Neuromuscular Password-Based User Authentication

Xinyu Jiang, Ke Xu, *Student Member, IEEE*, Xiangyu Liu, Chenyun Dai, *Member, IEEE*, David A. Clifton, *Member, IEEE*, Edward A. Clancy, *Senior Member, IEEE*, Metin Akay, *Fellow, IEEE*, and Wei Chen, *Senior Member, IEEE*

***Abstract*—In this article, we propose a novel neuromuscular password-based user authentication method. The method consists of two parts: surface electromyogram (sEMG) based finger muscle isometric contraction password (FMICP) and neuromuscular biometrics. FMICP can be entered through isometric contraction of different finger muscles in a prescribed order without actual finger movement, which makes it difficult for observers to obtain the password. In our study, the isometric contraction patterns of different finger muscles were recognized through high-density sEMG signals acquired from the right dorsal hand. Moreover, both time–frequency–space domain features at macroscopic level (interference-pattern EMG) and motor neuron firing rate features at microscopic level (via decomposition) were extracted to represent neuromuscular biometrics, serving as a second defense. The FMICP and macro–micro neuromuscular biometrics together form a neuromuscular password. The proposed neuromuscular password achieved an equal error rate (EER) of 0.0128 when impostors entered a wrong FMICP. Even when impostors entered the correct FMICP, the neuromuscular biometrics, as the second defense, inhibited impostors with an EER of 0.1496. To the best of our knowledge, this is the first study to use individually unique neuromuscular information during unobservable muscle isometric contractions for user authentication, with training and testing data acquired on different days.**

Manuscript received April 15, 2020; accepted May 30, 2020. Date of publication June 11, 2020; date of current version January 4, 2021. This work was supported in part by the National Key R&D Program of China under Grant 2017YFE0112000, in part by the Shanghai Pujiang Program under Grant 19PJ1401100, and in part by the Shanghai Municipal Science and Technology Major Project under Grant 2017SHZDZX01. Paper no. TII-20-1930. *(Corresponding authors: Chenyun Dai; Wei Chen.)*

Xinyu Jiang, Ke Xu, Chenyun Dai, and Wei Chen are with Center for Intelligent Medical Electronics, School of Information Science and Technology, Fudan University, Shanghai 200433, China (e-mail: jiangxy18@fudan.edu.cn; kexu18@fudan.edu.cn; chenyundai@fudan.edu.cn; w_chen@fudan.edu.cn).

Xiangyu Liu is with the School of Art Design and Media, East China University of Science and Technology, Shanghai 200237, China (e-mail: y12170017@mail.ecust.edu.cn).

David A. Clifton is with the Institute of Biomedical Engineering, Department of Engineering Science, University of Oxford, OX1 2JD Oxford, U.K. (e-mail: david.clifton@eng.ox.ac.uk).

Edward A. Clancy is with the Department of Electrical and Computer Engineering, Worcester Polytechnic Institute, Worcester, MA 01609 USA (e-mail: ted@wpi.edu).

Metin Akay is with the Department of Biomedical Engineering, University of Houston, Houston, TX 77204 USA (e-mail: makay@uh.edu).

Color versions of one or more of the figures in this article are available online at https://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2020.3001612

***Index Terms*—Biometrics, high-density surface electromyogram (sEMG), machine learning, neuromuscular password, user authentication.**

I. Introduction

THE DEMAND for secure user authentication systems is soaring in a wide variety of application scenarios, such as automatic teller machines (ATMs), access to mobile phones, secure payment, and even the permission to use military weapons. Approaches for user authentication can be divided into three categories, namely "what the user knows" (such as passwords), "what the user has" (such as ID cards), and "what the user is" (such as biometrics). However, these three approaches each have their own limitations. Passwords are easily stolen by surveillance cameras or "shoulder surfing." ID cards can also be accidentally lost or deliberately stolen. Besides, it is inconvenient to carry around an ID card all the time. Biometrics such as deoxyribonucleic acid (DNA), human face [1], fingerprint [2], iris [3], and physiological signals [4], [5] can, to a certain extent, make up for the disadvantages of the above approaches. However, all of the existing biometrics modalities have drawbacks. DNA is easily stolen through saliva and lost hair. The face and iris can be captured through depth photography. Fingerprints can be acquired through any touched surface and forged with plastic molds. Worse still, all the existing biometrics-based passwords are noncancelable. In other words, if the information from DNA, face, iris, or fingerprints is stolen, the user cannot volitionally replace them. Additionally, users may use the same biometrics in different applications. If the biometric template in one application is stolen, the ones in all other applications are compromised due to the noncancelability. On the other hand, novel biometric modalities based on physiological signals such as the electroencephalogram (EEG) [4] and electrocardiogram (ECG) [5] show great promise since they are difficult to steal or forge. However, their user authentication accuracy is currently far too low to support their practical application.

In contrast, surface electromyogram (sEMG) has shown different characteristics across subjects in multiuser myoelectric interface techniques [6]. This property indicates that sEMG might be employed as a new biometrics modality. Compared with EEG modality, the sEMG signal is convenient to collect. Furthermore, the sEMG signal characteristics vary with different muscle contraction patterns, allowing a second encryption—beyond a first encryption found through designing a unique pattern to exert force. So far, very few studies have explored the feasibility of sEMG as an authentication modality. Two previous studies have employed sEMG under specific hand gestures as biometrics [7], [8]. Other applications of sEMG signals have only been investigated as a complement to other biometric modalities (ECG [9] and keystroke dynamics [10], for example). However, the signal variability on different days was not taken into consideration in all the aforementioned studies. The training and testing data were not strictly recorded on different days. Besides, both the gestures in [7] and [8] and the keyboard typing in [10] were observable to impostors so that impostors can mimic users' gestures and motions to generate similar sEMG signals.

In this article, we propose a new user authentication paradigm based on neuromuscular password. The neuromuscular password can realize double security through finger muscle isometric contraction password (FMICP) and high-density sEMG (HD-sEMG) based neuromuscular biometrics. First, FMICP is a new password entry mode allowing users to enter the password through isometric contraction of different finger muscles in a prescribed order, without actual finger movements. Isometric contraction, in contrast to dynamic movement, is one kind of muscle contraction pattern during which the muscle tension increases but length remains the same. Since the finger orientations remain static during the password entry process, stealing the password becomes more difficult through peeping. Second, we acquired 64-channel HD-sEMG signals from the dorsum of the user's right hand when the subject performed isometric contraction of different finger muscles to enter the FMICP. The isometric contraction patterns of different finger muscles can be recognized between individuals through HD-sEMG signals. The HD-sEMG allows information mining in the spatial domain, as a complement to the time–frequency domain. Features in the time–frequency–space domain represent the macroscopic characteristics of neuromuscular biometrics. Moreover, the discharge timings of several individual motor units (MUs) at the microscopic level can be obtained through decomposition of the global HD-sEMG [11] using independent component analysis (ICA) [12]. The average firing rate (FR) of all obtained MUs summarizes the microscopic characteristics of neuromuscular biometrics. The FMICP and macro–micro neuromuscular biometrics together can be referred to as neuromuscular password. The HD-sEMG signal data for the model training and testing of the proposed authentication system were acquired on two different days (nine-day apart on average) for each subject. To the best of our knowledge, this is the first study to evaluate the effectiveness of neuromuscular information for user authentication, with training and testing data for validation acquired on different days. This study is also the first to employ a second encryption for HD-sEMG-based neuromuscular biometrics through the implicit FMICP. The proposed neuromuscular password can be used as the supplement to the existing methods, and overcome the aforementioned drawbacks of other authentication systems in some scenarios.

The rest of this article is organized as follows. In Section II, we introduce the dataset and data preprocessing method. In Section III, the sEMG feature extraction, user authentication algorithms, and validation methodologies are introduced. In Sections IV and V, the results and discussion are presented, respectively. Finally, Section VI concludes this article.

II. Materials

A. Data Acquisition

Experimental data from 22 healthy subjects (ten males, 12 females; aged 21–31 years) were acquired. Each subject was informed about the experiment procedure and the research purpose, and then provided written informed consent.

