Inertial-Measurement-Based Biometric Authentication of Handwritten Signature

Divas Subedi, Isabella Yung, Digesh Chitrakar, Kevin Huang

***Abstract*— With increased reliance of digital storage for personal, financial, medical, and policy information, a greater demand for robust digital authentication and cybersecurity protection measures results. Current security options include alpha-numeric passwords, two factor authentication, and bio-metric options such as fingerprint or facial recognition. However, all of these methods are not without their drawbacks. This projects leverages the fact that the use of physical handwritten signatures is still prevalent in society, and the thoroughly trained process and motions of handwritten signatures is unique for every individual. Thus, a writing stylus that can authenticate its user via inertial signature detection is proposed, which classifies inertial measurement features for user identification. The current prototype consists of two triaxial accelerometers, one mounted at each of the stylus' terminal ends. Features extracted from how the pen is held, stroke styles, and writing speed can affect the stylus tip accelerations which leads to a unique signature detection and to deter forgery attacks. Novel, manual spatiotemporal features relating to such metrics were proposed and a multi-layer perceptron was utilized for binary classification. Results of a preliminary user study are promising with overall accuracy of 95.7%, sensitivity of 100%, and recall rate of 90%.**

***Keywords*— security and privacy, embedded and cyber-physical systems, inertial measurement, biometrics, authentication**

I. Introduction

Security is a growing concern in today's technology-driven world. With many aspects of life pivoting towards digital and internet based information storage, computing and engineering research has increasingly been looking into improving security options. Currently, user-based systems need a method of authentication in order to verify the identity of the user. Several methods of authentication are commonly used such as alpha-numeric passwords, PINs, one-time passwords (OTP), facial recognition, fingerprints, and physical signatures depending on the need and ease of implementation in the system. Recently, data-driven biometric signatures such as fingerprint, DNA, facial structure classification, and iris has gained popularity. However, these authentication methods have salient drawbacks to them; passwords and PINs can be brute-force cracked given enough time, yet sufficiently complex passwords can be a hassle to remember for the user. OTP and two-factor authentication require a secondary device and a connection to a network.

As for biometric security measures like fingerprints and facial recognition, these features are intrinsic to the user and do not need to be learned or memorized by the user. However, these methods have their technological limitations and may not work reliably under certain conditions, e.g. wet skin, lighting conditions etc. Furthermore, if hacked, fingerprint and facial recognition authentication is not readily changed or updated due to their intrinsic nature. This work seeks a marriage of the password complexity paired with ease of use of biometric systems and the flexibility of more extrinsic security features. Physical handwritten signatures present a potential intersection of biometric features and extrinsic authentication.

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

A. Related Work

One's handwritten signature is typical practiced and evolved over many years. A written signature is composed of two parts: a complex kinetic and contact-driven one during the execution, and the final visual result. The current method of signature authentication is manual inspection of minor details and visual features in the visual signature. This is not only a cumbersome and slow process, but also inefficient and subjective. As signatures tend to vary greatly even within an individual, manual inspection leaves a lot of room for uncertainty in authentication. Additionally, there is no device currently readily available that can verify a user strictly using handwriting.

Inertial measurements of handwriting are proposed as methods of improving handwritten signature verification. Earlier studies with accelerometer-based pens were conducted using multiple accelerometers and a simple match-making algorithm [1], and also to reproduce handwriting samples [2]. They tracked the position, velocity, and acceleration of the stylus, and it was observed that significant variations exist among the representation spaces. Following this, some hand-crafted inertial features were used to train a neural network [3]. More recent work and technology investigate the use of complex neural networks like Hidden Markov Models (HMMs) [4], [5] and Recurrent Neural Networks (RNNs) [6], yet often aren't isolated to a single writing stylus embedded system.

