Multi-Day Analysis of Wrist Electromyogram-Based Biometrics for Authentication and Personal Identification

Ashirbad Pradhan, Jiayuan He, *Member, IEEE*, Hyowon Lee, and Ning Jiang, *Senior Member, IEEE*

***Abstract*—Recently, electromyogram (EMG) has been proposed for addressing some key limitations of current biometrics. Wrist-worn wearable sensors can provide a non-invasive method for acquiring EMG signals for gesture recognition or biometric applications. EMG signals contain individuals' information and can facilitate multi-length codes or passwords (for example, by performing a combination of hand gestures). However, current EMG-based biometric research has two critical limitations: small subject-pool for analysis and limited to single-session datasets. In this study, wrist EMG data were collected from 43 participants over three different days (Days 1, 8, and 29) while performing static hand/wrist gestures. Multi-day analysis involving training data and testing data from different days was employed to test the robustness of the EMG-based biometrics. The multi-day authentication resulted in a median equal error rate (EER) of 0.039 when the code is unknown, and an EER of 0.068 when the code is known to intruders. The multi-day identification achieved a median rank-5 accuracy of 93.0%. With intruders, a threshold-based identification resulted in a median rank-5 accuracy of 91.7% while intruders were denied access at a median rejection rate of 71.7%. These results demonstrated the potential of EMG-based biometrics in practical applications and bolster further research on EMG-based biometrics.**

***Index Terms*—Biometrics, electromyogram (EMG), biometric authentication, personal identification, multi-day dataset, intruder rejection.**

I. Introduction

BIOMETRICS has become an integral part of current authentication systems and has found application in consumer electronics, public security, and private security. These biological and behavioral traits have been utilized to identify an individual or verify an individual's identity. Conventional biometrics such as fingerprints and facial scans have been widely used in smartphones and laptops in our daily lives. However, with technological advancements, there are increasing risks of leakage of biometric data as well as artificial regeneration (also termed spoof), which can lead to identity theft. Recently, novel biometric traits based on bio-signals, such as the electrocardiogram (ECG), electroencephalogram (EEG), and electromyogram (EMG) have been shown to be more resilient to spoofing than the conventional biometric traits [1]. For example, it could be relatively easy to take pictures and record videos discreetly and use printed photos to deceive a facial recognition system. On the contrary, obtaining biosignals would require more coordination and attaching specialized sensors to unwilling subjects, which can be used as a liveness detection ability [1]. Among the bisoignals, surface EMG has been traditionally used in gesture recognition-based research, specifically for prosthetic control, where extensive investigation demonstrated EMG-based gesture control has poor cross-user transference performance [2]. In fact, a calibration-free EMG-based gesture recognition system that does not need new user training has been an elusive goal in myoelectric control literature. Such difficulty suggests that there exist inherent individual differences in surface EMG signals. And this is precisely a biometrics trait. Indeed, multiple recent studies have substantiated EMG as an accurate biometric trait [3], [4]. In this context, EMG has an inherent dual-property: gesture recognition and biometrics, providing it with a distinct and important advantage over other biometric traits. On the one hand, it is more covert than the traditional traits, such as fingerprint, and less likely to be compromised and spoofed. On the other hand, it enables the user to set customized gestures as passcodes for enhanced security, just like a user-defined password, not possible with EEG and ECG. Our recent study on multi-code EMG biometrics has provided a framework for the fusion/combination of these codes and to facilitate such a dual-mode (password and biometrics) authentication system [5]. Another recent study used a multi-code framework to incorporate password-based security and achieved similar results for biometric authentication [6].

A. State-of-the-Art in EMG-Based Biometrics

There are generally two common biometric modes: authentication and identification [7]. In the authentication mode,

Manuscript received 3 February 2023; revised 19 June 2023; accepted 22 July 2023. Date of publication 14 August 2023; date of current version 6 October 2023. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada under Grant 072169; in part by the National Clinical Research Center for Geriatrics, West China Hospital, Sichuan University under Grant Z2023YY001; and in part by the Med-X Center for Manufacturing, Sichuan University under Grant 0040206107007. This article was recommended for publication by Associate Editor Z. Lei upon evaluation of the reviewers' comments. *(Corresponding author: Ning Jiang.)*

This work involved human subjects or animals in its research. Approval of all ethical and experimental procedures and protocols was granted by the Office of Research Ethics of the University of Waterloo under Application No. ORE# 31346.

Ashirbad Pradhan and Hyowon Lee are with the Engineering Bionics Lab, Department of Systems Design Engineering, Faculty of Engineering, University of Waterloo, Waterloo, ON N2V 2T9, Canada.

Jiayuan He and Ning Jiang are with the National Clinical Research Center for Geriatrics, West China Hospital, and the Med-X Center for Manufacturing, Sichuan University, Chengdu 610017, Sichuan, China (e-mail: jiangning21@wchscu.cn).

Digital Object Identifier 10.1109/TBIOM.2023.3299948

the biometric system grants or rejects an access request of the presenting user (claimant) by comparing the presented biometric data to the template stored in the database. In this case, the presumed identity of the claimant is *a priori*. In the identification mode, however, the presumed identity of the claimant is unknown, and the biometric system has to identify the most likely identity from the database based on the presented biometric information. Some of the studies have reported a high biometric authentication [3], [6], [8], [9], [10], [11], [12] and identification performance [4], [13], [14], [15], [16], [17], [18], [19]. The number of hand gestures in these studies ranged from 1 to 34. The number of EMG channels varied from as low as one channel to as high as 256 channels. While most of the studies had fewer than 25 subjects, only three studies included larger numbers (>40) of subjects [3], [20], [21], more appropriate in the biometric context. In addition, one of the most important features of a viable biometric trait is its longitudinal robustness across multi-session and multi-day. However, most studies in the literature were limited to data acquired within only one session or one day. A few studies with a small subject pool (<22), with data from a two-day protocol [4], [9]. Only one study had five subjects with a four-day data collection protocol [22]. It has been established in the EMG processing literature, that in a multi-session protocol spreading across days, non-stationary factors including electrode shifts, sweat, dry skin, and physical conditions will affect the accuracy and consistency of the EMG processing system [23]. Therefore, the multi-day performance with a sufficiently large subject pool is a crucial step for validating the effectiveness of EMG as a biometric trait. Furthermore, in a more practical identification mode scenario, intruders (unregistered users) might claim access to a biometric system [13]. An intruder analysis should be further performed, where an initial threshold-based grant/reject is employed to check for the authenticity of a claiming user and then followed by individual recognition.

Most studies in the literature used EMG data acquired from the forearm, which is not convenient for consumer-based applications, such as biometrics. There has a been recent change in focus from the forearm to the wrist, specifically for gesture recognition applications for more general-consumer use [24]. The wrist presents a more feasible and attractive position for biometrics applications because wrist-worn devices are well-established and ubiquitous. For this purpose, the current study utilizes EMG signals collected from the wrist while performing hand gestures. A wrist electrode setup will facilitate the research and development of industry-grade wearable wrist- bands, which have previously been explored for gesture recognition [25] and biometric authentication applications [21], [26]. For the scope of this paper, the multi-day biometric analysis was performed on the wrist-worn EMG over three sessions over the span of 30 days. The biometric benchmarks of both authentication and identification were presented. Additionally, the intruder analysis for the identification mode was investigated.

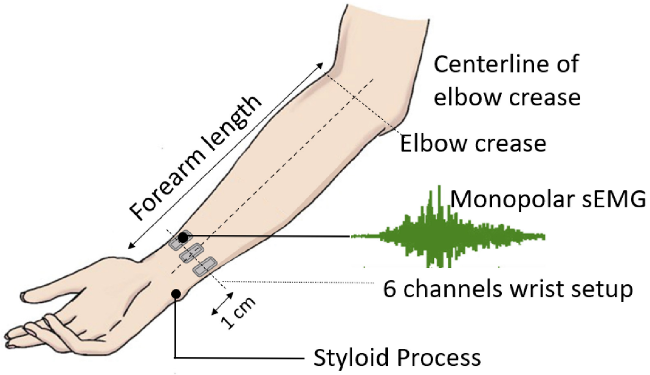

Fig. 1. Positions of the six electrodes on the wrist (dorsal view, three electrodes are on the posterior wrist surface). The electrodes were equally spaced around the wrist at a distance of one cm from the styloid process. The monopolar EMG of each ring was acquired for subsequent processing and analysis.

II. Methods

A. Participants

We recruited 43 healthy participants (23 M, 20 F) for the study. The average age was 26.4±2.89, and the average forearm length (measured from the styloid process on the wrist to the olecranon on the elbow) was 25.2±1.74 cm. The average wrist circumference (measured at a distance of one cm away from the ulnar styloid process) was 16.2±1.21cm. Before the experiment, the participants were informed of the procedures and signed an informed consent form. The experiments were conducted following the Declaration of Helsinki and the research protocol was approved by the Office of Research Ethics of the University of Waterloo (ORE# 31346).

B. Acquisition Setup

The experimental setup consisted of a PC and a monitor mounted on a desk, 0.75 m in front of a height-adjustable chair. The EMGUSB2+ (OT Bioelettronica, Italy), a biosignal commercial amplifier, was used for acquiring the EMG signals. The signals were bandpass filtered between 10 Hz and 500 Hz, with a gain of 500, and then sampled at 2048 Hz.

