applied sciences

MDPI

Article

Enhancing the Security of Pattern Unlock with Surface EMG-Based Biometrics

Qingqing Li, Penghui Dong and Jun Zheng *

Department of Computer Science and Engineering, New Mexico Institute of Mining and Technology, Socorro, NM 87801, USA; qingqing.li@student.nmt.edu (Q.L.); penghui.dong@student.nmt.edu (P.D.)

* Correspondence: jun.zheng@nmt.edu

Received: 6 December 2019; Accepted: 7 January 2020; Published: 11 January 2020

Abstract: Pattern unlock is a popular screen unlock scheme that protects the sensitive data and information stored in mobile devices from unauthorized access. However, it is also susceptible to various attacks, including guessing attacks, shoulder surfing attacks, smudge attacks, and side-channel attacks, which can achieve a high success rate in breaking the patterns. In this paper, we propose a new two-factor screen unlock scheme that incorporates surface electromyography (sEMG)-based biometrics with patterns for user authentication. sEMG signals are unique biometric traits suitable for person identification, which can greatly improve the security of pattern unlock. During a screen unlock session, sEMG signals are recorded when the user draws the pattern on the device screen. Time-domain features extracted from the recorded sEMG signals are then used as the input of a one-class classifier to identify the user is legitimate or not. We conducted an experiment involving 10 subjects to test the effectiveness of the proposed scheme. It is shown that the adopted time-domain sEMG features and one-class classifiers achieve good authentication performance in terms of the F_1 score and Half of Total Error Rate (HTER). The results demonstrate that the proposed scheme is a promising solution to enhance the security of pattern unlock.

Keywords: biometrics; sEMG; pattern unlock; time domain feature; one-class classification

1. Introduction

Mobile usage has grown tremendously in recent years. Mobile usage is surpassing desktop usage, as mobile devices are being widely used for a variety of online tasks, including web surfing, online shopping, mobile banking, and social media [1]. Fast-growing mobile usage has been leaving lots of sensitive private data and information in mobile devices. These data and information need to be protected against unauthorized access of the devices.

Screen unlock is a popular mechanism used to secure the mobile device from unauthorized access. A number of screen unlock schemes have been provided by popular mobile platforms (iOS and Android), including the slide, PIN, password, pattern, fingerprint, and face. Among them, pattern unlock provided by the Android platform has been widely adopted by mobile users. It was shown in a recent study [2] that about 40% of Android users use pattern unlock to secure their devices. Another study showed that pattern unlock was preferable over the password and PIN by mobile users, although the PIN outperforms patterns in terms of input speed and error rate [3].

Although pattern unlock is a convenient scheme for protecting the user's device, it is also susceptible to a number of attacks, including guessing attacks [4], shoulder surfing attacks [5], smudge attacks [6], and side-channel attacks [7,8]. It was shown in [6] that smudge attacks were able to break the pattern up to 68% of the time. The success rate of guessing attacks can be greatly improved from 13.33% to 74.17% when assisted by smudge attacks [4]. The study of [5] showed that patterns are more memorable and easier to be spied on through shoulder surfing attacks compared with PINs.

Ye et al. [8] developed a computer vision algorithm that can track the user's finger movement to infer the pattern drawn on the screen. Their approach can break over 95% of the patterns in five attempts before the device is automatically locked by the Android system. Thus, there is a great need to enhance the security of pattern unlock to defend the attacks.

In this paper, we propose a new two-factor screen unlock scheme that incorporates biometric information with patterns to achieve improved security. The proposed scheme not only verifies "what you possess" (pattern), but also "who you are" (unique biometric information) to authenticate the mobile user. Specifically, we use surface electromyography (sEMG)-based biometric information to enhance the security of pattern unlock. sEMG signals are generated by the electric activities of muscles and are recorded by the electrodes placed on the skin's surface. Since the sEMG signals are electric potentials generated by muscle cells, the same movements of different people will generate different electric potentials. Compared with existing biometric information used for screen unlocking, such as the fingerprint and face, sEMG signals are much harder to be forged, which makes the proposed scheme secure against attacks. Even the attackers can break the patterns using the aforementioned attacks, and they will not be able to forge the sEMG signals to gain access of the mobile device.

The rest of this paper is organized as follows. The related work on improving the security of pattern unlock and biometric-based mobile user authentication is described in Section 2. Section 3 introduces the background information of pattern unlock and EMG signals. The proposed method and experiment procedure are provided in Section 4. The experimental results are presented in Section 5. Finally, Section 6 concludes the paper.

2. Related Work

2.1. Improving the Security of Pattern Unlock

There are a number of schemes which have been proposed up to now to improve the security of pattern unlock. To defend against smudge attacks, Kwon et al. [9] proposed TinyLock, an affordable defense against smudge attacks. They made the size of the pattern grid very small and introduced a virtual wheel to wipe off the actual smudge. However, due to the tiny size grid, it has several drawbacks. Because the grid dots are not visible to the users, the error rate is very high, and it is very difficult to draw complex patterns. Concepts where the position of the pattern grid is translated to a different position, scale, and rotation on the screen for each unlock attempt have been explored by Schneegass et al. [10] and von Zezschwitz et al. [11]. However, they reported that users experienced difficulty in locating the grid due to its varying location. M-Pattern is a scheme which was proposed in [12] that employs multiple patterns to unlock the screen. The system randomly pick a pattern that can be inferred by the user from a visual cue, such as a background image. Since the smudges created by M-Pattern overlapped with each other, it was much harder for the attackers to recover the patterns compared with pattern unlock. The usability of the M-Pattern is compromised due to the memorization of multiple patterns by the user.