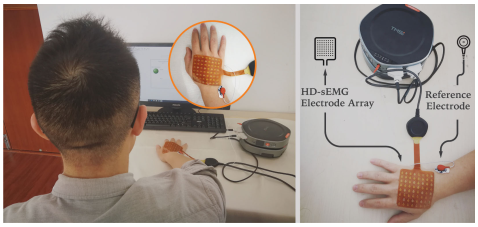


Fig. 1. Experiment setup.

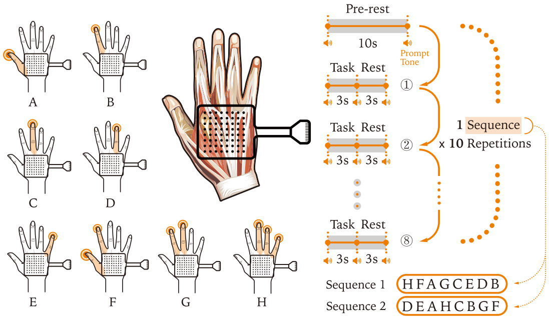


Fig. 2. Schematic sequence diagram of the experiment.

The 64-channel monopolar HD-sEMG signals were acquired using the SAGA 64+ system of Twente Medical Systems International BV at a sampling rate of 4000 Hz. The reference electrode was placed on the head of the ulna. Before data acquisition, the dorsum of a subject's right hand was cleaned with abrasive gel and then wiped with an alcohol cotton ball to reduce the impedance between skin and electrodes. The 8 × 8 flexible high-density electrode array with 8-mm interelectrode distance was placed in the center of the dorsal aspect of a subject's right hand, as shown in Fig. 1. During isometric contraction of different finger muscles, sEMG signals can be recorded on the forearm, palm, and dorsal hand. We chose to instrument the hand because, first, the measurement of sEMG of the forearm is not convenient in practical use. Second, sEMG signals of the palm can be easily disturbed by motion artifacts due to the direct contact between the palm and a desk. Therefore, sEMG signals from the dorsum of the hand were selected.

During data acquisition, subjects sat on a comfortable chair, watching a computer screen and following the experiment instructions on the screen. Subjects were asked to place their right hand comfortably on the experimental desk to perform the isometric contractions with the force at a self-selected level and exert the force at a similar level in different sessions. Subjects were asked to perform muscle isometric contractions in their most comfortable manner without any learning process. The schematic sequence diagram of the experiment is shown in Fig. 2. Each trial was compromised of a 10-s pretrial resting period, followed by eight task-rest pairs. For each pair, subjects performed a 3-s isometric contraction task controlling a specific finger (or finger combination) and then had a 3-s rest. The order of the performed task sequence was the FMICP. For each session, ten repeated trials were performed. The subjects were asked to inform the laboratory assistant if they performed a wrong task or missed a task due to inattention. The whole trial was removed from the acquired data if one of the 8 tasks in that

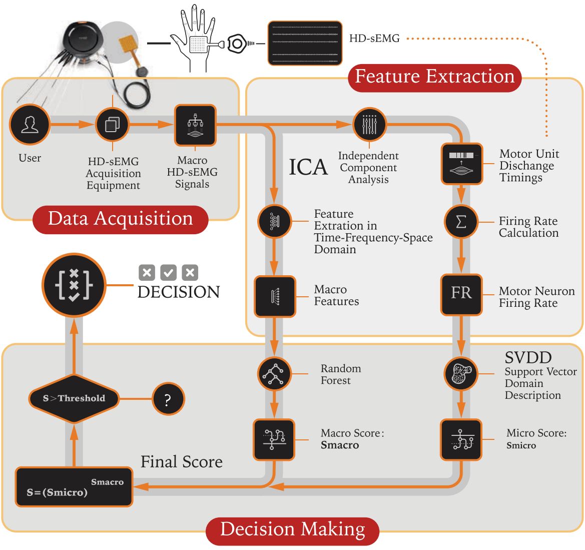


Fig. 3. Framework of user authentication based on neuromuscular password.

trial was wrong or missed. On average, 9.41 out of 10 trials for each session were preserved for further analysis. Three data collection sessions were acquired. For sessions 1 and 2, the same FMICP, "HFAGCEDB," following the symbol code in Fig. 2, was employed. For session 3, a different FMICP, "DEAHCBGF" with two symbols the same with that of sessions 1 and 2, was selected. Session 1 was used as the training dataset. Sessions 2 and 3 were acquired on the same day but several days (3–23 days, 9±6.67 days on average) later after session 1, which were used as the testing set. The electrode array was reapplied on the second day using the same approach as day 1, with no skin markings preserved between sessions.

B. Data Preprocessing

According to [13], the acquired HD-sEMG signals can be disturbed by a variety of noises such as noise inherent in electronic equipment (ranging from 0 to several thousand Hz), noise caused by the quasi-random nature of EMG (ranging from 0 to 20 Hz) and motion artifacts (ranging from 0 to 10 Hz). Because the noise spectrum overlaps that of HD-sEMG signals, to tradeoff retention of HD-sEMG signals versus noise removal, the acquired signals were bandpass filtered from 10 to 900 Hz using an eight-order Butterworth filter. This same filter band was also selected by previous work [14]. A 50-Hz notch filter was then used to attenuate power line interference. We evaluated the noise power of the preprocessed HD-sEMG signals using signals recorded during rest. A signal-to-noise ratio (SNR) of 8.58 dB was obtained. The filtered signals in each trial were segmented into the eight different tasks (each of 3-s duration) for further analysis.

III. Methods of Analysis

As shown in Fig. 3, the framework of the neuromuscular password can be divided into three parts: data acquisition, feature extraction, and decision-making. The last two parts each can be divided into two levels: the macrolevel and microlevel. Details of the proposed method are introduced in the following.

A. Macroscopic Feature Extraction

State-of-the-art feature sets in the time–frequency domain, consisting of sample entropy, spectral entropy, frequency median (FMD), waveform length (WL), and root mean square (RMS)—as employed in previous studies [15], were extracted from each channel in our work (one estimate of each from each full 3-s task). Sample entropy can measure the complexity of time-series. Spectral entropy can measure the complexity of time series in the frequency domain. The FMD feature is extracted based on the criterion that FMD splits the signal power spectral density into two equal parts. WL is a parameter reflecting the EMG standard deviation. RMS is an effective representation in the time domain to discriminate different sEMG patterns.

For each of the aforementioned five features, we extracted a 64-dimensional (64-D) feature vector with each dimension representing one specific channel. Then we concatenated all five features to obtain a 320-D (64×5) feature vector. The concatenated feature vector contains the information of the original signal in the time–frequency–space domain at the macroscopic level.

B. Macroscopic Matching Score Calculation

For the proposed neuromuscular password, the calculation of matching score used for user authentication takes two factors into consideration: 1) HD-sEMG patterns of different tasks in FMICP to verify the matching degree of FMICP and 2) HD-sEMG characteristics of different subjects to verify the matching degree of neuromuscular biometrics. At the macroscopic level, we integrated the two parts into one process. For each subject (the user), a random forest classifier was trained due to the high feature dimensionality, to discriminate patterns of different tasks using data of that specific subject from the training session (session 1). For new data of the user or impostors (the remaining 21 subjects serve as the imposters), an 8-D score vector $[s_A, s_B, \ldots, s_H]$ was calculated by the classifier for the active segment of each task, where $s_X, X \in \{A, B, \ldots, H\}$ refers to the probability that the true symbol of the input data is X. Then, the matching score of that signal segment was calculated according to the following formula:

$$S(i) = \frac{1}{2} s_{\text{true}} + \frac{1}{2M} \sum_{j=1}^{M} s_{\text{relevant}}(j) \tag{1}$$

where $i \in \{1, 2, \ldots, 8\}$ is the task index, s_{true} is the score of the true symbol (i.e., what symbol the input data should be), and s_{relevant} is the score set of all relevant symbols. M is the size of s_{relevant}. For example, if the true symbol is "B" (isometric contraction of index finger muscles), then $s_{\text{true}} = s_B$ and $s_{\text{relevant}} = [s_F, s_G]$ because the index finger is involved in tasks corresponding to both "F" and "G." Another example is that if the true symbol is "H," then $s_{\text{true}} = s_H$ and $s_{\text{relevant}} = [s_C, s_D, s_E]$ because the task corresponding to symbol "H" is the combination of the fingers corresponding to symbols "C," "D," and "E." Due to the similar patterns between the true and relevant symbols, the score of the true symbol is partly distributed to the relevant fingers to some extent. Therefore, the s_{relevant} term in (1) is introduced to increase the robustness of the matching score. The obtained score of the ith task can be viewed as a soft score, which measures the similarity between the input and signals corresponding to the true symbol in the training set, instead of rigidly classifying the input task into a specific symbol. For impostors, the score of each input task is expected to be lower than that of the user due to the different characteristics of HD-sEMG signals, thereby preventing the impostor's access to the neuromuscular password. The final matching score S_{macro} at the macroscopic level is the average of scores of all input tasks: $S_{\text{macro}} = \frac{1}{8}\sum_{i=1}^{8} S(i)$.