Before the experiment, the participant's forearm length is measured as the distance between the olecranon process and the ulnar styloid process. The wrist circumference is measured at one cm away from the ulnar styloid process in the proximal direction. After taking these measurements, the electrodes are placed on the wrist. Prior to electrode placement, the skin surface was shaved to remove hairs, cleaned with an alcohol swab, and abraded with a paper towel. Six monopolar EMG electrodes (AM-N00S/E, Ambu, Denmark) were placed in the form of a ring, equally spaced around the wrist. A detailed pictorial representation is provided in Fig. 1. To maintain consistency of the positions of the electrodes across all participants, the first electrode in the ring was anatomically positioned on the centerline of the elbow crease and the rest of the electrodes were numbered in clockwise order from one to six as shown in Fig. 1 [4], [10]. The electrodes were part of a multi-ring forearm and wrist setup as described in the data descriptor which also provides additional details on the acquisition setup [27], [28].

C. Experimental Protocol

After the completion of the experimental setup, the participant is seated comfortably on the chair with both their upper limbs in a resting position. Visual instructions for performing the gestures were provided on the computer screen placed in front of the participants. The following 16 hand and wrist gestures were included in the current study: Lateral prehension (LP), thumb adduction (TA), thumb and little finger opposition (TLFO), thumb and index finger opposition (TIFO), thumb and little finger extension (TLFE), thumb and index finger extension (TIFE), index and middle finger extension (IMFE), little finger extension (LFE), index finger extension (IFE), thumb extension (TE), wrist flexion (WF), wrist extension (WE), forearm supination (FS), forearm pronation (FP), hand open (HO), and hand close (HC). A pictorial representation of the gestures is provided in the Appendix. The order of the 16 gestures was randomized and a resting (REST) trial was collected after all 16 gestures were performed once. A ten-second relaxing period was provided between each trial. One continuous data acquisition of 17 gestures, including the REST, is called one run. Each subject performed seven runs, resulting in 119 trials or contractions (17 x 7). The subject could also request additional rest when he/she felt necessary.

D. EMG Signal Processing

The monopolar EMG signals from the six channels were first re-referenced by a common average procedure where for every sample, the mean of the six channels was subtracted from each channel. The processed signals were then segmented into 200 ms width windows, with a 150 ms overlap. Each window was then processed using the frequency division technique (FDT) feature extraction [29]. This method calculates the magnitude of L frequency bands. For the i^{th} band, let $f_{i,1,}$ and $f_{i,E}$ denote the frequency values of the two endpoints. As such, for each window, the i^{th} feature is calculated as:

$$FDT_i = F\left[\sum_{j=1}^{n_i} |X(f_{i,j})|\right], i \ = \ 1, 2, \ldots L, \qquad (1)$$

where $X(\cdot)$ denotes the magnitude of the FFT spectrum, and $F[\cdot]$ denotes a logarithm operator to obtain a smooth value for better classification results. In the current study, the whole EMG frequency band (20–450 Hz) is subdivided into six equal-width frequency bands: 20–92, 92–163, 163–235, 235–307, 307–378, and 378–450 Hz, consistent with prior studies [30]. Therefore, for a single sample recorded from the six channels, the feature vector extracted from each window comprises 36 FDT features. For each trial recording of five seconds long, the extracted features result in $P \times D$ matrix where P equals 33 and D equals 36. Multiple trials from different days were used for training (termed as enrollment) of biometric models as discussed in a later section (Section II-H). The testing data involved biometric matching as described below.

The Mahalanobis distance, which takes into consideration the correlation between features, was considered for biometric comparisons [4], [5], [10]. In these studies, the Mahalanobis distance was robust to the high similarities between the EMG signals from neighboring channels. For a given feature vector sample p, which is the input from a specific user (the claimant) while performing a specific gesture, its matching score, $S_{i,j}$, with the i^{th} gesture and the j^{th} user, was defined as the Mahalanobis distance between the sample and the class centroid:

$$S_{i,j}(p) = \sqrt{\left(p - \mu_{i,j}\right)^{\top} \Sigma_{i,j}^{-1} \left(p - \mu_{i,j}\right)}, \qquad (2)$$

where $\mu_{i,j}$ is the centroid of the gesture of the class and the user, and $\Sigma_{i,j}$ is the covariance matrix for the specific gesture and user class. Both the centroid and covariance were estimated from the enrollment data based on the within-day and cross-day analysis (details in Section II-H).

E. Multi-Code Biometric Framework

A standard biometric system consists of five modules: 1) sensor module which collects the biometric data, 2) feature extractor for generating feature vectors utilized as biometric entries, 3) matcher module that compares with the genuine user's template to generate a score, 4) ranking module that produces a rank after sorting the scores for all the users and 5) decision module to grant access or rejection based on a pre-set threshold [31]. In the authentication mode, the ranking module is absent and hence the decision is made on the scores (access granted or rejected). In the identification mode, the usual practice is that the K identities with the top K highest scores are stored, and if the claimed identity is one of these K identities, authorization of the claim is rendered. Fusion strategies at different modules for EMG-based biometric authentication have been investigated, and the decision-level fusion approach was found to produce the best overall performance [5]. The performed hand/wrist gestures are treated as codes in the context of EMG biometrics. An example of a user's authentication code sequence of code-length M can be denoted as $[C_1, C_2 \ldots C_m, \ldots, C_M]$, where C_m is the m^{th} code (gesture). For the analysis presented below, 50 random sequences were generated by combining randomly selected four gestures out of the 16 gestures performed by each participant. A decision-level fusion of each code sequence was employed as described below, and the evaluation metrics were compared for a single-code (M = 1) and a multi-code configuration (M = 4) based on previous findings [5]. For the identification mode, an additional parameter *rank-K* was analyzed by varying the value of K (K = 1–15) for the single-code and multi-code configurations for each code sequence.

A weighted majority scheme was used for the M codes of the multi-code framework. In the authentication mode, the extracted feature from claimant data is compared to the corresponding template in the database. Hence, the authentication result is binary: 1 (for genuine user) and 0 (for impostor).

The identification mode is a multi-class problem with J comparisons between the claimant and all the templates in the database (total users = J). However, only when the claimant is within the top K users, a positive identification will be rendered. For M codes, let $d_{m,j}$ be the degree of certainty or the

m^{th} code (C_m) and j^{th} user defined as

$$d_{m,j} = \begin{cases} 1, & C_m \text{ is correct for } j \\ 0, & \textit{otherwise} \end{cases}. \tag{3}$$

The discriminant function for each user 'j' obtained through the weighted voting is

$$g_j = \sum_{m=1}^{M} w_m d_{m,j}, \tag{4}$$

where w_m is the weight attached to the m^{th} code. Here w_m is the single-code recognition accuracy of each gesture, averaged over the three days. Based on the value of M, w_m is then normalized to 1.

$$\sum_{m=1}^{M} w_m = 1. \tag{5}$$

In the case of an authentication system, the claimant matches with the template if the discriminant g has a majority ($> 50\%$). For the identification system, the claimant is assigned with the template with the highest value of g. The weight w_m was previously determined by the recognition accuracy of individual gestures which are listed in the Appendix.

F. Authentication and Identification Evaluation

The false acceptance rate (*FAR*) and the false rejection rate (*FRR*) were calculated to evaluate biometric authentication. *FAR* is the rate of accepting an impostor, and *FRR* is the rate of rejecting a genuine user. In principle, the *FAR* and *FRR* should be as small as possible for biometric applications. The detection error tradeoff (DET) curve is the relationship between the *FAR* and *FRR*. The equal error rate (*EER*) is the point on the DET curve where the *FAR* is equal to the *FRR*. The *EER* is a commonly used authentication metric that can be used to compare the performance of different biometric traits: The lower the *EER* value, the better the performance. Additionally, the area under the DET curve (*AUC*) value was also evaluated. For an accurate assessment of the biometric authentication capacity of the EMG biometrics, two common authentication scenarios were investigated: 1) Normal Test: where the correct code sequence was only known to the genuine user, while the impostor had no knowledge of the code sequence and presented a random sequence different from the one used by the genuine user; 2) Leaked Test: where the correct code sequence for the genuine user was compromised, and the impostor presented the correct code sequence by performing the corresponding gestures. This is the scenario where the knowledge-based security is completely compromised, and the system is solely dependent on the biometric security.

In both cases, for the m^{th} code in a single-code ($M = 1$) or multi-code ($M = 4$) configuration, the genuine score, G_m, was obtained from the authentication gesture C_m of the genuine user. In the normal test, the impostor score I_m was obtained from the other gestures performed by other users. For the leaked-test scenario, I_m was obtained from C_m for all the other users. The weighted majority decision fusion scheme was implemented using G_m and I_m to obtain the final FAR_M, FRR_M, and EER_M.

