Enhancing IoT Security via Cancelable HD-sEMG-based Biometric Authentication Password, Encoded by Gesture

Xinyu Jiang, Xiangyu Liu, Jiahao Fan, Xinming Ye, Chenyun Dai*, *Member, IEEE*, Edward A Clancy, *Senior Member, IEEE*, Dario Farina, *Fellow, IEEE*, and Wei Chen*, *Senior Member, IEEE*

***Abstract*—Enhancing information security via reliable user authentication in wireless body area network (WBAN)-based Internet of Things (IoT) applications has attracted increasing attention. The noncancelability of traditional biometrics (e.g. fingerprint) for user authentication increases the privacy disclosure risks once the biometric template is exposed, because users cannot volitionally create a new template. In this work, we propose a cancelable biometric modality based on high-density surface electromyogram (HD-sEMG) encoded by hand gesture password, for user authentication. HD-sEMG signals (256 channels) were acquired from the forearm muscles when users performed a prescribed gesture password, forming their biometric token. Thirty four alternative hand gestures in common daily use were studied. Moreover, to reduce the data acquisition and transmission burden in IoT devices, an automatically generated password-specific channel mask was employed to reduce the number of active channels. HD-sEMG biometrics were also robust with reduced sampling rate, further reducing power consumption. HD-sEMG biometrics achieved a low equal error rate (EER) of 0.0013 when impostors entered a wrong gesture password, as validated on 20 subjects. Even if impostors entered the correct gesture password, the HD-sEMG biometrics still achieved an EER of 0.0273. If the HD-sEMG biometric template was exposed, users could cancel it by simply changing it to a new gesture password, with an EER of 0.0013. To the best of our knowledge, this is the first study to employ HD-sEMG signals under common daily hand gestures as biometric tokens, with training and testing data acquired on different days.**

***Index Terms*—biometrics, user authentication, IoT, HD-sEMG, pattern recognition.**

I. Introduction

With the rapid development of wireless body area network (WBAN)-based Internet of Things (IoT) in smart environment [1] and Internet of Medical Things (IoMT) in smart healthcare [2], the demand for reliable user authentication has been soaring in recent years. Authentication tokens encrypted via "what the user knows" (e.g. password) and "what the user has" (e.g. ID card) are very easy to reproduce for impostors once related tokens are exposed. Authentication via "what the user is" (e.g. biometrics, such as DNA, face and fingerprints) are more challenging to blindly replicate and thus intruding the authentication system is relatively more complex. However, traditional biometric tokens such as face recognition, voice and gait, are still naturally exposed to impostors while others, such as DNA and fingerprint, can be easily recorded by impostors without the user's knowledge. Moreover, most traditional biometrics are noncancelable. Once the biometric template is exposed to impostors, it is permanently compromised because the user cannot create a new template. Employing physiological signals acquired directly by WBAN devices in an IoT environment as biometric tokens, such as the electroencephalogram (EEG) [3] and electrocardiogram (ECG) [2], can mitigate the above risks because EEG and ECG are relatively difficult to expose. However, EEG acquisition is a relatively cumbersome procedure, currently impractical for authentication in real-life situations. Besides, ECG is sensitive to heart rate variations caused by environmental and physiological factors, which are not under the users' volitional control. Accordingly, ECG is still not an established cancelable biometric modality.

The inter-individual differences in surface electromyogram (sEMG) signals have long been a challenge in multi-user human-machine interfacing (HMI) [4], indicating its potential as a biometric modality. Moreover, EMG has been widely applied in WBAN-based IoT and IoMT applications. Rescio et al. [5] developed a sEMG-based pre-fall detection system. EMG-based gesture recognition techniques have also been embedded in a wearable interaction system for mobile devices [6]. Besides, with the advancement of portable and wearable high-density sEMG (HD-sEMG) acquisition systems [7], [8], muscle activity can be sampled with a sufficient spatial resolution for IoT-based smart environments. Accordingly, employing sEMG signals acquired directly by such wearable WBAN devices in IoT applications for user authentication is an efficient approach. Our previous work [9], for the first time, employed HD-sEMG as a biometric token, and proved the excellent cancelability of HD-sEMG signals [10], [11]. HD-sEMG signals acquired from the right dorsal side of the

Xinyu Jiang, Jiahao Fan, Chenyun Dai and Wei Chen are with the Center for Intelligent Medical Electronics, School of Information Science and Technology, Fudan University, Shanghai 200433, China.

Xiangyu Liu is with School of Art Design and Media, East China University of Science and Technology, Shanghai 200237, China.

Xinming Ye is with School of Sports Science and Engineering, East China University of Science and Technology, Shanghai 200237, China.

Edward A. Clancy is with Department of Electrical and Computer Engineering, Worcester Polytechnic Institute, Worcester, MA 01609, USA.

Dario Farina is with Department of Bioengineering, Imperial College London, SW7 2AZ, London, UK.

*Corresponding authors: Chenyun Dai (chenyundai@fudan.edu.cn), Wei Chen (w_chen@fudan.edu.cn)

This work is supported by National Key R&D Program of China (Grant No. 2017YFE0112000), Shanghai Pujiang Program (Grant No. 19PJ1401100) and Shanghai Municipal Science and Technology Major Project (Grant No. 2017SHZDZX01).

Manuscript received XX XX, XXXX; revised XX XX, XXXX.

hand during isometric contractions of muscles corresponding to a specific finger and finger combinations, were used as biometric tokens. If a biometric token is exposed, the users can replace it by changing muscle activations corresponding to another finger combination. Nonetheless, this previous work was limited by the use of isometric contractions, which are not a natural or comfortable way for users to generate sEMG signals. Using sEMG signals under more natural, dynamic hand gestures would contribute to the translation of this approach to daily IoT application scenarios where convenience of use is a key factor. EMG generated by hand gestures or motions has been used as biometrics in previous studies [12], [13], [14]. However, the training and testing data in these studies were not acquired on different days. Accordingly, inter-day variation of signal characteristics and inter-session electrode shift were not taken into account. Both factors are significant concerns for biometrics based on physiological signals.

In this work, we substantially advance sEMG biometrics with respect to those found in the literature by: (1) First, a diversity of 34 alternative hand gestures in common daily use was included in our gesture pool to generate sEMG signals. Dynamic contractions, compared with isometric contractions, are more natural and comfortable for the users, thus increasing the applicability in daily IoT applications. (2) Second, 256-channel HD-sEMG signals were acquired from muscles of the right forearm. Compared with HD-sEMG from the dorsal side of the hand used in our previous work [10], HD-sEMG signals acquired from the forearm are more informative as they capture the activity of extrinsic hand/wrist muscles active in most daily hand gestures. Signals acquired from 256 channels also provide high-resolution muscle activation information compared with traditional sEMG [12], [13], [14]. (3) Third, HD-sEMG signal acquisition can be implemented via integrated electrode arrays which are more convenient to wear than multiple separate conventional sEMG electrodes. (4) Fourth, to reduce the data acquisition and transmission burden in IoT devices, an automatically generated password-specific channel mask was employed to reduce the number of active channels. We also observed that the HD-sEMG biometric template is robust to reduced temporal sampling rate, which reduces power consumption. (5) Further, we also evaluated the security strength of HD-sEMG biometrics via password entropy analysis, demonstrating the high security of HD-sEMG against brutal attack. (6) Last, the training and testing data in our work were acquired on different days (separated by an 8.5 day interval, on average). Even in this cross-day validation, the HD-sEMG differences can be protective for authentication, both when the impostors know the gesture password and when impostors enter a random gesture password. The obtained results in the present work redefine the current state-of-the-art in sEMG biometric authentication.

II. Description of Experiment and Dataset

A total of 20 subjects (12 males, 8 females; aged 22 to 34 years) participated in the experiment. Each subject was informed about the research purpose and experiment procedure. Written informed consent was signed by all subjects. The experiment was reviewed and approved by the ethics committee of Fudan University (approval number: BE2035).