Besides smudge attacks, there are schemes proposed to defend against other attacks. Higashikawa et al. [13] proposed a shoulder-surfing-resistant scheme that uses a pass pattern of pattern unlock. The scheme utilizes challenge-and-response authentication and the user's short-term memory. In [14], a scheme called Pass-O was proposed, which employs a circular layout of the grid. Pass-O has a pattern space almost 2.5 times larger than pattern unlock, which makes it harder for guessing attacks. Chiang et al. [15] proposed a multi-layered drawing lock mechanism which greatly increases the pattern space compared with pattern unlock. Warp cells at the corners of the grid enable more complex patterns by using multiple layers. For example, when a warp cell is touched as part of pattern entry, a second empty grid layer is displayed, obscuring the original grid layer, on which the pattern entry can continue.

Some other schemes were also proposed to improve the security by encouraging users to create more complex patterns. Sun et al. [16] proposed a formula to calculate the pattern strength quantitatively.

The quantitative strength score is displayed through a pattern strength meter when the user creates a pattern. Their study showed that users created more complex patterns with the help of a pattern strength meter. TinyPal is an enhanced interface proposed in [17] for pattern unlock, which highlights the set of available dots that can be connected from the currently connected dot. TinyPal helps users create patterns containing more visual features, like overlaps and knight moves, to resist attacks. Their experimental results showed that users created more secure patterns using TinyPal than those using the original interface.

2.2. Biometrics-Based Mobile User Authentication

Biometrics have been widely used in the user authentication of mobile devices. The Apple Touch ID utilizes fingerprints to unlock the user's device and authenticate Apple Pay. However, it was shown in [18] that fingerprints can be easily forged. Face recognition is used by Apple Face ID and Android Face Unlock to unlock the screen, which is susceptible to attacks, such as using a photo or video of the authorized user.

Besides the traditional biometrics like the fingerprint and face, behavioral biometrics have also been used for user authentication of mobile devices. In [19], keystroke dynamics were combined with the PIN as multifactor authentication for the mobile user. Data from the motion sensors, such as the accelerometer, gyroscope, and rotation was included to improve the performance of authentication. Lamiche et al. [20] proposed a scheme that uses the gait pattern from the accelerometer and keystroke dynamics of text input for continuous authentication. The scheme was proved to be secure against the zero-effort attack and minimal-effort mimicking attack. SwipeVLock is a screen unlock mechanism proposed in [21] based on swipe dynamics. Touch features, such as the coordinates of location, touch pressure, touch size, touch time, and touch speed were used to model the swipe behavior.

Recently, the use of physiological biometrics for mobile user authentication has increased significantly. Huang et al. [22] proposed a privacy-preserving ECG-based authentication scheme that utilizes the ECG signal acquired by a medical IoT for ECG monitoring to authenticate the patient. A mobile EEG-based biometric authentication system was developed in [23] that combines EEG recordings with other techniques, such as nearfield communication (NFC) and face recognition. Kumar et al. [24] proposed a framework to enhance the pattern-based authentication with EEG signals. The Hidden Markov Model (HMM) was applied to model the EEG signals recorded during pattern drawing. The Support Vector Machine (SVM) classifier was then used to verify the authenticity of the drawn pattern. In the studies of [25,26], sEMG signals generated from a list of gestures were used for mobile user authentication. A list of gestures is used as the password, which is combined with the features extracted from the sEMG signals to defend against shoulder-surfing attacks.

In this paper, we propose to enhance the security of pattern unlock with sEMG-based biometrics. To the best of our knowledge, the proposed scheme is the first work that incorporates sEMG-based biometrics with pattern unlock for mobile user authentication.

3. Background

In this section, we provide the background information of pattern unlock and EMG signals.

3.1. Pattern Unlock

Pattern unlock was introduced by Google in 2008 as a graphic-based screen unlock scheme for Android devices. Instead of entering a PIN or typing a password, the user draws a pattern by connecting dots in a 3×3 grid. Figure 1 shows the pattern unlock grid with the dots labeled from 1 to 9. A pattern is represented as a sequence of connected dots, such as the pattern shown in Figure 1 is $1 \rightarrow 5 \rightarrow 9 \rightarrow 8 \rightarrow 7$.

A pattern has to follow the following rules to be valid: (1) It has to connect at least 4 dots; (2) each dot can only be connected once; (3) a pattern always connects the first unconnected dot along its path; (4) a pattern can go through a previously connected dot to connect an unconnected dot. Based on these

rules, it has been shown that the total number of valid patterns is 389,112 [6,16], which is less than the number of possible passwords for a four-character, case-insensitive alphabetic password. This indicates that pattern unlock is relatively weak in security compared with other schemes, such as the PIN and password, in terms of pattern space.

Figure 1. The 3 × 3 pattern unlock grid and a pattern 1 → 5 → 9 → 8 → 7.

3.2. EMG Signals

EMG signals record the electric activities produced by skeletal muscles, which usually have a potential difference. Therefore, when recording EMG signals, at least one pair of electrodes are needed. Sometimes a more complex array of multiple electrodes is used to record the activities of more than one muscle.

There are two types of EMG: surface EMG (sEMG) and intramuscular EMG (imEMG). sEMG signals are obtained by measuring muscle activities on the skin surface above the muscle. On the contrary, imEMG signals are recorded from the muscle tissue which are acquired by percutaneous wire needle electrodes inserted into muscle. Compared with imEMG, sEMG is convenient to acquire and is non-invasive. In this study, we used sEMG signals recorded from the forearm muscle as the biometric information for user authentication.

4. Materials and Methods

In this paper, we propose a new two-factor screen unlock scheme that utilizes sEMG-based biometric information to enhance the security of pattern unlock. In the following, we first provide an overview of the proposed scheme. The subjects recruited for this study are then introduced, followed by the description of the experiment protocol. The experiment serves as a proof-of-concept for the proposed scheme. Next, we present the features extracted from the sEMG signals. Finally, the one-class classification algorithms for user classification are introduced.