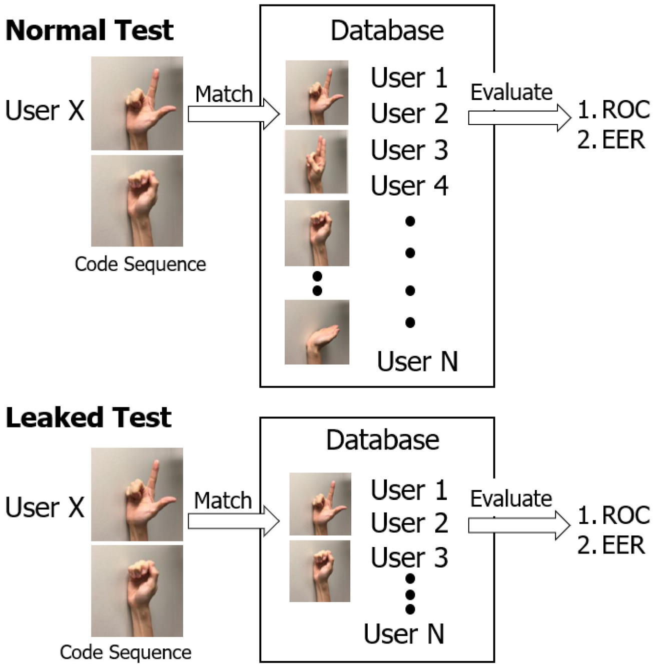

Fig. 2. The normal test and the leaked test scenarios for biometric authentication. In both the scenarios the target user's identity is known to the claimant. The access code is unknown to the claimant in the normal test scenario, while it is known to the claimant in a leaked test scenario.

For the identification mode, the *rank-K* accuracy is defined as the probability of correctly predicting the genuine user within the top K likely users returned by the system for a code sequence of codelength M. As the identification is a 1:J comparison (J = total users), the unknown presenting user is compared to J templates in the database, and J scores are generated. The returned identities are sorted according to the scores and the top-K users are selected. The value of *rank-K accuracy* is proportional with respect to the value of K, *i.e.,* the higher the K, the more likely it is for the genuine user to be returned. Their relation was summarized by the cumulative match characteristic (CMC) curve, which plotted rank-K against K, where K varied from 1–15. This analysis was repeated 50 times for randomly generated code sequences for the single-code and multi-code configurations as described previously in Section II-E. For both the authentication and identification mode, a cross-validation scheme corresponding to the multiple days and trials was incorporated as described in Section II-H. As the commonly used metrics, the values of *rank-1, rank-3* and *rank-5 accuracy* were reported in this study.

G. Intruder Analysis for Identification mode

The standard identification analysis does not include the scenario in which an intruder is an unregistered user. For such a scenario, an "authentication + identification" approach is taken, where the intruder can be rejected by a threshold-based authentication stage before the identification stage [13]. This threshold-based authentication stage introduces the threshold value ($Th_{i,j}$) for the i^{th} gesture and the j^{th} along with template parameters $\mu_{i,j,}$ and $\sum_{i,j}$. From N training samples, the

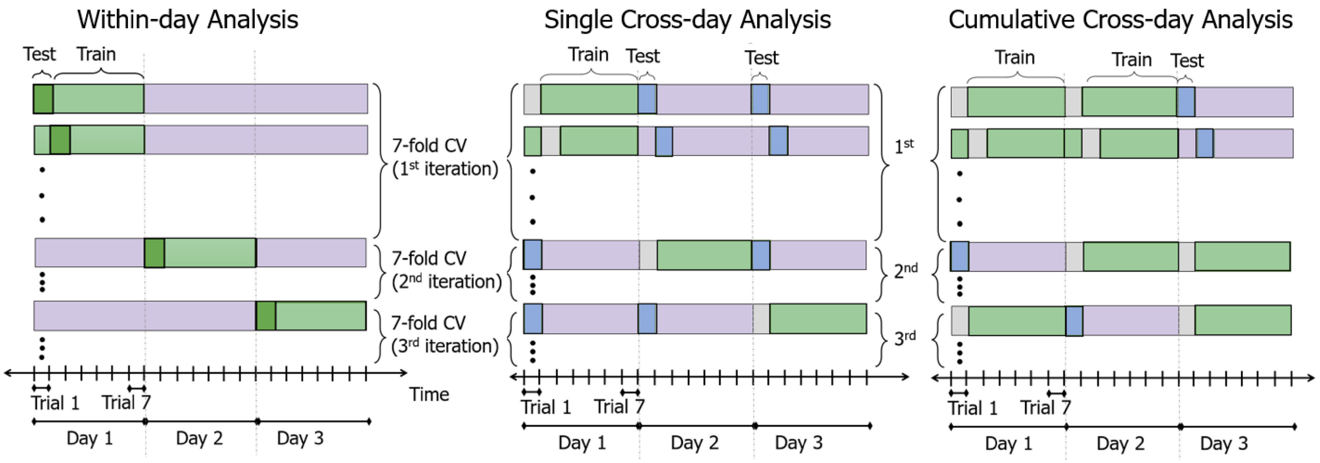

Fig. 3. (From left to right) Within-day, Single cross-day and Cumulative cross-day analysis. The corresponding training (enrollment) data for each analysis are represented in green; the testing (claimant) data are represented in dark green (for within-day analysis) and blue (for cross-day analysis). The x-axis represents the timeline of the study consisting of multiple days; the x-axis tick marks represent the different trials performed in one day. Each of the analysis is repeated for the three days.

threshold value is defined as the upper limit of the scores obtained by matching with the template mean and covariance (Eqn (2))

$$\mathrm{Th}_{i,j} = max\left(\left[S_{i,j,1}, S_{i,j,2}, \ldots, S_{i,j,N}\right]\right) \qquad (6)$$

Decreasing the threshold value reduces the number of intruder matches, however, the correct identification of the true user also decreases. Based on preliminary results and due to its simplicity, the maximum training score was chosen as the threshold value. For the intruder analysis, score $S_{i,j}$was obtained from Eqn. (2) by matching an unknown user with a template, which is further compared to the threshold $Th_{i,j}$

$$S_{i,j} = \begin{cases} S_{i,j}, & S_{i,j} \leq \mathrm{Th}_{i,j} \\ \text{False}, & S_{i,j} > \mathrm{Th}_{i,j}. \end{cases} \qquad (7)$$

For a registered user, only the true matches (Eqn. (3)) were returned, and the scores were further sorted. The *rank-5 accuracy* was estimated similar to the standard identification analysis as described previously. In the case of an intruder, successful rejection (Eqn. (3)) from all the registered users' contributed to the *rank-5 accuracy*. A different evaluation metric, the intruder rejection rate *(IRR)* was defined as the ratio of correct rejections after matching an intruder's data with all the registered users

$$ORR = \frac{\left[\sum_{i=1}^{N} S_j == False\right]}{\sum j}, \mathrm{j} \;=\; 1, 2 \ldots, J \qquad (8)$$

For the intruder analysis, the data from 42 users were registered to the biometric system and one user was considered an intruder. This was repeated 43 times in a leave-one-out cross-validation scheme and the *rank-5 accuracy* and *IRR* were reported. This was repeated 50 times for randomly generated code sequences used as biometric tokens for identification. Further, this entire analysis was repeated in cross-validation schemes corresponding to the multiple days and trials, which were incorporated as described in the following section. The purpose of the intruder analysis is to assess the performance degradation in the presence of unregistered users and the threshold-based rejection schemes for reducing such intrusions.

H. Multi-Day Analysis

In the current study, data was collected from each user over three different days comprising seven trials each and 16 gestures in each trial. The biometric authentication and identification performance evaluation was investigated in three multi-day analyses: within-day analysis and two separate cross-day analyses, namely single cross-day (SCD) and cumulative cross-day (CCD). For the within-day analysis, six trials of the gestures each day were used as enrollment data (training) and the remaining one trial of that day was used as claimant data (testing), resulting in a leave-one-out (LOO) cross-validation scheme, equivalent to seven-fold cross-validation. The biometric performance for each fold was estimated as described in Section II-F. The cross-validation was repeated for each of the three days and the average performance metrics were reported.

For the single cross-day analysis, six trials of the gestures from one day were used as the enrollment data and the data from one trial from each of the remaining two days were used as the claimant data. This step was repeated seven times by varying the enrollment and claimant trials from the specific days and thus resulting in between-day seven-fold cross-validation. The cross-validation was repeated three times each day and the average biometric performance was reported.

For the cumulative cross-day analysis, six trials of the gestures from two of the three days were used as the enrollment data and the data from one trial from the remaining one day was used as the claimant data. Seven-fold cross-validation for all seven trials was implemented by varying the enrollment and claimant trials from the specific days. The cross-validation was repeated three times each day and the average biometric performance was reported. A graphical representation of the within-day, single cross-day, and cumulative cross-day analysis is provided in Fig. 3.

