IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 28, 2022, accepted May 18, 2022, date of publication May 25, 2022, date of current version June 6, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3177905

Sensing In-Air Signature Motions Using Smartwatch: A High-Precision Approach of Behavioral Authentication

GEN LI AND HIROYUKI SATO, (Member, IEEE)
Department of Electrical Engineering and Information Systems, Graduate School of Engineering, The University of Tokyo, Tokyo 113-8656, Japan
Corresponding author: Hiroyuki Sato (schuko@satolab.itc.u-tokyo.ac.jp)

This work was supported by KAKENHI (Grants-in-Aid for Scientific Research) under Grant (C) 19K11958, Grant (B) 19H04098, and Grant (B) 20H04168.

ABSTRACT By virtue of the stability of signatures and the high difficulty of imitation, handwriting signatures, as an important behavioral biometric trait, have been broadly adopted for authorization and identity verification. The emergence of consumer-level wrist-worn devices incorporating rich sensors has profoundly changed human-machine interactions, enabling new signature observation method. In this study, we investigate the feasibility of authenticating users by sensing hand motions of signing in air using fingers. Each signature is represented by the readings of the gyroscope and accelerometer which are compensated by the device attitude readings. A recurrent neural network-based algorithm is proposed to characterize signatures and accurately determine whether a signature is from the claimed genuine user or an imposter. We empirically investigate 22 participants by recording their in-air signing gestures using smartwatch motion sensors. The verification shows that despite the inevitable variability of repeating genuine signature drawing, forged signatures tend to show more dissimilarity than variability. The high-precision experimental result (i.e., equal error rate of 0.83%) against insider adversaries not only demonstrates the effectiveness of our proposed approach but also indicates the feasibility of a more user-friendly signature authentication method by signing their names in the air. Moreover, we investigate the impact of the properties of motion sensory data on signature authentication. In addition, we include more details of the experiments, validation of the proposed pre-processing method, and analysis of the circumvention as one of the desirable properties of biometrics of signing motions by measuring the skill of forgery.

INDEX TERMS Behavioral authentication, in-air signature, smartwatch, motion sensors.

I. INTRODUCTION

Nowadays with advancements in the information technology and frequent human-computer interactions (HCIs), a huge amount of data is continuously generated and consumed every day. The growing number of security incidents [2] has increased the requirements for reliable user authentication [3]. Knowledge-based authentication schemes like passcodes or lock patterns, as the current major approaches, are theoretically secure enough guaranteed by large enough password space. However, security is often compromised because of the practical bias of selecting secrets in which users tend to select easy-to-remember passcodes and easy-to-draw lock patterns [4]. Alternatively, biometrics provide a trade-off between strong security and high usability and have been gaining popularity in both academia and industry [5], [6]. Biometrics are often categorized into *biological* and *behavioral* ones, which rely on innate properties of human bodies (e.g., face, fingerprint, or iris) or personal manners of performing specific tasks (e.g., gait, keystroke) respectively.

Handwritten signatures are one of the most studied and developed behavioral biometrics [7]. From the cultural aspect, handwritten signatures have long been established, broadly accepted as the symbol of consent and authorization on many occasions such as issuing documents and financial transactions [8]–[11]. Besides, a signature is heavily

The associate editor coordinating the review of this manuscript and approving it for publication was Andrea F. Abate.

practiced, unintentionally consolidating muscle memory. It not only enables the stable personal signing manners over time but also preserves the unique characteristics that are resistant to forgeries [12]–[15]. From the aspect of data acquisition ways, signature authentication has been extended from *offline*, in which signatures are mainly produced with conventional pen and paper-based tools, to *online* where signatures start to be acquired by electronic signature pads and pens. Because online acquisition can record not only completed signature images, but also more dynamic information (e.g., x, y coordinates, pressure, and pen-up/down) during signing processes [16], it tends to facilitate the system's accuracy and robustness [10], [11], [16]–[18] and consequently has been increasingly adopted by organizations [19], [20]. However, the traditional online signature acquisition systems are often based on dedicated digitizing devices (i.e., electronic signature pads and pens) and lacks portability. This results in the performance loss in usability and limits the signing scenarios. With the development of digitizing devices and sensing technologies, further studies have focused on *emerging ways* to record signing processes for authentication using smartphones [21], [22], attachable motion sensors [23], and cameras [24]–[26].

Recent years have witnessed a rapid growth in the wrist-worn devices (e.g., smartwatch) market which is forecast to further increase from 66.5 million units in 2019 to 105.3 million units by the end of 2022 [27]. Modern smartwatches, as general devices, are often equipped with a variety of embedded sensors, such as motion sensors (e.g., gravity, accelerometer, gyroscope, and magnetometer), environmental sensors (e.g., light, temperature, barometer, and proximity), and position sensors (e.g., GPS and compass), to fulfill the needs of various applications [28]–[30]. Furthermore, the longitudinal activity analysis [31] has shown fairly high and consistent smartwatch usage throughout the days with only a few short breaks, enabling high availability for HCIs. As a result, modern wrist-worn devices, such as smartwatches and fit bands, have been increasingly used to analyze users' activities, which also enables efficient and ubiquitous body motion observation as behavioral biometrics [32].

Numerous studies have explored methods for biometric authentication using modern mobile technologies and embedded sensors to model user behavior, which shows the high effectiveness of motion sensors in capturing discriminative behavioral characteristics that can be used to accurately authenticate users. There are two main types of biometrics, gait and gesture, which have been extensively studied. In gesture-based authentication, motion sensors are used to capture the user's hand movement while performing certain gestures, such as hand circle and rotation [33], flick wrist [34], grasp [35], handshaking [36], free handwriting [37], finger-snapping [38], arm-raising [39], and thumb up [40]. In gait-based authentication, motion sensors record walking in a personal manners [41]–[44].

Research on handwritten signature authentication using wrist-worn devices is still underdeveloped, focusing more on *Table Signature* that users sign their names on a plane using pens or touchscreens [45], [46]. In contrast, *In-air Signature* refers to a more flexible way of signing that allows users to perform signing processes with their fingers in the air. Although studies on in-air signature authentication have emerged in recent years, most of them either construct strokes from videos recorded by depth cameras [24]–[26] or require dedicated devices (e.g., Leap Motion [47]). As modern wrist-worn devices with rich sensors can capture user activities, the potential of recording in-air signatures using such devices can be explored. However, this research currently still remains at an early stage, with few studies [48].

To address this gap, we explored the feasibility of in-air signature authentication using modern wrist-worn devices during an empirical investigation with invited 22 participants. Our study reveals that sensing in-air signature motions well satisfies the desirable properties to serve as a high-precision behavioral authentication approach with improved usability. Users can be authenticated by freely signing their names in air. We use readings from motion sensors, a combination of an acceleration sensor that measures changes in velocity, and a gyroscope that measures angular velocity to depict the corresponding hand movement during signing. A recurrent neural network (RNN)-based algorithm is proposed to process sequential sensory data and verify if an unknown signature originates from the claimed genuine user. In Particular, we adopt an *active attack* model, assuming the existence of *insider adversaries* who possesses basic knowledge about their victims. In addition, we leverage dynamic time wrapping(DTW) to assess the similarity distribution, the resistance to circumvention of in-air signatures, and the effectiveness of calibration pre-processing of rotation.

To sum up, the main contributions of this work are listed as follows:

1) We conduct a preliminary experiment analyzing the differences in signing behavior between the traditional method (i.e., table signing) and in-air writing.
2) We provide insights into an emerging behavioral authentication approach for in-air signatures using smart wrist-worn devices that has the potential to serve as a more user-friendly alternative to conventional signature authentication. Specifically, we empirically investigate the in-air signature motions of 22 participants from the perspective of behavioral biometric authentication.[1]
3) We propose an in-air signature authentication scheme using smartwatch motion sensors. It can characterize signatures and accurately distinguish genuine signatures from skilled forgeries; We avoid sophisticated feature design; instead, a Siamese RNN is used to learn signature representations. Furthermore, the system has to only store signature representations rather

[1]The dataset presented in this study is available on an agreement of use, following the Japanese privacy regulations. Please contact schuko@satolab.itc.u-tokyo.ac.jp with Subject: SIGNATURE DATASET.

than original data, which hides original sensitive user data and saves space;

4) We evaluate the proposed authentication method, successfully demonstrate its effectiveness, and comprehensively analyze the properties of signature motion sensory data, including input patterns, the impact of length, circumvention, and performance comparison with related work.

The remainder of this paper is organized as follows. Section II clarifies the problems that need to be solved. Section IV provides an overview of related work. Section V demonstrates the methodology. Section V shows the experimental results. Section VI discusses the properties and limitations of the study. Finally, Section VII concludes this paper.

II. PROBLEM STATEMENT

The main goal of this study is to investigate the feasibility of in-air signature authentication using smartwatch motion sensors including 1) proposing an appropriate scheme for authentication and 2) revealing the characteristics of signatures' sensory representations.

As for the authentication scheme, it is to correctly distinguish between signatures from imposters and genuine users. A typical signature authentication process comprises two main phases: an enrollment phase and a verification phase consisting of the following processing steps [10], [16], [49]–[52] as shown in the Figure 1.