4.1. Overview of Proposed Scheme

The workflow of the proposed two-factor screen unlock scheme is illustrated in Figure 2. During the screen unlocking process, the user draws the unlock pattern on the screen of the device while the sEMG signals of the user are simultaneously recorded. The pattern drawn on the screen is first checked regarding whether it is the same as the one set by the authorized user or not. The access is denied if it is the wrong pattern. Otherwise, the recorded sEMG signals will further be used to verify the user. The verification is performed by extracting the time domain features from the recorded sEMG signals first. The features are then used as the input of a one-class classifier to classify the user as legitimate or not. Note that the one-class classifier is trained only using the data from the authorized user.

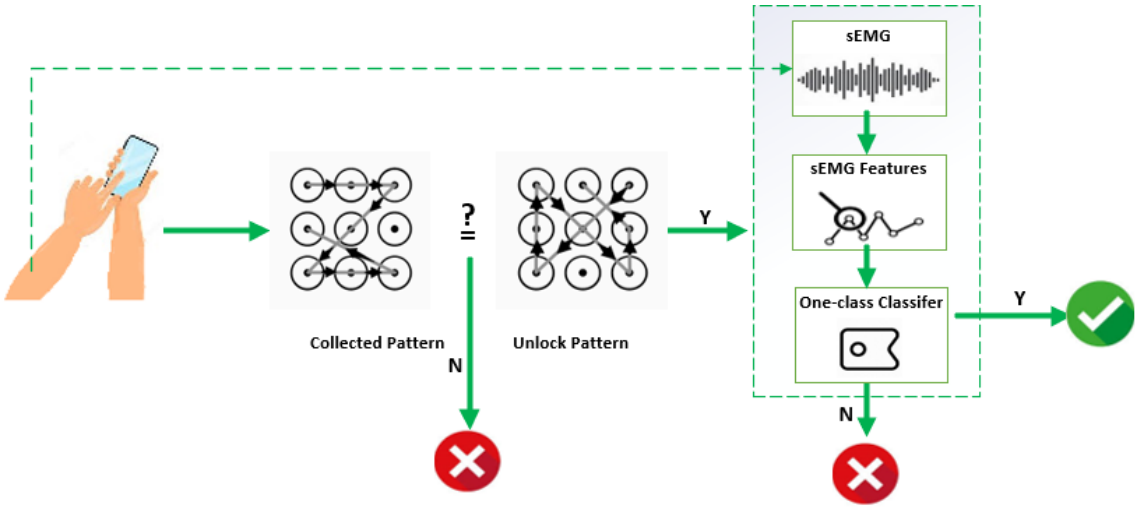

Figure 2. The workflow of the proposed two-factor screen unlock scheme.

4.2. Subjects

This study was approved by the Institutional Review Board (IRB) of New Mexico Institute of Mining and Technology. We recruited 10 subjects from the school (7 males and 3 females, age = 23.8 ± 2.5 years, height = 173.9 ± 9.7 cm, weight = 70.0 ± 15.6 kg, all right-handed) for this study. All participants reported that they did not have upper limb musculoskeletal and nervous system diseases.

4.3. Experimental Protocol

4.3.1. sEMG Signal Acquisition and Pre-Processing

The experiment setting is shown in Figure 3. The raw sEMG signal is recorded by a gold cup electrode (OpenBCI) placed on the FDS (Flexor Digitorum Superficialis) muscle of the forearm, which is connected to a Cyton biosensing board (OpenBCI). It is known that the activation of FDS corresponds to finger flexion [27]. The electrode placement of the experiment is shown in Figure 4. The sampling rate of the Cyton board is 250 Hz. The acquired sEMG signal is then sent from the Cyton board to the Cyton Dongle (OpenBCI), a Bluetooth adaptor plugged into a laptop. The OpenBCI GUI software installed on the laptop then records the acquired data in the local storage.

The quality of the recorded raw sEMG signals was affected by noises, such as direct current offset, environment noises, and artifact noises. We applied a 5Hz high-pass filter to eliminate the direct current offset, baseline drift due to the movement in recording, and perspiration. A 60Hz notch filter was then applied to filter out the power-line noise. Figure 5 shows an example of recorded sEMG signal after pre-processing.

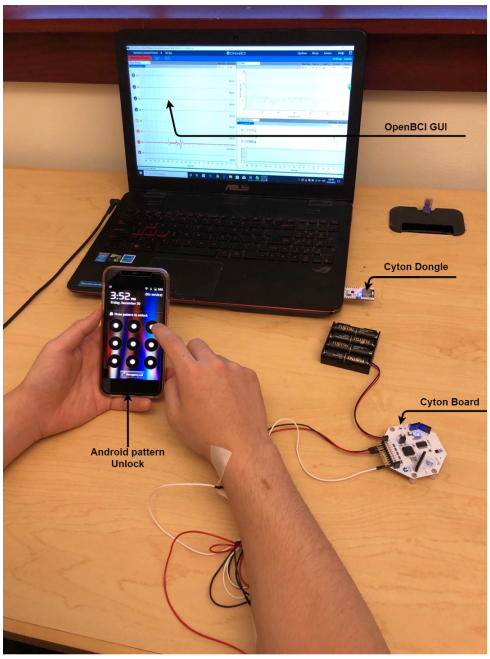

Figure 3. Experiment setting.

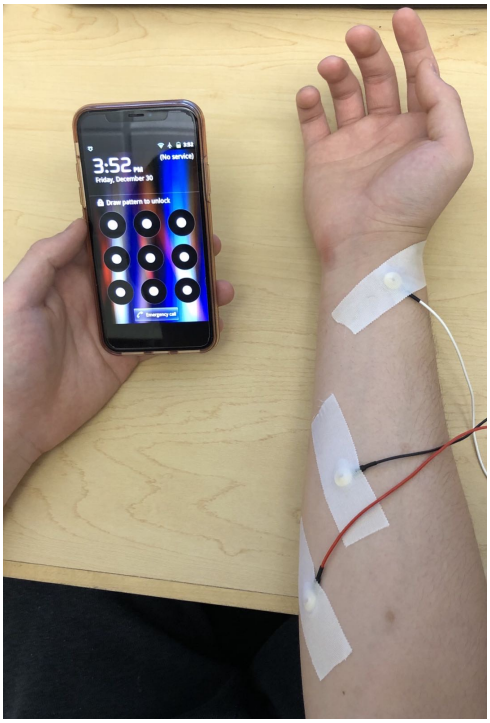

Figure 4. Electrode placement.