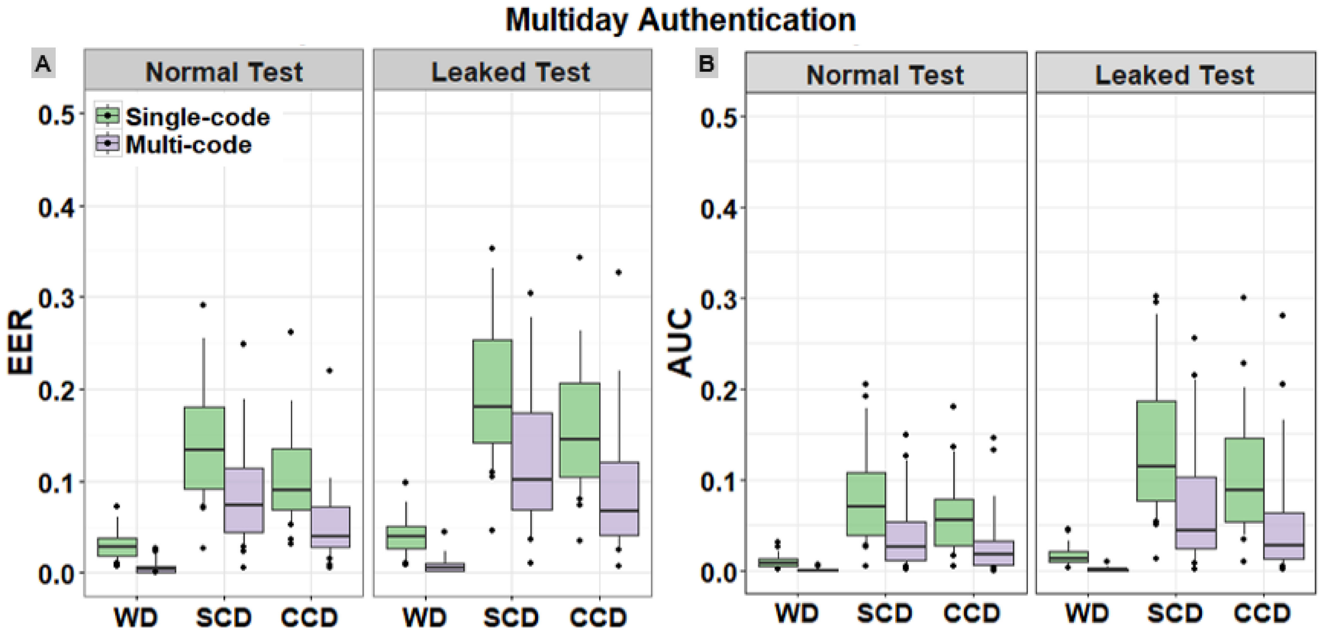

Fig. 4. Biometric authentication performance using EER (A) and AUC (B). For the multi-day authentication performance (A), the single-code and multi-code *EER* values for the normal test and leaked test scenario are shown. The x-axis represents the three multi-day analyses: within-day (WD), single cross-day (SCD) and the cumulative cross-day (CCD) and the y-axis represents the performance error. Each boxplot represents the interquartile range (IQR, 25th – 75th percentile) and the center horizontal line represents the median EER value. The whiskers (solid vertical lines) represent the datapoints within the 1.5*IQR threshold. The outliers (solid black circles) are defined as those individuals whose EER was greater than the 1.5*IQR threshold.

I. Statistical Analysis

The study aimed to investigate the multi-day biometric performance of the wrist EMG biometric system. The performance of a multi-code EMG system was compared to the single-code configuration. For each of the three analysis scenarios, *i.e.,* within-day, single cross-day, and cumulative cross-day, a Wilcoxon rank sum test was performed on the *EER* and *AUC* of the authentication mode, *rank-1, rank-3* and *rank-5 accuracy* of the identification mode, *rank-5 accuracy* and *IRR* of the intruder analysis to determine if there was any significant difference between the single-code and multi-code configuration. To compare the performance of each metric between the three multi-day analyses (WD, SCD, and CCD), pairwise comparisons were performed using the Wilcoxon rank sum test, while keeping the configuration level (single-code and multi-code) fixed. Additionally, for the intruder analysis, the Wilcoxon rank sum test was used to compare the *rank-5 accuracy* to the corresponding values for the standard identification analysis. All statistical tests were performed using RStudio 1.0. 136 (RStudio, Boston, MA, USA).

III. Results

Fig. 4 shows the biometric performance in a single-code and multi-code configuration for the three timeline-specific analyses (termed as multi-day analysis for further representation): within-day, single cross-day, and cumulative cross-day for the biometric authentication. Fig. 4A shows the *EER* and Fig. 4A shows the *AUC* distribution in a normal test and leaked test scenario of the authentication mode. Fig. 5 presents rank-*1, rank-3* and *rank-5 accuracy* of the identification mode. The individual user performance for the identification mode (*rank-5 accuracy*) for the three multi-day analyses is shown in Fig. 6. Fig. 7 shows the DEC curves for the two scenarios of the authentication mode and the CMC curve for the identification mode.

As expected and evident from Fig. 4, the within-day performance was significantly higher (p<0.001) than the other two timeline-specific analyses. Further, the median EER of the cumulative cross-day analysis was significantly lower than the single cross-day analysis (p<0.001) which is described in Section III-C.

While comparing CCD performance to the SCD performance, an overall dominance of CCD was observed for the testing scenarios (normal test, leaked test, and identification). Specifically, for the multi-code configuration in a normal test scenario, the median *EER* (0.068, Q1 = 0.041, Q3 = 0.125) for the CCD was significantly lower (p<0.001) than the corresponding median *EER* (0.039, Q1 = 0.029, Q3 = 0.072) for SCD analysis. For the identification mode, the multi-code configuration resulted in a median *rank-5 accuracy* of 93.0% (Q1 = 82.3%, Q3 = 98.0%) for the CCD which was significantly higher (p<0.001) than the corresponding SCD median *rank-5 accuracy* of 85.1% (Q1 = 66.6%, Q3 = 91.6%). This result was particularly encouraging, as it indicates the training data from two different days were homogeneous enough to provide significant benefits for biometric authentication, providing a basis for further incremental adaptive training. For each of the three timeline-based analyses and the two biometric application modes, the detailed analysis of single-code and multi-code performance is presented below.

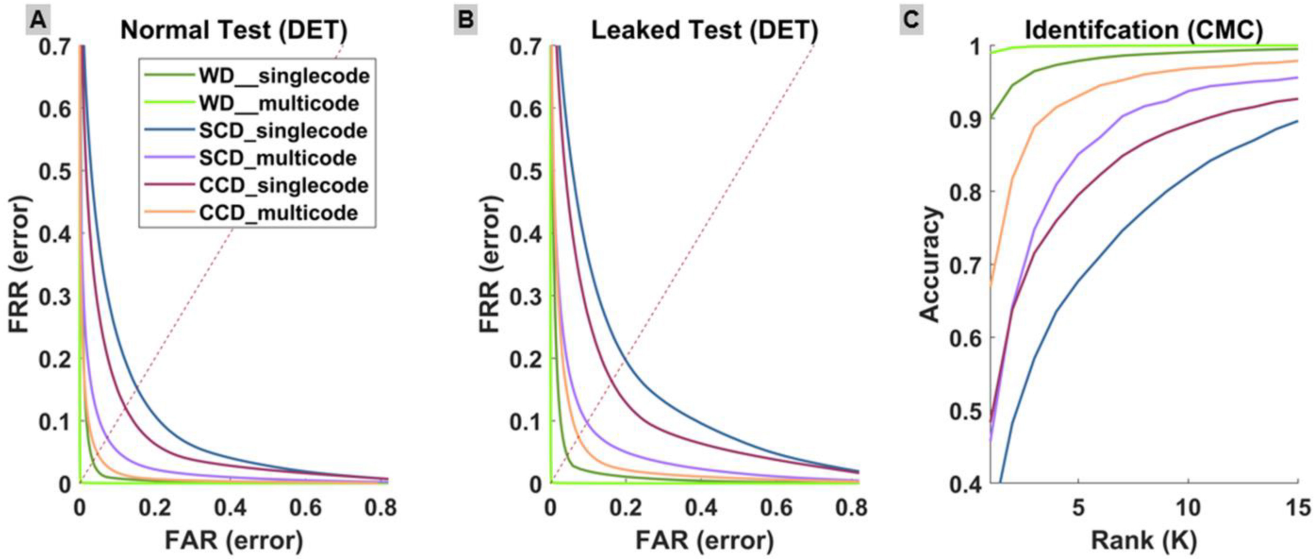

Fig. 5. DET and CMC curves for the biometric tests. The averaged detection error DET curves for the two authentication scenarios: normal test (A) and leaked test (B), in three multi-day analyses: within-day (WD), single cross-day (SCD) and cumulative cross-day (CCD) and the two configurations: single-code and multi-code. The x axis represents the FAR values, and the y axis represents the FRR values. The averaged CMC curves (B) is shown for the identification mode in the three multi-day analysis and the two configurations. The x axis represents the Rank (K) of the identification system, and the y axis represents the identification accuracy.

A. Within-Day Analysis

For the authentication mode, the within-day performance of the single-code ($M = 1$) configuration in the normal and leaked test scenarios had a median *EER* of 0.028 (Q1 = 0.018, Q3 = 0.038) and 0.04 (Q1 = 0.026, Q3 = 0.052), respectively. The performance of the multi-code framework (M = 4) was significantly improved (p<0.001), as expected and the performance reached a median *EER* value of 0.004 (Q1 = 0.001, Q3 = 0.008) for the normal test and median *EER of* 0.006 (Q1 = 0.002, Q3 = 0.011) for the leaked test scenario. A similar trend was observed for the median *AUC* values (Fig. 4B). The median *AUC* values for the multi-code framework were 0.001 (Q1 = 10^{-5}, Q3 = 0.002) in the normal test scenario and 10^{-5} (Q1 = 10^{-5}, Q3 = 0.001) in the leaked test scenario.