1) *Data acquisition and preprocessing*: Regardless of the phases, signing processes should be initially collected by acquisition devices (i.e., touchscreen, sensor, camera, and scanner), generating images or electronic signals representative of the signatures. The signatures are then preprocessed using appropriate techniques to reduce noise and improve data quality.
2) *Knowledge extraction*: This step extracts knowledge that can reflect the discriminative characteristics of signatures. Extracted knowledge can be divided into two main types: functions and features. The former refers to time functions that can be calculated from given raw signals (e.g., velocity, derivative, and consecutive distances), while the latter often refers to discrete parameters (e.g., mean, variation, length, and entropy). Knowledge extraction way often depends on the data formats of signatures and applied methods.
3) *Templates generation*: The enrollment phase refers to sample collection and subsequent template generation, during which a user has to provide a set of signatures to the authentication system. After the previous steps, properly extracted knowledge is used to generate reference templates, which are then stored in the database (may together with the original signature data).
4) *Matching*: The verification phase refers to the acquisition of unknown signatures and matching with the templates. In this step, the authentication system acquires a new signature sample with a claimed user identity id that has already been enrolled and then processes the sample in the same way to match it with the template. The system retrieves the corresponding template $t_{id} = \{t|ID = id, t \in T\}$ according to the claimed identity in the knowledge base. Proper algorithms (e.g., Euclidean distance and DTW) are then used to measure the similarity $s(q, t_{id})$ between the questioned signature q and its template t_{id}. Depending on the comparison between the similarity score and its threshold value Δ, the authentication system decides whether the given signature originates from an imposter Sig_{Forged} or the genuine user $Sig_{Genuine}$.

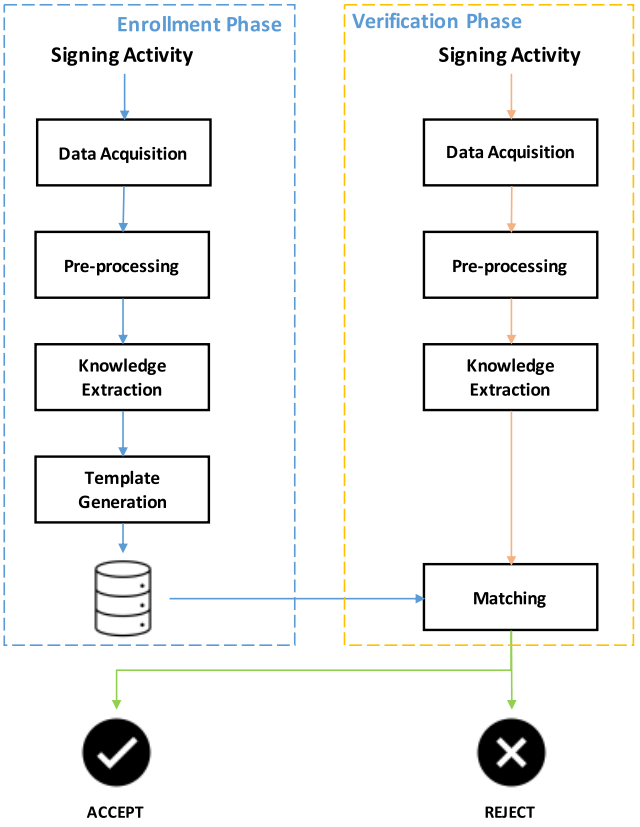


FIGURE 1. Overview of signature authentication task.

Therefore, in this study, the authentication scheme should address the problem of acquiring in-air signing activities using smart wrist-worn devices, processing raw signals, extracting discriminative information, and matching questioned signatures with corresponding templates to determine whether they belong to the claimed genuine signer or adversary.

As for the characteristic revealing, we seek to answer the following three questions corresponding to the three critical desirable properties of biometrics:

1) *Collectability*: How easy can we observe and record in-air signature motions/gestures using modern wrist-worn devices?

2) *Performance*: How much capacity do the motion sensory readings have to discriminate users?
3) *Circumvention*: How difficult it is for imposters to generate forgery for mimicry attack?

III. RELATED WORK

Signature verification is one of the most frequently used biometric techniques for personal authentication [53] owing to its high usability, acceptability, and efficiency. As the result, the studies about it show remarkable progress from the traditional stage (i.e., offline) when a signature is acquired by scanning the signature written on papers to the form of images, to advanced stage (i.e., online), at which a signature is acquired using a tablet or touch screen to include more dynamic information of the signing process. Furthermore, in recent years, the development of mobile and sensing technologies has encouraged many studies to explore emerging methods of signature acquisition.

A. OFFLINE SIGNATURE AUTHENTICATION

Offline signature authentication deals with data in the form of static grayscale images, the pixels of which reflect the signature shape. The verification process relies mainly on feature-based methods that extract feature vectors from signatures and match them to distinguish between genuine and forged signatures.

Some studies have focused on specific parts of signatures. For example, based on the characteristics that pixels of signature with high pressure appear as dark zones and therefore corresponds with gray levels conforming histogram, Vargas *et al.* [54] computed pseudo-cepstral coefficients from the histogram of the static signature images as feature vectors for verification. Using signatures from 100 individuals, the author trained a least squares support vector machine(LS-SVM) for classification and achieved a 6.20% EER. In addition, Shekar *et al.* [55] investigated the characteristics of bound regions starting by identifying and filling them with intensity values. After processing the bounded regions into a matrix, they calculated the eigenvectors corresponding to q largest eigenvalues to determine the most dominant characteristics while reducing the size of the feature vector, which was finally evaluated with 30 subjects to obtain an EER of 8.78%. In addition to the local features characterizing specific parts, global features concerning the entire signature images have also been investigated for authentication. RamachandraA *et al.* [56] extracted five global features including a)maximum horizontal and vertical histograms, b)horizontal and vertical center points, c)edge points, d)signature area, e)aspect ratio. By measuring the Euclidean distance between feature vectors, their method achieved a 5.4% FRR and 4.6% FAR in their experiment, including 21 participants. Regarding the feature extraction method, as neural networks have become more prevalent in pattern recognition, they have been adopted to avoid the difficulty of feature crafting while efficiently preserving intrinsic characteristics. Hafemann *et al.* [57] leveraged convolutional neural networks (CNNs) to learn user-dependent and feature spaces. The best results that their methods achieved were 1.72% EER with 160 subjects.

B. ONLINE SIGNATURE AUTHENTICATION

Online signature authentication deals with the dynamic information of user signatures. With the signatures acquired by electronic signature pads and pens, online verification can not only consider the signature as a static image, but also take more dynamic writing process details into consideration, such as x, y coordinates representing the dynamic handwritten strokes, and possibly pen pressure, angle, and velocity at each timestamp [58]. This provides a greater quantity of information, thereby improving the system's accuracy and robustness of systems [17].

On one hand, additional dynamic information enables many new feature extraction approaches that are specifically devoted to online signatures [10]. For example, Guru and Prakash [59] focused on the specific characteristics of online signature representation by selecting features such as signing duration, number of pen ups, and derivative of velocity, and finally obtained 3.8% EER on a dataset including 100 subjects. On the other hand, online signature representations also enable function-based methods that directly compute using the functions of time. Dynamic time warping (DTW) is one of the most widely used elastic matching algorithms to measure similarity. Many studies [19], [49], [52] have explored the utilization of DTW in online signature authentication problems. Combined with different extra function generation and matching schemes, DTW shown its effectiveness by achieving 1.6% FAR and 2.8% FRR (102 subjects) [52], 1.4% EER (94 subjects) [19], and 1.28% EER (100 subjects) [49]. Meanwhile, neural networks have also been used to process temporal functions of online signatures. Bromley *et al.* [60] implemented a Siamese time-delay neural network to address the function-based online signature verification problem. The study fixed the signature lengths and calculated ten functions of time describing the signing movement, signature shape, position, direction, and curvature. The dual branch of the networks was arranged to measure the dissimilarity between temporal functions. The approach correctly recognized 95.5% of genuine signatures and 80% of forged signatures from 219 individuals. Furthermore, by virtue of the strong capacity of recurrent neural networks (RNNs) in processing sequential data and pattern recognition, Tolosana *et al.* [61] implemented RNN variations to deal with 23 expanded time functions of signatures and achieved 4.75% EER on a dataset including 400 subjects.

C. EMERGING SIGNATURE AUTHENTICATION

With the development of mobile and sensing technologies, many emerging studies have attempted to explore novel methods for signature data acquisition and appropriate processing methods for authentication. For example, Sae-Bae and Memon [62] collected signatures from 180 users who on

smartphones touchscreen with fingers. By calculating the histograms of both Cartesian and polar signature representations as features, they achieved 2.67% EER. Cheng *et al.* [23] showed that an attachable motion sensor can be used to acquire signing activities by installing it at the top of a pen. They digitized the handwritten signatures of the 63 participants into sensory traces. Their DTW-based approach could distinguish between genuine and forged signatures according to the sensor readings, achieving 5.04% FRR and 7.92% FAR. Instead of attachable sensors, Nassi *et al.* [45] and Taimoor *et al.* [46] attempted a more user-friendly way to acquire signatures by using wrist-worn devices incorporating motion sensors. By using function-based and feature-based methods respectively, they obtained 5.4% EER with 66 participants [45] and 4% EER with 10 participants [46].

Despite the common online signature verification systems adopting the *contacted* model of signing on a tablet or touch screen, the in-air signature, as a more user-friendly technique to conduct *contactless* authentication, has been attracting attention. In-air signature authentication studies have started from using cameras, such as Fang *et al.* [24] and Malik *et al.* [25], [26]. Signature data were collected from 14, 15, and 40 subjects respectively. In their studies, in-air signing activities were recorded into videos, which were then used to track fingertips and recover in-air signature trajectories in a series of coordinates. Their function-based methods achieved 2.86% FRR and 1.90% FAR [24], 0.46% EER [25], and 0.055% EER [26]. Guerra-Segura *et al.* [47] found that dedicated motion tracking devices of Leap Motion show advantages in 3D spatial measurements of hands compared with cameras. After extracting feature vectors from 21 temporal functions, their method achieved an EER of 1.20% with 100 users. Instead of signature trajectory recovery using the dedicated devices, Bailador *et al.* [21] attempted to acquire in-air signing activities using a smartphone accelerometer and directly authenticate users based on acceleration signals. Their DTW-based matching method obtained 4.58% EER with 96 participants. Buriro *et al.* [48] are presented the only study that attempted to demonstrate the feasibility of in-air signature authentication using smartwatches. However, their study focused more on different scenarios including signing during sitting, standing, walking in the corridor, upstairs, and downstairs, obtaining a 19.48% FRR 21.65% FAR using a feature-based method using the signature data collected from 11 individuals. Therefore, this study currently still remains at an early stage.