Several automatic signature verification systems have explored both offline and online signature authentication. In the case of offline signature authentication, several techniques have been employed, such as pixel matching techniques [7], SVM classifiers [8]. For online signature verification, several methods such as Dynamic Time Wrapping [9], hidden markov models [10], and neural network networks [11], [12] have been explored.

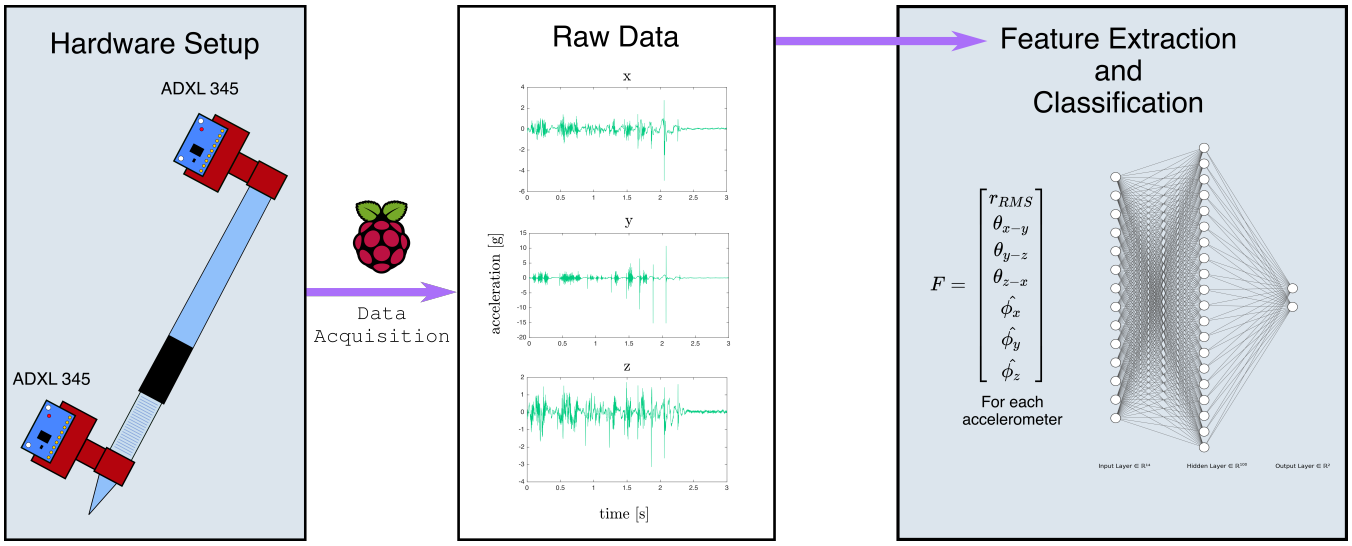


Fig. 1: Flowchart of sensorized writing stylus authentication scheme. Off-the-shelf accelerometers are mounted to a standard writing stylus, and raw data is continually logged first for feature extraction and network training. Once training is complete, the user will utilize the sensorized stylus, and real-time inertial data is processed via the trained perceptron network for authentication.

B. Contributions

To the best of authors' knowledge, this work is the first to introduce simultaneously in a single, embedded biometric authentication system:

- inertial measurements of writing stylus for user authentication during handwritten signature;
- novel hand-picked spatiotemporal features;
- preliminary user study demonstrating online perceptron-based authentication.

Figure 1 depicts the general workflow of the biometric security stylus and classification scheme.