For the identification mode, the within-day performance of the single-code configuration reported a median *rank-1 accuracy* of 90.0% (Q1 = 86.9% and Q3 = 91.4%) and median *rank-5 accuracy* of 97.9% (Q1 = 97.3%, Q3 = 98.4%). For the multi-code configuration, the median *rank-1 accuracy* was 99.0% (Q1 = 98.1% and Q3 = 99.5%) and the median *rank-5 accuracy* was 99.9% (Q1 = 99.8%, Q3 = 99.98%) which was significantly higher than the corresponding single-code performances (p<0.001).

B. Single Cross-Day Analysis

For the authentication mode in an SCD analysis, the single-code configuration had a median *EER* of 0.133 (Q1 = 0.091, Q3 = 0.191) for the normal test scenario, which was significantly higher (p<0.001) than the median *EER* (0.72, Q1 = 0.044, Q3 = 0.115) of the multi-code configuration. Similarly, for the leaked test scenario, the single-code configuration resulted in a median *EER* of 0.181 (Q1 = 0.136, Q3 = 0.256) which was significantly higher (p<0.001) than the median *EER* (0.101, Q1 = 0.068, Q3 = 0.189) of the multi-code configuration. A similar trend was observed for the median *AUC* values (Fig. 4B). The median *AUC* values for the multi-code framework were 0.026 (Q1 = 0.011, Q3 = 0.053) in the normal test scenario and 0.043 (Q1 = 0.024, Q3 = 0.103) in the leaked test scenario. As expected, the median *EER* values for the leaked test were significantly higher (p<0.001) than the median *EER* values of the normal test, for both the single-code and multi-code configurations.

For the identification mode in an SCD analysis, it was found that significantly better performances (p<0.001) were obtained for the multi-code configuration than for the single-code configuration. The multi-code configuration reported a median *rank-1 accuracy* of 45.7% (Q1 = 30.1%, Q3 = 67.6%) and a median *rank-5 accuracy* of 85.1% (Q1 = 66.6%, Q3 = 91.6%) which was higher than the corresponding single-code *rank-1 accuracy* of 33.6% (Q1 = 21.0%, Q3 = 46.6%) and *rank-5 accuracy* of 67.7%, (Q1 = 54.1%, Q3 = 76.3%).

C. Cumulative Cross-Day Analysis

For the authentication mode in the CCD analysis, the single-code configuration had a median *EER* of 0.09 (Q1 = 0.069, Q3 = 0.136) for the normal test scenario, which was significantly higher (p<0.001) than the median *EER* of 0.039 (Q1 = 0.029, Q3 = 0.072) of the multi-code configuration. Similarly, for the leaked test scenario, the single-code configuration resulted in a median *EER* of 0.145 (Q1 = 0.101, Q3 = 0.209) which was significantly higher (p<0.001) than the median *EER* (0.068, Q1 = 0.041, Q3 = 0.125) of the multi-code configuration. A similar trend was observed for the median *AUC* values (Fig. 4B). The median *AUC* values for the multi-code framework were 0.028 (Q1 = 0.012, Q3 = 0.063)

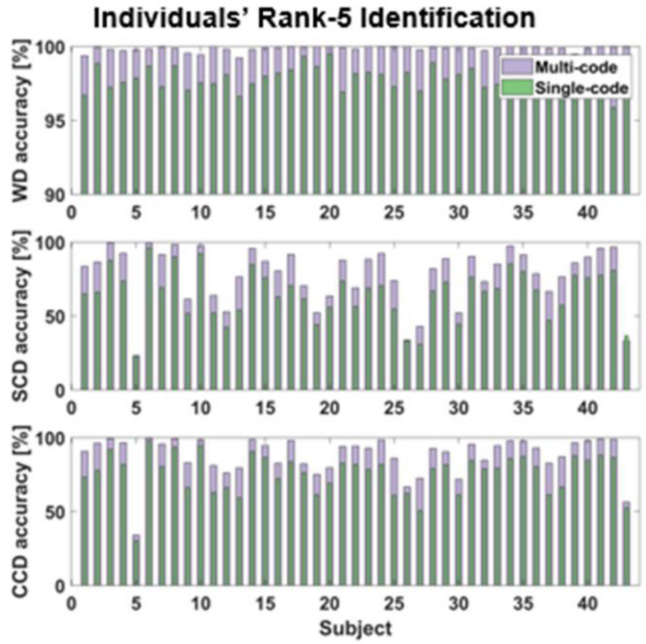

Fig. 6. Individual identification performance. The rank-5 accuracy for all the users for the WD (top), SCD (middle) and CCD (bottom) analysis is illustrated. The multi-code values are shown in violet color and the corresponding single-code values are shown in green color.

in the normal test scenario and 0.017 (Q1 = 0.006, Q3 = 0.033) in the leaked test scenario. Similar to the WD and SCD analysis, the median *EER* values for the leaked test were significantly higher (p<0.001) than the median *EER* values of the normal test, for both the single-code and multi-code configurations.

For the identification mode in a CCD analysis, it was found that the multi-code configuration performed significantly better (p<0.001) than the single-code configuration. The multi-code configuration reported a median *rank-1 accuracy* of 66.9% (Q1 = 51.4%, Q3 = 80.9%), median *rank-3 accuracy* of 88.8% (Q1 = 70.9%, Q3 = 95.9%) and a median *rank-5 accuracy* of 93.0% (Q1 = 82.3%, Q3 = 98.0%) which was higher than the corresponding single-code *rank-1 accuracy* of 48.4% (Q1 = 33.3%, Q3 = 58.1%), median *rank-3 accuracy* of 71.5% (Q1 = 54.8%, Q3 = 78.5%) and *rank-5 accuracy* of 79.5%, (Q1 = 66.2%, Q3 = 86.0%).

D. Intruder Analysis for Identification Mode

The effect of an intruder was analyzed for the identification mode in each of the three multi-day analyses. Fig. 7 shows the *rank-5 accuracy* and the *IRR* in a single-code and multi-code configuration identification mode. As expected, it was observed that the *rank-5 accuracy* decreased in all three multi-day analyses (WD, SCD, and CCD), compared to the standard identification analysis. Specifically for the CCD scenario, the multi-code configuration reported a significant decrease (p<0.001) in median *rank-5 accuracy* from 93.0% (Q1 = 82.3%, Q3 = 98.0%) for the standard analysis to 91.7% (Q1 = 79.3%, Q3 = 96.5%) for the intruder analysis. For the SCD scenario, the multi-code configuration reported a significant decrease (p<0.001) in median *rank-5 accuracy* from 85.1% (Q1 = 66.6%, Q3 = 91.6%) for the standard analysis to 82.9% (Q1 = 61.7%, Q3 = 90.6%) for the intruder analysis. For all three multi-day analyses, the multi-code configuration had significantly higher *rank-5 accuracy* (p<0.001) than the single-code configuration.

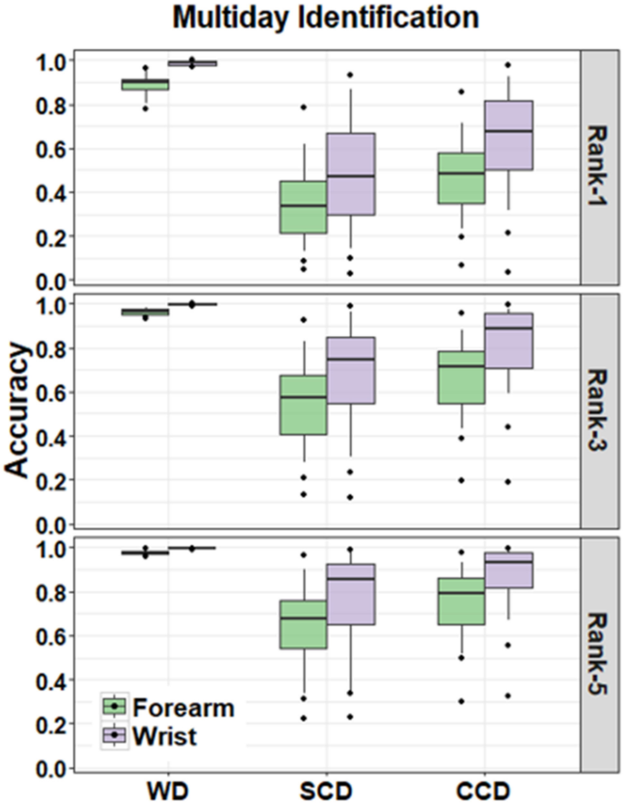

Fig. 7. Biometric identification performance. The *rank-1, rank-3* and *rank-5 accuracy* for the single-code and multi-code configuration are shown. The x-axis represents the three multi-day analyses, and the y axis represents the *rank-K accuracy* where K = 1,5. Each boxplot represents the interquartile range (IQR, 25th – 75th percentile) and the center horizontal line represents the median accuracy value. The whiskers (solid vertical lines) represent the datapoints within the 1.5*IQR threshold. The outliers (solid black circles) are defined as those individuals whose accuracy was greater than the 1.5*IQR threshold.

For the multi-code configuration, the median *IRR* was significantly higher (p<0.001) for the WD (96.1%, Q1 = 95.6%, Q3 = 96.8%) than the SCD (75.5%, Q1 = 70.4%, Q3 = 80.8%) which was significantly higher than the CCD (71.7%, Q1 = 65.7%, Q3 = 77.1%) analysis. For the CCD analysis, it was observed that the multi-code configuration had a significantly higher (p<0.001) median *IRR* (71.7%, Q1 = 65.7%, Q3 = 77.1%) than the single-code configuration (67.3%, Q1 = 62.1%, Q3 = 70.7%). This was also consistent with SCD and WD analysis. For all three multi-day analyses, the multi-code configuration had significantly higher *rank-5 accuracy* (p<0.001) than the single-code configuration.