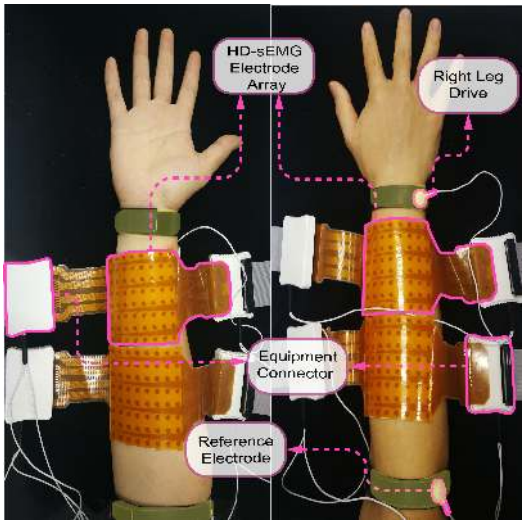


Fig. 1: Electrode placement

Before the experiment, the right forearm was cleansed with abrasive gel. To reduce the skin-electrode impedance, the subject's forearm was then wiped using an alcohol pad. Four 8×8 electrode arrays (Adhesive Matrix ELSCH064NM1, OT Bioelettronica, Torino, Italy) were used to acquire the 256-channel HD-sEMG signals from the forearm. Each gelled electrode in the array is elliptical in shape (5-mm major axis, 2.8-mm minor axis) with 10-mm center-to-center inter-electrode distances. The extensor and flexor muscles were each covered by two arrays, as shown in Fig. 1, forming combined 16×8 electrode arrays for each muscle group. For each subject, we labeled an area on each side of the forearm (extensor and flexor muscles) via anatomical landmarks to place the electrode array. The left and right boundaries of the labeled area were set to the radial and ulnar aspects of the forearm. The distal and proximal boundaries of the labeled area were set to the head of the ulna and the humeroulnar joint. We then aligned the center of the combined 16×8 electrode array with the center of the labelled area. The long axis of the array was placed along the long axis of the forearm. The right leg drive electrode was placed on the head of the ulna. The reference electrode of the acquisition device was placed on the elbow. The HD-sEMG signals were acquired using the Quattrocento system (OT Bioelettronica, Torino, Italy), with a passband of 10–500 Hz, a sampling rate of 2048 Hz, a resolution of 16 bits, and a gain of 150.

During the experiment, subjects sat on a comfortable chair, watching the experiment instructions shown on the computer screen in front of them. Subjects were queued to perform 34 hand gestures in common daily use activating one or multiple degrees of freedom (DoFs), using their most comfortable effort levels. The gestures were the following: (1) thumb extension, (2) index finger extension, (3) middle finger extension, (4) ring finger extension, (5) little finger extension, (6) wrist flexion, (7) wrist extension, (8) wrist radial, (9) wrist ulnar, (10) wrist pronation, (11) wrist supination, (12) thumb + index finger extension, (13) index finger + middle finger extension, (14)

Fig. 2: The 34 gestures used in the experiment.

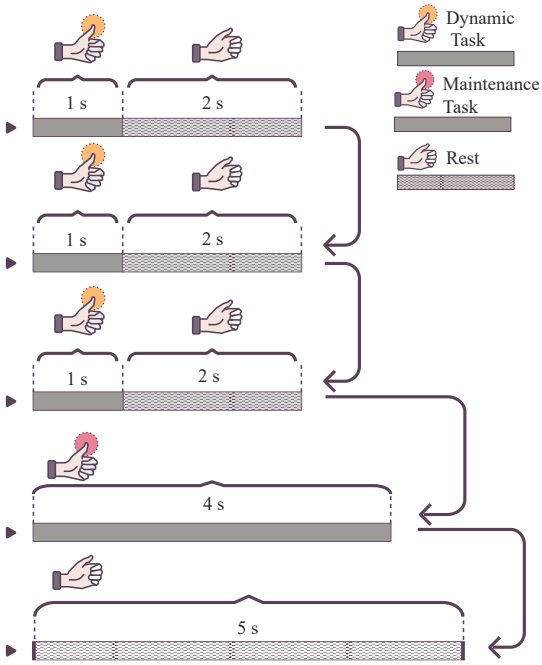


Fig. 3: Schematic sequence diagram of each trial.

wrist flexion + hand close, (15) wrist extension + hand close, (16) wrist radial + hand close, (17) wrist ulnar + hand close, (18) wrist pronation + hand close, (19) wrist supination + hand close, (20) wrist flexion + hand open, (21) wrist extension + hand open, (22) wrist radial + hand open, (23) wrist ulnar + hand open, (24) wrist pronation + hand open, (25) wrist supination + hand open, (26) thumb + index finger + middle finger extension, (27) index finger + middle finger + ring finger extension, (28) middle finger + ring finger + little finger extension, (29) index finger + middle finger + ring finger + little finger extension, (30) hand close, (31) hand open, (32) thumb + index finger pinch, (33) thumb + index finger + middle finger pinch, (34) thumb + middle finger pinch. Subjects were asked to not activate any muscles not involved in the queued task. The hint pictures of the above gestures are shown in Fig. 2. Subjects performed two trials for each gesture and then

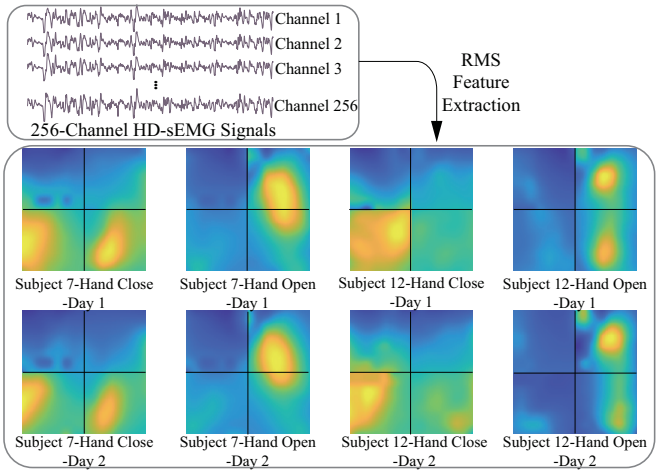


Fig. 4: Examples of HD-sEMG signals and the converted RMS maps of 2 representative subjects (subjects 7 and 12) under 2 hand gestures (hand close and hand open) on 2 days. The RMS maps were computed from all 256 channels in the 16×16 electrode array. The 16×16 electrode array was formed by four 8×8 electrode arrays. The upper left, lower left, upper right and lower right 8×8 electrode arrays of each 16×16 electrode array in this figure correspond to the upper left, lower left, upper right and lower right 8×8 electrode arrays in Fig. 1, respectively. Each single 8×8 electrode array was up-sampled to 100×100 through bicubic interpolation to obtain a sufficient resolution for better visualization.

continued to the next gesture. The gestures were performed following the order shown in Fig. 2. In each trial, three 1-s dynamic tasks (moving from the relaxed state to the target gesture) and one 4-s gesture maintenance task (moving from the relaxed state to the target gesture and then maintaining that specific target gesture) were performed with a 2-s inter-task resting period, as shown in Fig. 3. A 5-s inter-trial resting period was provided. The data acquisition procedure takes about 20 minutes totally. For each subject, HD-sEMG signals during 204 (34 gestures $\times$ 2 trials $\times$ 3 tasks) dynamic tasks and 68 (34 gestures $\times$ 2 trials $\times$ 1 task) maintenance tasks were acquired. Subjects were asked to inform the laboratory assistant if they missed a task or performed a wrong task. The missed or wrong tasks were removed from the dataset. On average, 2.30 $\pm$ 2.71 out of 204 (1.13%) dynamic tasks and 0.85 $\pm$ 1.05 out of 68 (1.25%) maintenance tasks were removed. HD-sEMG signals were acquired in two sessions on different days (interval: from 3 days to 25 days with an average of 8.50 $\pm$ 6.72 days) for each subject. Sessions 1 and 2 were used as training and testing dataset, respectively. Fig. 4 presents examples of acquired HD-sEMG signals and the converted root mean square (RMS) maps of 2 representative subjects (subjects 7 and 12) under 2 hand gestures (hand close and hand open) on 2 days. The RMS maps show a similar pattern for the same subject under the same hand gesture, but vary with either different subjects or different hand gestures, indicating the feasibility of HD-sEMG based user authentication encoded by hand gestures. Therefore, a feasible authentication method

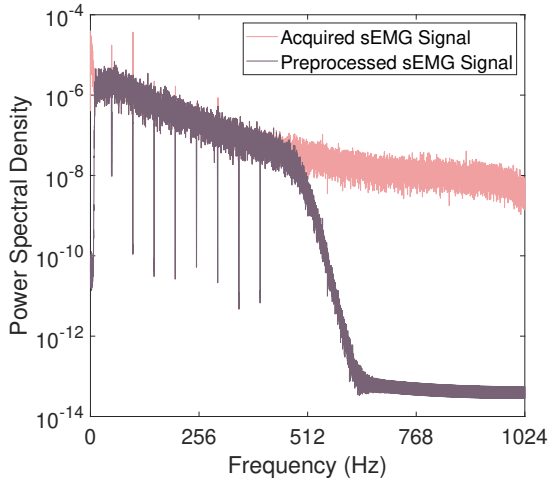


Fig. 5: Power spectral density of the raw and preprocessed (filtered) EMG signals from a representative subject.