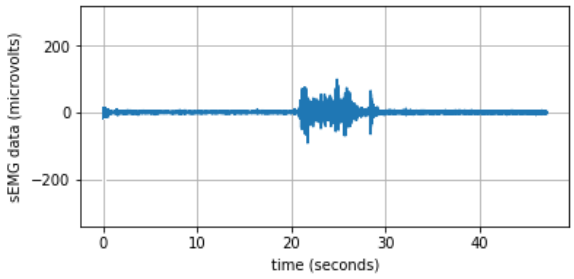

Figure 5. An example of recorded sEMG signal after pre-processing.

4.3.2. Experiment Procedure

During the experiment, each subject was comfortably seated on a chair before a table. The electrodes were placed on the subject's forearm, as shown in Figure 4. Before electrodes were placed, an alcohol pad was used to clean the skin of the electrode sites. The electrode cap gel was applied to the cleaned skin's surface to reduce electrode–skin impedance for better recording.

After the setting was done, the subject was instructed to draw the two patterns shown in Figure 6. Each pattern was repeated for 20 trials. sEMG signals were recorded for each trial. The subject was instructed to rest the arm on the table for one minute before the next trial to avoid muscle fatigue. The whole process for a subject lasted about one hour and twenty minutes, which consisted of 40 trials for the two patterns.

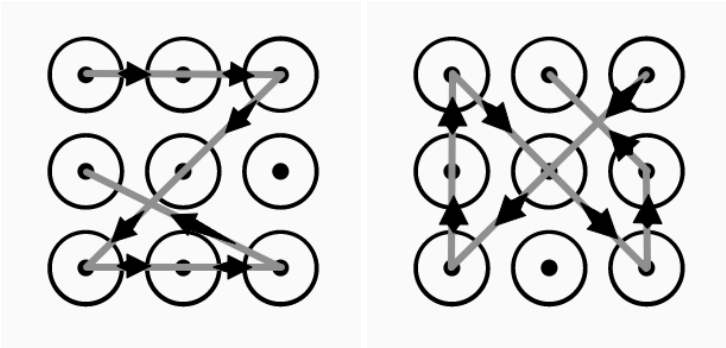

Figure 6. Two patterns used in the experiment. Left: $1 \rightarrow 2 \rightarrow 3 \rightarrow 5 \rightarrow 7 \rightarrow 8 \rightarrow 9 \rightarrow 4$; Right: $3 \rightarrow 5 \rightarrow 7 \rightarrow 4 \rightarrow 1 \rightarrow 9 \rightarrow 6 \rightarrow 2$.

4.4. sEMG Feature Extraction

There are three types of features that can be extracted from sEMG signals: time domain features, frequency domain features, and time-frequency domain features [28]. In our study, we concentrated on using features extracted from the time domain, which are widely used in studies and practices due to their low computational complexity compared with frequency domain and time-frequency domain features and performance in low-noise environments [29–32]. We selected the following 11 time domain features in this study.

4.4.1. Mean Absolute Value (MAV)

MAV is one of the most popular time domain features for EMG signal analysis [28]. It has been widely used as an onset detection index for applications like prosthetic limb control [33]. MAV is calculated as the mean absolute value of the EMG signal in a segment, as shown in Equation (1), where N is the number of samples in the segment, and X_i is the ith sample of the segment.

$$MAV = \frac{1}{N} \sum_{i=1}^{N} |X_i| \tag{1}$$

4.4.2. Variance (VAR)

VAR is a measure of the power of the EMG signal [34]. Since the mean value of the EMG signal is close to zero, VAR is defined as:

$$VAR = \frac{1}{N-1} \sum_{i=1}^{N} {X_i}^2. \tag{2}$$

4.4.3. High-Order Temporal Moment (TM)

The temporal moment (TM) was proposed in [35] as a statistical analysis of EMG signals for prosthetic arm control. The first-order TM is the same as MAV, and the second-order TM is similar to

VAR. High-order TMs from Order 3 to Order 5 (TM3, TM4, and TM5) used in [35] were employed in our study. They are defined in Equations (3)–(5). Note that for the calculation of odd moments, the absolute value was taken to reduce within-class separation [35].

$$TM3 = |\frac{1}{N}\sum_{i=1}^{N} {X_i}^3| \tag{3}$$

$$TM4 = \frac{1}{N}\sum_{i=1}^{N} {X_i}^4 \tag{4}$$

$$TM5 = |\frac{1}{N}\sum_{i=1}^{N} {X_i}^5| \tag{5}$$

4.4.4. Mean Square Root (MSR)

The Mean Square Root (MSR) is a time-domain feature proposed in [31] for limb motion classification. The feature provides an estimation of the total amount of activity.

$$MSR = \frac{1}{N}\sum_{i=1}^{N} |X_i|^{1/2} \tag{6}$$

4.4.5. Root Mean Square (RMS)

The Root Mean Square (RMS) is another popular feature for EMG pattern recognition [30,32], which is related to constant force and non-fatiguing contraction. RMS is similar to the standard deviation of the EMG signal, as the mean of the signal is close to zero.

$$RMS = \sqrt{\frac{1}{N}\sum_{i=1}^{N} {X_i}^2} \tag{7}$$

4.4.6. Log Detector (LD)

The Log Detector (LD) is a non-linear detector that provides an estimation of the muscle contraction force [34]. LD is defined in Equation (8) where $exp(\cdot)$ is the exponential function.

$$LD = exp(\frac{1}{N}\sum_{i=1}^{N} log(|X_i|)) \tag{8}$$

4.4.7. Waveform Length (WL)

Waveform Length (WL) is a measure of the waveform complexity of the EMG signal [33], which is defined as the cumulative length of the waveform over the segment, as shown in Equation (9).