IV. PROPOSED METHOD

Our research provides a Siamese RNN-based in-air signature authentication method in which signatures are represented by motion sensor signals. It can not only deal with sequential data with different lengths while avoiding the use of manually designed sophisticated features but also encode reference signatures to compressed representations to improve storage efficiency and privacy.

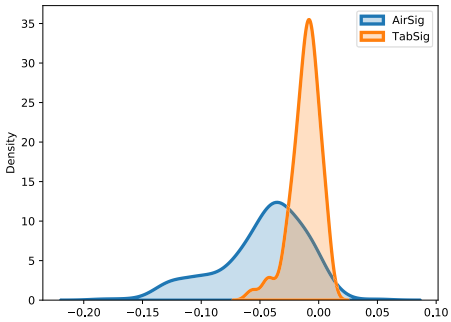


FIGURE 2. Comparison of attitude distribution between table signing and in-air signing.

A. DATA ACQUISITION

This is the first step as shown in Fig1, the singing actions are recorded and digitized into electronic signals. This study focuses on the signing activity of *In-air Signature*, which is a more flexible and user-friendly signing method performed by fingers. Smartwatches with motion sensors are used to acquire data of hand movements during the in-air signing. An in-air signature is represented by a combination of three-axis gyroscope and three-axis acceleration readings of a time-dependent variable length.

Because table signing actions are often restricted by hard plane (e.g., tables) and writing borders (e.g., size of paper or touch screen), they often can be repeated in a more stable way; however, less restriction makes in-air signatures tend to be performed in different positions and orientations, which can bring extra variety between genuine signatures of the same individual, undermining the stability and accuracy of authentication. Therefore, we conducted a prior survey to investigate the differences by recruiting 15 subjects, each of whom provided 10 table signatures and 10 in-air signatures, while the *device attitude* readings were recorded. *Device attitude* represents the orientation of the smartwatch relative to a reference [63]. Specifically, *pitch*, *roll* and *yaw* show the amount of rotation angle in radians around x, y and z axis. Therefore, the changes in the hand positions and orientations can be captured and reflected by the *device attitude* readings.

As a result of the prior survey, we observed a high variety of in-air signing gestures by analyzing 300 signatures with different signing ways (i.e., table or in air). Fig. 2 shows the density plot comparing the averaged device attitude (i.e., pitch, roll, and yaw) distribution between in-air signatures and table signatures from 15 participants. It is noticeable that table signing is often conducted in similar gestures, whereas in-air signing is freer in hand attitude. Therefore, to deal with the high variability of in-air signing, we additionally recorded *device attitude* data while performing in-air signing to calibrate the accelerometer and gyroscope measurements. Table 1 shows 9-tuple data representation of the in-air signatures.

B. PREPROCESSING

1) *Rotation*: The high variability of in-air signatures can undermine the stability and accuracy of the

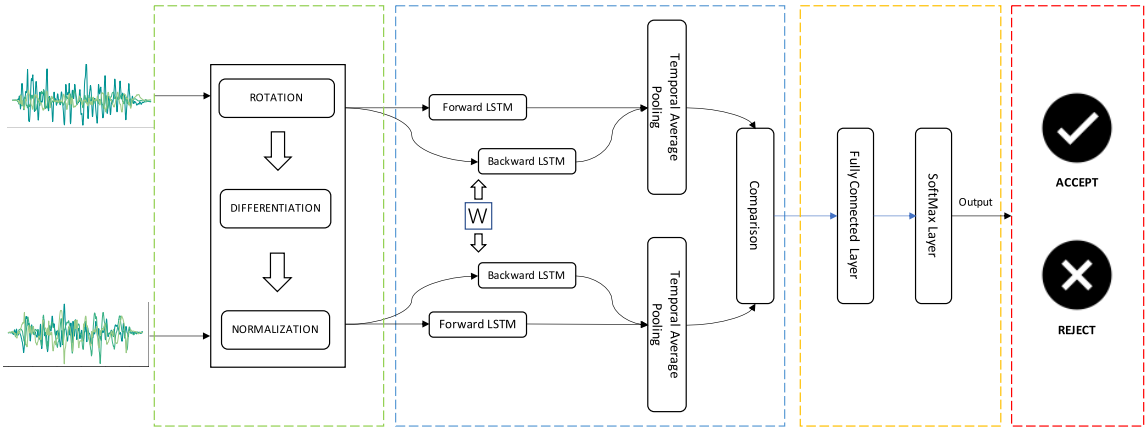


FIGURE 3. Architecture of the proposed authentication method used to classify in-air signature pairs.

TABLE 1. Data representation of in-air signatures.

Dimension	Signal
1	x-axis gyroscope: g_x
2	y-axis gyroscope: g_y
3	z-axis gyroscope: g_z
4	x-axis accelerometer: a_x
5	y-axis accelerometer: a_y
6	z-axis accelerometer: a_z
7	pitch-axis attitude: at_p
8	roll-axis attitude: at_r
9	yaw-axis attitude: at_y

authentication system. For this reason, we conduct the calibration by rotating the three-axis gyroscope and three-axis accelerometer signals to the reference orientation using the three-axis *device attitude* readings. After the rotation, the rotated three-axis gyroscope and accelerometer signals are maintained, while the three-axis attitude data are discarded.

2) *Differentiation*: Because the changing rate of motion sensor readings can also contain discriminative information [59], [61], we apply first-order differentiation on the rotated gyroscope and accelerometer data. The calculated derivative signals are then concatenated with the rotated motion sensory readings to compose a 12-dimensional function of time.
3) *Normalization*: The high flexibility of in-air signatures not only results in a high diversity of positions and orientations but also increases the variety of hand movement scales as there are no writing borders compared with signing on papers or tablets. Therefore, it is necessary to normalize the extended data obtained from the previous stage before using them in the authentication system.
4) *Pairing*: Because the authentication system deals with pairs of signatures (i.e., $[Sig_{unknow}, Sig_{reference}]$), the signatures of the same individual, including genuine signatures performed by themselves and forged signatures produced by imposters/adversaries, need to be pairwise aligned.

C. KNOWLEDGE EXTRACTION AND MATCHING

We design our authentication scheme to consist of three steps (i.e., Encoder, Classifier, and Decision) after signature preprocessing, as depicted in Fig.3. The encoder is composed of a dual-branch bidirectional LSTM network, named the Siamese architecture, in which two subnetworks are identical in structure and share the same weights. The Siamese recurrent architecture is a variation of the vanilla recurrent neural networks that is suitable for pairs of variable-length sequences. Inspired by the utilization of the Siamese recurrent architecture by [64] in the field of natural language processing to measure the semantic similarity between sentences, we introduced it to deal with paired sequential motion sensory data for authentication. Within the encoder, LSTM, a variant of the RNN unit, provides long-term connections while processing temporal signals of motion sensors with variable lengths. The following equations show the calculations performed in an LSTM unit, where the unit accepts a segment of sequential data $[x^{<1>}, x^{<2>}, \ldots, x^{<k>}]$ with length k and can update the hidden state $a^{<t>}$ at each time step t.

$$f_t = \sigma(W_f[a^{<t-1>}, x^{<t>}] + b_f) \quad (1)$$
$$i_t = \sigma(W_i[a^{<t-1>}, x^{<t>}] + b_i) \quad (2)$$
$$o_t = \sigma(W_o[a^{<t-1>}, x^{<t>}] + b_o) \quad (3)$$
$$\tilde{c}_t = tanh(W_c[a^{<t-1>}, x^{<t>}] + b_c) \quad (4)$$
$$c^{<t>} = f_t \circ c^{<t-1>} + i_t \circ \tilde{c}_t \quad (5)$$
$$a^{<t>} = o_t \circ tanh(c^{<t>}) \quad (6)$$

Additionally, we arrange the network bidirectionally to capture forward and backward information. The outputs of the BiLSTM are connected to temporal average pooling, which

can convert temporal sequential data into vectors with a fixed length used to measure their dissimilarity. During classification, the fully connected layer processes the concatenated feature vectors of signature pairs generated by the encoder, while the SoftMax layer calculates the score of whether the incoming pair is a $(S_{genuine}|S_{genuine})$ or $(S_{genuine}|S_{forged})$ pair. Finally, the authentication result is obtained by comparing the score with a predefined threshold λ to determine whether the unknown signature should be accepted or rejected. In particular, the RNN-based method enables the representation learning from sequential data, thereby reducing the burden of feature engineering.

D. LENGTH UNIFORMITY

Temporal function representations of signatures often have different lengths depending on the time consumption and sampling frequency. A variety of lengths has already been utilized as a critical feature in many studies [59], [65]–[67] to distinguish between genuine and forged signatures, as signature forgery tends to consume more time than genuine signing processes [62]. In this research, we also attempt to quantify the effect of length variety by equaling the lengths of all samples and analyze the performance. We apply the discrete cosine transform (DCT) [68], a widely used transformation technique in signal processing and compression, to obtain fixed-length full signals. The DCT can be used to uniform lengths of sequential signals by fixing the number of coefficients in the frequency domain while maintaining the signal shapes, which provides an effective way to determine the influence of lengths [69]. To obtain fixed-length full signals, we scale all signals to the maximum length of the signal using the following steps:

1) *Domain transformation*: The DCT as shown in Equation 7 is applied to all full motion sensor signals to obtain their representations in the frequency domain.

$$y_k = 2\sum_{n=0}^{N-1} x_n \cos(\frac{\pi k(2n+1)}{2N}), k = 0, \ldots, N-1 \tag{7}$$

2) *Padding*: The coefficients of the frequency-domain representations are padded with 0 to the maximum length.
3) *Inverse transformation*: We apply the inverse DCT, as shown in Equation 8, to shift the padded frequency-domain representations back to the time domain.

$$y_k = x_0 + 2\sum_{n=1}^{N} x_n \cos(\frac{\pi(2k+1)n}{2N}), k = 0, \ldots, N-1 \tag{8}$$

4) *Normalization*: We normalize the fixed-length time domain signals.