IV. Discussion

The study presented the multi-day performance of biometric authentication and identification on the largest EMG hand-gesture dataset. The single-code configuration was compared to the multi-code configuration as the latter facilitates the fusion of hand gestures for improved biometric

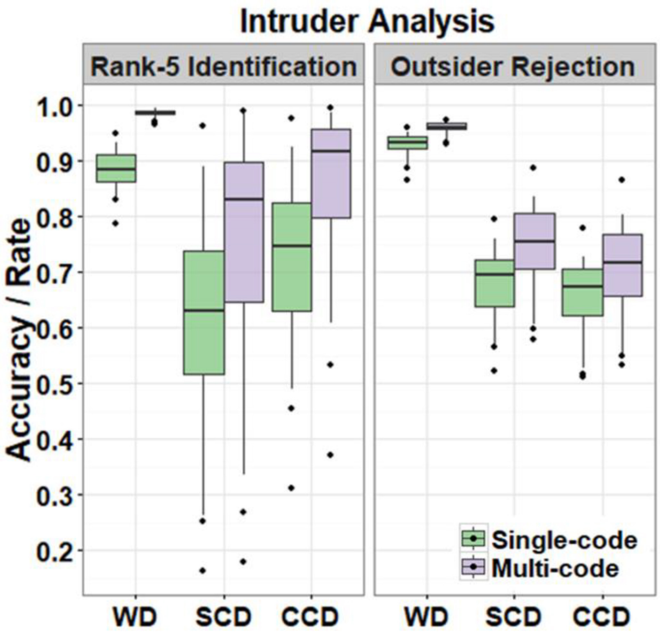

Fig. 8. Intruder analysis for the identification mode. For the multi-day authentication performance, the single-code and multi-code *rank-5 accuracy* and *IRR* values are shown. The x-axis represents the three multi-day analyses: within-day (WD), single cross-day (SCD) and the cumulative cross-day (CCD) and the y-axis represents the rank-5 accuracy (left) and the IRR (right). Each box-plot represents the interquartile range (IQR, 25^{th} – 75^{th} percentile) and the center horizontal line represents the median rank-5 accuracy/IRR value.

performance. Two evaluation scenarios for the authentication mode, i.e., the normal and leaked test, and the identification mode were investigated. The normal test scenario corresponds to the dual-security comprising both biometric-level (i.e., individual-specific characteristics in EMG signal) and knowledge-level (specific hand-gesture/code sequence). The leaked test scenario corresponds to the situation when the knowledge-level security (code sequence) is compromised, and only the biometric-level security is retained. The identification mode corresponds to the scenario where the system performs individual recognition from a database. Additionally, a more practical identification analysis involving intruders and their rejection was investigated. A within-day (WD) and cross-day, (SCD and CCD) analyses were performed for each of the comparisons and the results demonstrated the biometric performance, as discussed in the following sections.

A. Single-Code vs Multi-Code Biometric Performance

The single-code (or the single gesture) configuration was compared to the multi-code (code sequence of four randomly selected gestures) configuration. As expected, there was an overall reduction in authentication *EER* and an increase in identification accuracy with the multi-code configuration than with the single-code configuration. These findings were in agreement with multiple password-based studies using EMG from gestures [4], [6], [9], [13]. The findings in the current study were also consistent with a previous study that performed only the within-day analysis on a forearm setup [5]. For all the codelengths, it was observed that the leaked test scenario had a higher *EER* than the normal test scenario, thus suggesting that an improved performance is achieved by leveraging the knowledge-level security mode of EMG, *i.e.,* with user-defined code sequences. This is a unique advantage of EMG-based biometrics as compared to other biosignals such as EEG and ECG, for which such knowledge-level security feature is not available [5]. While the identification mode inherently does not allow customized codes for individuals, it facilitates the fusion of multiple codes to form a universal code sequence which can improve personal recognition.

B. Multi-Day Analysis

For both the single-code and multi-code configurations, it was observed that there was significant degradation in the authentication and identification performance in the cross-day analysis as compared to a within-day analysis. This is expected as the EMG signals are affected by non-stationary factors such as electrode shift, skin conditions (dry vs sweat), and physical conditions (rested vs exercising) [32]. While comparing the two cross-day analyses for the authentication mode, the CCD authentication *EER* was significantly lower than the SCD authentication *EER* for both the normal and leaked test scenarios. Similarly, it was observed that CCD identification accuracy was significantly higher than the SCD identification accuracy. This suggests that EMG data from different days do have enough homogenous information such that training with data from multiple days improves the biometric authentication performance. For the CCD analysis (training data from multiple days), a multi-code configuration resulted in a median authentication *EER* of 0.039 for the normal test and a median accuracy of 93% for the identification mode, which are comparable to most conventional biometrics as discussed in the following section. It was observed that some participants had an abnormally low identification performance, as compared to the rest of the participant pool (Fig. 6). This could be due to the shift in electrode positions causing a mismatch in the feature vectors. Some strategies to address electrode-shifts in future studies are discussed in Section IV-E. This would also help achieve higher rank-1 accuracy than the present study (66.9%). The cross-day analysis is crucial for evaluating a biometric system, as the results need to be consistent over multiple days. In the following sections, the CCD analysis (unless specified otherwise) will be used to discuss the biometric performance.

C. Comparison With State-of-the-Art EMG Biometrics

A systematic comparison with EMG baseline studies has been challenging due to the differences in experimental protocol, feature extraction strategies, biometric analysis, and fusion strategies used. The WD performance was comparable to an identical forearm electrode setup [5], [10], suggesting that the wrist, a more convenient position for wearable devices can be considered for biometric applications. This finding was in agreement with another study where the wrist setup performed comparably if not better than the forearm setup in a gesture recognition application [24]. For the cross-day comparisons, we have focused on comparing the results of those biometric studies that incorporated a multi-day factor.

TABLE I
BIOMETRIC TRAITS CHARACTERISTICS [1]

Biometric	Spoofing	Customizeable	Environment factors	Accuracy
Fingerprint	Easy	No	Robust	High
Iris	Easy	No	Sensitive	High
Face	Easy	No	Sensitive	High
Voice	Easy	Yes	Sensitive	Low
Gait	Hard	Yes	Sensitive	Low
Keystroke Dynamics	Hard	Yes	Robust	Low
Biosignals				
EEG	Hard	No	Sensitive	Low
ECG	Hard	No	Robust	Low
EMG	Hard	Yes	Sensitive	Acceptable

1) Biometric Authentication: One study investigated a password-based EMG biometrics of codelength eight and reported a normal-test *EER* of 0.012 and the leaked-test *EER* of 0.1496 [6]. Another study involving a similar multi-code password of codelength 12 reported a normal-test *EER* of 0.0013 and the leaked-test *EER* of 0.0273 [9]. Another study incorporated a multi-day investigation, however, different codelengths were not investigated. They reported an average EER of 0.1634 for eight individual gestures [22]. While comparing these studies, the current study reported a median EER of 0.039 for the normal test and a median EER of 0.068 for the leaked test scenario which is in agreement. These findings can help further ongoing research on unlocking smartphones, or developing wristband devices for biometric authentication [20], [21].

2) Biometric Identification: Another identification study has investigated multiple protocols, codelengths, and electrode layouts for improving biometric performance [13]. For a fixed gesture sequence protocol and a codelength four (closest configuration to the present study), a mean *rank-1 accuracy* of 86.1% was reported which was higher than the current study (66.9%). This could be mostly due to: 1) the number of users in the previous study was 22 compared to 43 in the present study, and 2) the number of electrode channels was 256 compared to six in the present study. Another study with a similar setup of 22 users and 256 channels reported a *rank-1 accuracy* of 85.8%, however, the gesture task of each participant was different, and they reported a decrease in accuracy (<50%) with more than 30 inactive electrodes [4]. This further shows that the increased *rank-1 accuracy* could be due to the greater number of channels. The high-density electrode setup (256 channels) can have multiple limitations such as practical viability, inactive channels, and model training time, which are comparatively low while using a 6-channel setup. Another study involving a similar setup (22 gestures and 256 channels) and a codelength of eight used a deep learning model and reported a *rank-1 accuracy* of 87.2% and a *rank-5 accuracy* of 91.2% [17]. The present study reported a slightly higher *rank-5 accuracy* of 93%. The performance was also comparable to two other studies that involved multi-day testing data from 5 subjects and reported an identification accuracy of 74.1% and 93% [18], [22].

3) Protocols With Intruder Analysis: To the best of our knowledge, only one study has investigated the effect of intruders on identification performance [13]. They have reported a decrease in identification performance from 99% to 93.1% while introducing unregistered users to the system. The experimental factors included 22 users, a codelength of 12, and 256 channels. The present study reported a decrease in rank-5 identification accuracy from 93% to 91.7% for a codelength of four, which was in agreement with the previous study. Additionally, we observed that for a database of 42 users (one user removed as an intruder), an intruder is more likely to find a match with at least one of the registered users. We introduced a metric *IRR* to quantify the number of threshold-based rejections for each multi-day scenario. It was reported that for a multi-day analysis, an $IRR > 70\%$ was achieved. The results suggest that the intruder encountered rejection from most of the registered users' threshold values. Reducing the threshold limit might improve intruder rejection, however, the genuine user might not be correctly identified. Additional research could explore approaches to enhance both identification performance and intruder rejection, ultimately leading to a more practical and robust biometric system.