$$WL = \sum_{i=1}^{N-1} |X_{i+1} - X_i| \tag{9}$$

4.4.8. Difference Absolute Standard Deviation Value (DASDV)

The Difference Absolute Standard Deviation Value (DASDV) is a feature similar to RMS, which uses the difference value between two adjacent samples instead of the sample value [36].

$$DASDV = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N-1} (X_{i+1} - X_i)^2} \tag{10}$$

4.4.9. Number of Zero Crossing (NZC)

Number of Zero Crossing (NZC) is a time-domain feature that measures the frequency information of an EMG signal [33]. It is defined as the number of times the signal crosses zero. A threshold, T, was included in the calculation to reduce the effect of noise-induced zero-crossings [33].

$$NZC = \sum_{i=1}^{N-1} [sgn(X_i \times X_{i+1}) \cap |X_i - X_{i+1}| \geq T] \tag{11}$$

$$sgn(x) = \begin{cases} 1, & \text{if } x < 0, \\ 0, & \text{otherwise.} \end{cases}$$

4.5. One-Class Classification Algorithms

For the purpose of user authentication, all users were considered as abnormal except for the authorized user. One-class classification algorithms are suitable for the task, as they are trained only using the data from the authorized user. In this study, two popular one-class classification algorithms were employed: the one-class SVM (OCSVM) and local outlier factor (LOF).

4.5.1. OCSVM

SVM is a widely used supervised learning algorithm for multi-class classification. It was extended for the one-class classification problem in [37,38]. OCSVM looks for a non-linear decision boundary by mapping the training samples $x_i (i = 1, 2, ..., n)$ into a higher dimension feature space using a non-linear kernel map function $\Phi(\cdot)$. A hyperplane was then calculated to separate the mapped training samples from the origin with maximal margin, which will be used as the decision boundary. The quadratic programming minimization function used to separate the training samples from the origin is defined below, where ω is the normal vector to the hyperplane, ξ is for penalization, ρ is the margin, and $\nu \in (0, 1)$ is a parameter to control the ratio of anomalies in the training samples.

$$\begin{gathered} min \left(\frac{1}{2} ||\omega||^2 + \frac{1}{\nu n} \sum_{i=1}^{n} \xi_i - \rho \right) \\ \text{subject to} \\ (\omega \cdot \Phi(x_i)) \geq \rho - \xi_i, \quad \xi_i \geq 0 \end{gathered} \tag{12}$$

After solving the problem with ω and ρ, the decision function is defined in Equation (13). A new sample y was classified as an anomaly if $f(y)$ was negative.

$$f(x) = sgn((\omega \cdot \Phi(x)) - \rho) \tag{13}$$

There are several choices of the kernel function for OCSVM. In this study, the radial basis function (RBF) kernel was chosen, which produced the best results among all kernels. The RBF kernel is defined in Equation (14), where $||x - x'||^2$ is the squared Euclidean distance between two data points x and x', and σ is a parameter related to the decision region. A smaller σ leads to a broader decision region.

$$K(x, x') = exp\left(-\frac{||x - x'||^2}{2\sigma^2} \right) \tag{14}$$

4.5.2. LOF

LOF is a popular anomaly detection algorithm proposed in [39]. LOF is based on the idea of local reachability density (LRD) which is calculated as the inverse of the average distance from a sample to its k nearest neighbors. The LOF score of a sample x is then calculated as the degree of x isolated

from its k nearest neighbors, as shown in Equation (15). A LOF score larger than one indicates that the sample is an anomaly.

$$LOF(x) = \frac{\sum_{p \in N_k(x)} \frac{LRD(p)}{LRD(x)}}{k}, \tag{15}$$

where $N_k(x)$ is the set of k nearest neighbors for x.

5. Performance Evaluation and Results

5.1. Dataset

During the experiment, we collected the sEMG signals of 10 subjects when they were drawing unlock patterns. For each subject, 20 trials of sEMG signals were recorded for each of the two patterns shown in Figure 6. A 6*s* signal segment was extracted from each trial, starting from the time when the subject started the drawing of the unlock pattern. Each segment was further divided into a series of overlapping analysis windows with a window length of 2 s and a 1 s overlapping, which is shown in Figure 7. The 11 time domain features described in Section 4.4 were then calculated for each analysis window. A total of 55 features were extracted for each segment, which is an instance of a dataset. Finally, we obtained two datasets for the two patterns. Each dataset contains 200 instances for the 10 subjects.

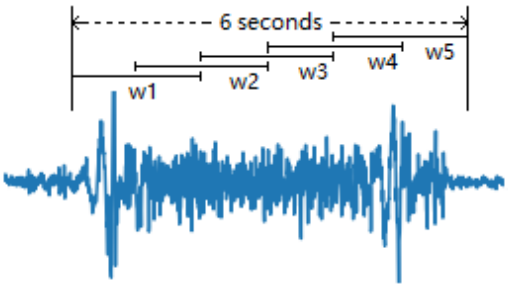

Figure 7. sEMG signal segment divided into a series of overlapping analysis windows.

5.2. Performance Metrics

The proposed scheme was evaluated using two popular metrics for measuring the performance of authentication systems: F_1 score and Half of Total Error Rate (HTER). Here, the patterns from the authorized user or client were treated as negatives, while the patterns from the unauthorized users or impostors were positives. The two metrics were calculated from the four elements of the confusion matrix, true positives (TP), false positives (FP), true negatives (TN), and false negatives (FN). TP and TN are the numbers of correctly classified patterns from the impostors and client, respectively. FP and FN are the numbers of misclassified patterns from the client and impostors, respectively.