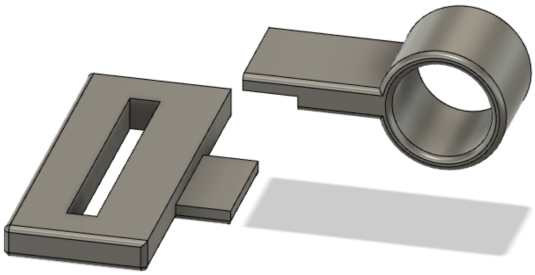
II. Methods

A. Hardware Design

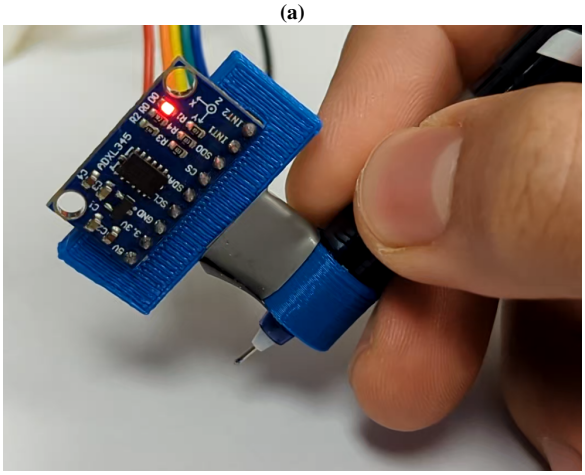
1) Accelerometer: Characterizing kinetic and kinematic properties of handwriting is needed to properly specify sensing requirements. In kinematic analysis of handwriting, it has been documented that acceleration during human hand writing is limited to around 10g [13]. Similarly, current literature has shown that the handwriting relevant features are within the lower frequency bands of 100Hz [14]. Thus, a suitable sensor must meet the following of requirements:

i) Support measurements below 10g;
ii) Sensitive to change in acceleration;
iii) Sampling frequency of at least 1000Hz;
iv) Operate at low power;

Based on these constraints, the ADXL-345 – a readily available and off-the-shelf item – was chosen as it meets aforementioned necessary features. In addition to this, the accelerometer is compact and some packages are of a form factor that can extend this work to be embedded within the writing stylus. The sensor additionally is equipped with an in-built low pass filter to remove irrelevant noise.

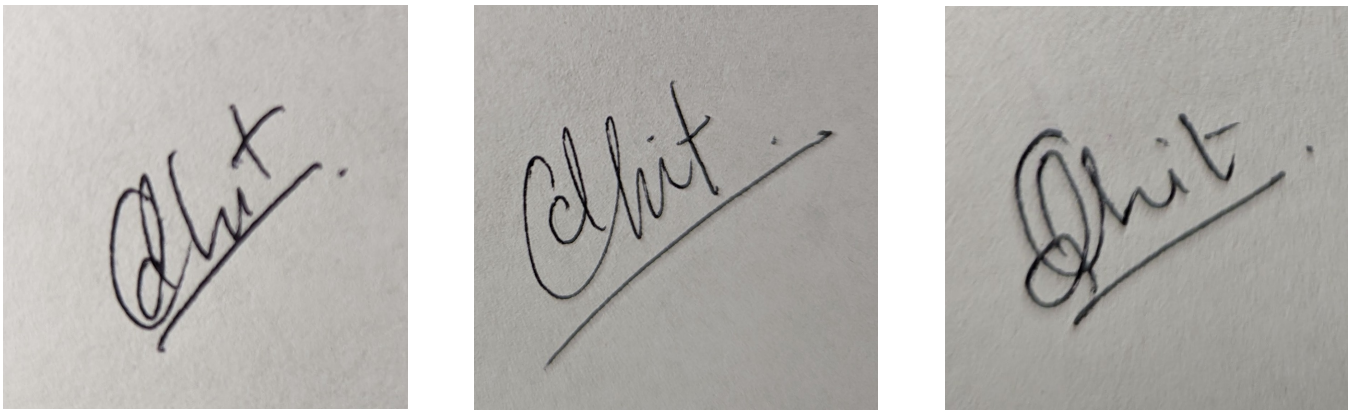


(a)



(b)

Fig. 2: (a) CAD models of accelerometer mounts to affix to writing stylus. Parts were printed via fused deposition with PLA plastic (b) Sensor mounts affixed to the writing utensil. This mount introduces a small moment arm since the sensor is not on the stylus axial axes. However, consistent stylus grip is encouraged due to the mount placement on the grip area of the stylus.



