, 2022.

[10] P. Ghaderyan, A. Abbasi, and S. Saber, "A new algorithm for kinematic analysis of handwriting data; towards a reliable handwriting-based tool for early detection of alzheimer's disease," *Expert Systems with Applications*, vol. 114, pp. 428–440, 2018.

[11] G. Pirlo, M. Diaz, M. A. Ferrer, D. Impedovo, F. Occhionero, and U. Zurlo, "Early diagnosis of neurodegenerative diseases by handwritten signature analysis," in *International Conference on Image Analysis and Processing*. Springer, 2015, pp. 290–297.

[12] A. B. Hernandez, A. Fischer, and R. Plamondon, "Omega-lognormal analysis of oscillatory movements as a function of brain stroke risk factors," in *17th Biennial Conference of the International Graphonomics Society*, 2015.

[13] C. Bidet-Ildei, P. Pollak, S. Kandel, V. Fraix, and J.-P. Orliaguet, "Handwriting in patients with parkinson disease: effect of l-dopa and stimulation of the sub-thalamic nucleus on motor anticipation," *Human movement science*, vol. 30, no. 4, pp. 783–791, 2011.

[14] D.-W. Kim, J. Lee, H. Lim, J. Seo, and B.-Y. Kang, "Efficient dynamic time warping for 3d handwriting recognition using gyroscope equipped smartphones," *Expert systems with applications*, vol. 41, no. 11, pp. 5180–5189, 2014.

[15] J. K. Oh, S.-J. Cho, W.-C. Bang, W. Chang, E. Choi, J. Yang, J. Cho, and D. Y. Kim, "Inertial sensor based recognition of 3-d character gestures with an ensemble classifiers," in *Ninth international workshop on frontiers in handwriting recognition*. IEEE, 2004, pp. 112–117.

[16] H. Yin, A. Billard, and A. Paiva, "Bidirectional learning of handwriting skill in human-robot interaction," in *Proceedings of the Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction Extended Abstracts*, 2015, pp. 243–244.

[17] K. Erdélyi and B. Molnár, "Similarity measurement of handwriting by alignment of sequences," in *Intelligent Computing-Proceedings of the Computing Conference*. Springer, 2019, pp. 463–473.

[18] N. Sae-Bae and N. Memon, "Online signature verification on mobile devices," *IEEE transactions on information forensics and security*, vol. 9, no. 6, pp. 933–947, 2014.

[19] R. Plamondon and M. Parizeau, "Signature verification from position, velocity and acceleration signals: A comparative study," in *9th International Conference on Pattern Recognition*. IEEE Computer Society, 1988, pp. 260–261.

[20] L. Tencer, M. Reznakova, and M. Cheriet, "Evaluation of techniques for signature classification from accelerometer and gyroscope data," in *2015 13th International Conference on Document Analysis and Recognition (ICDAR)*. IEEE, 2015, pp. 1066–1070.

[21] K. Bhattarai, P. Prasad, A. Alsadoon, L. Pham, and A. Elchouemi, "Experiments on the mfcc application in speaker recognition using matlab," in *2017 Seventh International Conference on Information Science and Technology (ICIST)*. IEEE, 2017, pp. 32–37.

[22] V. Tiwari, "Mfcc and its applications in speaker recognition," *International journal on emerging technologies*, vol. 1, no. 1, pp. 19–22, 2010.

[23] D. Subedi, E. Schoemer, D. Chitrakar, Y.-H. Su, and K. Huang, "Contact localization via active oscillatory actuation," in *2022 IEEE/SICE International Symposium on System Integration (SII)*. IEEE, 2022, pp. 344–350.