D. Comparison With Other Biometrics

Conventional biometric traits such as fingerprint and facial recognition have already been widely implemented in daily consumer applications. It can be difficult to compare with conventional benchmarks because research in this area has been ongoing for several decades [1]. Datasets including thousands of individuals are available online, which indicates the abundance of resources for researching such traits [33]. However, with advancing technology, data leakage and spoofing have become increasingly easier, affecting an important aspect of our digital society. Therefore, unconventional biometric traits such as biosignals, gait, keystroke dynamics, etc., have been investigated to address the limitations associated with conventional biometric traits [1]. The previous studies suggest that the biometric authentication performance of these traits ranges from $EER = 10^{-4} - 0.20$ [1]. From this review, it was suggestive that an accurate biometric authentication *EER*<0.05, while most of the novel biometric traits reported *rank-5 accuracies* > 90% [1]. The findings of the current study (authentication $EER = 0.039$ and identification *rank-5 accuracy* = 93%) suggest that wrist EMG-based biometrics resulted in accurate authentication and identification using a multi-code framework for combining hand gestures. This property of customizing a code based on knowledge can be achieved using some form such as voice, gait, and keystroke dynamics for improved security. This is an advantage over other biosignals such as ECG and EEG, which are highly difficult to be customizable, if possible at all [10]. Overall, the biosignals are more difficult to spoof and are one of the main indicators of liveness detection [4], a security feature requiring the user was physically present while an authentication claim is attempted. While the EMG signals are affected by multiple non-stationary factors, the cross-day analysis suggests there are sufficient commonalities in multi-day EMG data for biometric authentication. A detailed comparison of EMG-based biometrics with the other common biometrics is provided in Table I [1]. As EMG-based biometrics holds distinct advantages over other common biometrics, further research involving wearable devices and extensive datasets will aid its social acceptance. Future research could record collect EMG as well as another conventional biometric (fingerprint/facial recognition) from individuals to facilitate easier comparison with baselines in the biometric field.

E. Limitations and Future Research Directions

The results of the study addressed two major challenges in the current EMG-based research by analyzing a large sample-size of participants and multi-day (N = 3) recordings of EMG signals. However, there exist some limitations in the present study. Multiple force levels for the same gesture could not be collected. Due to the large sample size, it was not timely feasible to collect different levels of force. The participant was instructed to perform the gestures at a convenient force level (as they would normally perform a gesture in their daily lives). Furthermore, no marks were left on the participants' skin during the multiple sessions. While the electrode positioning was kept consistent to the best of our ability, there might have been some electrode shifts between days. Although a limitation, such a situation is more realistic than tightly controlling electrode positions. It can facilitate research into transfer learning approaches that are insensitive to electrode shift, and hence, beneficial for accurate biometric authentication [34]. A different study investigated EEG biometric characteristics such as permanence and uniqueness by analyzing six recording sessions over spanning over 3 years [35]. The inclusion of transfer learning in EMG biometric analysis can facilitate such a longitudinal investigation.

The 6-channel electrode setup was part of a bigger dataset, *i.e.,* GRABMyo, which includes 28 channels recorded from the forearm and wrist region [27], [28]. While preliminary results suggested no difference between the forearm and the wrist setup, further investigations could lead to novel findings [36]. Other strategies to improve the authentication and identification performance can be further investigated by implementing different fusion strategies [5]. Recently, deep learning studies have improved biometric performance and can be incorporated in similar analyses for more accurate results [14], [15], [16], [17].

V. Conclusion

The study presented the multi-day EMG Biometrics performance of the largest EMG-based hand gestures dataset (43 users x 3 sessions = 129 recordings) over the span of 30 days. A detailed multi-day analysis considering within-day and cross-day scenarios was performed for the feasibility of EMG-based biometrics as a novel trait for biometric authentications/identification. A multi-code biometric framework had superior performance than the single-code system, suggesting enhanced security with customizable gesture passwords. The authentication mode resulted in an *EER* value (0.039) for the normal test, which is comparable to conventional biometrics. The identification mode presented a *rank-5 accuracy* of 93% which is comparable to most novel biometric traits. In the presence of intruders, a threshold-based identification was able to achieve a *rank-5 accuracy* of 91.7%. The findings are close-to-practical due to the more realistic analyses

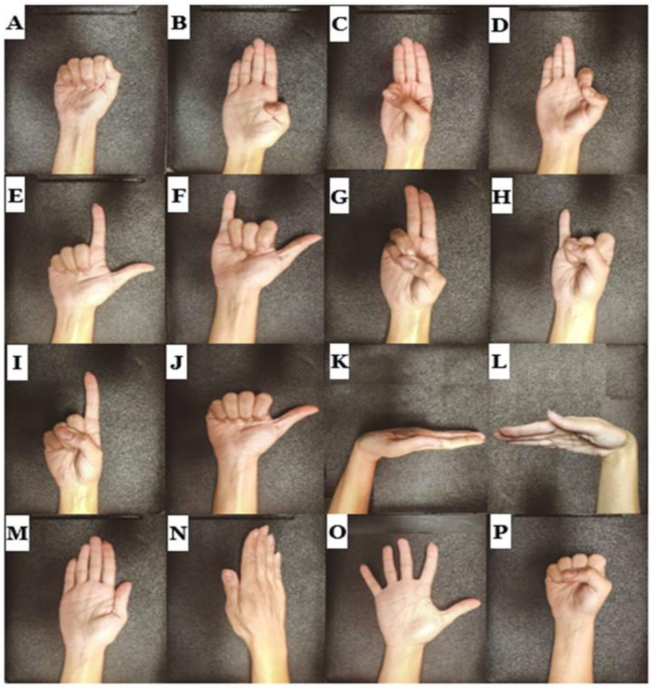

Fig. 9. The 16 gesture classes investigated in the study: (A) lateral prehension (LP), (B) thumb adduction (TA), (C) thumb and little finger opposition (TLFO), (D) thumb and index finger opposition (TIFO), (E) thumb and little finger extension (TLFE), (F) thumb and index finger extension (TIFE), (G) index and middle finger extension (IMFE), (H) little finger extension (LFE), (I) index finger extension (IFE), (J) thumb extension (TE), (K) wrist flexion (WF), (L) wrist extension (WE), (M) forearm supination (FS), (N) forearm pronation (FP), (O) hand open (HO), (P) hand close (HC).

TABLE II
Within Day Identification Performance of Gestures

Sl No	Gesture	Rank-1 Accuracy
1	LP	83.98
2	TA	92.64
3	TLFO	93.07
4	TIFO	88.46
5	TLFE	93.22
6	TIFE	94.23
7	IMFE	91.05
8	LFE	91.34
9	IFE	91.63
10	TE	92.64
11	WF	93.07
12	WE	88.02
13	FS	90.62
14	FP	91.05
15	HO	91.77
16	HC	90.04

The individual gesture performance is utilized as weights for the majority voting decision level fusion.

such as cross-day, leaked test, and intruder analysis. This could further facilitate the development of wearable EMG-based bracelets and wristbands for biometric authentication and identification purposes. The high cross-day performance was consistent over multiple days, a necessary characteristic for biometric authentication. Therefore, the presented findings could facilitate further research on EMG-based biometrics.

Appendix

See Fig. 9 and Table II.

References

[1] G. Dahia, L. Jesus, and M. Pamplona Segundo, "Continuous authentication using biometrics: An advanced review," *Wiley Interdiscip. Rev.: Data Min. Knowl. Discov.*, vol. 10, no. 4, 2020, Art. no. e1365.

[2] E. Campbell, A. Phinyomark, and E. Scheme, "Deep cross-user models reduce the training burden in myoelectric control," *Front. Neurosci.*, vol. 15, May 2021, Art. no. 657958.

[3] S. Said, A. S. Karar, T. Beyrouthy, S. Alkork, and A. Nait-ali, "Biometrics verification modality using multi-channel sEMG wearable bracelet," *Appl. Sci.*, vol. 10, no. 19, p. 6960, 2020.

[4] X. Jiang et al., "Cancelable HD-sEMG-based biometrics for cross-application discrepant personal identification," *IEEE J. Biomed. Health Inform.*, vol. 25, no. 4, pp. 1070–1079, Apr. 2021.

[5] A. Pradhan, J. He, and N. Jiang, "Score, rank, and decision-level fusion strategies of multicode electromyogram-based verification and identification biometrics," *IEEE J. Biomed. Health Inform.*, vol. 26, no. 3, pp. 1068–1079, Mar. 2022.

[6] X. Jiang et al., "Neuromuscular password-based user authentication," *IEEE Trans. Ind. Informat.*, vol. 17, no. 4, pp. 2641–2652, Apr. 2021.

[7] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior, *Guide to Biometrics*. Berlin, Germany: Springer, 2013.

[8] J. He and N. Jiang, "Biometric from surface electromyogram (sEMG): Feasibility of user verification and identification based on gesture recognition," *Front. Bioeng. Biotechnol.*, vol. 8, p. 58, Feb. 2020.