(a) Authentic Signature **(b)** Forged Signature 1 **(c)** Forged Signature 2

Fig. 3: Example true and forged written signature visual outputs. While the forgeries are amateur, and could likely be discounted by a written signature specialist, the process of authenticating these visual outputs is cumbersome, delayed, and subjective. The proposed device uses biometric markers of how a subject produces this visual output to authenticate the user rapidly.

2) Sensor Mount Design: In this prototype design, two readily available, off-the-shelf accelerometers (ADXL 345) were used. These sensors were affixed near the two ends of the writing stylus, as depicted in Fig. 1. The mounts were created via fused deposition of PLA plastic, and extend the sensor outside of the writing stylus axis. While this introduces a moment arm that may amplify inertial signals, the design also encourages a consistent stylus grip (as opposed to a full-embedded design). The prototype mount CAD drawing and final mount are depicted in Fig. 2.

3) Data Collection: A Raspberry Pi single board computer was used to facilitate data collection and storage from the sensorized writing stylus. The two accelerometers were connected to Raspberry Pi through SPI serial protocol, thus sharing serial clock for synchronization – they were configured to collect samples at 1000Hz.

B. Experimental Procedure

Three human subjects were recruited for a preliminary user study. Subject 0 performed their authentic signature while Subject 1 and Subject 2 attempted to forge Subject 0's signature. Subjects 1 and 2 were presented only the final visual output of Subject 0's signature, as depicted in Fig. 3a. During the experimental procedure, the two accelerometer 3-axis acceleration measurements were sampled. 50 trials from each subject were taken with each spanning 3 seconds, resulting in total of 50 true signatures and 100 forged, totalling 450 seconds worth of acceleration data.

C. Feature Spaces

Manually selected features F were determined by observations from data in transient behavior.

$$F = \begin{bmatrix} r_{RMS} & \theta_{x-y} & \theta_{y-z} & \theta_{z-x} & \hat{\phi}_x & \hat{\phi}_y & \hat{\phi}_z \end{bmatrix}^T \quad (1)$$

The following equations depict the chosen features

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

$$\theta_{i-j} = \arctan\left(\frac{a_{i_{RMS}}}{a_{j_{RMS}}}\right) \quad (3)$$

$$\hat{\phi}_i = \arg\left(\frac{1}{N}\sum_t a_i(t) \cdot \exp\left(2\pi\frac{t}{T}\right)\right) \quad (4)$$

where, T is the total time of data collection per sample, N is the total number of data points per sample, i and j one of the 3 spatial dimensions, viz. x, y, or z. The features were designed with motivation to study energy distribution both along the spatial axes (r_{RMS}, θ_{i-j}) and the temporal distribution of energy ($\hat{\phi}_i$).

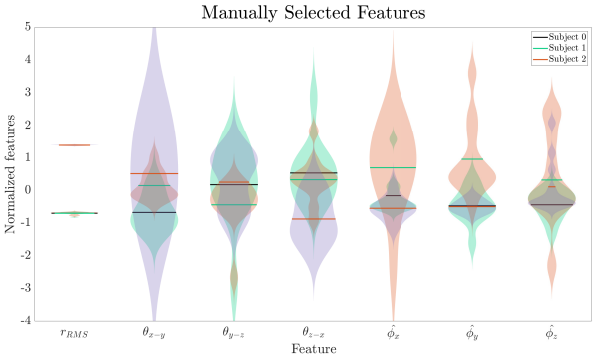


Fig. 4: F Feature Space - bean plots show distributions of feature values for individual's real signatures.

After data collection but prior to classification, the feature space was pre-processed and normalized along all feature dimensions via Z-score normalization. Figure 4 shows the distribution of each feature stratified by individual subjects' signatures. Subsequently, the same set of features were generated for the second accelerometer and concatenated with the former to generate an expanded feature space, F, of 14 features. Figure 5 shows the distribution of each feature for the authentic and forged signatures.