C. Microscopic Feature Extraction

A significant breakthrough of HD-sEMG electrode arrays is to shift the perspective of signal analysis from the macroscopic to the microscopic level. In this work, we also employed neural information at the microscopic level as part of the neuromuscular biometrics. Since the global sEMG is the summation of hundreds of independent motor unit action potentials (MUAPs), the MU spike trains can be obtained through HD-sEMG decomposition using ICA. Performance comparison of several ICA algorithms on sEMG decomposition has been investigated in previous work [12]. In this article, fast ICA was selected due to its high computational efficiency [12]. The application of ICA in sEMG decomposition can be found in [11]. Here, we give the main steps of sEMG decomposition, shown as follows.

1) Stack the original sEMG signal and eight delayed signal copies with one more delayed sample in each copy [11]. The number of sEMG channels is extended from 64 to 576.
2) Whiten the extended 576-channel sEMG signal through eigenvalue decomposition.
3) Apply fastICA to the whitened sEMG signal to obtain the independent sources corresponding to different MUs.
4) Perform peak detection and *k*-means clustering to identify discharge timings (spike train) of each individual MU.
5) Remove the duplicate MUs. ICA-based sEMG decomposition algorithm may converge repetitively to both the same MU and its delayed replicas due to limitations of the algorithm itself or the extension operation in step 1). If two decomposed MUs share more than 50% synchronized discharge events within a ±1 ms match window after delay compensation, then remove the one with a lower Silhouette distance value (SIL) [12]. It has been reported that the SIL value, representing the index value of the *k*-means clustering step, shows a positive correlation with decomposition accuracy [12].

Following the steps above, the global HD-sEMG is decomposed into different MU spike trains. Then, we pooled all these MUs together into one aggregative spike train. The FR of the aggregative spike train during each 3-s period of the eight tasks and the average FR across all of the eight tasks were extracted to construct a 9-D feature vector.

D. Microscopic Matching Score Calculation

Due to the relatively low feature dimensionality, the 9-D microscopic features extracted from the whole period of neuromuscular password entry was considered as an entirety. Therefore, the microscopic feature was not used for task pattern classification, since the labels of eight tasks were combined. Instead, we aimed to give a description of the feature distribution of the specific subject (the user) in the 9-D feature space. Given a new feature vector, either from the user or impostors, we gave a matching score through comparison with the feature distribution. To this end, the support vector domain description (SVDD) [16], also known as "one-class support vector machine," was used to characterize the feature distribution. SVDD was proposed to estimate the underlying distribution of a particular dataset. A spherically shaped boundary of the training dataset can be constructed by finding several support vectors. The principle of SVDD is introduced in brief.

For a dataset $\{\mathbf{X}_i\}_{i=1}^{N}$, where N is the dataset size, a sphere with the minimum volume that contains all data is required as the description to characterize the data distribution. However, this procedure is normally sensitive to outliers. One outlying sample can lead to a sphere with a large volume, which cannot characterize the data distribution perfectly. SVDD can address this issue by introducing slack variables ξ_i, allowing a couple of remote samples outside the obtained sphere boundary. To obtain the sphere boundary with center C and radius R, the objective function takes the following form:

$$\begin{aligned} &\min_{\xi_i, R, C} \; R^2 + \lambda \sum_{i=1}^{N} \xi_i \\ &\text{s.t.}\, (X_i - C)^T (X_i - C) \le R^2 + \xi_i \\ &\text{s.t.}\, \forall_i, \xi_i \ge 0. \end{aligned} \tag{2}$$

The two terms in the objective function (2) quantify the volume of the obtained sphere and the number of rejected outliers, respectively. λ acts as a tradeoff parameter between the two terms. According to the first constraint, a larger *R* can result in a smaller ξ, which means fewer samples are outside the sphere boundary. The detailed optimization procedure can be found in [16]. Note that the data may not be spherically distributed. Therefore, to obtain a compact boundary that can characterize the data distribution accurately using a sphere, the above procedure in the original input space can be generalized to other kernel spaces. In this work, a Gaussian kernel space was selected. Previous study [16] has reported that the performance of SVDD is not sensitive to different choices of parameter λ. In our work, $\lambda = 0.25$, the same choice as [16], was selected.

For a testing sample, the distance from the sample to the center of the hypersphere obtained by SVDD was calculated, denoted by d. The matching score at the microscopic level was assigned by $S_{\text{micro}} = 1/d$. The final integrated matching score was given as: $S_{\text{integrated}} = (S_{\text{micro}})^{S_{\text{macro}}}$. Because S_{macro} was smoothed by taking the average of s_{true} and s_{relevant} as the matching score, as shown in formula (1), the fluctuations of S_{macro} are relatively low, compared with S_{micro} given directly by SVDD. Therefore, we selected the exponential form, $(S_{\text{micro}})^{S_{\text{macro}}}$, to integrate the matching scores from the macrolevel and microlevel, thus balancing the contribution of the two scores. This exponential form is equivalent to the following logarithmic form: $S_{\text{integrated}} = S_{\text{macro}} \ln(S_{\text{micro}})$, where the contribution of S_{micro} is weakened by the natural logarithm.

E. Validation Methodologies

1) Feature Quantification: We quantified both the macroscopic and microscopic features, to intuitively show the distribution of HD-sEMG features within and across individuals during each isometric contraction task. At the macroscopic level, due to the high dimensionality of the feature space, we selected the centroid location of the 2-D RMS map as the representation

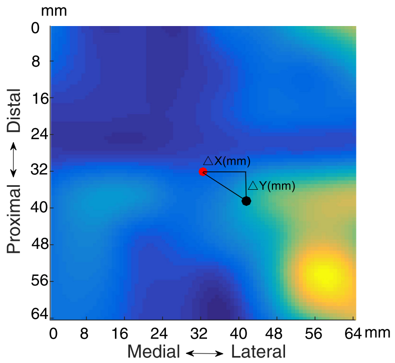


Fig. 4. 2-D RMS map of ring finger.
Note: The red and black points are the center and centroid of the RMS map, respectively. The RMS map was up-sampled from 8×8 to 80×80 through bicubic interpolation to obtain a sufficient resolution for visualization.

of HD-sEMG spatial activation pattern. The 2-D RMS map was constructed by RMS features in all channels of the 8×8 HD-sEMG electrode array. An example 2-D RMS map is shown in Fig. 4. The centroid location represented by the distance of the centroid from the center in the X-axis and Y-axis (ΔX and ΔY, as shown in Fig. 4) depicts the activation pattern of all HD-sEMG channels. At the microscopic channel, we also quantified the FR features. Data from sessions 1 and 2 acquired on different days were used to obtain the distribution of features within and across individuals.

To quantify the difference of features across different finger muscle contraction tasks, one-way analysis of variance (ANOVA) was performed on features during individual finger muscle contractions (symbols A–E without F–H). Before ANOVA, we performed Lilliefors test to validate that the data of each contraction task followed a Gaussian distribution. Bartlett's test was also performed to ensure that all these Gaussian distributions have the same variance. Posthoc pairwise tests were applied if statistical significance was observed.

2) Validation Protocols: In this work, we designed five validation protocols to evaluate the proposed neuromuscular password.