F_1 score is a widely used metric for evaluating the performance of classifiers which is defined as the harmonic mean of precision and recall, as shown in Equation (16).

$$F_1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{16}$$

$$Precision = \frac{TP}{TP + FP} \tag{17}$$

$$Recall = \frac{TP}{TP + FN} \tag{18}$$

HTER has been used for evaluating the performance EEG-based authentication systems [24,40]. HTER is defined as the average of the False Acceptance Rate (FAR) and False Rejection Rate (FRR):

$$HTER = \frac{FAR + FRR}{2} \tag{19}$$

FAR is the ratio of the number of false acceptances to the number of attempts from the impostors. FRR is the ratio of the number of false rejections to the number of attempts from the client.

$$FAR = \frac{FN}{TP + FN} \tag{20}$$

$$FRR = \frac{FP}{TN + FP} \tag{21}$$

5.3. Results

We tested the authentication performance using sEMG-based biometrics for each of the 10 subjects as the client. Subjects other than the client were considered as impostors for the test. For a dataset obtained in Section 5.1, we randomly selected 10 instances from the client for training. Other instances of the dataset were used for testing. The data was normalized using min–max normalization. The process was repeated 10 times for each subject. Python and the scikit-learn library [41] were used for the experiment.

Tables 1 and 2 show the test results for unlock patterns 1 and 2, respectively. The mean and standard deviation of the results obtained from the 10 repeated tests on a subject are reported in the tables. It can be seen that both OCSVM and LOF achieve good performance in terms of the F_1 score, indicating that they are good at finding attempts from impostors. On the other hand, LOF has significantly better performance than OCSVM in terms of HTER, which is due to the high FRR obtained by OCSVM. Thus, LOF is a better classifier than OCSVM for our task. We also observe that the results obtained from the two patterns are similar. The performance evaluation demonstrates that using LOF with time domain features extracted from sEMG signals for user identification is a viable solution for enhancing the security of pattern unlock.

Table 1. Authentication test results of 10 subjects (Pattern 1).

	OCSVM		**LOF**	
Subject	F_1	**HTER**	F_1	**HTER**
1	0.9760 ± 0.0054	0.1911 ± 0.0505	0.9755 ± 0.0060	0.1200 ± 0.0338
2	0.9746 ± 0.0066	0.2350 ± 0.0626	0.9882 ± 0.0045	0.1031 ± 0.0383
3	0.9786 ± 0.0075	0.1931 ± 0.0740	0.9812 ± 0.0070	0.1144 ± 0.0720
4	0.9786 ± 0.0042	0.1975 ± 0.0399	0.9789 ± 0.0067	0.1281 ± 0.0363
5	0.9764 ± 0.0071	0.1706 ± 0.0496	0.9751 ± 0.0072	0.1003 ± 0.0388
6	0.9602 ± 0.0104	0.2042 ± 0.0478	0.9617 ± 0.0109	0.1094 ± 0.0256
7	0.9831 ± 0.0064	0.1550 ± 0.0599	0.9912 ± 0.0046	0.0733 ± 0.0442
8	0.9759 ± 0.0052	0.2225 ± 0.0492	0.9920 ± 0.0049	0.0725 ± 0.0045
9	0.9812 ± 0.0058	0.1725 ± 0.0546	0.9920 ± 0.0047	0.0725 ± 0.0432
10	0.9807 ± 0.0054	0.1775 ± 0.0506	0.9844 ± 0.0033	0.0844 ± 0.0254

Table 2. Authentication test results of 10 subjects (Pattern 2).

	OCSVM		LOF	
Subject	F_1	**HTER**	F_1	**HTER**
1	0.9780 ± 0.0051	0.2025 ± 0.0480	0.9892 ± 0.0047	0.0731 ± 0.0337
2	0.9386 ± 0.0085	0.1931 ± 0.0452	0.9402 ± 0.0162	0.1328 ± 0.0253
3	0.9779 ± 0.0058	0.1870 ± 0.0605	0.9789 ± 0.0047	0.1100 ± 0.0215
4	0.9762 ± 0.0068	0.2200 ± 0.0643	0.9885 ± 0.0050	0.0850 ± 0.0564
5	0.9804 ± 0.0044	0.1800 ± 0.0415	0.9898 ± 0.0027	0.0814 ± 0.0303
6	0.9717 ± 0.0058	0.2625 ± 0.0556	0.9901 ± 0.0054	0.0771 ± 0.0592
7	0.9767 ± 0.0053	0.2106 ± 0.0537	0.9763 ± 0.0111	0.1192 ± 0.0405
8	0.9748 ± 0.0045	0.2325 ± 0.0426	0.9920 ± 0.0044	0.0725 ± 0.0399
9	0.9523 ± 0.0899	0.2500 ± 0.0402	0.9465 ± 0.0083	0.1272 ± 0.0442
10	0.9745 ± 0.0057	0.2008 ± 0.0581	0.9733 ± 0.0118	0.1042 ± 0.0412

6. Conclusions

Pattern unlock is a popular screen unlock mechanism, but has relatively weak security compared with other mechanisms, such as the PIN and password. It is susceptible to various attacks, including guessing attacks, over-the-shoulder attacks, smudge attacks, and side channel attacks. In this paper, we proposed a new two-factor authentication scheme that utilizes sEMG-based biometrics to enhance the security of pattern unlock. The proposed scheme uses time domain features extracted from recorded sEMG signals and one-class classifiers to determine the authenticity of the user. To test the effectiveness of the proposed scheme, 10 subjects were recruited for the study. The results show that the proposed scheme achieves good authentication performance in terms of F_1 score and HTER. In addition to mobile devices, the proposed scheme has the potential to be applied for the vehicle access control system of electrical vehicles (EVs) which is projected to be a 22.6 billion market by 2027 [42]. There are several limitations of the current research. First, the sEMG acquisition system used in the experiment was for the purpose of proof-of-concept, which is not intended for real-world applications. Wearable wireless sEMG acquisition devices, such as the MyoWare Muscle Sensor [43] or Myo Armband [44] with better usability should be considered in those scenarios. The second limitation is the relatively small number of subjects recruited for the experiment. We plan to perform larger-scale testing of the proposed scheme in the future. Finally, the experiment conducted in the paper only considered the scenario of using both hands to unlock the device. In future studies, we will also consider the scenario of using only one hand to unlock the device.