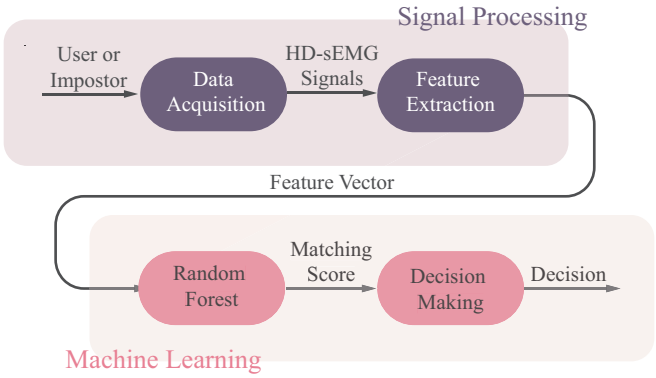


Fig. 6: Framework of the proposed method.

can be implemented by estimating a matching score between the input signals for authentication and the enrolled signals via the similarity between the feature maps. Input signals with a wrong user identity or a wrong gesture password lead to a low matching score.

III. Methods

A. Data Preprocessing

The acquired HD-sEMG data were first bandpass filtered from 10–500 Hz using an 8-order Butterworth filter. A cascade of several notch filters was then employed to attenuate power line interference (50 Hz) and each of its harmonic components up to 400 Hz. Fig.5 presents the power spectral density of representative sEMG signals. The filtered HD-sEMG signals were segmented into different tasks for further analysis. Signals in the first 0.25 s of reaction time after each task onset were removed from the analysis, retaining only the remaining stable period of each task.

B. Feature Extraction

The framework of the proposed method is shown in Fig. 6. Features widely applied in EMG pattern recognition studies, consisting of RMS [10], variance of central frequency (VCF) [15], Hjorth2 parameter [16], and spectral entropy [10], were extracted from each channel of the HD-sEMG electrode array during each task to represent the HD-sEMG biometric template. Each of the four features was computed once per task using the entire available task interval (less the 0.25 s reaction time startup). For each of the four features, a 256-length feature vector was constructed with each element in the vector corresponding to one specific channel. The four vectors were concatenated together to construct a 1024-length feature vector.

C. Matching Score Calculation

The constructed 1024-length feature vectors corresponding to all task labels were fed into a random forest classifier with an ensemble of 1000 decision trees. We selected the random forest classifier due to the high-dimensionality of the feature space. The user-specific random forest classifiers of dynamic tasks and maintenance tasks were trained separately, using the user's data acquired in session 1. For each user, a task sequence in a prescribed order was set as the gesture password. The gesture password is the combination of N gestures selected from the pool of 34 gestures. The gesture passwords were constructed by either dynamic tasks or maintenance tasks and their respective performance was compared. When users or impostors performed a specific task sequence to get access into the authentication system, the HD-sEMG of each task was fed into the random forest classifier successively. For each performed task, a 34-length score vector $[s_1, s_2, ..., s_i, ..., s_{34}]$ was calculated by the classifier, where s_i represented the probability that the true label of the performed task was i. The matching score between the task sequence performed by a user or impostor and the enrolled gesture password was given by: $S = \frac{1}{N}\sum_{j=1}^{N} s_{pwd(j)}$, where N is the length of gesture password and $pwd(j)$ is the label of the j^{th} task in the enrolled password. Because the user-specific random forest classifier was trained using only the user's HD-sEMG signals, the score of impostors' data when performing the correct gesture password was expected to be lower than the user's due to the inter-individual differences of HD-sEMG biometric patterns. If impostors entered a wrong gesture password, the matching score was expected to be further lower due to the inter-task differences of HD-sEMG patterns.

We trained the random forest model using all 34 hand gestures. In practice, the gesture password could be set by simply selecting a combination of gestures (with a specific order) from the pool of 34 gestures, using a smart phone or other user interfaces. When the HD-sEMG biometric token encoded by a specific gesture password is compromised, users can cancel the compromised token and simply set a new gesture password on a smart phone without new HD-sEMG data. Even if HD-sEMG under all gestures are exposed during the enrollment procedure, users can still include new gestures into the pool or change the muscle contraction efforts (with different force or torque values) of specific gestures. A large amount of alternative gestures provide numerous biometric tokens, in contrast to the human face and DNA. In practical applications, users may

trade-off between the effort required to train the model (e.g., the number of training gestures in the pool and the number of repetitions for each single gesture) vs. the security of the authentication system (a higher diversity of gestures increases the security of the gesture password).

D. Performance Evaluation Metrics

User authentication systems normally make two kinds of mistakes, namely False Rejection (FR) and False Acceptance (FA). The former one means the system rejects the user in error. The latter implies that the system accepts the impostor in error. Accordingly, we used False Rejection Rate (FRR) and False Acceptance Rate (FAR) as evaluation metrics. The threshold of matching score was tuned to obtain the receiver operating characteristic (ROC) curve. The Equal Error Rate (EER), i.e. the FRR when FRR=FAR, was extracted from the ROC curve to evaluate the authentication performance.

Considering we trained user-specific random forest models and the matching score was calculated specific to each gesture password, we assigned thresholds independently to each gesture password of each subject. An ROC curve was obtained for each gesture password of each user. Previous studies on user-specific authentication models using other biometric modalities, such as face [17] and palm print [18], employed the same strategy. The overall EER can be obtained in two different manners. In the first manner, an EER value was calculated for each individual ROC curve. The overall EER was taken as the average of all EER values. In the second manner, an ensemble average ROC curve was obtained by calculating the average FRR from all ROC curves at the threshold corresponding to each FAR value. The overall EER was extracted from the ensemble average ROC curve. The EER values obtained via the first and second manner were termed EER1 and EER2, respectively. Because EER1 [18] and EER2 [10], [17] are both used in biometric authentication studies, we reported both metrics in our work to provide benchmarks for future studies.

E. Validation Methodologies

Three validation situations were considered to evaluate the proposed user authentication method:

Situation 1: We aimed to evaluate the authentication performance when impostors do not know the gesture password. For each subject (user), all other subjects were viewed as impostors. For each user, a N-length gesture sequence (constructed separately for dynamic tasks and maintenance tasks) was randomly generated as the user's gesture password. We varied N from 1–12. To take into account the performance variation with different gesture passwords, 5 repetitions of random gesture password generation were performed for each user. Each gesture password of each user was generated independently, and tested against all impostors. A user's HD-sEMG pattern may vary when entering the same gesture password multiple times. To further take this factor into account, for each of the 5 generated gesture passwords of a specific user, tasks with the same gesture label were selected randomly and independently when tested against each impostor. To generate enough testing samples for each gesture password, the above random selection of tasks with the same label was further repeated for 10 times when tested against each impostor. For each user-impostor adversarial validation, the task sequence for impostors was generated independently, thus not necessarily the same as the sequence of users. The authentication system was trained using the user's data acquired in session 1. In the testing procedure, each user and impostor used their own HD-sEMG signals acquired in session 2 as the biometric token. Overall, 19000 testing samples (20 users $\times$ 5 repetitions of gesture password generation $\times$ 19 impostors $\times$ 10 repetitions of random selection of tasks with the same gesture label) were generated per value of N for both users and impostors.