Protocol 1: The goal of this protocol is to evaluate the potential of the proposed system when the impostors do not know the FMICP. For each subject (user), we selected data in session 1 as the training set. User's data in session 2 (same FMICP) and impostors' (the remaining 21 subjects) data in session 3 (different FMICP) were used as the testing set. This protocol can simulate the scenario when the users enter the correct FMICP and impostors enter the wrong one.

Protocol 2: This protocol is an extension of protocol 1, to evaluate the potential of the proposed system in a more realistic scenario. In real-life situations, impostors can choose an arbitrary sequence (besides the predefined ones) as FMICP to intrude a system. Accordingly, in this protocol, we randomly resequenced the order of all eight tasks within each trial in session 3. For each subject (user), we selected data in session 1 as the training set. User's data in session 2 (same FMICP) and impostors' (the remaining 21 subjects) data in session 3 (different FMICP after randomly resequencing the task order in each trial) were used as the testing set. This protocol can simulate a more realistic scenario where users enter the correct FMICP and impostors enter an arbitrary one.

Protocol 3: The goal of this protocol is to evaluate the potential of the proposed system when the impostors enter the correct FMICP. For each subject (user), we selected data in session 1 as the training set. Data of both the user and impostors (the remaining 21 subjects) in session 2 (same FMICP) were used as the testing set.

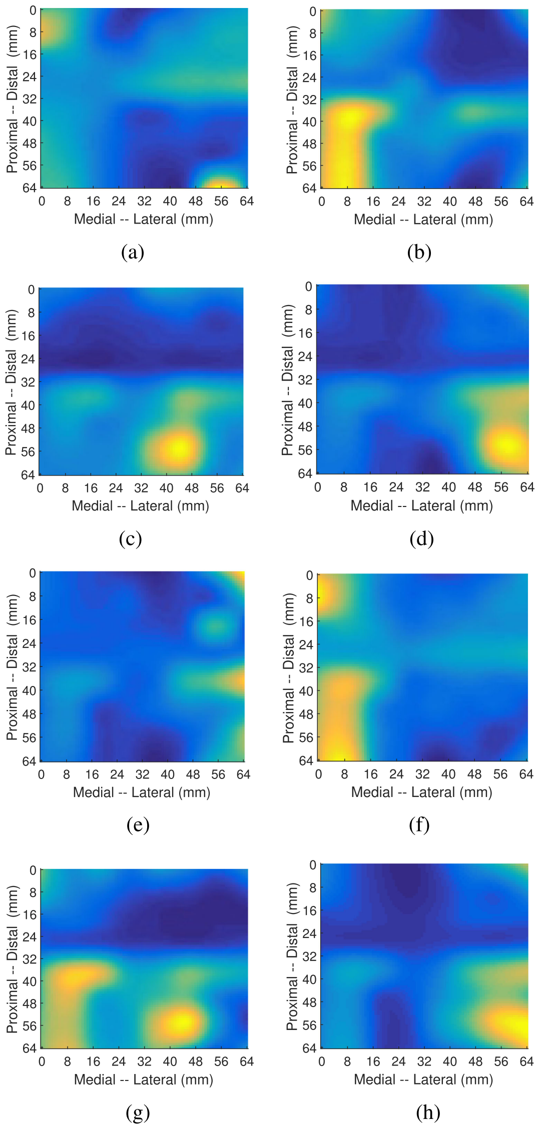
Protocol 4: The goal of this protocol is to evaluate the cancelability of the proposed system when the neuromuscular password including both FMICP and neuromuscular biometrics is stolen. As aforementioned, the user can replace the previous neuromuscular password by simply changing into a new FMICP. For each subject (user), we selected data in session 1 as the training set. Data from the same user in session 2 (same FMICP) and session 3 (different FMICP) were used as the testing set and assigned to the label "user" and "impostor," respectively.

Protocol 5: This protocol is an extension of protocol 4, to evaluate the cancelability of the proposed system in a more realistic scenario, where the FMICP of the compromised neuromuscular password can be any arbitrary sequence instead of exactly the predefined one. In this protocol, we randomly resequenced the order of all eight tasks within each trial in session 3, but keep the randomly resequenced task order different from that of sessions 1 and 2. We did so, because in realistic scenarios the compromised and replaced FMICPs would be different. For each subject (user), we selected data in session 1 as the training set. Data from the same user in session 2 (same FMICP) and session 3 (different FMICP via randomly resequencing the task order) were used as the testing set and assigned to the label "user" and "impostor," respectively.

Since data of session 1 were acquired nine days (on average) before sessions 2 and 3, each of the five protocols takes signal variation across different days into consideration.

3) Performance Evaluation Metrics: User authentication systems usually make two types of mistakes, namely false acceptance, which means the system accepts an impostor, and false rejection, which means the system rejects the user. Accordingly, we used false acceptance rate (FAR) and false rejection rate (FRR) as evaluation metrics. The equal error rate (EER), i.e., the FAR when FAR=FRR, was also employed as an evaluation metric.

4) Chaotic Property Evaluation Metrics: Chaotic property is an essential factor to evaluate the security of a biometric modality. A chaotic biometric modality is difficult to reproduce and robust to brutal attack. The chaotic property of biometrics can be evaluated via entropy analysis, with a higher entropy contributing to a more chaotic biometric modality. Because the brutal attack can be launched in the domain of either the original HD-sEMG signals or the extracted features, we analyzed the chaotic property of both signal and feature domains using Shannon entropy. We first quantized the amplitude range of a sample sequence (HD-sEMG signals or features). A larger number of quantized bits contribute to a higher entropy. To avoid overevaluation of the chaotic property, we quantized the HD-sEMG signals and the extracted features using only 8 bits (256 discrete values). The Shannon entropy is given by $-\sum_{\epsilon} p_{\epsilon}\log_2 p_{\epsilon}$, where p_{ϵ} is the frequency of the ϵth discrete value of the quantized sample sequence, $\epsilon \in \{1, 2, \ldots, 256\}$. Then, the success chance of each attempt in brutal attack was calculated by $1/2^{E\times L}$, where



(a) (b) (c) (d) (e) (f) (g) (h)

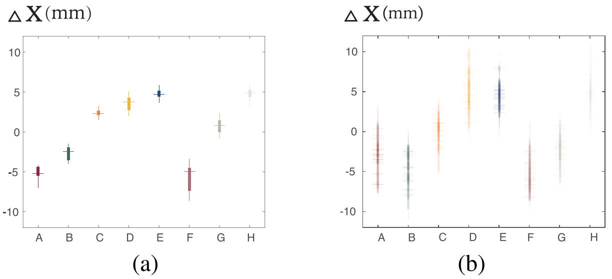
Fig. 5. RMS maps of different fingers (and combinations). (a) Thumb finger. (b) Index finger. (c) Middle finger. (d) Ring finger. (e) Little finger. (f) Combination of thumb and index finger. (g) Combination of index and middle finger. (h) Combination of middle, ring, and little finger.

E and L are the Shannon entropy and sample number of the sequence (the HD-sEMG signal or feature vector).

IV. Results

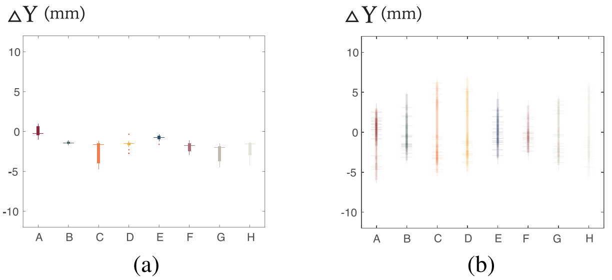
A. Quantification of Macroscopic and Microscopic Features

At the macroscopic level, the representative RMS maps of all contraction tasks are shown in Fig. 5. The centroid distribution for a representative subject (subject 2) in the X-axis (ΔX) and Y-axis (ΔY) is shown in Figs. 6(a) and 7(a), respectively. Also, the overlap of centroid distribution for all subjects in the X-axis (ΔX) and Y-axis (ΔY) is shown in Figs. 6(b) and 7(b), respectively. The mean and standard deviation values of data shown in Figs. 6 and 7 are presented in Table I. We find that the centroid locations of RMS map in the X-axis (the medial-lateral direction) are visibly separable for different tasks, as shown in Fig. 6. To further validate this claim, we calculated the average centroid location of data corresponding to each finger of each subject. ANOVA on all calculated average centroid locations of individual finger muscle contractions yielded $[F(4,105) = 156.9, p < 0.01]$. The posthoc pairwise tests achieved $p < 0.05$ for centroid location comparison between each finger pair in the X-axis except that between ring and little finger. ANOVA to compare the centroid location in the Y-axis showed no significant difference ($[F(4,105) = 1.7, p = 0.1559 > 0.05]$). The separability of different tasks (especially in the medial-lateral direction) allows pattern recognition between different FMICPs. Besides, as shown in Figs. 6(b) and 7(b), the centroid location in both X-axis and Y-axis varies greatly if the distributions of all subjects were overlapped, compared with those within a specific subject, shown in Figs. 6(a) and 7(a). The different characteristics of EMG signals across subjects have also been reported in previous studies [6]. The individual difference of sEMG at the macroscopic level makes it possible to identify a particular user.