Author Contributions: Conceptualization, J.Z.; methodology, J.Z.; software, Q.L. and P.D.; data curation, Q.L. and P.D.; writing–original draft preparation, Q.L. and J.Z.; writing-review and editing, J.Z.; supervision, J.Z.; funding acquisition, J.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This material is based upon work funded by the National Science Foundation EPSCoR Cooperative Agreement OIA-1757207.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Mobile vs. Desktop Usage. Available online: https://www.broadbandsearch.net/blog/mobile-desktop-internet-usage-statistics (accessed on 6 December 2019).
2. Bruggen, D.V. Studying the Impact of Security Awareness Efforts on User Behavior. Ph.D. Thesis, University of Notre Dame, Notre Dame, IN, USA, 2014.

3. Von Zezschwitz, E.; Dunphy, P.; de Luca, A. Patterns in the wild: A field study of the usability of pattern and pin-based authentication on mobile devices. In Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services, Munich, Germany, 27–30 August 2013; pp. 261–270.
4. Cha, S.; Kwag, S.; Kim, H.; Huh, J. Boosting the guessing attack performance on android lock patterns with smudge attacks. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, Abu Dhabi, UAE, 2–6 April 2017; pp. 313–326.
5. Aviv, A.J.; Wolf, F.; Kuber, R. Comparing video based shoulder surfing with live simulation. In Proceedings of the 34th Annual Computer Security Applications Conference (ACSAC'18), San Juan, PR, USA, 3–7 December 2018; pp. 452–466.
6. Aviv, A.J.; Gibson, K.; Mossop, E.; Blaze, M.; Smith, J.M. Smudge attacks on smartphone touch screens. In Proceedings of the 4th USENIX Conference on Offensive Technologies (WOOT'10), Washington, DC, USA, 9 August, 2010; pp. 1–7.
7. Aviv, A.J.; Sapp, B.; Blaze, M.; Smith, J.M. Practicality of accelerometer side channels on smartphones. In Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC'12), Orlando, FL, USA, 3–7 December 2012; pp. 41–50.
8. Ye, G.; Tang, Z.; Fang, D.; Chen, X.; Kim, K.; Taylor, B.; Wang, Z. Cracking Android pattern lock in five attempts. In Proceedings of the 2017 Network and Distributed System Security Symposium (NDSS'17), San Diego, CA, USA, 26 February–1 March 2017.
9. Kwon, T.; Na, S. TinyLock: Affordable defense against smudge attacks on smartphone pattern lock systems. *Comput. Secur.* **2014**, *42*, 137–150. [CrossRef]
10. Schneegass, S.; Steimle, F.; Bulling, A.; Alt, F.; Schmidt, A. SmudgeSafe: Geometric image transformations for smudge resistant user authentication. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp'14), Seattle, MA, USA, 13–17 September 2014; pp. 775–786.
11. von Zezschwitz, E.; Koslow, A.; de Luca, A.; Hussmann, H. Making graphic-based authentication secure against smudge attacks. In Proceedings of the 2013 International Conference on Intelligent User Interfaces (IUI'13), Santa Monica, CA, USA, 19–22 March 2013; pp. 277–286.
12. Zheng, J.; Chigurupati, S.K. M-Pattern: A novel scheme for improving the security of Android pattern unlock against smudge attacks. *ICT Express* **2019**, *5*, 192–195. [CrossRef]
13. Higashikawa, S.; Kosugi, T.; Kitajima, S.; Mambo, M. Shoulder-surfing resistant authentication using pass pattern of pattern lock. *IEICE Trans. Inf. Syst.* **2018**, *E101.D*, 45–52. [CrossRef]
14. Tupsamudre, H.; Banahatti, V.; Lodha, S.; Vyas, K. Pass-O: A proposal to improve the security of pattern unlock scheme. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS'17), Abu Dhabi, UAE, 2–6 April 2017; pp. 400–407.
15. Chiang, H.; Chiasson, S. Improving user authentication on mobile devices: A touchscreen graphical password. In Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI'13), Munich, Germany, 27–30 August 2013; pp. 251–260.
16. Sun, C.; Wang, Y.; Zheng, J. Dissecting pattern unlock: The effect of pattern strength meter on pattern selection. *J. Inf. Secur. Appl.* **2014**, *19*, 308–320. [CrossRef]
17. Tupsamudre, H.; Vaddepalli, S.; Banahatti, V.; Lodha, S. TinPal: An enhanced interface for pattern locks. In Proceedings of the 2018 Workshop on Usable Security (USEC 2018), Cambridge, UK, 19–21 March 2018; pp. 1–11.
18. Matsumoto, T.; Matsumoto, H.; Yamada, K.; Hoshino, S. Impact of artificial 'gummy' fingers on fingerprint systems. In Proceedings of the SPIE Optical Security and Counterfeit Deterrence Techniques IV, Berlin, Germany, 19 April 2002; Volume 4677, pp. 275–289.
19. Lee, H.; Hwang, J.Y.; Kim, D.I.; Lee, S.; Lee, S.-H.; Shin, J.S. Understanding keystroke dynamics for smartphone users authentication and keystroke dynamics on smartphones built-in motion sensors. *Secur. Commun. Netw.* **2018**, *2018*, 2567463. [CrossRef]
20. Lamiche, I.; Bin, G.; Jing, Y.; Yu, Z.; Hadid, A. A continuous smartphone authentication method based on gait patterns and keystroke dynamics. *J. Ambient Intell. Humaniz. Comput.* **2019**, *10*, 4417–4430. [CrossRef]
21. Li, W.; Tan, J.; Meng, W.; Wang, Y.; Li, J. SwipeVLock: A supervised unlocking mechanism based on swipe behavior on smartphones. In Proceedings of the International Conference on Machine Learning for Cyber Security (ML4CS 2019), Xi'an, China, 19–21 September 2019; pp. 140–153.