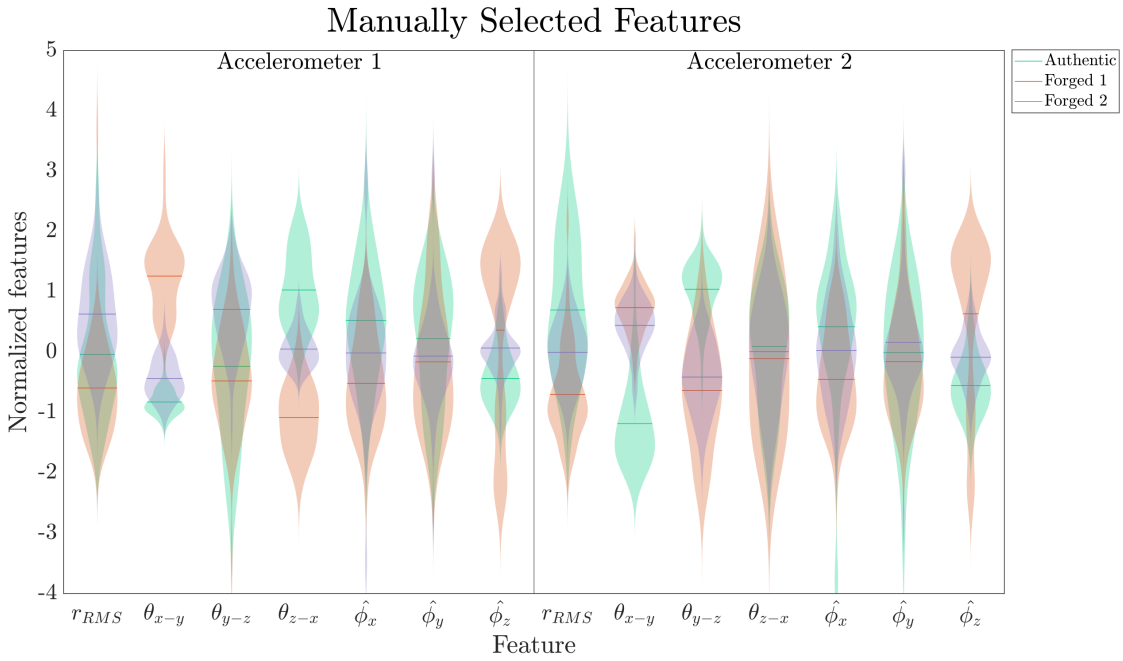


Fig. 5: F Feature Space - bean plots show distributions of feature values for authentic and forged signatures.

D. Classification

For classification, a multilayer perceptron, $\mathscr{A}_{MP}$, was trained with a single layer of 100 perceptrons using scaled conjugate gradient backpropogation to optimize cross entropy. The fourteen features in F served as an input to the classifier which yielded an output of vector with size two (forged vs. authentic). The network was trained to learn the authentic signature. 127 samples (40 authentic signature and 77 forged signature) were used for training while 23 samples (10 authentic signature and 13 forged signature) were used for testing, resulting in a roughly 85% to 15% split.

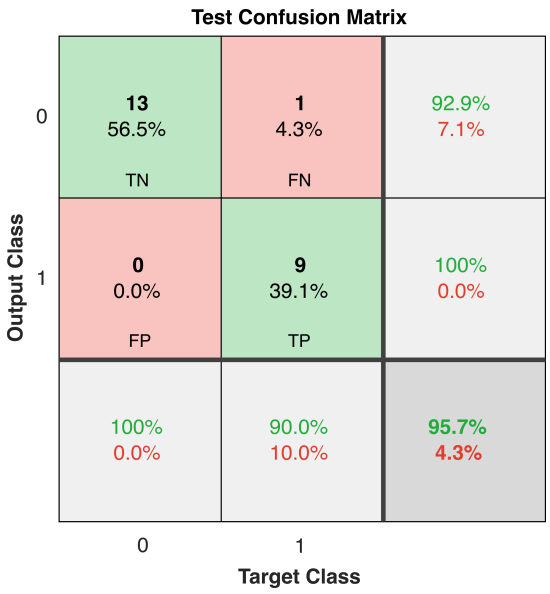


Fig. 6: F Confusion matrix depicting binary classification using $\mathscr{A}_{MP}$