(a) (b)

Fig. 6. Centroid distribution in the X-axis for all eight tasks. (a) Centroid distribution for a representative subject (ΔX). (b) Centroid distribution overlap for all subjects (ΔX).



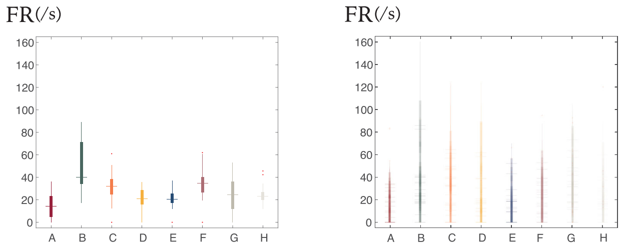
(a) (b)

Fig. 7. Centroid distribution in the Y-axis for all eight tasks. (a) Centroid distribution for a representative subject (ΔY). (b) Centroid distribution overlap for all subjects (ΔY).

At the microscopic level, we quantified FR during each of the eight tasks, as shown in Fig. 8. ANOVA on FR for symbols A–E achieved $[F(4,105) = 4.72, p < 0.01]$. The posthoc pairwise tests achieved $p < 0.05$ only for FR comparison between finger pairs thumb-index, thumb-middle, and index-little. Through a comparison between Fig. 8(a) and (b), the intersubject variation is much larger than that of intrasubject. Since all decomposed MUs were pooled as a composite discharge train, the FR value was largely determined by the number of decomposed MUs. Previous studies on HD-sEMG decomposition have shown a high deviation on the number of identified MUs across subjects [17]. Algorithms that attempt to reduce the intersubject variability in the number of identified MUs have been an

TABLE I
QUANTIFICATION RESULTS OF THE MACROSCOPIC FEATURES

Task Symbol	A	B	C	D	E	F	G	H
Centroid (ΔX) Within Subject (mm)	-5.12±0.74	-2.66±0.80	2.33±0.44	3.53±0.89	4.75±0.59	-5.76±1.71	0.77±0.96	4.80±0.69
Centroid (ΔX) Across Subjects (mm)	-3.28±2.04	-4.80±2.03	-0.03±1.71	5.27±2.36	4.45±1.66	-5.39±2.05	-2.60±1.79	5.02±1.97
Centroid (ΔY) Within Subject (mm)	-0.08±0.66	-1.42±0.15	-2.59±1.38	-1.61±0.57	-0.78±0.33	-1.93 ±0.55	-2.70±1.11	-2.12±1.00
Centroid (ΔY) Across Subjects (mm)	0.33±2.02	-0.67±1.79	-1.16±3.19	-0.91±3.00	-1.17±1.62	-0.44±1.35	-1.07±2.47	-0.97±3.04



(a) (b)

Fig. 8. Firing rate distribution for all eight tasks. (a) Firing rate distribution for a representative subject. (b) Firing rate distribution overlap for all subjects.

important topic in the literature for decades [18]. The high intersubject variability of identified MUs is due to the fact that the muscle structure of individuals is diverse for individuals, and only large and superficial MUs can be identified using HD-sEMG decomposition [19]. This property can be used as an advantage in user authentication field, as a complement to the macroscopic neuromuscular representations.

B. Performance Evaluation of Protocol 1

Through tuning the matching score threshold, we can obtain the average receiver operating characteristic (ROC) curve, as shown in Fig. 9(a). The EER values are 0.0102 and 0 using macrofeatures and macro–micro features, respectively. Most biometrics-based authentication systems are faced with one challenge: the similar characteristics between users and impostors. For the proposed method, besides the neuromuscular biometrics, users can add their unique characteristics through designing a unique FMICP. The zero EER using both macrofeature and microfeature with an average nine-day interval between training and testing sessions proves its high potential for user authentication.

C. Performance Evaluation of Protocol 2

Fig. 9(b) shows the ROC curve of protocol 2. When impostors enter a neuromuscular password with arbitrary FMICPs, the EER values using macrofeatures and macro–micro features are 0.0153 and 0.0128, respectively. Although the macro–micro features have not contributed to a zero EER, the EER of 0.0128 also shows the promising perspectives of the proposed neuromuscular password in a more realistic scenario.

D. Performance Evaluation of Protocol 3

Since the FMICP is entered through isometric contraction of finger muscles without actual movement, it is almost impossible for an impostor to steal the password. Even if the FMICP is stolen, the neuromuscular biometrics can still work as the second defense. Fig. 9(c) shows the performance of the proposed user authentication system when the impostors enter the correct FMICP. The EER values using macrofeatures and macro–micro features are 0.1543 and 0.1496, respectively. In the most challenging protocol 3, we further evaluated the necessity of using all six features by progressively increasing the feature number. As shown in Fig. 10, a continuing EER reduction was achieved when progressively adding sample entropy, spectral entropy, FMD, WL, RMS, and FR to the process of matching score calculation, demonstrating the necessity of all extracted macro–micro features. We also evaluated the authentication performance with different SNR values in the most challenging protocol 3. As aforementioned, the SNR of the acquired HD-sEMG signals is 8.58 dB. We added additional bandlimited white Gaussian noise (10–900 Hz, similar to the frequency band of sEMG signals) for the acquired signals to obtain signals with a desired SNR. As shown in Fig. 11, even with the 3-dB SNR, an EER of 0.1857 can be achieved using macro–micro features. These results further validate that the proposed method is robust to noise.

E. Performance Evaluation of Protocol 4

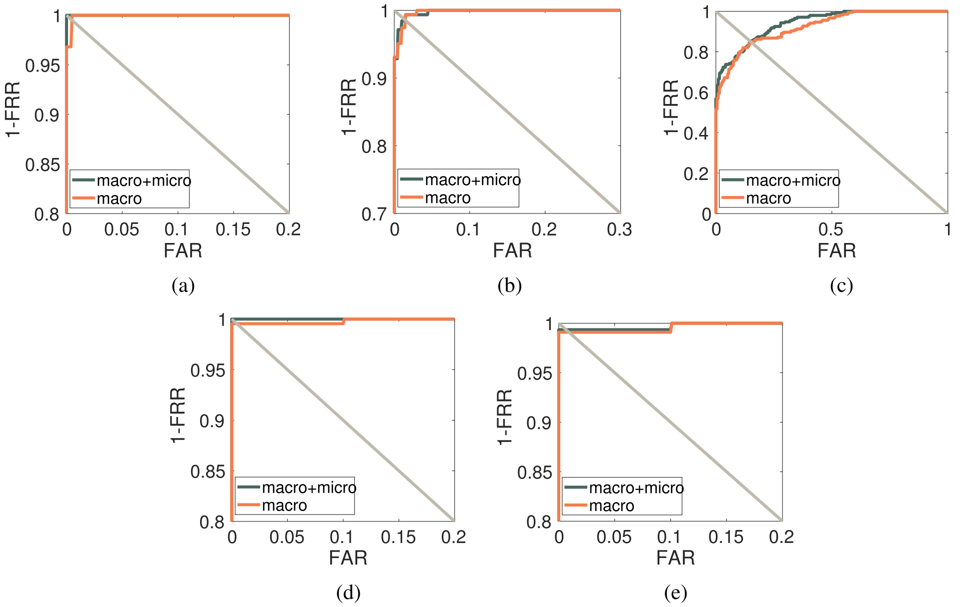
The ROC of protocol 4 is shown in Fig. 9(d). If the neuromuscular password is stolen, the user can simply change to a new FMICP to block the original one. The EER values of protocol 4 using macrofeatures and macro–micro level are 0.0065 and 0, respectively, demonstrating the high cancelability of the proposed neuromuscular password.