Situation 2: We aimed to evaluate the authentication performance when impostors entered the correct gesture sequence to mimic the users' EMG patterns. The only difference with respect to situation 1 was that the task sequence of impostors was set as the same as users. Accordingly, the effect of individual differences of EMG patterns when performing the same task sequence was evaluated.

Situation 3: We aimed to evaluate the cancelability of HD-sEMG biometrics. The only difference with respect to situation 1 was that for each user-impostor pair, the impostor employed the user's HD-sEMG signals as the biometric token. This simulates the scenario where the users' biometric template is stolen by impostors and used to attack the authentication system. But, the task sequence of the impostor was generated independently from that of the user. This choice is in line with the real world situation because users can change to a different gesture password to cancel the stolen one.

F. Ablation Experiment

In the most challenging situation 2, we evaluated the contribution and necessity of each feature used in our method (i.e., RMS feature, VCF feature, Hjorth2 feature, and SE feature) via the ablation method. Specifically, we dropped out one of the four features at a time and kept the remaining three features. The performance variation was used to evaluate the contribution and necessity of each feature.

G. Evaluation of the Impact of Different Factors

Factor 1, Different Types of Tasks: To compare the authentication performance of dynamic tasks and maintenance tasks, we generated gesture passwords using the two different tasks separately. The total signal duration was kept the same. Specifically, a 12-length gesture password constructed from dynamic tasks (a total of 12 s of signal via 1 s per task) and a 3-length gesture password constructed by maintenance tasks (a total of 12 s of signal via 4 s per task) were used and their corresponding EER values in situations 1, 2 and 3 were compared. We also kept the total number of task the same to compare the performance of dynamic and maintenance tasks.

Factor 2, Length of Gesture Password: We investigated EER variation when progressively reducing the length of the gesture password.

Factor 3, Active Channel Number: In lightweight IoT application scenarios, reducing the data acquisition and transmission burden reduces power consumption, which is essential. Accordingly, we investigated EER variation with a different number of active channels. We designed a channel mask with only a proportion of channels active to acquire sEMG signals. The channel mask was designed automatically and specific for each gesture password. For each password, we calculated the RMS in all 256 channels for each task involved in the gesture password. For each channel, the maximum RMS value when performing the N tasks in the gesture password was used to represent the activation level of that specific channel. We ranked the maximum RMS values across the 256 channels. The leading P channels were set to be active in the channel mask. In our work, the range of P was set from 16 to 256, with an increment of 16. The EER variation as a function of the P value was investigated. The channel mask was generated automatically using data of session 1.

Factor 4, Sampling Rate: To further promote lightweight IoT applications with efficient power consumption, authentication performance using HD-sEMG signals with progressively reduced sampling rate f_s was investigated. EER values with $f_s = \{2048$ Hz, 1844 Hz, 1639 Hz, 1434 Hz, 1229 Hz, 1024 Hz$\}$ were evaluated. The original signal in each channel was resampled separately using an anti-aliasing filter, followed by interpolation. The lower boundary of the sampling rate was set to 1024 Hz, higher than the Nyquist sampling frequency of the preprocessed HD-sEMG signals with 10–500 Hz spectral band.

H. Security Strength Analysis

We performed security strength analysis to evaluate the robustness of the proposed authentication system against brutal attack from impostors. Specifically, we focus on spoofing attack where impostors use manufactured biometric data to intrude the system. We assume that the feature types of the system are known to impostors so that they can guess a feature vector and then manufacture fake biometric data via a reverse feature extraction algorithm. Impostors can repeat the same random guessing operation until a successful attack is achieved. When guessing the feature vector, we assume impostors know the range of the feature space constructed by a large population of people. We also assume a uniform distribution of the feature space (same as [19] in which the security of EEG biometrics was analyzed).

The probability of a successful attack is defined as:

$$\mathcal{P} = \frac{V_{user} - \sum_{k=1}^{K} V_{\epsilon}^{k}}{V_{total}} \tag{1}$$

where V_{total} and V_{user} refer to the volume of feature space constructed by all subjects and a specific user, respectively. V_{ϵ}^{k} is the volume of space near the k^{th} history signal and K is the number of all history signals. The term $-\sum_{k=1}^{K} V_{\epsilon}^{k}$ can avoid a replay attack (reusing exposed data) by applying a similarity check between incoming new testing data and history (both training data and all data with successful access into the system). In practical application, the similarity check can be implemented by calculating the distance between a history feature vector and an incoming new testing feature vector.

To avoid over-estimation of the security of our system against brutal attack, we applied the following operations to calculate the maximal $\mathcal{P}$ (the most challenging threat).

1) We pooled data acquired on two days together to estimate V_{user}. Cross-day factors increased the variation of biometric patterns of the same user.

2) We performed security analysis using only a 1-length gesture password to encode the HD-sEMG biometrics. Increasing the number of gestures contributes to higher security, but here we consider the worst case.

3) Different users with different gestures as password may show different variations of biometric patterns (i.e., different values of V_{user}). To analyze the security of HD-sEMG biometrics against brutal attack in the worst case (to avoid over-estimation), we selected the user and gesture with largest V_{user} to calculate $\mathcal{P}$.

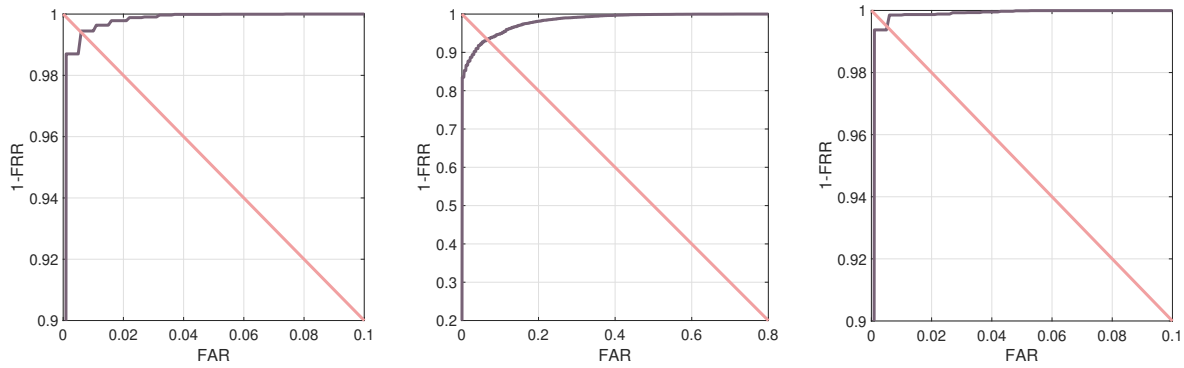
4) A large V_{ϵ}^{k} contributes to a higher difficulty of brutal attack. We set $V_{\epsilon}^{k} = 0$, so that $\mathcal{P} = \frac{V_{user}}{V_{total}} > \frac{V_{user} - \sum_{k=1}^{K} V_{\epsilon}^{k}}{V_{total}}$.

5) We removed the dependence between features via principal component analysis (PCA). A higher dimensionality of the feature space normally contributes to a higher difficulty of brutal attack. But the dimensionality of the space constructed by m-length feature vectors may be lower than m due to feature dependence. For example, if the system repeats the same feature 1000 times to construct a 1000-length feature vector, impostors only need randomly guess one feature value to intrude the system. Equivalently, the dimensionality of the space of such a 1000-length feature vector is 1. We performed security analysis of the system in a dependence-removed feature space, with 100%, 99%, 98%, 97%, 96% and 95% variance preserved.

V_{total} is the volume of a hypercube (same assumption in study [19]) constructed by features of all gestures and all subjects. The exact volume of the feature space corresponding to a specific user depends on the boundary surface given by the employed machine learning algorithm. To make the results more general to most machine learning algorithms and simplify the analysis, here we also assume a hypercube-shaped feature space of a single user. Accordingly, V_{total} and V_{user} can be obtained via $V_{total} = \prod_{m=1}^{M} q_{total}^{m}$ and $V_{user} = \prod_{m=1}^{M} q_{user}^{m}$, respectively, where M is the dimensionality of the dependence-removed feature space, q_{total}^{m} and q_{user}^{m} refer to the length of hypercube side in dimension m, determined by the difference between the maximal and minimal values in that dimension. We employed password entropy [20], i.e., the base 2 logarithm of expected total number of brutal attack attempts to successfully guess the correct biometric token, to evaluate the security. Specifically, the entropy $\mathbf{E}$ (bits) was calculated via $\mathbf{E} = log_2(\frac{1}{\mathcal{P}})$. A higher $\mathbf{E}$ represents a higher security against brutal attack.