V. EVALUATION

This section presents a comprehensive evaluation of the proposed in-air signature authentication approach. We conduct an empirical investigation with our participants to determine the performance of distinguishing whether a signature comes from imposters and genuine users and analyze related security properties.

A. EXPERIMENTAL APPARATUS

Our experiment is device-dependent using Apple Watch Series 6 to acquire in-air signatures. We implemented an application using Swift and installed it on our experimental smartwatches. Through the Apple Core Motion framework, the application records the accelerometer, gyroscope sensory readings, and device attitude during the interval between the two ''button pressed'' events indicating the beginning and ending of collection. These two timestamps are used to ease the extraction of valid segments from the signing processes. Sensory data are recorded at a rate of $100Hz$ and then written into files.

B. THREAT MODEL

As signature forgery can be highly uncertain depending on prior information about the victim possessed by an adversary, it is important to consider the type of adversary presence for empirical evaluation. The main goal of adversaries is to spoof authentication systems to be authenticated as the victims, so that they can access their valuable assets and private information. The studies in the field of biometric authentication generally consider two major types of adversaries [51], [70], [71]: insider and stranger adversaries.

1) *Insider Adversary*: who is familiar with the victim. The adversary can possess some knowledge of the victim's behavior and has the opportunity to observe and capture biometric information in proximity. Therefore, an insider adversary is able to launch effective attacks, namely active attacks, towards the victims, depending on their prior knowledge.
2) *Stranger Adversary*: who is not familiar with the victim. The adversary usually has no prior knowledge of the victim and is not able to access biometric information. A stranger adversary can only launch attacks based on general knowledge about used biometrics, namely random attacks.

Specifically, in this study, we adopt the *insider adversary* threat model and set an experiment scenario consisting of two roles.

1) *Victim Genuine User*: who wears the smartwatch and signs his name in the air for authentication. The genuine user is not aware of the presence of imposters, so that they do not deliberately hide their in-air signing gestures.
2) *Insider Imposter*: who can have 1) a visual observation of the victim's hand gesture of in-air signing activity and 2) the chance of practice before forging signatures to generate *skilled forgeries*. In addition, the insider imposter is considered to have knowledge of the authentication protocol and the user ID of the victim.

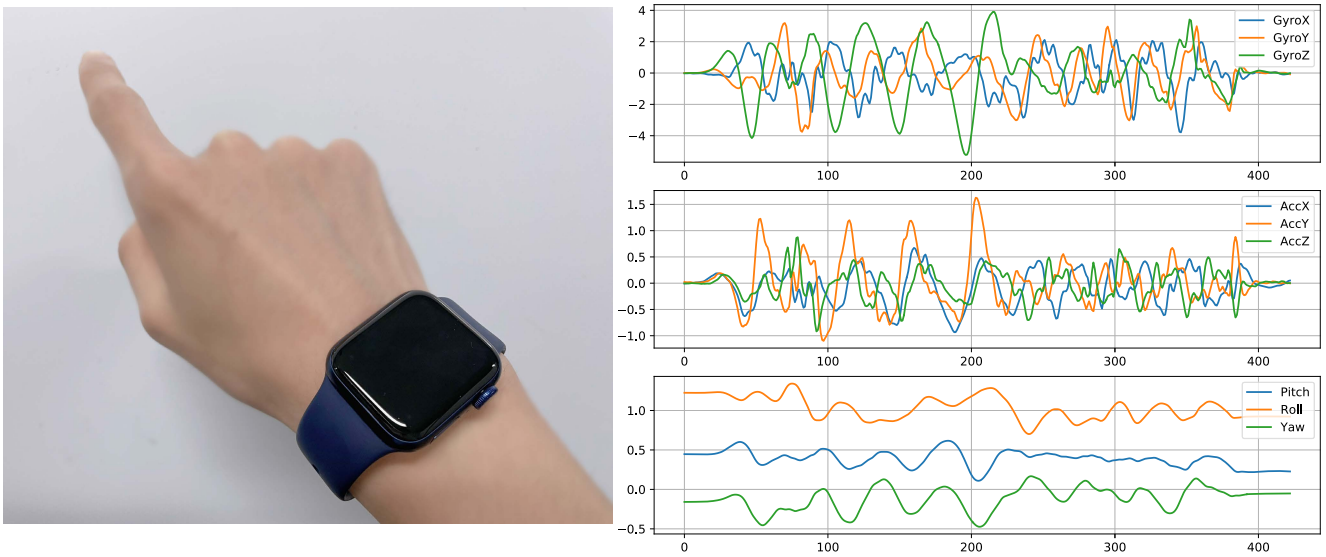


FIGURE 4. The in-air signing process (left) and corresponding motion sensor readings of the smartwatch (right).

C. SUBJECT AND INSTRUCTION

We empirically investigate the in-air signatures of 22 participants, who are generally students or staff at our university located in Tokyo, Japan, and evaluate our proposed method. Our experiment attempts to focus on the in-air signing behavior. Therefore, to control for the effects on other variables, the participants are asked to sit in a similar position to provide in-air signature samples while avoiding hand movement before and after signing. Each of them provides 10 genuine signatures and forges 10 chosen signatures; therefore, we collect a total of 440 signatures, most of which are written in Japanese or Chinese characters. As the same session data collection in which genuine samples are all acquired within a short period may result in an unrealistic level of consistency in the genuine comparisons, we arrange two signature collection sessions for each person about one week apart. Each session contains two steps to obtain 5 genuine signatures by repeating for a given person and then letting him forge 5 chosen victim signatures.

Following the *insider adversary* threat model, each participant is trained to act as an *insider imposter* for *skilled forgery*. Regarding the ''visual observation of the victim's signing activity'', we alternatively record the genuine signing video of each person instead of direct observation because of the difficulty of gathering all participants in the same room. Thus, the signature collection procedures for a session are designed as follows.

1) *Genuine in-air signature acquisition:* In this step, we collect motion sensory data when our participants sign in the air while wearing the smartwatch. In addition, we record the signing processes as videos and ask the participants to provide their signature images.
2) *Forged in-air signature acquisition:* In this step, we let our participants forge the signatures of others to generate *skilled forgeries* by imitating the hand movements of the victims. The mimicry attack is conducted after having a visual observation of the victim's signing video and multiple practices, while the victim's signature image is available for reference.

Our experimenters also record the timestamps of beginning and end. Additionally, to minimize the extra variability that might be introduced by repositioning the smartwatch, we require every participant to wear the smartwatch following the habit in the first session and keep the position in the second session. The reasonableness of this experimental condition is also supported by the study [72] that suggests that switching the locations of wrist-worn devices is not very frequent. It is noticeable that the experiment contents and how their data will be used were clearly explained to all participants, while the data were collected after obtaining signed informed consent forms from subjects without any force. Moreover, we also fairly compensate for the time and troubles of participants with about 1000 JPY (about 10 USD) Amazon Gift Card and provide the right to withdraw at any time if they have any discomfort. In addition, the acquired signature data are securely stored without personal identifiers (using generic identifiers such as U01).

D. DATA REPRESENTATION

Fig.4 depicts an example of in-air signing at the left part that a user signs their name in the air using fingers while wearing a smartwatch, while the right part shows the corresponding valid segment of the three-axis gyroscope, accelerometer, and device attitude readings, where the valid signature segment is extracted from the raw sensory readings between the two timestamps indicating the beginning and end.

As in-air signing activities often cost different amounts of time, the corresponding lengths of the valid motion sensor

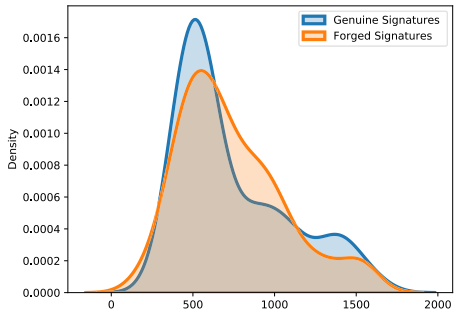


FIGURE 5. Comparison of length density between genuine and forged signatures.

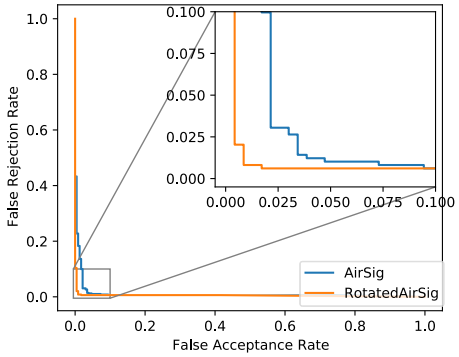


FIGURE 6. ROC curve compares performance with or without rotation.

signals vary from 166 to 1637. Furthermore, the density plot in Fig.5 compares the length distribution of sensory readings between genuine and forged signatures, revealing that forged signatures have a slightly higher variety than genuine signatures in terms of length.