F. Performance Evaluation of Protocol 5

In realistic scenarios, the FMICP of the stolen neuromuscular password can be an arbitrary sequence instead of exactly the predefined one. When the stolen FMICP was randomly resequenced, we still achieved low EER values of 0.0093 and 0.0065, using macrofeatures and macro–micro features, respectively.

G. Chaotic Property of the Neuromuscular Password

The Shannon entropy of the proposed neuromuscular password (in both the signal domain and the feature domain) and the success chance of each attempt in brutal attack are shown in Table II. In the signal domain, the success chance of each attack attempt is only $1/2^{(1.06\times6.144\times10^6)}$, an extremely low chance value. Even in the feature domain, the success chance of each attack attempt is only $1/2^{(1.36\times10^4)}$. Note that the calculated success chance of attack is an estimated value. In practical situations, the number of quantization bits is usually larger than 8 bits, increasing the Shannon entropy of the quantized signals and features. With a larger number of quantization bits,



(a) (b) (c)

(d) (e)

Fig. 9. ROC curve of (a) protocol 1, (b) protocol 2, (c) protocol 3, (d) protocol 4, and (e) protocol 5.
Note: All of the five ROC curves are the average performance of all subjects. In (a)–(c), for each subject (the user), the remaining 21 subjects (session 3, session 3 (after resequencing), and session 2, respectively) were regarded as imposters. The ROC curves (a)–(c) take 22 users and $21 \times 21 = 441$ imposters into consideration. In (d) and (e), for each subject, data from sessions 2 (the same FMICP) and 3 (the different FMICP) of the same subject were assigned to the label user and imposter, respectively. Data from 21 users and 21 imposters were taken into consideration. The FAR of imposters and FRR of users were shown in *X*-axis and *Y*-axis, respectively. Also, note that we used different axis scales for ROC curves in different protocols.

TABLE II
Shannon Entropy and Success Chance of Each Attempt in Brutal Attack

	Signal Domain	Feature Domain					
	HD-sEMG Signal	Sample Entropy	Spectral Entropy	FMD	WL	RMS	FR
Shannon Entropy	1.06 bits/sample	6.81 bits/sample	6.35 bits/sample	2.74 bits/sample	5.33 bits/sample	5.27 bits/sample	6.01 bits/sample
Sample Number	6.144×10^6 samples (64 channels × 8 tasks × 3 seconds × 4000 Hz)	512 samples (64 channles × 8 tasks)	512 samples (64 channles × 8 tasks)	512 samples (64 channles × 8 tasks)	512 samples (64 channles × 8 tasks)	512 samples (64 channles × 8 tasks)	9 samples (8 tasks + 1 average FR)
Success Chance of Attack (Each Attempt)	$\frac{1}{2^{(1.06\times 6.144\times 10^6)}}$	$\frac{1}{2^{(6.81\times 512\,+\,6.35\times 512\,+\,2.74\times 512\,+\,5.27\times 512\,+\,5.33\times 512\,+\,6.01\times 9)}} = \frac{1}{2^{(1.36\times 10^4)}}$					

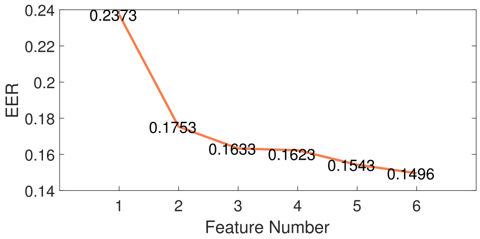


Fig. 10. Continuing EER reduction with progressively increasing feature numbers (progressively add sample entropy, spectral entropy, FMD, WL, RMS, and FR features).

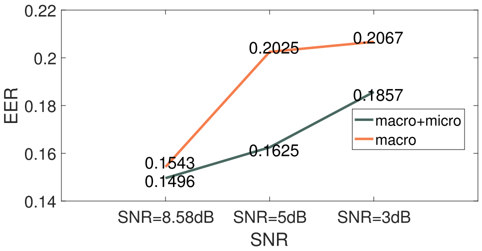


Fig. 11. EER variation with decreasing SNR.

the success chance to reproduce a neuromuscular password can be further reduced significantly. However, a larger number of quantization bits may also overestimate the chaotic property because impostors do not have to reproduce exactly the same (or high-resolution) signals or features. Accordingly, a low resolution with the quantization number of 8 was selected. Altogether, the chaotic property analysis indicates that brutal attack is almost impossible to precisely intrude the neuromuscular password-based authentication system.

H. Evaluation of Computational Efficiency

Here, we report the computation time of the processing pipeline for an individual trial. The computation time reported was the mean value of 100 repetitions (tested on: Intel(R)

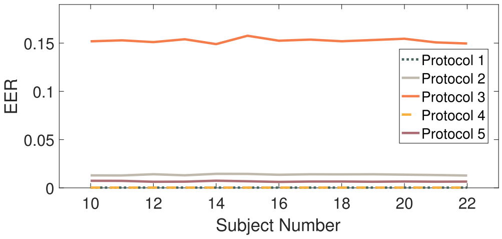


Fig. 12. EER variation with different number of subjects.

Xeon(R) CPU E5-2650 v2 @ 2.60 GHz). Specifically, the longest computation time of all dependent processing pipelines was reported. If several processing pipelines are independent (e.g., extraction of each macrofeature), they can be computed in parallel and the longest computation time is taken into consideration, thus reducing the time delay. The longest dependent processing pipeline of the proposed method is: ICA-based microfeature extraction for data of each 3-s task (1.9661 s) + microscopic matching score calculation (0.0033 s), with a total computational time of 1.9694 s. Considering the microfeatures of data acquired during each 3-s task were extracted separately in our work, a 1.9661-s (less than the 3-s task duration) computational time can satisfy the real-time microfeature extraction requirement of the successively acquired signals of each individual task. If using macrofeatures only, we achieved a total computation time of 0.9417 s.

I. EER Variation With Different Subject Numbers

To guarantee the reported performance is reliable using data from 22 subjects, we evaluated system performance using different numbers of subjects between 10 and 22. For subject numbers less than 22, the subjects were randomly selected and the average performance of 100 repetitions was reported. The plot of EER in each protocol versus subject number is shown in Fig. 12. As the subject number increases, the EER value remains stable. For user authentication, in contrast with person identification, the problem we are faced with is a binary classification task. No matter how many subjects are involved, the mathematical expectation of the result does not vary with the subject number. As the data volume increases, the results converge to the mathematical expectation of the true EER.

V. Discussion

A. Privacy Preservation of Neuromuscular Password

For a biometrics-based authentication system, preserving privacy is essential because the stolen biometric template can be used to track the user in other applications. One solution to address this issue is to apply a one-way function (such as hash functions) to transform the original biometric template to a protected one while reserving the discriminative information of users at the same time. Once the transformed template is stolen, a new function can be applied to encrypt the original biometric template. Since different applications employ different transform functions, the stolen transformed template in a specific application does not threaten the others. Besides, considering that reconstructing the original biometric template through the transformed one is impossible (or computationally difficult), the stolen template does not threaten users' privacy. For the proposed authentication method, we perform user authentication using extracted features. The one-way function (such as hash functions) can be applied to the extracted features to further encrypt the neuromuscular password. Moreover, due to the high cancelability of the proposed neuromuscular password, even if the original biometric template is stolen, users can replace the original one by simply changing to a new FMICP to avoid being tracked in other applications. In other words, the neuromuscular biometrics can be changed on users' choices, thus reducing the privacy risks of biometrics theft.