22. Huang, P.; Guo, L.; Li, M.; Fang, Y. Pratical privacy-preserving ECG-based authentication for IoT-based healthcare. *IEEE Internet Things J.* **2019**, *6*, 9200–9210. [CrossRef]
23. Klonovs, J.; Petersen, C.K.; Olesen, H.; Hammershoj, A. ID proof on the go: Development of a mobile EEG-based biometric authentication system. *IEEE Veh. Technol. Mag.* **2013**, *8*, 81–89. [CrossRef]
24. Kumar, P.; Saini, R.; Roy, P.P.; Dogra, P.D. A bio-signal based framework to secure mobile devices. *J. Netw. Comput. Appl.* **2017**, *89*, 62–71. [CrossRef]
25. Yamaba, H.; Kurogi, K.; Kubota, S.; Katayama, T.; Park, M.; Okazaki, N. Evaluation of feature values of surface electromyograms for user authentication on mobile devices. *Artif. Life Robot.* **2017**, *22*, 108–112. [CrossRef]
26. Yamaba, H.; Aburada, K.; Katayama, T.; Park, M.; Okazaki, N. Evaluation of user identification methods for realizing an authentication system using s-EMG. In Proceedings of the International Conference on Network-Based Information Systems (NBiS 2018), Bratislava, Slovakia, 10–12 September 2018; pp. 733–742.
27. Tendons. Available online: http://www.assh.org/handcare/Anatomy/Tendons (accessed on 6 December 2019).
28. Phinyomark, A.; Phukpattaranont, P.; Limsakul, C. Feature reduction and selection for EMG signal classification. *Expert Syst. Appl.* **2012**, *39*, 7420–7431. [CrossRef]
29. Phinyomark, A.; Quaine, F.; Charnonnier, S.; Serviere, C.; Tarpin-Bernard, F.; Laurillau, Y. Feature extraction of the first difference of EMG time series for EMG pattern recognition. *Comput. Methods Programs Biomed.* **2014**, *117*, 247–256. [CrossRef] [PubMed]
30. Yang, Z.; Chen, Y. Surface EMG-based sketching recognition using two analysis windows and gene expression programming. *Front. Neurosci.* **2016**, *10*, 445. [CrossRef] [PubMed]
31. Samuel, O.W.; Zhou, H.; Li, X.; Wang, H.; Zhang, H.; Sangaiah, A.K.; Li, G. Pattern recognition of electromyography signals based on novel time domain features for amputees' limb motion classification. *Comput. Electr. Eng.* **2018**, *67*, 646–655. [CrossRef]
32. Qi, J.; Jiang, G.; Li, G.; Sun, Y.; Tao, B. Intelligent human-computer interaction based on surface EMG gesture recognition. *IEEE Access* **2019**, *7*, 61378–61387. [CrossRef]
33. Hudgins, B.; Parker, P.; Scott, R.N. A new strategy for multifunction myoelectric control. *IEEE Trans. Biomed. Eng.* **1993**, *40*, 82–94. [CrossRef] [PubMed]
34. Zardoshti-Kermani, M.; Wheeler, B.C.; Badie, K.; Hashemi, R.M. EMG feature evaluation for movement control of upper extremity prostheses. *IEEE Trans. Rehabil. Eng.* **1995**, *3*, 324–333. [CrossRef]
35. Saridis, G.N.; Gootee, T.P. EMG pattern analysis and classification for a prosthetic arm. *IEEE Trans. Biomed. Eng.* **1982**, *29*, 403–412. [CrossRef] [PubMed]
36. Kim, K.S.; Choi, H.H.; Moon, C.S.; Mun, C.W. Comparison of k-nearest neighbor, quadratic discriminant and linear discriminant analysis in classification of electromyogram signals based on the wrist-motion directions. *Curr. Appl. Phys.* **2011**, *11*, 740–745. [CrossRef]
37. Scholkopf, B.; Williamson, R.C.; Smola, A.J.; Shawe-Taylort, J.; Platt, J. Support vector method for novelty detection. In Proceedings of the 12th International Conference on Neural Information Processing Systems, Denver, CO, USA, 29 November–4 December 1999; pp. 582–588.
38. Scholkopf, B.; Smola, A.J.; Williamson, R.C.; Bartlett, P.L. New support vector algorithms. *Neural Comput.* **2000**, *12*, 1207–1245. [CrossRef] [PubMed]
39. Breunig, M.M.; Kriegel, H.-P.; Ng, R.T.; Sander, J. LOF: Identifying density-based local outliers. In Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, Dallas, TX, USA, 16–18 May 2000; pp. 93–104.
40. Chuang, J.; Nguyen, H.; Wang, C.; Johnson, B. I think, therefor i am: Usability and security of authentication using biometrics. In Proceedings of the International Conference on Financial Cryptography and Data Security, Okinawa, Japan, 1–5 April 2013; pp. 1–16.
41. Scikit-Learn: Machine Learning in Python. Available online: https://scikit-learn.org/ (accessed on 6 December 2019).
42. Vehicle Access Control Market by Biometric (Fingerprint, Face, Iris, Voice), Non-biometric (Stolen Vehicle Assist, Keyless, Immobilizer, Alarm, Steering Lock), Technology (Bluetooth, NFC, RFID, Wi-Fi), Vehicle Type, EV & Region—Global Forecast to 2027. Available online: https://www.marketsandmarkets.com/Market-Reports/vehicle-access-control-market-266613080.html (accessed on 6 December 2019).

43. MyoWare Muscle Sensor. Available online: http://www.advancertechnologies.com/p/myoware.html (accessed on 6 December 2019).
44. Myo Armband. Available online: https://newatlas.com/myo-gesture-control-armband-review/39103/ (accessed on 6 December 2019).