I. Statistical Analysis

To quantify performance variation due to a specific factor, statistical analysis was performed. Because the obtained data did not satisfy the normality assumption of parametric test, the two-sided sign test was applied. Bonferroni-Holm correction



(**a**) ROC curve of situation 1 (**b**) ROC curve of situation 2. (**c**) ROC curve of situation 3.

Fig. 7: ROC curves.

*All ROC curves present the average performance of all gesture passwords of all subjects. All ROC curves are with a 12-length gesture password constructed by dynamic tasks. The intersection of the diagonal and each ROC curve represents the EER2 in each situation. Also note that we used different axis scales for ROC curves in different situations.

was also performed to avoid multiple comparison errors. In the remaining part of the paper, only Bonferroni-Holm corrected p-values are reported. A significant difference was reported if $p < 0.05$ was achieved. Because EER2 is an overall average of all users, statistical analysis is not applicable on an individual element. Accordingly, statistical analysis was performed on EER1 values of all users.

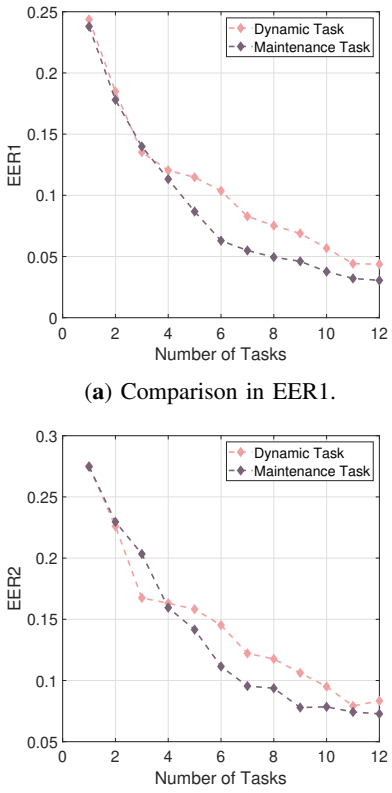
IV. Results

A. Performance of Situation 1

The ROC curve of situation 1 with 12-length gesture passwords constructed by dynamic tasks is presented in Fig. 7a. An average EER1 of 0.0013 and EER2 of 0.0074 was achieved. By further encoding users' HD-sEMG biometrics using gesture passwords, the unique patterns of users' HD-sEMG signals could be strengthened. The low EER1 and EER2 with an average 8.5-day interval between training and testing sessions proved its high practical potential in real world scenarios.

B. Performance of Situation 2

The ROC curve of situation 2 with 12-length gesture passwords constructed by dynamic tasks is presented in Fig. 7b. Even when impostors enter the correct gesture password, the individual differences of HD-sEMG biometric patterns under the same muscle task can still serve as a second defense. In this case, the proposed authentication approach could inhibit impostors with an EER1 of 0.0273 and EER2 of 0.0674. In the most challenging situation 2, we performed an ablation experiment to evaluate the necessity of all features employed in our work. With RMS, VCF, Hjorth2 and spectral entropy features dropped out (keeping the remaining 3 features each time), an EER1 of 0.0311, 0.0300, 0.0320 and 0.0300 were obtained, respectively, which was always greater than the error achieved using all features (0.0273) (but with no significance, $p > 0.05$ in all cases). EER2 of 0.0678, 0.0704, 0.0774 and 0.0729, respectively, were likewise obtained, higher than when using all features (0.0674).



(**a**) Comparison in EER1.

(**b**) Comparison in EER2.

Fig. 8: Performance comparison between dynamic and maintenance tasks with different number of tasks.

*The EER values shown in this figure are validated in situation 2. For dynamic tasks, the duration to perform each gesture is 1 s. Because we removed the first 0.25 s of reaction time after each task onset, the signal duration for analysis is 0.75 s for each task. For maintenance tasks, the duration to perform each gesture 4 s. We take signals from 1.25 s to 2 s after task onset (also with a total duration of 0.75 s), during which period, subjects have reached the target gesture and maintained the steady gesture. The training samples of dynamic tasks were also reduced to the same size as maintenance tasks for a fair comparison.

We then compared the performance of gesture passwords constructed by dynamic tasks and maintenance tasks in the most challenging situation 2. As shown in Fig. 8, for both dynamic and maintenance tasks, a larger number of tasks contributes to a significantly lower EER1. For dynamic tasks, significant differences were found for comparisons between the 12 tasks and all numbers of tasks from 1 to 10. For maintenance tasks, significant differences were found for comparisons between the 12 tasks and all numbers of tasks from 1 to 7. However, EER1 of maintenance tasks shows no significant differences compared with dynamic tasks for all numbers of tasks from 1 to 12 ($p > 0.05$ in all cases). To perform the maintenance tasks, subjects have to first perform dynamic tasks to reach the target gesture, which increases the duration to enter the gesture password in practical scenarios. A longer duration to enter the gesture password may greatly reduce the convenience of the proposed method. Considering dynamic tasks show no significant differences in performance compared with maintenance tasks and each dynamic task takes a shorter duration in practical use, all the following evaluations were based on the dynamic tasks.

C. Performance of Situation 3

Fig. 7c shows the results of situation 3 (using 12-length dynamic task gesture password), where the HD-sEMG biometric token of users encoded by a specific gesture password was exposed to impostors. Then, impostors used the exposed HD-sEMG biometric token to spoof the authentication system. In a similar scenario, users can cancel the exposed biometric token by simply changing to a new gesture password. An average EER1 of 0.0013 and EER2 of 0.0047 was achieved, demonstrating excellent cancelability of the proposed HD-sEMG biometric modality.

D. Performance Variation with the Number of Active Channels

Fig. 9 shows the EER variation (situation 2) with the number of active channels. With the number of active channels progressively increasing, EER showed a reduction trend, for both EER1 and EER2. Moreover, significant differences were found for comparisons between the channel number 256 and all channel numbers from 16 to 160 ($p < 0.05$ in all cases). The trend is particularly sharp when the number of active channels is lower than 48. With 48 active channels, the HD-sEMG biometrics-based user authentication achieved an EER1 of 0.0483 and an EER2 of 0.0908.

E. Performance Variation vs. Sampling Rate

We further investigated the EER variation using different temporal sampling rates under situation 2, with the number of active channels fixed at 48. As shown in Fig. 10, with sampling rate f_s decreasing from 2048 Hz to 1024 Hz, both EER1 and EER2 remained at a low value. The EER1 comparison between each pair of sampling rate shown in Fig. 10 shows no significant differences ($p > 0.05$ in all cases). With the sampling rate of 1024 Hz and the channel number of 48, the authentication system yielded an EER1 of 0.0505 and an EER2 of 0.0943. The HD-sEMG biometrics-based user authentication was therefore robust against sampling rate. Accordingly, in IoT devices, the sampling rate of the proposed system can be reduced to half for efficient power consumption. We also evaluated the authentication performance in situations 1 and 3, with the channel number of 48 and the sampling rate of 1024 Hz, achieving an EER1 of 0.0036 and 0.0043, and EER2 of 0.0104 and 0.0132, respectively.

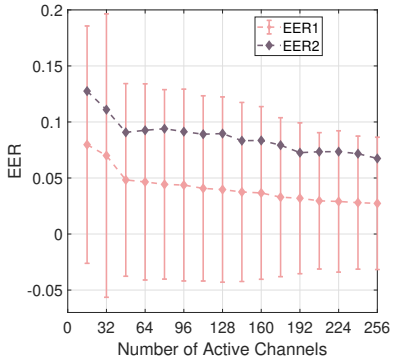


Fig. 9: Performance variation with different number of active channels.

*The EER values shown in this figure are validated with 12-length gesture password constructed by dynamic tasks in situation 2. Because EER1 is calculated for each gesture password and each subject, the standard deviation was also shown here.