E. PROCEDURE

We start with the preprocessing of acquired in-air signatures as depicted in the previous section by inversely rotating accelerometer ($\{a_x(t), a_y(t), a_z(t)\}$) and gyroscope signals ($\{g_x(t), g_y(t), g_z(t)\}$) according to the attitude data (i.e., $\{at_p(t), at_r(t), at_y(t)\}$). After the differentiation and normalization steps, the rotated signatures are then paired into ($Sig_{genuine} - Sig_{genuine}$) and ($Sig_{genuine} - Sig_{forged}$) pairs, and labeled them with corresponding binary numbers. Consequently, the pairwise aligned signature dataset consisted of 3190 pairs of signatures from 22 participants. We adopt an open-set protocol to divide the dataset by users. Specifically, a total of 2465 pairs from 17 participants are selected to train our RNN-based method, whereas the remaining signatures are used for testing.

For details of the network architecture, the encoder part contains two identical branches, each of which contains two hidden layers of BiLSTM with 24 memory blocks. It is used to process 12-dimensional pre-processed in-air signatures. Temporal average pooling is then applied to the output of BiLSTM with the dimension doubled twice to generate the signature feature vectors with the length of 48. In the next step, scores are obtained from the dense layer classifier activated by SoftMax with the input of the Euclidean distance between the feature vectors of the two branches. An implemented authentication method can be empirically evaluated by estimating the probability of the error case occurrence as follows:

$$FAR = \frac{|\{s|q \in Sig_{Forged}, s \geq \Delta\}|}{|Sig_{Forged}|}$$

$$FRR = \frac{|\{s|q \in Sig_{Genuine}, s < \Delta\}|}{|Sig_{Genuine}|}$$

where the false acceptance rate (FAR) is caused by accepting imposters, whereas the false rejection rate (FRR) is concerned about rejecting genuine users. The authentication scheme makes a decision regarding acceptance or rejection, depending on whether the similarity exceeds the threshold value Δ [73]. Particularly, with the increase in threshold value Δ meaning high conditions to be matched as the genuine user, the FAR and FRR witness a decrease and increase respectively, and vice versa. Therefore, from the viewpoint of performance evaluation, there is a commonly used quantity, namely Equal Error Rate (EER). The EER refers to the error rate when the matching threshold is determined to make FAR and FRR the same value.

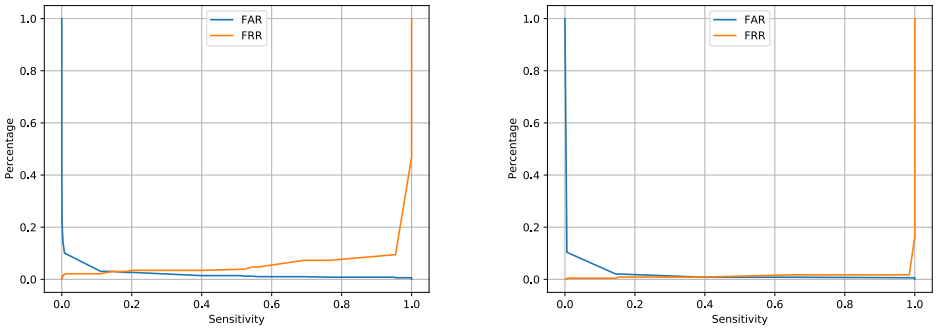
VI. RESULT

A. PERFORMANCE

Initially, we assess the accuracy of the proposed method in distinguishing genuine signatures from forged signatures. The evaluation result reveals that our proposed in-air signature authentication method achieves a high-precision of EER value of 0.83% when distinguishing genuine in-air signatures from their skilled forgeries generated by insider adversaries. For in-air signature authentication, to evaluate the contribution of rotation, we use the raw accelerometer and gyroscope measurements without rotation based on the attitude. Figure 7 and Figure 6 compare both the FAR and FRR changes over the threshold and the ROC curves, indicating performance improvement by introducing rotation, while the EER of the system is reduced from 3.03% to 0.83%. It is noticeable that our approach outperforms comparable related works using smartphones [21] and smartwatches [48], while achieving a relatively similar level to studies using depth cameras [24]–[26] and the dedicated device of Leap Motion [47].

B. INPUT ANALYSIS

Then, we are motivated to figure out the extent to which different kinds of input data contribute to the discrimination task between genuine and forged signatures using ablation. Therefore, we compare the performance differences using different sensory readings as inputs. In addition, the influence of the variety of lengths is also assessed by fixing the input



(a) FRR and FAR curve without rotation.

(b) FRR and FAR curve with rotation.

FIGURE 7. Error rate change comparison for rotation.

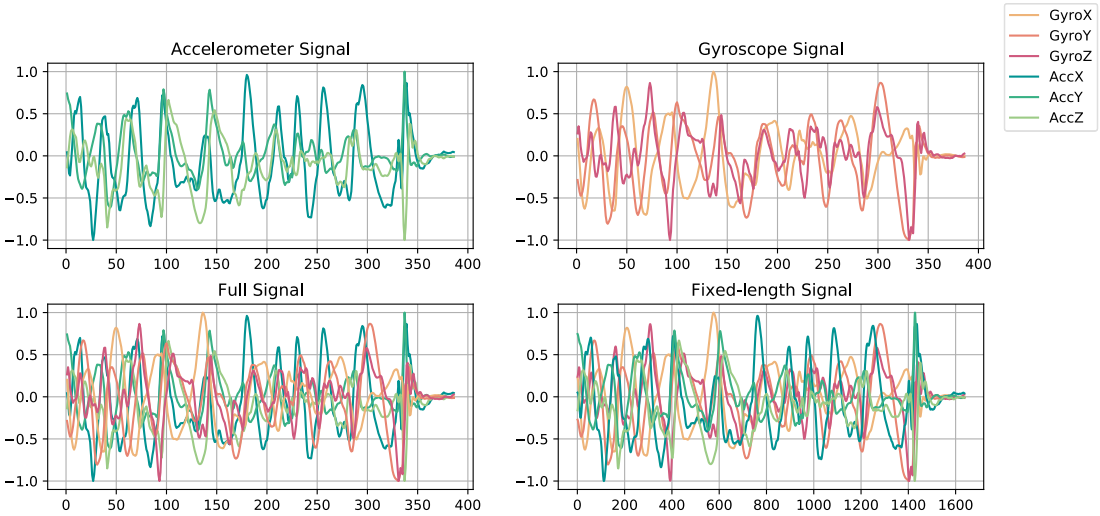


FIGURE 8. An example of four kinds of input signals of a signature.

signals to an identical length using the DCT-based length uniformity method described in Section IV. Specifically, we use 1) only accelerometer signals, 2) only gyroscope signals, 3) full signals, and 4) fixed-length full signals as inputs respectively. Figure 8 shows an example of the corresponding input signals of a signature. We evaluate our proposed method using different types of signals as the input described above. Figure 9 demonstrates the changes in both the FRR and FAR over the threshold. Table 2 numerically depicts the EER differences when different input patterns are used. The system using only gyroscope data achieved a better result (i.e., 2.44%) than the system using only accelerometer data (i.e., 3.05%). The best result of 0.83% EER can be achieved by combining both the sensory readings. However, when we fix the lengths of the signatures, the performance decreased slightly to 1.22% EER.

C. METHOD COMPARISON

In addition, we compare our proposed method with the algorithms used in related work (i.e.,GRU RNN [61], DTW [19], [45], [49], [52]) that can deal with data with variable lengths. Due to the limitations of our laboratory-scale experiment.

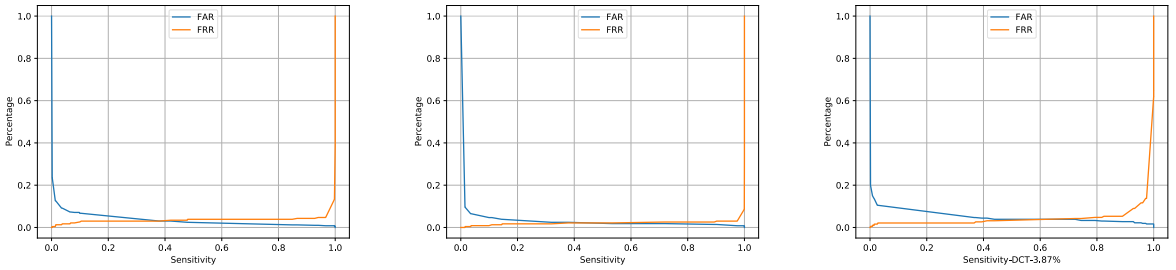
TABLE 2. Performance comparison when different input signals are used.

Input	Accelerometer	Gyroscope	Fixed-length
EER	3.05%	2.44%	1.22%

We implement and apply the algorithms to our acquired in-air signatures under the same conditions to quantify the performance difference.

GRU is another type of RNN unit with fewer gates (an update gate z_t and a reset gate r_t) compared with the LSTM used in our proposed method. The following equations show the calculation of the GRU. We arrange the GRU in a bidirectional structure with the Siamese architecture to evaluate it on the pairwise aligned signatures.

$$z_t = \sigma(W_z[c^{<t-1>}, x^{<t>}] + b_z) \tag{9}$$
$$r_t = \sigma(W_r[c^{<t-1>}, x^{<t>}] + b_r) \tag{10}$$
$$\tilde{c}_t = tanh(r_t \circ W_c[c^{<t-1>}, x^{<t>}] + b_c) \tag{11}$$
$$c^{<t>} = z_t \circ \tilde{c}_t + (1 - z_t) \circ c^{<t-1>} \tag{12}$$
$$a^{<t>} = c^{<t>} \tag{13}$$



(a) FRR and FAR curve using accelerometer signals.

(b) FRR and FAR curve using gyroscope signals.

(c) FRR and FAR curve using fixed-length full signals.

FIGURE 9. Error rate changes comparison between different input signals.

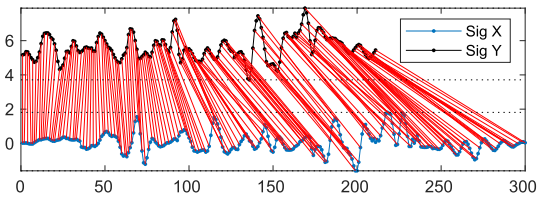


FIGURE 10. The DTW bridge between two signatures in the dimension of gyroscope x axis.