B. Comparison With Other Biometric Modalities

According to the above results, the proposed theft-resistant user authentication system shows high potentials in practical application scenarios. Although other biometrics based on other electrophysiological signals (e.g., EEG and ECG) are also theft-resistant, the proposed EMG-based biometrics show great advantages over the existing ones. First, ECG is noncancelable since the ECG variation cannot be volitionally controlled by users. Second, we compare the proposed approach with another biometrics modality—EEG. EEG-based biometrics have been extensively studied in the past twenty years [4], [20]. EEG signals can exhibit different characteristics under different mental states [21] so it is promisingly cancelable. There are two types of experimental setups in the literature, namely biased setup and rigorous setup. In a biased setup, the training and testing data are randomly selected from all obtained data regardless of the acquisition day. In this case, the validation procedure does not take data variation across days into account, leading to a greatly overestimated performance. In the worst case, the training and testing data may be acquired in the same session. The variation in experiment configuration, such as electrode position and background noise was not considered either. In the rigorous setup, the training and testing data were acquired on different days, so as to prove the robustness and feasibility of the systems. Since the rigorous setup was selected in our work, EEG-based user authentication systems using the same rigorous setup was taken as a comparison. Marcel and Millan [4] proposed a user authentication system based on EEG and maximum *a posteriori* model adaptation. Their EEG-based system employed data from multiple days in the training set and data from another day as the testing set, reducing the performance degradation due to signal variation across days. Their results showed an FRR of 24.9% and an FAR of 13.7%, evaluated by data acquired from nine subjects over three days. Comparatively, our system only collected data from one day for training. Even so, our results (protocol 3) show that the FRR is 16.8% at the same FAR. Furthermore, when only using training data from one day, their system achieved a poorer performance [4] with an FRR of 50.3% and an FAR of 19.6%. In addition, EEG acquisition is a cumbersome process for both experimenters and subjects. Therefore, data acquisition in several days is a heavy workload, which does not satisfy the "collectability" requirement for a user authentication system. Another EEG-based biometrics study [20] using rigorous setup employed a wearable in-ear EEG sensor with a relatively convenient configuration process, to fulfill the collectability requirement. The FRR was 32.2% at a FAR of 2.3% using 60-s EEG segments acquired from 15 subjects. Our proposed neuromuscular biometrics can achieve a 30.4% FRR at the same FAR. Therefore, the performance of our approach achieved a comparable and slightly better results in protocol 3 compared with EEG biometrics. Moreover, EER values of 0 and 0.0128 in

TABLE III
COMPARISON OF NEUROMUSCULAR PASSWORD AND OTHER BIOMETRIC MODALITIES

	DNA	Face	Fingerprint	Iris	ECG	EEG	Neuromuscular Password
Authentication Accuracy Across Days	Very High	High	High	High	Acceptable	Acceptable	High
Theft-Resistance	Low	Low	Low	Low	High	High	High
Cancelability	Low	Low	Low	Low	Low	Acceptable	High
User Protection	Low	Low	Low	Low	High	High	High
Convenience to Use	Low	High	High	High	Acceptable	Low	Acceptable
Protection of Users' Voluntariness	Low	Low	Low	Low	Low	Acceptable	High

protocols 1 and 2 demonstrate a significantly better performance compared with EEG.

The comparison of the proposed neuromuscular password and other widely studied biometric modalities regarding several important properties is shown in Table III. A more detailed discussion on the properties of the neuromuscular password is given as follows.

1) *Theft-resistant:* As aforementioned, the FMCIP is difficult to be stolen through peeping. Besides, the electrode array must be attached to the skin during HD-sEMG signal acquisition. Therefore, it is almost impossible for impostors to steal a user's neuromuscular biometrics without their knowledge. In contrast, biometrics like DNA, face, fingerprint, and iris can be easily stolen through a noncontact way. With the development of noncontact ECG measurement [22], ECG can also be easily stolen without direct contact with users.

2) *Cancelable:* The low EER values of protocols 4 and 5 demonstrate the excellent cancelability of the proposed authentication method. EEG has also shown its potential as a cancelable biometric modality because EEG signals show different characteristics under different intention-driven mental states (such as imaginary motion of the left and right hand) [21]. However, the classification of different mental states is quite challenging due to the low SNR of scalp EEG signals, limiting the cancelability of EEG biometrics in practical use.

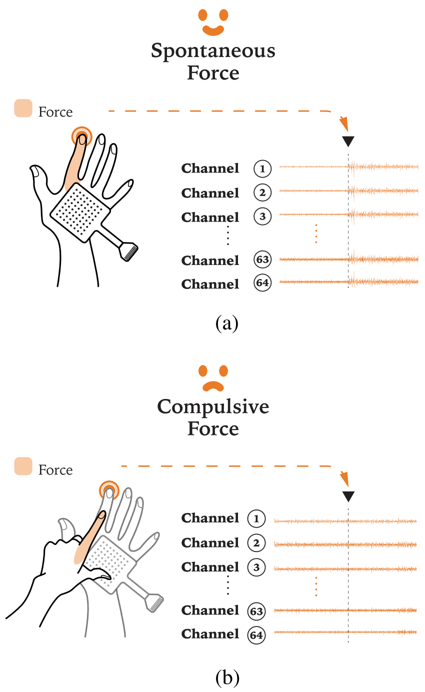
3) *Highly distinguishable:* By using neuromuscular biometrics together with FMICP, users can add their unique properties of their neuromuscular password.

4) *Robust over time:* The neuromuscular password achieved a low EER when testing the performance several days (nine days on average) later after model training.

5) *Capable to protect users:* EMG can be detected only when the user is alive.

6) *Convenient to use:* HD-sEMG signal acquisition is relatively convenient to set up compared with EEG. Besides, DNA measurement takes relatively longer time to achieve the result and requires high-cost and specialized equipment so it is also not convenient to be applied in daily life situations.

7) *Capable to ensure users' voluntariness:* For the majority of biometrics-based authentication systems, users can be forced to unlock the password. For example, the impostors can control the user's hand to obtain the fingerprint regardless of the user's voluntariness. In other words, there is no difference between a spontaneous fingerprint and a compulsive one. The issue also exists in biometrics such as face, iris, and DNA. However, sEMG can overcome this drawback. As shown in Fig. 13, we present the sEMG signals under spontaneous and compulsive force. Obviously, compulsive force cannot generate any sEMG signals. This is mainly due to the fact that sEMG is the summation of MUAPs generated from the muscle contraction. Accordingly, the proposed neuromuscular password is capable to ensure users' voluntariness. To a certain extent, EEG has also shown this superiority because users cannot be forced to perform any thinking activity to generate EEG signals under a specific mental state. However, the characteristics of baseline EEG and thinking activity EEG share a high similarity because our brain is engaged in countless background activities all the time. The difficulty to discriminate between baseline EEG and thinking activity EEG weakens the capacity of EEG biometrics to protect users' voluntariness.



(a)

(b)

Fig. 13. Comparison of HD-sEMG signals of (a) spontaneous force and (b) compulsive force.

8) *Convenient to be integrated with other modalities:* Considering that the neuromuscular password is based on HD-sEMG acquired only on the dorsum of the right hand, it is very convenient to achieve modality fusion with a fingerprint [2], finger vein [23], palm print [24], and neuromuscular password without data acquired from other body parts. For example, the acquisition of fingerprint, finger vein, palm print and HD-sEMG can be achieved by a wearable glove-like acquisition device. Considering an increasing number of wearable and wireless HD-sEMG acquisition devices have been developed by recent studies [25], the integration of these modalities is promising.

C. Future Work

The presented work has demonstrated promising prospects of our neuromuscular password. However, several important factors need to be investigated in the future.

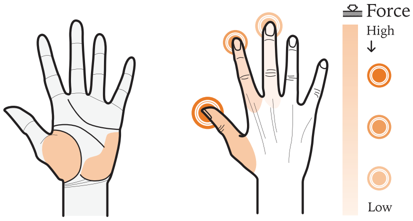


Fig. 14. Complex encoding of the neuromuscular password via (left) muscles other than finger flexors and (right) different force levels.

1) *Validate the proposed method on a larger number of subjects:* Although our subject size of 22 achieved reliable performance in this initial study (as shown in Fig. 12), validation on a larger number of subjects is still necessary before practical application. Moreover, validation on a more general population (e.g., both young and elderly subjects) is required in future studies.