[9] X. Jiang et al., "Enhancing IoT security via cancelable HD-sEMG-based biometric authentication password, encoded by gesture," *IEEE Internet Things J.*, vol. 8, no. 22, pp. 16535–16547, Nov. 2021.

[10] A. Pradhan, J. He, and N. Jiang, "Performance optimization of surface electromyography based biometric sensing system for both verification and identification," *IEEE Sensors J.*, vol. 21, no. 19, pp. 21718–21729, Oct. 2021.

[11] Q. Li, Z. Luo, and J. Zheng, "A new deep anomaly detection-based method for user authentication using multichannel surface EMG signals of hand gestures," *IEEE Trans. Instrum. Meas.*, vol. 71, pp. 1–11, Apr. 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9745921

[12] H. Yamaba et al., "On applying support vector machines to a user authentication method using surface electromyogram signals," *Artif. Life Robot.*, vol. 23, no. 1, pp. 87–93, 2018.

[13] X. Jiang et al., "Measuring neuromuscular electrophysiological activities to decode HD-sEMG biometrics for cross-application discrepant personal identification with unknown identities," *IEEE Trans. Instrum. Meas.*, vol. 71, pp. 1–15, Jun. 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9789143

[14] M. Pleva, Š. Korečko, D. Hladek, P. Bours, M. H. Skudal, and Y.-F. Liao, "Biometric user identification by forearm EMG analysis," in *Proc. 2022 IEEE Int. Conf. Consumer Electron.-Taiwan*, 2022, pp. 607–608.

[15] Y.-H. Byeon and K.-C. Kwak, "Individual identification by late information fusion of EmgCNN and EmgLSTM from electromyogram signals," *Sensors*, vol. 22, no. 18, p. 6770, 2022.

[16] Q. Hu, A. Sarmadi, P. Gulati, P. Krishnamurthy, F. Khorrami, and S. F. Atashzar, "X-MyoNET: Biometric identification using deep processing of transient surface electromyography," presented at bioRxiv, 2021.

[17] J. Fan et al., "Cancelable HD-SEMG biometric identification via deep feature learning," *IEEE J. Biomed. Health Inform.*, vol. 26, no. 4, pp. 1782–1793, Apr. 2022.

[18] J.-S. Kim, C.-H. Song, E. Bak, and S.-B. Pan, "Multi-session surface electromyogram signal database for personal identification," *Sustainability*, vol. 14, no. 9, p. 5739, 2022.

[19] L. Lu, J. Mao, W. Wang, G. Ding, and Z. Zhang, "A study of personal recognition method based on EMG signal," *IEEE Trans. Biomed. Circuits Syst.*, vol. 14, no. 4, pp. 681–691, Aug. 2020.

[20] B. Fan, X. Su, J. Niu, and P. Hui, "EmgAuth: Unlocking smartphones with EMG signals," 2021, *arXiv:2103.12542*.

[21] S. Shin, M. Kang, J. Jung, and Y. T. Kim, "Development of miniaturized wearable wristband type surface EMG measurement system for biometric authentication," *Electronics*, vol. 10, no. 8, p. 923, 2021.

[22] S. A. Raurale, J. McAllister, and J. M. D. Rincón, "EMG biometric systems based on different wrist-hand movements," *IEEE Access*, vol. 9, pp. 12256–12266, 2021.

[23] S. Benatti, E. Farella, E. Gruppioni, and L. Benini, "Analysis of robust implementation of an EMG pattern recognition based control," in *Proc. BIOSIGNALS*, 2014, pp. 45–54.

[24] F. S. Botros, A. Phinyomark, and E. J. Scheme, "Electromyography-based gesture recognition: Is it time to change focus from the forearm to the wrist?" *IEEE Trans. Ind. Informat.*, vol. 18, no. 1, pp. 174–184, Jan. 2020.

[25] S. Jiang et al., "Feasibility of wrist-worn, real-time hand, and surface gesture recognition via sEMG and IMU sensing," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3376–3385, Aug. 2018.

[26] R. Shioji, S.-i. Ito, M. Ito, and M. Fukumi, "Personal authentication and hand motion recognition based on wrist EMG analysis by a convolutional neural network," in *Proc. 2018 IEEE Int. Conf. IoT Intell. Syst. (IOTAIS)*, 2018, pp. 184–188.

[27] N. Jiang, A. Pradhan, and J. He. "Gesture recognition and biometrics electromyogram (GRABMyo)." PhysioNet. Jul. 2022. [Online]. Available: https://doi.org/10.13026/rtfc-np50

[28] A. Pradhan, J. He, and N. Jiang, "Multi-day dataset of forearm and wrist electromyogram for hand gesture recognition and biometrics," *Sci. Data*, vol. 9, no. 1, pp. 733–743, 2022.

[29] A. Pradhan, N. Jiang, V. Chester, and U. Kuruganti, "Linear regression with frequency division technique for robust simultaneous and proportional myoelectric control during medium and high contraction-level variation," *Biomed. Signal Process. Control*, vol. 61, Aug. 2020, Art. no. 101984.

[30] J. He, D. Zhang, X. Sheng, S. Li, and X. Zhu, "Invariant surface EMG feature against varying contraction level for myoelectric control based on muscle coordination," *IEEE J. Biomed. Health Inform.*, vol. 19, no. 3, pp. 874–882, May 2015.

[31] W. Kabir, M. O. Ahmad, and M. N. S. Swamy, "A multi-biometric system based on feature and score level fusions," *IEEE Access*, vol. 7, pp. 59437–59450, 2019.

[32] M. B. I. Reaz, M. S. Hussain, and F. Mohd-Yasin, "Techniques of EMG signal analysis: Detection, processing, classification and applications," *Biol. Proced. Online*, vol. 8, no. 1, pp. 11–35, 2006.

[33] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, "Vggface2: A dataset for recognising faces across pose and age," in *Proc. 2018 13th IEEE Int. Conf. Autom. Face Gesture Recognit. (FG 2018)*, 2018, pp. 67–74.

[34] C. Prahm et al., "Counteracting electrode shifts in upper-limb prosthesis control via transfer learning," *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 27, no. 5, pp. 956–962, May 2019.

[35] E. Maiorana and P. Campisi, "Longitudinal evaluation of EEG-based biometric recognition," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 5, pp. 1123–1138, May 2018.

[36] A. Pradhan, J. He, and N. Jiang, "Hand gesture recognition and biometric authentication using a multi-day dataset," in *Proc. Int. Conf. Intell. Robot. Appl.*, 2022, pp. 375–385.

Ashirbad Pradhan received the Bachelor of Technology degree in biomedical engineering from the National Institute of Technology Rourkela, India, in 2016, and the M.Sc. degree in kinesiology from the University of New Brunswick, Canada, in 2018. He is currently pursuing the Ph.D. degree with the Department of Systems Design Engineering, University of Waterloo. His research interests include biomedical signal processing, biometrics, myoelectric control of prosthetics, sensor design, and biomechanics. He received multiple awards, including the MITACS Globalink Graduate Award in 2016, the Queen Elizabeth Scholarship in 2017, the Natural Sciences and Engineering Research Council of Canada Doctoral Award in 2022.

Jiayuan He (Member, IEEE) received the B.S. degree in mechanical engineering and automation from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2010, and the Ph.D. degree in mechanical engineering from Shanghai Jiao Tong University, Shanghai, China, in 2016. From 2016 to 2022, he was a Postdoctoral Research Fellow and then a Research Assistant Professor with the Department of Systems Design Engineering, University of Waterloo, Canada. He is currently a Full Professor with the West China Hospital, Sichuan University, Chengdu, China. His research interests include neural interface and biomechatronics system.

Hyowon Lee received the B.S. and first M.Sc. degrees in mechanical engineering from Ulsan University, South Korea, in 2013, and the second M.Sc. degree in mechanical engineering from the University of Wisconsin-Madison, USA, in 2017. He is currently pursuing the Ph.D. degree with the Department of System Design Engineering, University of Waterloo, Canada. He did research on the internal combustion engine and as a Graduate Research Assistant. His current research interests include signal processing, physiological signals, human-robot interaction, and human factors in semi-autonomous vehicles.

Ning Jiang (Senior Member, IEEE) received the B.S. degree in electrical engineering from Xi'an Jiaotong University, Xi'an, China, in 1998, and the M.Sc. and Ph.D. degrees in engineering from the University of New Brunswick, Fredericton, NB, Canada, in 2004 and 2009, respectively. He had research and academic positions in Denmark, Germany, and Canada, before he was promoted to a Tenured Associate Professor with the Department of Systems Design Engineering, University of Waterloo, Canada. He also held a Canadian Research Chair (Tier II) in artificial intelligence and human-machine interface. He is currently a Full Professor with the West China Hospital Sichuan University, Sichuan, China, leading the Huaxi Smart Wearable Health Systems Lab. His research interests include signal processing of physiological signals, such as electromyography, electroencephalogram, and electrocardiography, as well as advanced brain-computer interfaces, prosthetic control, and neuromuscular modeling, with a focus on clinical translation of neural technologies in to clinical rehabilitation applications. He is currently an Associate Editor of IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, IEEE TRANSACTIONS ON NEURAL SYSTEMS AND REHABILITATION, the *Brain Computer Interface*, *Frontiers in Neuroscience*, and *Journal of Neuroscience Methods*.