DTW is a widely used algorithm for measuring the distance between two temporal sequences of different lengths. For two signature series $X(x_1, x_2, \ldots, x_n)$ and $Y(y_1, y_2, \ldots, y_m)$ with lengths of n and m, respectively, DTW is to find a time warping path $W =< w_1, w_2, \ldots, w_k >$ reaching a minimum:

$$DTW(X, Y) = \min_{W}\{\sum_{k=1}^{K} d_k, W =< w_1, w_2, \ldots, w_k >\} \tag{14}$$

where d_k indicates the distance between x_i and y_i represented as $w_k = (i, j)$ on the path. Therefore, in the first step of evaluating DTW-based methods, the corresponding time warping distance dataset is generated from pairwise aligned signatures by applying DTW to each pairs. Figure 10 shows the point-to-point alignment and matching relationship between signatures X and Y in the dimensions of the gyroscope x-axis measurement [74]. The distances are represented by 12-dimensional vectors, which are then used to trained an MLP classifier.

Table 3 compares the performance of different algorithm-based systems in terms of EER, and Figure 11 shows their ROC curves. The changes in FRR and FAR over the threshold are depicted in Figure 12. Under the same conditions, the GRU-based method achieved an EER of 0.97%, which is almost equal to that of our approach, whereas the DTW-based method shows a relatively high EER of 8.97% when it is applied to distinguish our acquired in-air signatures.

VII. DISCUSSION

In this section, we present the verification from the aspect of *similarity* and discuss the properties of in-air signing activities and the effectiveness of the pre-preprocessing of rotation.

TABLE 3. Performance comparison for three algorithms.

Algorithm	this paper	GRU RNN	DTW
EER	0.83%	0.97%	8.97%

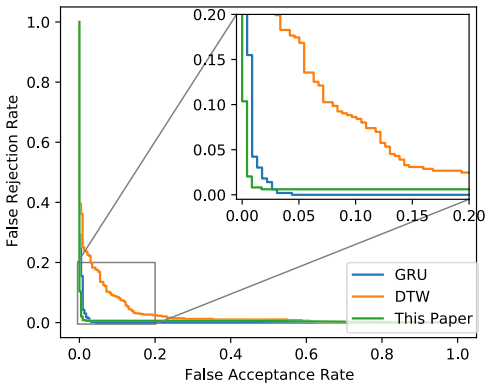


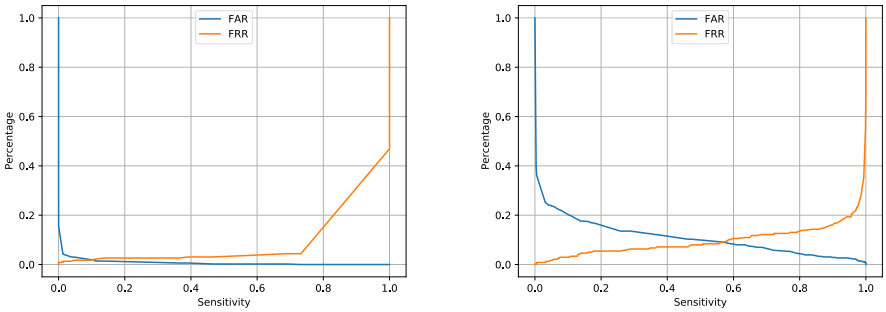
FIGURE 11. Receiver Operating Characteristic (ROC) curve.

A. SIGNATURE SIMILARITY

We utilize DTW as a non-machine-learning algorithm to stably measure the similarities (distances) between signature samples by calculating six-dimensional (i.e., three-axis gyroscope and accelerometer) wrapping. Two kinds of distances are calculated for a given person: 1) the distance between a genuine signature pair ($S_{genuine}|S_{genuine}$) and 2) the distances between a genuine and a forged signature ($S_{genuine}|S_{forgery}$). Fig.13 shows the best (left) and worst (right) cases that we observed from two participants respectively, comparing the distribution of the two kinds of distances in the dimension of g_x. It can be seen that repeating genuine signatures preserve a certain extent of consistency (with inevitable variability) and the forged signatures tend to be more different and consequently show greater distances, whereas the extent of consistency of genuine signatures and the "reality" of forged signatures can change the separability.

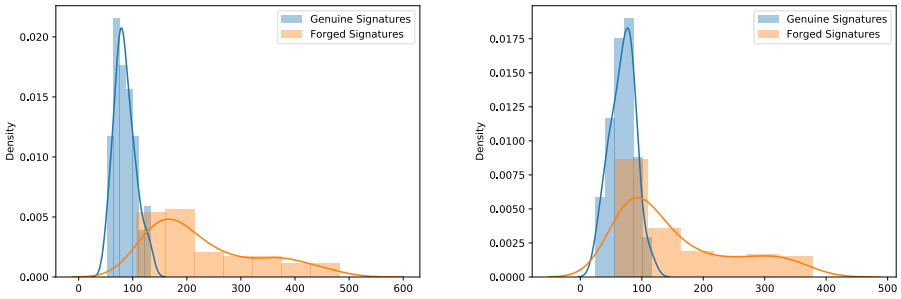
B. COLLECTABILITY, PERFORMANCE, AND CIRCUMVENTION

As for the *performance*, according to the empirical evaluation results in the previous section, the achieved high level of



(a) FRR and FAR curve of GRU-based method. (b) FRR and FAR curve of DTW-based system.

FIGURE 12. Error rate change comparison between different algorithms.



(a) The best case of signature distance distribution.

(b) The worst case of signature distance distribution.

FIGURE 13. Examples of DTW distance distribution.

accuracy (i.e., 0.83%) EER of in-air signature authentication indicates observing in-air signature motions using smartwatches as a high-precision alternative to traditional methods. Regarding the *collectability*, our experiment shows that in-air signature motions can be easily acquired into motion sensory readings, with the users wearing the smartwatch. In contrast to the example of footprints that need to remove shoes and socks in order to enroll [75], in-air signature acquisition requires no more difficulties than enabling sensors and signing.

DTW is also utilized to evaluate the *circumvention* property of in-air signatures by quantifying the advantages that the insider adversaries can have compared to stranger adversaries to determine their resistance against circumvention. Particularly, we compare the similarity between genuine signatures and their active forgery samples, on the one hand, and between genuine signatures and random forgeries, on the other. For random forgeries $S_{randomforgery}$, we randomly choose 10 genuine signature samples from other subjects, instead of carefully forged signatures in the active attack model, to be paired with each targeted signature. Fig. 14 demonstrates the distance distributions of one dimension (g_z) between ($S_{genuine}|S_{genuine}$), ($S_{genuine}|S_{forgery}$) (active) and ($S_{genuine}|S_{randomforgery}$) pairs. Even though by virtue of personal knowledge, active forgery samples can be more closer to genuine targets than random ones, it is still difficult to generate forgeries with genuine level similarity (real fakes), revealing the high circumvention of the in-air signature captured by smartwatch motion sensors. It is reasonable to believe that the high accuracy of in-air authentication is ensured by not only the consistency in repeating genuine signatures but also the difficulty of launching mimicry attacks. Furthermore, we emphasize an important in-air signature property of *"traceless"*. Specifically, traditional table signing usually leaves concrete traces (i.e., signature image) that can be potentially used as knowledge for forgery, whereas signing in the air using fingers is often *"traceless"* leaving little knowledge and hard to be observed. This would also contribute to the property of circumvention.

C. ROTATION VERIFICATION

In addition, we utilized DTW to verify the pre-processing step of *rotation* using device attitude readings, which are introduced to deal with the possible variability between genuine signatures caused by the high variety of signing gestures that we observed in the preliminary experiment. Therefore, to verify the effectiveness of rotation processing to deal with the variability between genuine signatures, we similarly calculate the six-dimensional (i.e., three-axis gyroscope and accelerometer) DTW distances between genuine signature pairs before and after rotation. Figure 15 compares the DTW distance distributions of the one dimension a_z before and

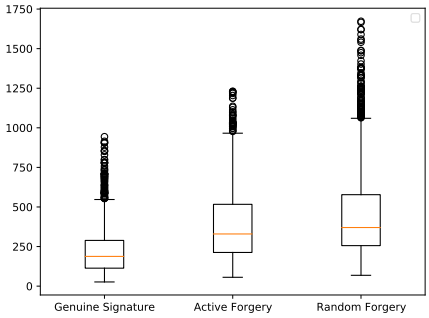


FIGURE 14. Distance comparison of active and random attacks.

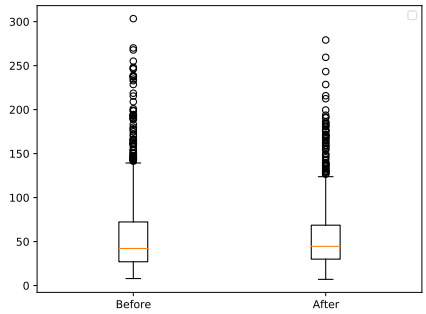


FIGURE 15. Change of distances between genuine samples before and after rotation.

after rotation. It is clear to observe the distance decrease after applying *rotation*, which indicates the effectiveness of introducing this pre-processing step to calibrate unexpected variability.