2) *Investigate the performance of HD-sEMG of other body parts and isometric contraction patterns:* In our work, we chose to use HD-sEMG signals of the right dorsal hand as biometrics due to its convenience in practical use. The forearm is a good alternative choice. Actually, the extensor and flexor digitorum muscles controlling different fingers are located in the forearm [26]. Also, the activation pattern of muscle contractions corresponding to different fingers is quite distinguishable in the forearm [26]. As an initial study, we have investigated muscle isometric contractions of individual finger and several finger combinations. In practical situations, users can design a more complex pattern of finger forces. For example, users can perform isometric contraction of muscles controlling the palm, in addition to fingers, as shown in the left panel of Fig. 14. Moreover, the FMICP can be further encrypted through exerting different force levels for different fingers, as shown in the right panel of Fig. 14. Since the final decision of user authentication is given by the matching score based on the similarity of the entered neuromuscular password and the enrolled one, instead of rigidly classifying the entered patterns, a more complex FMICP pattern should not increase the pattern recognition difficulty, but enhance the robustness of the system.

3) *Investigate the authentication performance when reducing the time of each task and resting period between tasks:* This may contribute to a more convenient neuromuscular password in practical use.

4) *Investigate the fusion method of the proposed neuromuscular password and other modalities:* The development of effective frameworks for modality fusion is quite important and challenging for user authentication tasks, which may further enhance the robustness of the sEMG-based biometrics.

5) *Investigate the robustness of neuromuscular password against interference factors (e.g., emotion, temperature, body condition, and more types of noise):* Although HD-sEMG signals cannot be directly interfered by users' emotion and stress, such factors may influence authentication performance in an indirect way. External temperature and body conditions may also influence the performance. Herein, we only investigated the authentication performance of the proposed method in Gaussian noise with different SNR values. The interference of more types of noise remains a future work. Investigating all these factors is necessary before practical application of the proposed neuromuscular password.

VI. Conclusion

In this article, we proposed a novel user authentication paradigm based on neuromuscular password. The neuromuscular password consisted of two parts, namely the FMICP and neuromuscular biometrics, serving as double-layer defenses. Compared with traditional keyboard-based password, the FMICP was more secure since users could enter the password without any actual movement. Accordingly, impostors were almost impossible to steal the FMICP by inferring through the user's movement or shoulder surfing. Moreover, even if an impostor entered the correct FMICP, the neuromuscular biometrics, as the second defense, could still prohibit the impostor with its low EER. The neuromuscular password also possessed other superiorities, such as cancelability. Through validation on data acquired from 22 subjects across different days, the neuromuscular password-based user authentication system achieved an EER of 0.0128 using features at both the macroscopic and the microscopic level, indicating the high practical potential of the proposed authentication paradigm.

References

[1] C. Peng, N. Wang, J. Li, and X. Gao, "Re-ranking high-dimensional deep local representation for NIR-VIS face recognition," *IEEE Trans. Image Process.*, vol. 28, no. 9, pp. 4553–4565, Sep. 2019.

[2] Y. Xun, J. Liu, N. Kato, Y. Fang, and Y. Zhang, "Automobile driver fingerprinting: A new machine learning based authentication scheme," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 1417–1426, Feb. 2020.

[3] K. Wang and A. Kumar, "Toward more accurate iris recognition using dilated residual features," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 12, pp. 3233–3245, Dec. 2019.

[4] S. Marcel and J. R. Millan, "Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 743–752, Apr. 2007.

[5] C. L. P. Lim, W. L. Woo, S. S. Dlay, and B. Gao, "Heartrate-dependent heartwave biometric identification with thresholding-based GMM–HMM methodology," *IEEE Trans. Ind. Informat.*, vol. 15, no. 1, pp. 45–53, Jan. 2019.

[6] T. Matsubara and J. Morimoto, "Bilinear modeling of EMG signals to extract user-independent features for multiuser myoelectric interface," *IEEE Trans. Biomed. Eng.*, vol. 60, no. 8, pp. 2205–2213, Aug. 2013.

[7] 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, Mar. 2018.

[8] J. He and N. Jiang, "Biometric from surface electromyogram (sEMG): Feasibility of user verification and identification based on gesture recognition," *Frontiers Bioeng. Biotechnol.*, vol. 8, Feb. 2020, Art. no. 58.

[9] N. Belgacem *et al.*, "A novel biometric authentication approach using ECG and EMG signals," *J. Med. Eng. Technol.*, vol. 39, no. 4, pp. 226–238, May 2015.

[10] S. Venugopalan, F. Juefei-Xu, B. Cowley, and M. Savvides, "Electromyograph and keystroke dynamics for spoof-resistant biometric authentication," in *Proc. IEEE Conf. Comput. Vision Pattern Recognit. Workshops*, Boston, MA, USA, Jun. 2015, pp. 109–118.

[11] F. Negro *et al.*, "Multi-channel intramuscular and surface EMG decomposition by convolutive blind source separation," *J. Neural Eng.*, vol. 13, no. 2, Apr. 2016, Art. no. 026027.

[12] C. Dai and X. Hu, "Independent component analysis based algorithms for high-density electromyogram decomposition: Systematic evaluation through simulation," *Comput. Biol. Med.*, vol. 109, pp. 171–181, Jun. 2019.

[13] N. Nazmi *et al.*, "A review of classification techniques of EMG signals during isotonic and isometric contractions," *Sensors*, vol. 16, no. 8, Aug. 2016, Art. no. 1304.

[14] M. K. Butugan *et al.*, "Multichannel EMG-based estimation of fiber conduction velocity during isometric contraction of patients with different stages of diabetic neuropathy," *J. Electromyography Kinesiol.*, vol. 24, no. 4, pp. 465–472, Aug. 2014.

[15] A. Phinyomark *et al.*, "EMG feature evaluation for improving myoelectric pattern recognition robustness," *Expert Syst. Appl.*, vol. 40, no. 12, pp. 4832–4840, Sep. 2013.

[16] D. M. J. Tax and R. P. W. Duin, “Support vector domain description,” *Pattern Recognit. Lett.*, vol. 20, no. 11, pp. 1191–1199, Nov. 1999.

[17] T. Kapelner, F. Negro, O. C. Aszmann, and D. Farina, “ Decoding motor unit activity from forearm muscles: Perspectives for myoelectric control,” *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 26, no. 1, pp. 244–251, Jan. 2018.

[18] J. M. Shefner *et al.*, “Reducing intersubject variability in motor unit number estimation,” *Muscle Nerve*, vol. 22, no. 10, pp. 1457–1460, 1999.

[19] D. Farina *et al.*, “Decoding the neural drive to muscles from the surface electromyogram,” *Clin. Neurophysiol.*, vol. 121, no. 10, pp. 1616–1623, Oct. 2010.

[20] T. Nakamura, V. Goverdovsky, and D. P. Mandic, “In-ear EEG biometrics for feasible and readily collectable real-world person authentication,” *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 3, pp. 648–661, Mar. 2018.

[21] Y. Jiao *et al.*, “Sparse group representation model for motor imagery EEG classification,” *IEEE J. Biomed. Health Informat.*, vol. 23, no. 2, pp. 631–641, Mar. 2019.

[22] S. Peng *et al.*, “Comparison of active electrode materials for non-contact ECG measurement,” *Sensors*, vol. 19, no. 16, Jan. 2019, Art. no. 3585.

[23] W. Yang, S. Wang, J. Hu, G. Zheng, J. Yang, and C. Valli, “Securing deep learning based edge finger vein biometrics with binary decision diagram,” *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4244–4253, Jul. 2019.

[24] L. Fei, B. Zhang, Y. Xu, D. Huang, W. Jia, and J. Wen, “Local discriminant direction binary pattern for palmprint representation and recognition,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 30, no. 2, pp. 468–481, Feb. 2020.

[25] G. L. Cerone, A. Botter, and M. Gazzoni, “A modular, smart, and wearable system for high density sEMG detection,” *IEEE Trans. Biomed. Eng.*, vol. 66, no. 12, pp. 3371–3380, Dec. 2019.

[26] C. Dai and X. Hu, “Extracting and classifying spatial muscle activation patterns in forearm flexor muscles using high-density electromyogram recordings,” *Int. J. Neural Syst.*, vol. 29, no. 1, Jun. 2018, Art. no. 1850025.