III. Results

Figure 6 depicts the binary classification results from the user study. Classification results show a sensitivity of 100%, hence, assuring minimal chances of false positive authentication, which is essential for security implementations. An observed recall rate of 90% indicates that the classification takes into account the variability of a single user's signature. In summary overall accuracy of 95.7% was achieved using the multilayer perceptron classifier and manually extracted spatiotemporal feature vector. The results of this preliminary study show that the system can reliably authenticate a true signature and it is worthwhile to extend this platform in future work.

IV. Discussion

In this paper, a proof of concept, preliminary study for signature authentication utilizing inertial measurements was conducted. By implementing a multilayer perceptron with 14 manually selected spatiotemporal features, an overall accuracy of 95.7% was achieved. There are several possible areas for improvement, including:

- The current model analyzes complete samples of a signature for authentication. For true online, continuous use, real-time signature authentication is required. To do so, networks with memory elements like Long Short-Term Memory (LSTM) can be used for continuous authentication.
- The hardware design of the writing stylus can be improved and streamlined. Currently the design is preliminary and utilizes off the shelf equipment for initial prototyping. Small package accelerometers encapsulated in a fully embedded system can minimize intrusive sensorization.

- The feature space of the signatures can be expanded. In addition to the proposed manually extracted features, automatic filter-based feature generation techniques can be used to distinguish less explainable correspondences. Other known features amenable to accelerometer data, such as the Mel-cepstrum features [15]–[18] or for contact detection [19], might also be implemented in future iterations.
- The database will be expanded to include more users and more trials. Furthermore, synthetically generated kinematic information can provide additional data. Simulation approaches have been successful in areas such as gesture recognition [20], and generative adversarial networks have gained much traction in generating new image data [21].
- Finally, the system might be augmented with additional sensing modalities. For example, a pressure sensor might be embedded to capture more contact dynamics localized to the stylus-surface interface.

V. Conclusion

This work presented a sensorized writing stylus system that captures inertial data in order to classify handwritten signatures. The proposed method shows some robustness with signature variability of individual users. In addition to this, the system protects against fraudulent signatures as none of the forged signatures were authenticated in current model or study. Compared to common password models, such as alphanumeric systems, the proposed model relies on the user's signature, which introduces complexity that is difficult to replicate, yet leverages an individual's years of practice and familiarity with handwritten signatures. This increases the security of the system and makes it less susceptible to attacks without incurring undue burden on the user. This work demonstrates that using inertial measurements of signature for signature authentication can be secure and robust, and embedded in a streamline package.

References

[1] R. Plamondon and M. Parizeau, "Signature verification from position, velocity and acceleration signals: a comparative study," in *[1988 Proceedings] 9th International Conference on Pattern Recognition*, 1988, pp. 260–265 vol.1.

[2] T. Miyagawa, Y. Yonezawa, K. Itoh, and M. Hashimoto, "Handwritten pattern reproduction using pen acceleration and angular velocity," *IEICE Trans. Inform. Syst., Pt. 1 (Jpn. ed.)*, vol. 83, no. 10, pp. 1137–1140, 2000.

[3] O. Rohlik, P. Mautner, V. Matousek, J. Kempf, and K. Weinzierl, "A new approach to signature verification: digital data acquisition pen," *Neural Network World*, vol. 11, no. 5, pp. 493–502, 2001.