D. LIMITATION

We acknowledge some limitations of this study. As with many emerging studies [25], [46], [48], [55], our study is based on a laboratory-scale experiment with a relatively small number of participants. The participants are generally students or staff at our institution, most of whom sign their names in Japanese or Chinese characters. They may not be fully representative of the population using other writing systems. Also, the collected signatures show variety not only in length but also in complexity from person to person. Combined with the forgery ability of imposters, the variety may vary the quality of signature forgery, leading to the difference we observed between the best and worst cases discussed in the previous section. Determining the general variety may need statistical analysis. Therefore, the feasibility revealed by this study of sensing in-air signature motions using smartwatches for authentication suggests the future direction of more extensive investigation on an industrial scale to include a larger size of both participants with wide distribution and signature samples from each of them. This would also enable the method performance comparison under different conditions. Furthermore, this study focuses more on the in-air signature gesture. Quantifying the effects of the environment (e.g., indoor and outdoor) and user activities (e.g., sitting, walking, and running) may prove important. As our in-air signature authentication method using smartwatches only records motion sensor readings and lacks recorded images of the signatures, it is valuable in the future work to determine the effect of recording images of the signatures and further explore the potential of combining different observation sources (e.g., camera and smartwatch) of in-air signatures as multimodal signature authentication to improve performance. In addition, the signature sample acquisition is only performed under device-dependent conditions using the Apple Watch Series 6. Considering a real scenario in which a user may enroll her motion sensory traces from one device and try to be authenticated using another device with different manufacturers and operating systems, it is desirable for future work to investigate cross-device authentication using multiple popular smartwatches (e.g., Apple Watch, Honor band, Microsoft band, and Mi band).

VIII. CONCLUSION

In this paper, we have studied an emerging biometrics authentication of signing in the air using smartwatches. Towards this goal, we empirically investigated in-air signing activities acquired using smartwatch motion sensors from 22 participants. We proposed an RNN-based authentication scheme to deal with smartwatch motion sensors readings, which showed advantages over comparable methods by achieving outperformed results of 0.83% EER. Particularly, our method avoided sophisticated feature design and can guarantee that only signature representations instead of original data are stored, which saved space and is more secure. Our property analysis has shown that the in-air signature activities can be effectively acquired for authentication, while the naturally preserved consistency of repeating genuine signatures makes them separable from forgeries. These indicate the high feasibility of sensing in-air signing gestures using smartwatches as an easily collectible, high-precision, and strongly forgery-resistant behavioral biometric traits for authentication.

ACKNOWLEDGMENT

An earlier version of this paper was presented at the 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC) titled "In-Air Signature Authentication Using Smartwatch Motion Sensors," Virtual Event, in July 2021, [DOI: 10.1109/COMPSAC51774.2021.00061].

REFERENCES

[1] G. Li, L. Zhang, and H. Sato, "In-air signature authentication using smartwatch motion sensors," in *Proc. IEEE 45th Annu. Comput., Softw., Appl. Conf. (COMPSAC)*, Jul. 2021, pp. 386–395.

[2] (2020). *Facts + Statistics: Identity Theft and Cybercrime*. [Online]. Available: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

[3] N. Nandini and R. Ajay, "A study on impact of forensic audit towards investigation and prevention of frauds," *Asian J. Manage.*, vol. 12, no. 2, pp. 186–192, May 2021.

[4] E. Cheon, Y. Shin, J. H. Huh, H. Kim, and I. Oakley, "Gesture authentication for smartphones: Evaluation of gesture password selection policies," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2020, pp. 249–267.

[5] K. W. Boyer, V. Govindaraju, and N. K. Ratha, "Introduction to the special issue on recent advances in biometric systems [guest editorial]," *IEEE Trans. Syst., Man, B, Cybern.*, vol. 37, no. 5, pp. 1091–1095, Oct. 2007.
[6] D. Zhang, J. P. Campbell, D. Maltoni, and R. M. Bolle, "Guest editorial special issue on biometric systems," *IEEE Trans. Syst., Man, C, Appl. Rev.*, vol. 35, no. 3, pp. 273–275, Aug. 2005.
[7] S. Liu and M. Silverman, "A practical guide to biometric security technology," *IT Prof.*, vol. 3, no. 1, pp. 27–32, Jan. 2001.
[8] H. Lv, W. Wang, C. Wang, and Q. Zhuo, "Off-line Chinese signature verification based on support vector machines," *Pattern Recognit. Lett.*, vol. 26, no. 15, pp. 2390–2399, Nov. 2005.
[9] I. A. Ismail, M. A. Ramadan, T. El Danf, and A. H. Samak, "Automatic signature recognition and verification using principal components analysis," in *Proc. 5th Int. Conf. Comput. Graph., Imag. Visualisation*, Aug. 2008, pp. 356–361.
[10] D. Impedovo and G. Pirlo, "Automatic signature verification: The state of the art," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 38, no. 5, pp. 609–635, Sep. 2008.
[11] A. Yannopoulos, V. Andronikou, and T. Varvarigou, "Behavioural biometric profiling and ambient intelligence," in *Profiling the European Citizen*. Cham, Switzerland: Springer, 2008, pp. 89–109.
[12] W. Hou, X. Ye, and K. Wang, "A survey of off-line signature verification," in *Proc. Int. Conf. Intell. Mechatronics Autom.*, 2004, pp. 536–541.
[13] J. F. Vargas, M. A. Ferrer, C. M. Travieso, and J. B. Alonso, "Off-line signature verification based on grey level information using texture features," *Pattern Recognit.*, vol. 44, no. 2, pp. 375–385, 2011.
[14] K. Franke, J. Ruiz del Solar, and M. Köppen, "Soft-biometrics: Soft-computing for biometric-applications," *Int. J. Fuzzy Syst.*, vol. 4, no. 2, pp. 665–672, 2012.
[15] J. F. Vargas, M. A. Ferrer, C. M. Travieso, and J. B. Alonso, "Offline signature verification based on pseudo-cepstral coefficients," in *Proc. 10th Int. Conf. Document Anal. Recognit.*, Jul. 2009, pp. 126–130.
[16] M. Stauffer, P. Maergner, A. Fischer, and K. Riesen, "A survey of state of the art methods employed in the offline signature verification process," in *New Trends in Business Information Systems and Technology*. Cham, Switzerland: Springer, 2021, pp. 17–30.
[17] J. Fierrez and J. Ortega-Garcia, "On-line signature verification," in *Handbook of Biometrics*. Cham, Switzerland: Springer, 2008, pp. 189–209.
[18] A. Jain, S. K. Singh, and K. P. Singh, "Handwritten signature verification using shallow convolutional neural network," *Multimedia Tools Appl.*, vol. 79, pp. 19993–20018, Jul. 2020.
[19] A. Kholmatov and B. Yanikoglu, "Identity authentication using improved online signature verification method," *Pattern Recognit. Lett.*, vol. 26, no. 15, pp. 2400–2408, 2005.
[20] A. Fallah, M. Jamaati, and A. Soleamani, "A new online signature verification system based on combining Mellin transform, MFCC and neural network," *Digit. Signal Process.*, vol. 21, no. 2, pp. 404–416, Mar. 2011.
[21] G. Bailador, C. Sanchez-Avila, J. Guerra-Casanova, and A. de Santos Sierra, "Analysis of pattern recognition techniques for in-air signature biometrics," *Pattern Recognit.*, vol. 44, nos. 10–11, pp. 2468–2478, Oct. 2011.
[22] S. Jabin, S. Ahmad, S. Mishra, and F. J. Zareen, "ISignDB: A database for smartphone signature biometrics," *Data Brief*, vol. 33, Dec. 2020, Art. no. 106597.
[23] C.-C. Cheng, Y.-C. Chen, and Y.-T. Ching, "Handwritten signature verification by using a six-axis motion sensor and SVM," in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput., ACM Int. Symp. Wearable Comput.*, Sep. 2019, pp. 25–28.
[24] Y. Fang, W. Kang, Q. Wu, and L. Tang, "A novel video-based system for in-air signature verification," *Comput. Electr. Eng.*, vol. 57, pp. 1–14, Jan. 2017.
[25] J. Malik, A. Elhayek, S. Ahmed, F. Shafait, M. Malik, and D. Stricker, "3DAirSig: A framework for enabling in-air signatures using a multi-modal depth sensor," *Sensors*, vol. 18, no. 11, p. 3872, Nov. 2018.
[26] J. Malik, A. Elhayek, S. Guha, S. Ahmed, A. Gillani, and D. Stricker, "DeepAirSig: End-to-end deep learning based in-air signature verification," *IEEE Access*, vol. 8, pp. 195832–195843, 2020.
[27] (2020). *Forecast Unit Shipments of Wrist-Worn Wearables Worldwide From 2019 to 2024*. [Online]. Available: https://www.statista.com/statistics/296565/wearables-worldwide-shipments/
[28] M. M. Luna, T. P. Carvalho, F. A. A. M. N. Soares, H. A. D. Nascimento, and R. M. Costa, "Wrist player: A smartwatch gesture controller for smart TVs," in *Proc. IEEE 41st Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jul. 2017, pp. 336–341.
[29] Y. Li, K. Zhao, M. Duan, W. Shi, L. Lin, X. Cao, Y. Liu, and J. Zhao, "Control your home with a smartwatch," *IEEE Access*, vol. 8, pp. 131601–131613, 2020.
[30] F. Nurwanto, I. Ardiyanto, and S. Wibirama, "Light sport exercise detection based on smartwatch and smartphone using k-nearest neighbor and dynamic time warping algorithm," in *Proc. 8th Int. Conf. Inf. Technol. Electr. Eng. (ICITEE)*, Oct. 2016, pp. 1–5.
[31] H. Jeong, H. Kim, R. Kim, U. Lee, and Y. Jeong, "Smartwatch wearing behavior analysis: A longitudinal study," *ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 1, no. 3, pp. 1–31, Sep. 2017.
[32] J. Blasco, T. M. Chen, J. Tapiador, and P. Peris-Lopez, "A survey of wearable biometric recognition systems," *ACM Comput. Surveys*, vol. 49, no. 3, pp. 1–35, Dec. 2016.
[33] J. Yang, Y. Li, and M. Xie, "MotionAuth: Motion-based authentication for wrist Worn smart devices," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2015, pp. 550–555.
[34] T. Ohtsuki and H. Kamoi, "Biometrie authentication using hand movement information from wrist-worn PPG sensors," in *Proc. IEEE 27th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Sep. 2016, pp. 1–5.
[35] Z. Sitová, J. Sedenka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. S. Balagani, "HMOG: New behavioral biometric features for continuous authentication of smartphone users," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 877–892, May 2016.
[36] Z. Wang, C. Shen, and Y. Chen, "Handwaving authentication: Unlocking your smartwatch through handwaving biometrics," in *Proc. Chin. Conf. Biometric Recognit.* Cham, Switzerland: Springer, 2017, pp. 545–553.
[37] I. Griswold-Steiner, R. Matovu, and A. Serwadda, "Handwriting watcher: A mechanism for smartwatch-driven handwriting authentication," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Oct. 2017, pp. 216–224.
[38] A. Buriro, B. Crispo, M. Eskandri, S. Gupta, A. Mahboob, and R. Van Acker, "SnapAuth: A gesture-based unobtrusive smartwatch user authentication scheme," in *Proc. Int. Workshop Emerg. Technol. Authorization Authentication*. Cham, Switzerland: Springer, 2018, pp. 30–37.
[39] Y. Zhao, R. Gao, and H. Tu, "Smartwatch user authentication based on the arm-raising gesture," *Interacting Comput.*, vol. 32, nos. 5–6, pp. 569–580, Sep. 2020.
[40] X. Yu, Z. Zhou, M. Xu, X. You, and X.-Y. Li, "ThumbUp: Identification and authentication by smartwatch using simple hand gestures," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, Mar. 2020, pp. 1–10.
[41] G. Cola, M. Avvenuti, F. Musso, and A. Vecchio, "Gait-based authentication using a wrist-worn device," in *Proc. 13th Int. Conf. Mobile Ubiquitous Systems: Comput., Netw. Services*, Nov. 2016, pp. 208–217.
[42] A. H. Johnston and G. M. Weiss, "Smartwatch-based biometric gait recognition," in *Proc. IEEE 7th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, Sep. 2015, pp. 1–6.
[43] R. Kumar, V. V. Phoha, and R. Raina, "Authenticating users through their arm movement patterns," 2016, *arXiv:1603.02211*.
[44] W.-H. Lee and R. Lee, "Implicit sensor-based authentication of smartphone users with smartwatch," in *Proc. Hardw. Architectural Support Secur. Privacy (HASP)*, 2016, p. 9.
[45] B. Nassi, A. Levy, Y. Elovici, and E. Shmueli, "Handwritten signature verification using hand-worn devices," 2016, *arXiv:1612.06305*.
[46] M. Taimoor, H. Butt, T. Khadim, M. Ehatisham-Ul-Haq, A. Raheel, and A. Arsalan, "REALME: An approach for handwritten signature verification based on smart wrist sensor," in *Proc. IEEE 23rd Int. Multitopic Conf. (INMIC)*, Nov. 2020, pp. 1–6.
[47] E. Guerra-Segura, A. Ortega-Pérez, and C. M. Travieso, "In-air signature verification system using leap motion," *Expert Syst. Appl.*, vol. 165, Mar. 2021, Art. no. 113797.
[48] A. Buriro, R. Van Acker, B. Crispo, and A. Mahboob, "AirSign: A gesture-based smartwatch user authentication," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2018, pp. 1–5.
[49] M. Okawa, "Online signature verification using single-template matching with time-series averaging and gradient boosting," *Pattern Recognit.*, vol. 102, Jun. 2020, Art. no. 107227.
[50] O. S. Adeoye, "A survey of emerging biometric technologies," *Int. J. Comput. Appl.*, vol. 9, no. 10, pp. 1–5, Sep. 2010.
[51] A. Mahfouz, T. M. Mahmoud, and A. S. Eldin, "A survey on behavioral biometric authentication on smartphones," *J. Inf. Secur. Appl.*, vol. 37, pp. 28–37, Dec. 2017.
[52] A. K. Jain, F. D. Griess, and S. D. Connell, "On-line signature verification," *Pattern Recognit.*, vol. 35, no. 12, pp. 2963–2972, 2002.