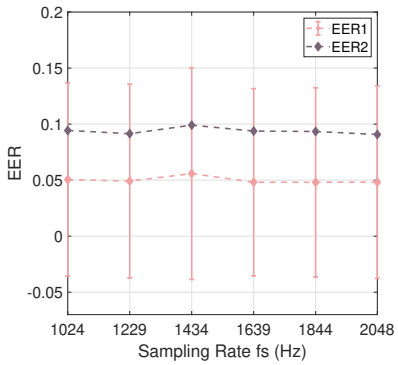


Fig. 10: Performance variation vs sampling rate f_s.

*The EER values shown in this figure are validated with 12-length gesture password constructed by dynamic tasks in situation 2. Because EER1 is calculated for each gesture password and each subject, the standard deviation was also shown here.

F. Performance Variation with Subject Number

We evaluated the EER variation with different number of subjects included in the analysis under situation 2. For each number of subjects, the subjects were randomly selected for 5000 times. The average EER in this analysis is presented in Fig. 11. With subject number increasing, both EER1 and EER2 do not show an obvious growth trend. For both EER1 and EER2 with 20 subjects, the EER values show significant differences only for subject number ≤ 13. For subject number larger than 13, no significant differences were found, indicating the performance converged to the mathematical expectation.

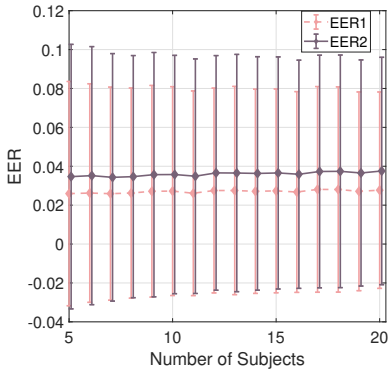


Fig. 11: Performance Variation with Subject Number.

*The EER values shown in this figure are validated with 12-length gesture password constructed by dynamic tasks in situation 2. The number of active channels is fixed at 256. The sampling rate is fixed at 2048 Hz. For the curve of EER2, we add a slight shift (shift value = 0.1) on the x-axis to avoid overlap with the curve of EER1.

TABLE I: Security strength against brutal attack.

Preserved Variance With PCA-based Dependence Removal	Entropy $\mathbf{E}$
100%	1318 bits
99%	313 bits
98%	238 bits
97%	198 bits
96%	164 bits
95%	140 bits

G. Results of Security Strength Analysis

The security strength of HD-sEMG biometrics against brutal attack is presented in Table I. With 95% variance preserved, the security of the proposed HD-sEMG biometrics is equivalent to a 140-bit key with a total of 2^{140} expected attempts of brutal attack required to intrude the system. As a comparison, Feng et al. [21] showed that the human face biometric template has a 75-bit entropy. Sadeghi et al. [19] evaluated the security strength of EEG biometrics, with an 81-bit entropy achieved. Assuming each attack attempt takes 1000 flops, using a supercomputer with 10 petaFLOPS to intrude our 140-bit authentication system takes $\frac{2^{140}\times 10^3}{10\times 10^{15}} \approx 1.39\times 10^{29}$ seconds, i.e., $\approx 4.41\times 10^{21}$ years. So, intruding the HD-sEMG biometric authentication system via brutal attack is almost impossible with currently available computation.

V. Comparison with Related Work

EMG-based biometric authentication has recently emerged as a new area. There are two different evaluation methods in the literature, namely biased evaluation and rigorous evaluation. In the biased evaluation method, the training and testing data are acquired on the same day. Therefore, signal variation across days is not taken into consideration. In some cases, the data may even be acquired in the same session, which ignores electrode shifts. The rigorous evaluation, by contrast, employs data acquired on separate days as training and testing sets, to simulate a relatively realistic scenario. Venugopalan et al. [12] achieved a FRR of 2.7% (Genuine Accept Rate of 97.3%) at 10% FAR, using the K-Nearest Neighbor (K-NN) technique, with training and testing data acquisition sessions performed on the same day. He et al. [14] employed an improved Discrete Fourier Transform-based method to construct the sEMG biometric template, yielding an EER of 0.035 using training and testing data sets acquired on the same day. In previous study [10], 64-channel HD-sEMG signals acquired with a 4000 Hz sampling rate from the right dorsal side of the hand during muscle isometric contractions were employed as biometric tokens, achieving an average EER2 of 0.1496 in a cross-day evaluation. The present study is based on the same rigorous cross-day evaluation method, with training and testing from data acquired on different days. We therefore compared our method with previous state-of-the-art studies that used the same evaluation method. A detailed comparison between the previous study [10] and this work (both used cross-day evaluation) is shown in Table II. Because users and impostors entered the same gesture password each day, EER in this situation was mainly regulated by the inter-individual differences of sEMG characteristics. As shown in Table II, our present method achieved a largely reduced EER2 (from 0.1496 to 0.0674) when impostors entered the correct gesture password, with respect to the previous study. If we applied a channel mask with only 48 active channels and reduced the sampling rate for efficient power consumption in IoT devices, both a largely reduced EER2 with respect to the previous study (from 0.1496 to 0.0943) and a largely reduced data transmission rate (from 6.144×10^6 bits/s to 7.864×10^5 bits/s) were obtained. Moreover, the results shown in Table II were obtained with 12-s signal duration (12 tasks $\times$ 1 s per task), which is one half the duration used in the previous work. Therefore, the total data volume to be acquired, transmitted and processed can be further reduced (from 1.475×10^8 bits to 9.437×10^6 bits). The all-round performance improvement of our present work promotes the practical use of HD-sEMG biometrics in IoT applications.

We propose possible hypotheses to explain the excellent performance in the present work with respect to our previous study [10] from the following perspectives: (1) algorithms, (2) anatomical structure of the forearm, (3) human gesture kinematics, (4) hardware sensing and (5) experiment design. (1) For the algorithms, the present work employed RMS, VCF, Hjorth2 parameter and spectral entropy features to represent biometric templates. RMS represents the amplitude of sEMG in each channel, with a decoding of the HD-sEMG biometrics in the temporal domain. VCF, Hjorth2 parameters and spectral entropy all represent unique characteristics of the power spectrum, with a decoding of the sEMG biometrics in the spectral domain. Moreover, the above features extracted from all 256 channels further decoded the sEMG biometrics in the spatial domain. The combination of temporal-spectral-spatial domain features likely contributed to the excellent authentication performance in our work. (2) For the anatomical structure, the forearm contains several muscle groups active during most activities of daily living, and contain the extrinsic muscles of the hand. Accordingly, EMG signals acquired from the forearm should provide more discriminative information than signals acquired from the dorsal side of the hand (used in

TABLE II: Comparison with state-of-the-art EMG biometric authentication.

Study	EMG Channels	Sampling Rate (Hz)	ADC Resolution (bit)	Required Acquisition and Transmission Rate (bit/s)	Number of Tasks	Signal Duration (s)	Data Volume (bits)	EER1	EER2
Jiang *et al. [10]*	64	4000	24	6.144×10^6	8	8×3=24	1.475×10^8	-	0.1496
This Work	48	1024	16	7.864×10^5	8	8×1=8	6.291×10^6	0.0872	0.1353
This Work	256	2048	16	8.389×10^6	8	8×1=8	6.711×10^7	0.0495	0.0976
This Work	48	1024	16	7.864×10^5	12	12×1=12	9.437×10^6	0.0505	0.0943
This Work	256	2048	16	8.389×10^6	12	12×1=12	1.007×10^8	0.0273	0.0674

*The EER values shown in this figure are validated in the most challenging situation 2, where users and impostors enter the same gesture password.

our previous work [10]). Besides, the extensor digitorum muscle has a cylindrical shape along the proximal-distal direction of the forearm. Different muscle compartments have oblique fascicle overlap instead of running in parallel [22], therefore resulting in a complex anatomical structure. The inter-individual differences of signal characteristics may also result from the variability in volume conductor properties (e.g., thickness of subcutaneous tissues). These sources of variability in anatomical structure make sEMG a promising biometric modality. (3) For human gesture kinematics, dynamic contractions are a more natural way to exert force and generate EMG signals, compared with isometric contractions. With repeated practice of frequently used hand gestures, users can easily repeat a specific motor pattern (e.g., the efforts of muscle groups) to perform a gesture sequence, further contributing to a similar EMG pattern when performing the same gesture sequence on a second day. (4) For hardware sensing, we acquired 256 channels in our data acquisition experiment. The area of the forearm covered by our electrodes was very large since we used four electrode arrays. Although we applied a channel mask to reduce the number of active channels, the larger total area seems to have reduced the impact of a relatively small electrode shift on a second day. Therefore, the cross-day variation of signal characteristics was largely reduced. (5) Additionally, for the experimental design in the present work, we acquired sEMG during a total of 34 hand gestures, providing a large pool of alternative muscle contraction tasks to encode the HD-sEMG biometric template. Previous work has quantified the spatial activation patterns of HD-sEMG in the forearm under different muscle contraction tasks, at both the macroscopic level (global sEMG) [23] and the microscopic level (motor units decomposed from global sEMG) [24]. Significant differences across different muscle contraction tasks were found at both levels [23], [24]. The larger inter-task differences due to the larger gesture pool in the present work also contributed to the excellent authentication performance when impostors enter the wrong gesture password.