[4] 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.

[5] 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.

[6] 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.

[7] I. Bhattacharya, P. Ghosh, and S. Biswas, "Offline signature verification using pixel matching technique," *Procedia Technology*, vol. 10, pp. 970–977, 2013.

[8] F. E. Batool, M. Attique, M. Sharif, K. Javed, M. Nazir, A. A. Abbasi, Z. Iqbal, and N. Riaz, "Offline signature verification system: a novel technique of fusion of glcm and geometric features using svm," *Multimedia Tools and Applications*, pp. 1–20, 2020.

[9] R. Al-Hmouz, W. Pedrycz, K. Daqrouq, A. Morfeq, and A. Al-Hmouz, "Quantifying dynamic time warping distance using probabilistic model in verification of dynamic signatures," *Soft Computing*, vol. 23, no. 2, pp. 407–418, 2019.

[10] L. Nanni, E. Maiorana, A. Lumini, and P. Campisi, "Combining local, regional and global matchers for a template protected on-line signature verification system," *Expert Systems with Applications*, vol. 37, no. 5, pp. 3676–3684, 2010.

[11] V. Iranmanesh, S. M. S. Ahmad, W. A. W. Adnan, F. L. Malallah, and S. Yussof, "Online signature verification using neural network and pearson correlation features," in *2013 IEEE conference on open systems (ICOS)*. IEEE, 2013, pp. 18–21.

[12] N. Xu, Y. Guo, L. Cheng, X. Wu, and J. Zhao, "A method for online signature verification based on neural network," in *2011 IEEE 3rd International Conference on Communication Software and Networks*. IEEE, 2011, pp. 357–360.

[13] A. Bisio, L. Pedullà, L. Bonzano, A. Tacchino, G. Brichetto, and M. Bove, "The kinematics of handwriting movements as expression of cognitive and sensorimotor impairments in people with multiple sclerosis," *Scientific reports*, vol. 7, no. 1, pp. 1–10, 2017.

[14] J.-S. Wang and F.-C. Chuang, "An accelerometer-based digital pen with a trajectory recognition algorithm for handwritten digit and gesture recognition," *IEEE Transactions on Industrial Electronics*, vol. 59, no. 7, pp. 2998–3007, 2011.

[15] K. S. Rao and A. K. Vuppala, *Speech processing in mobile environments*. Springer, 2014.

[16] S. Gupta, J. Jaafar, W. F. wan Ahmad, and A. Bansal, "Feature Extraction Using Mfcc," *Signal & Image Processing : An International Journal*, vol. 4, no. 4, pp. 101–108, Aug. 2013. [Online]. Available: http://www.aircconline.com/sipij/V4N4/4413sipij08.pdf

[17] M. Strese, J.-Y. Lee, C. Schuwerk, Q. Han, H.-G. Kim, and E. Steinbach, "A haptic texture database for tool-mediated texture recognition and classification," in *2014 IEEE International Symposium on Haptic, Audio and Visual Environments and Games (HAVE) Proceedings*, 2014, pp. 118–123.

[18] 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.

[19] R. Mitra, K. Boyd, D. Subedi, D. Chitrakar, E. Aldrich, A. Swamy, and K. Huang, "Contact sensing via active oscillatory actuation," in *2020 3rd International Conference on Mechatronics, Robotics and Automation (ICMRA)*. IEEE, 2020, pp. 99–104.

[20] K. Lindgren, N. Kalavakonda, D. E. Caballero, K. Huang, and B. Hannaford, "Learned hand gesture classification through synthetically generated training samples," in *2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. IEEE, 2018, pp. 3937–3942.

[21] Y.-H. Su, W. Jiang, D. Chitrakar, K. Huang, H. Peng, and B. Hannaford, "Local style preservation in improved gan-driven synthetic image generation for endoscopic tool segmentation," *Sensors*, vol. 21, no. 15, p. 5163, 2021.