[53] H.-H. Kao and C.-Y. Wen, "An offline signature verification and forgery detection method based on a single known sample and an explainable deep learning approach," *Appl. Sci.*, vol. 10, no. 11, p. 3716, May 2020. [Online]. Available: https://www.mdpi.com/2076-3417/10/11/3716
[54] J. F. Vargas, M. A. Ferrer, C. M. Travieso, and J. B. Alonso, "Offline signature verification based on pseudo-cepstral coefficients," in *Proc. 10th Int. Conf. Document Anal. Recognit.*, Jul. 2009, pp. 126–130.
[55] B. H. Shekar and R. K. Bharathi, "Eigen-signature: A robust and an efficient offline signature verification algorithm," in *Proc. Int. Conf. Recent Trends Inf. Technol. (ICRTIT)*, Jun. 2011, pp. 134–138.
[56] A. C. Ramachandra, J. S. Rao, K. B. Raja, K. R. Venugopla, and L. M. Patnaik, "Robust offline signature verification based on global features," in *Proc. IEEE Int. Advance Comput. Conf.*, Mar. 2009, pp. 1173–1178.
[57] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, "Learning features for offline handwritten signature verification using deep convolutional neural networks," *Pattern Recognit.*, vol. 70, pp. 163–176, Oct. 2017.
[58] A. Karouni, B. Daya, and S. Bahlak, "Offline signature recognition using neural networks approach," *Proc. Comput. Sci.*, vol. 3, pp. 155–161, 2011. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050910004023
[59] D. S. Guru and H. N. Prakash, "Online signature verification and recognition: An approach based on symbolic representation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 31, no. 6, pp. 1059–1073, Jun. 2008.
[60] J. Bromley, I. Guyon, Y. LeCun, E. Säckinger, and R. Shah, "Signature verification using a 'Siamese' time delay neural network," in *Proc. Adv. Neural Inf. Process. Syst.*, 1994, pp. 737–744.
[61] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "Exploring recurrent neural networks for on-line handwritten signature biometrics," *IEEE Access*, vol. 6, pp. 5128–5138, 2018.
[62] N. Sae-Bae and N. Memon, "Online signature verification on mobile devices," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 6, pp. 933–947, Jun. 2014.
[63] *Apple Developer Documentation*. Accessed: Apr. 9, 2022. [Online]. Available: https://developer.apple.com/documentation/coremotion/cmdevicemotion/1616050-attitude
[64] J. Mueller and A. Thyagarajan, "Siamese recurrent architectures for learning sentence similarity," in *Proc. AAAI Conf. Artif. Intell.*, 2016, vol. 30, no. 1, pp. 1–7.
[65] L. Hu and Y.-H. Wang, "On-line signature verification based on fusion of global and local information," in *Proc. Int. Conf. Wavelet Anal. Pattern Recognit.* Cham, Switzerland: Springer, Nov. 2005, pp. 523–532.
[66] A. Kholmatov and B. Yanikoglu, "SUSIG: An on-line signature database, associated protocols and benchmark results," *Pattern Anal. Appl.*, vol. 12, no. 3, pp. 227–236, 2009.
[67] B. Yanikoglu and A. Kholmatov, "Online signature verification using Fourier descriptors," *EURASIP J. Adv. Signal Process.*, vol. 2009, no. 1, pp. 1–13, Dec. 2009.
[68] N. Ahmed, T. Natarajan, and K. R. Rao, "Discrete cosine transform," *IEEE Trans. Comput.*, vol. COM-23, no. 1, pp. 90–93, Jan. 1974.
[69] Y. Liu, Z. Yang, and L. Yang, "Online signature verification based on DCT and sparse representation," *IEEE Trans. Cybern.*, vol. 45, no. 11, pp. 2498–2511, Dec. 2015.
[70] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov, "Understanding users' requirements for data protection in smartphones," in *Proc. IEEE 28th Int. Conf. Data Eng. Workshops*, Apr. 2012, pp. 228–235.
[71] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov, "Know your enemy: The risk of unauthorized access in smartphones by insiders," in *Proc. 15th Int. Conf. Hum.-Comput. Interact. Mobile Devices Services (MobileHCI)*, 2013, pp. 271–280.
[72] R. Darbar, P. K. Sen, and D. Samanta, "PressTact: Side pressure-based input for smartwatch interaction," in *Proc. Conf. Extended Abstr. Hum. Factors Comput. Syst.*, May 2016, pp. 2431–2438.
[73] S. Marcel, "BEAT–biometrics evaluation and testing," *Biometric Technol. Today*, vol. 2013, no. 1, pp. 5–7, Jan. 2013.
[74] J.-S. R. Jang. *Machine Learning Toolbox*. Accessed: Nov. 18, 2020. [Online]. Available: http://mirlab.org/jang/MATLAB/toolbox/machineLearning
[75] J. Andress, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Waltham, MA, USA: Syngress, 2014.

GEN LI received the B.E. degree in computer science and technology from the Beijing Institute of Technology, China, in 2015, and the M.Sc. degree in computer science from The University of Manchester, U.K., in 2017. He is currently pursuing the Ph.D. degree with the Department of Electrical Engineering and Information Systems, School of Engineering, The University of Tokyo. His research interests include the field of signal processing, biometrics, and access control.

HIROYUKI SATO (Member, IEEE) received the B.Sc., M.Sc., and D.Sc. degrees from the Department of Information Science, The University of Tokyo, in 1985, 1987, and 1990, respectively. In 1990, he was an Assistant Professor with Kyushu University. He is currently an Associate Professor with the Information Technology Center, The University of Tokyo. His specialties are security and internet trust. He is also an Accredited Assessor of LoA 1 for Kantara Initiative.