In both this work and the previous work [10], most of the results were evaluated via EER. EER is an effective criterion to compare the performance of different authentication systems. The computation of EER requires the data from both users and impostors, thereby the threshold corresponding to the point in the ROC curve where FAR=FRR can be found. In practical applications, users may prefer a rigorous system (with a low FAR) or a soft system (with a low FRR). In such cases, the threshold can be selected according to the ROC curve obtained by the training data of the user and other subjects (as impostors) already stored in the database.

VI. Discussion

A. Performance Variation with Different Factors

The inter-individual characteristics differences of physiological signals (e.g. EEG and EMG) have long been a big challenge in diverse applications [25]. In this work, we proposed a user authentication method using HD-sEMG biometrics encoded by a prescribed gesture password. The volitional selection of different gesture passwords allows users to cancel the original biometric token once it is exposed to impostors. We investigated the performance variation of HD-sEMG biometrics with different factors, including different types of tasks with number of tasks, number of active channels and sampling rate. For the selection of task type and password length, our results demonstrate that dynamic and maintenance tasks show no significant differences in performance. However, dynamic tasks take a shorter duration to perform, thus contributing to more convenient use in practical IoT applications. The key factor to improve the authentication performance is to increase the length of the gesture password. With more tasks involved, the useful muscular information contained in HD-sEMG signals greatly increased.

We also investigated the authentication performance with reduced number of active channels and sampling rate. By reducing the number of active channels and sampling rate, the data acquisition, transmission and processing burden in IoT devices is greatly reduced. In IoT application scenarios, efficient power consumption is indeed one of the key factors. This is especially true for HD-sEMG, with a large number of channels and a high sampling rate. A recent study [26] has developed a wearable HD-sEMG acquisition system with modular architecture. Each 32-channel sensor unit of the wearable system is small in size (3.4 cm × 3 cm × 1.5 cm) and light in weight (16.7 g), which would simplify the application of HD-sEMG. The wearable HD-sEMG acquisition system allows continuous acquisition for up to 5 hours, at 2048 Hz sampling rate, with all channels (for each sensor unit) active. Using the proposed authentication method, with a sampling rate reduced from 2048 Hz to 1024 Hz and only a proportion (48 out of 256) of channels active, it would be possible to greatly prolong the continuous acquisition duration. The channel mask is obtained automatically during model training. After that, the signal acquisition system for a specific user can just activate a proportion of channels according to the channel mask.

In practical use, adaptively triggered HD-sEMG acquisition, transmission and processing can be achieved via a low-cost and energy-efficient continuous key gesture spotting technique [27]. This key gesture spotting module can be embedded into the wearable HD-sEMG acquisition system. Once the key gesture (e.g., an additional trigger gesture in the gesture password) is detected, the HD-sEMG acquisition is then triggered. Otherwise, the HD-sEMG acquisition system would stay in the idle state, further reducing the power consumption of IoT devices. Recent advances of event-based sEMG acquisition [28] and an analog-compressed sensing techniques for low-power wearable sEMG acquisition systems can also contribute to an extremely energy-efficient wearable HD-sEMG acquisition system in the near future. Additionally, in this work, we aimed to evaluate the performance of HD-sEMG generated under hand gestures as biometrics, with a reduced sampling rate and number of channels. The signal acquisition system (Quattrocento system) used in our work is designed for laboratory use. Wearable HD-sEMG systems [7], [8] are the topic of intense research. For example, Farina et al. [29] used Smart Fabric and Interactive Textile (SFIT) systems to record HD-sEMG signals with high-density electrodes embedded in a sleeve. This system is promising to be applied in real world IoT scenarios. Our work proceeds in parallel with hardware developments to investigate the feasibility of applying HD-sEMG biometric authentication to IoT applications.

B. Possible Risks of Information Disclosure

With the wide application of WBAN in daily IoT environments, the risk of information disclosure substantially increases. Traditional biometrics are vulnerable once exposed due to their noncancelability and cross-application invariance. Even worse, the exposed biometric template normally contains private information. For example, exposed DNA via lost hair or saliva can be used to extract highly sensitive information, such as possible diseases and congenital disabilities. Similarly, the exposed human face can be used to recognize the user and disclosing the exposed face template to the public may largely affect the user's social life. Previous studies propose to employ one-way functions [30] to transform the original biometric template to an encrypted one. The encrypted template, instead of the original one, is then transmitted, processed and saved in the database. Once the encrypted templates are stolen, simply changing a new one-way transform function eliminates the above risks. However, no solutions can eliminate privacy disclosure risks once the original biometric template is exposed. For HD-sEMG biometrics, the original biometric template is almost impossible to be exposed without a user's knowledge because the HD-sEMG electrode array must be in close contact with the user's skin. The one-way function can be embedded directly in the data acquisition procedure. For example, a more complex channel mask can be employed to further encrypt the acquired HD-sEMG signals, with a time-variant and channel-dependent amplifier gain, instead of only reducing the number of active channels. One-way functions can also be embedded in the signal preprocessing module of the HD-sEMG acquisition system. In this way, the HD-sEMG biometric template would be encrypted at the initial stage of the signal processing pipeline. The original HD-sEMG biometric template can be hardly exposed through other means.

Although the proposed HD-sEMG biometrics show superiorities in certain aspects, replay attack is still a threat to the authentication system. Impostors can spoof the system by directly replaying an exposed biometric token, or incorporating small-scale noises into the exposed biometric token before replaying. This issue can be addressed in at least two ways: (1) liveness detection and (2) similarity check. Liveness detection techniques are very convenient to embed into a HD-sEMG biometric authentication system. For example, because electrode arrays need to be in close contact with a user's skin to acquire sEMG signals, a movement detection sensor can be directly embedded into the array to detect small muscle movements during muscle contractions to verify the liveness of the current object for identity authentication. As another option, a low-cost photoplethysmography (PPG) sensor [31] can be used to acquire the PPG signals which reflects blood oxygen saturation and pulse rate, for liveness detection. For the second approach, an intuitive similarity check is to verify if the input biometric token is close to a history sample in the signal or feature domain. To this end, previous studies have proposed advanced algorithms for replay detection, which have been applied to other modalities. For example, Sriskandaraja et al. [32] proposed a novel algorithm to estimate similarities between pairs of genuine speech samples for the detection of replayed samples, using a suitable learned embedding via deep Siamese architectures. Gui et al. [33] employed an ensemble classifier and noise residual features to detect if the input EEG biometrics have been compromised and manipulated. These algorithms are promising to be adapted for replay detection of HD-sEMG biometrics.

C. Limitations and Future Work

Limitations of the present work and perspectives for future studies need to be clarified. First, our study investigated HD-sEMG biometrics with subjects performing different hand gestures in a sitting position. Future studies need to consider a more realistic application scenario, where subjects perform different hand gestures to generate HD-sEMG biometrics with varying posture. Second, advanced algorithms to prevent replay attack in the context of HD-sEMG biometric authentication have not been systematically investigated in our work. A deep investigation into the replay threats and the security protocol to utilize HD-sEMG biometrics is required in future studies. Third, further improving the hardware design to facilitate HD-sEMG recordings is essential for practical applications. Future studies should also investigate the performance of HD-sEMG biometrics acquired via wearable sleeves or wristbands. Other strategies to improve the convenience to use HD-sEMG biometrics, such as reducing training efforts, are also necessary. Practical factors, such as the impact of weather, clothes and user sweating, on authentication performance need to be studied to facilitate practical applications. Additionally, although we re-applied the electrode arrays on the second day to avoid over-estimation of the performance, future studies focusing

on the electrode shift issue are needed. For example, rotation and translation-invariant learning algorithms [34], [35] are promising to adapt to electrode shift on multiple days, which can further improve authentication performance.

VII. Conclusion

In this work, we proposed a cancelable HD-sEMG-based biometrics encoded by gesture password. The proposed HD-sEMG biometrics can achieve a low EER when impostors enter a wrong gesture password. Even if impostors enter the correct gesture password, the inter-individual differences of HD-sEMG signals, as the second defense layer, can still recognize impostors with a low EER. The inter-task differences of HD-sEMG signals also allow users to cancel the original HD-sEMG biometric token by changing to a new gesture password. With a lower number of channels and sampling rate, the proposed user authentication system can achieve a greatly reduced data acquisition and transmission rate, while maintaining a low EER, further contributing to efficient power consumption in IoT applications. The proposed method can advance the limits of information security in IoT application scenarios.

References

[1] S. Mandal *et al.*, "Certificateless-Signcryption-Based Three-Factor User Access Control Scheme for IoT Environment," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3184–3197, Apr. 2020.

[2] P. Huang *et al.*, "Practical Privacy-Preserving ECG-Based Authentication for IoT-Based Healthcare," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9200–9210, Oct. 2019.

[3] 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.

[4] 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.

[5] G. Rescio *et al.*, "Supervised machine learning scheme for electromyography-based pre-fall detection system," *Expert Syst. Appl.*, vol. 100, pp. 95–105, Jun. 2018.

[6] Z. Lu *et al.*, "A Hand Gesture Recognition Framework and Wearable Gesture-Based Interaction Prototype for Mobile Devices," *IEEE Trans. Human-Mach. Syst.*, vol. 44, no. 2, pp. 293–299, Apr. 2014.

[7] U. Barone and R. Merletti, "Design of a Portable, Intrinsically Safe Multichannel Acquisition System for High-Resolution, Real-Time Processing HD-sEMG," *IEEE Trans. Biomed. Eng.*, vol. 60, no. 8, pp. 2242–2252, Aug. 2013.

[8] G. L. Cerone and M. Gazzoni, "Wearable and Wireless HD-sEMG Acquisition Systems: Recent Advances," in *Converging Clinical and Engineering Research on Neurorehabilitation III*, ser. Biosystems & Biorobotics, L. Masia *et al.*, Eds. Cham: Springer International Publishing, 2019, pp. 1156–1160.

[9] X. Jiang *et al.*, "High-Density Surface Electromyogram-based Biometrics for Personal Identification," in *2020 42nd Annual International Conference of the IEEE Engineering in Medicine Biology Society (EMBC)*, Jul. 2020, pp. 728–731, iSSN: 2694-0604.

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

[11] X. Jiang *et al.*, "Cancelable HD-sEMG-Based Biometrics for Cross-Application Discrepant Personal Identification," *IEEE J. Biomed. Health Inform.*, pp. 1–1, 2020.

[12] S. Venugopalan *et al.*, "Electromyograph and keystroke dynamics for spoof-resistant biometric authentication," in *2015 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. Boston, MA, USA: IEEE, Jun. 2015, pp. 109–118.

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

[14] J. He and N. Jiang, "Biometric From Surface Electromyogram (sEMG): Feasibility of User Verification and Identification Based on Gesture Recognition," *Frontiers in Bioengineering and Biotechnology*, vol. 8, 2020, publisher: Frontiers.

[15] A. Phinyomark *et al.*, "Feature reduction and selection for EMG signal classification," *Expert Syst. Appl.*, vol. 39, no. 8, pp. 7420–7431, Jun. 2012.

[16] W. Caesarendra *et al.*, "A classification method of hand EMG signals based on principal component analysis and artificial neural network," in *2016 International Conference on Instrumentation, Control and Automation (ICA)*, Aug. 2016, pp. 22–27.

[17] P. J. Phillips, "Support Vector Machines Applied to Face Recognition," in *Advances in Neural Information Processing Systems 11*, M. J. Kearns *et al.*, Eds. MIT Press, 1999, pp. 803–809.

[18] P. H. Hennings-Yeomans *et al.*, "Palmprint Classification Using Multiple Advanced Correlation Filters and Palm-Specific Segmentation," *IEEE Trans. Inf. Forensic Secur.*, vol. 2, no. 3, pp. 613–622, Sep. 2007.

[19] K. Sadeghi *et al.*, "Geometrical analysis of machine learning security in biometric authentication systems," in *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, 2017, pp. 309–314.

[20] W. Burr *et al.*, "Electronic Authentication Guideline," National Institute of Standards and Technology, Tech. Rep. NIST Special Publication (SP) 800-63 Ver. 1.0 (Withdrawn), Jun. 2004.

[21] Y. C. Feng and P. C. Yuen, "Binary discriminant analysis for generating binary face template," *IEEE Trans. Inf. Forensic Secur.*, vol. 7, no. 2, pp. 613–624, 2012.

[22] J. Leijnse *et al.*, "Anatomic Basis for Individuated Surface EMG and Homogeneous Electrostimulation With Neuroprostheses of the Extensor Digitorum Communis," *J. Neurophysiol.*, vol. 100, no. 1, pp. 64–75, Jul. 2008.

[23] 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. 01, p. 1850025, Jun. 2018.

[24] X. Jiang *et al.*, "Quantifying Spatial Activation Patterns of Motor Units in Finger Extensor Muscles," *IEEE J. Biomed. Health Inform.*, 2020.

[25] X. Jiang *et al.*, "Transfer Component Analysis to Reduce Individual Difference of EEG Characteristics for Automated Seizure Detection," in *2019 IEEE Biomedical Circuits and Systems Conference (BioCAS)*, Oct. 2019, pp. 1–4, iSSN: 2163-4025.

[26] G. L. Cerone *et al.*, "A Modular, Smart, and Wearable System for High Density sEMG Detection," *IEEE Trans. Biomed. Eng.*, vol. 66, no. 12, pp. 3371–3380, Dec. 2019.

[27] H. P. Gupta *et al.*, "A Continuous Hand Gestures Recognition Technique for Human-Machine Interaction Using Accelerometer and Gyroscope Sensors," *IEEE Sens. J.*, vol. 16, no. 16, pp. 6425–6432, Aug. 2016.

[28] D. A. F. Guzman *et al.*, "Very low power event-based surface EMG acquisition system with off-the-shelf components," in *2017 IEEE Biomedical Circuits and Systems Conference (BioCAS)*, Oct. 2017, pp. 1–4.

[29] D. Farina *et al.*, "High-density EMG E-Textile systems for the control of active prostheses," in *2010 Annual International Conference of the IEEE Engineering in Medicine and Biology*, Aug. 2010, pp. 3591–3593, iSSN: 1558-4615.

[30] V. M. Patel *et al.*, "Cancelable Biometrics: A Review," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 54–65, Sep. 2015.

[31] J. Schuiki and A. Uhl, "Improved Liveness Detection in Dorsal Hand Vein Videos using Photoplethysmography," in *2020 International Conference of the Biometrics Special Interest Group (BIOSIG)*, Sep. 2020, pp. 1–5, iSSN: 1617-5468.

[32] K. Sriskandaraja *et al.*, "Deep Siamese Architecture Based Replay Detection for Secure Voice Biometric," in *Interspeech 2018*. ISCA, Sep. 2018, pp. 671–675.

[33] Q. Gui *et al.*, "A residual feature-based replay attack detection approach for brainprint biometric systems," in *2016 IEEE International Workshop on Information Forensics and Security (WIFS)*, Dec. 2016, pp. 1–6, iSSN: 2157-4774.

[34] G. L. Bezerra Ramalho *et al.*, "Rotation-invariant feature extraction using a structural co-occurrence matrix," *Measurement*, vol. 94, pp. 406–415, Dec. 2016.

[35] J. Yang *et al.*, "Supervised translation-invariant sparse coding," in *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, Jun. 2010, pp. 3517–3524, iSSN: 1063-6919.