Hindawi
Security and Communication Networks
Volume 2020, Article ID 9282380, 14 pages
https://doi.org/10.1155/2020/9282380

Research Article

User Authentication Method Based on MKL for Keystroke and Mouse Behavioral Feature Fusion

Xiujuan Wang,[1] Qianqian Zheng,[1] Kangfeng Zheng,[2] and Tong Wu[2]

[1]*Information Technology Institute, Beijing University of Technology, Beijing 100124, China*
[2]*School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China*

Correspondence should be addressed to Kangfeng Zheng; kfzheng@bupt.edu.cn

Received 17 September 2019; Revised 8 February 2020; Accepted 5 May 2020; Published 20 May 2020

Academic Editor: Gregorio Martinez Perez

In order to improve the recognition rate of users with single behavioral feature and prevent impostors from restricting an input device to avoid detection, a dual-index user authentication method based on Multiple Kernel Learning (MKL) for keystroke and mouse behavioral feature fusion was proposed in this paper. Due to the heterogeneity between the keystroke features and the mouse features, we argue that each type of features is mapped to a suitable kernel and the weights of each kernel are obtained through computing and then summed to obtain a compound kernel that implements the multifeature fusion. The dataset used in this paper was collected under complete uncontrolled condition from some volunteers by using our data collection program. The experimental results show that the proposed method can obtain the best recognition accuracy of 89.6%. Compared to the traditional methods of single feature, the dual-index method can get more stable and effective authentication. Therefore, the proposed method in this paper fully demonstrates the reliability of dual-index user authentication.

1. Introduction

With the rapid development of the Internet, the lives of people have been related to the Internet closely, and information systems can bring convenience to everyone in many aspects. However, security guarantees have aroused the concerns of people, and how to protect the privacy of users has become a vital research topic. User authentication is an important security means and can be seen everywhere in daily lives [1]. Most authentication systems are designed to identify the user's operational rights to the system, for instance, logging into a computer system, entering a mobile phone system, and performing business at a bank and so on. The simplest and most traditional authentication method is achieved by using username and password. Once a user enters the system, the resources in the system can always be viewed by the user until the user logs out [2]. However, during the period from the user logging in to exiting the system, the whole system is in a low-security environment, and impostors can steal some important resources. For example, when people leave the unlocked computer for a short or long time to drink water or talk with colleagues, or because they are not accustomed to lock the computer at any time, the possibility that the system information is stolen by others is very high during these periods. Therefore, it is extremely important to continuously check the identity of users, and continuous authentication is not an alternative to the initial login scheme but provides additional safety measures [3].

Identity authentication has always been an active research topic in the academic field. As a new identity authentication technology, biometric authentication has been widely and extensively applied to various fields and has higher reliability compared with traditional technologies [4]. Biometric authentication includes physiological and behavioral characteristics. Physiological characteristics have become the focus of the certification due to their unique characteristics, including fingerprint features, iris features, and facial features. But the use of physiological features requires not only additional hardware support but also the verification and collection of individual features, which does not support continuous interference-free authentication.

While behavior-based biometric authentication systems utilize commonly available computer interface devices to collect data, such as keyboard and mouse, the behaviors taken during human-computer interaction do not require additional auxiliary equipment, so it has the advantage of the low cost [5, 6].

Researches based on user behavioral features have been extensively studied, mainly including keystroke dynamics (KD) and mouse dynamics (MD) (for more researches based on these features, see Sections 2.1, 2.2, and 2.3). A large number of techniques on KD and MD have been considered as an effective means, including machine learning algorithms and statistical learning methods, and the continuous improvement of various methods has yielded remarkable results. However, due to the enormous differences in various data acquisition and data processing, the final recognition effects exit otherness and it is discovered that there were few researches on the combination of KD and MD [7]. But the user behaviors of the keystroke and the mouse operation are very different in a certain period of time, so the dual-index behavioral features can not only compensate for the instability caused by single behavioral features but also improve the accuracy and security of identity authentication.

In order to further improve the accuracy of identity authentication, this article proposes a new user authentication method based on MKL [8] for the keystroke and mouse behavioral feature fusion. In uncontrolled environments, human-computer interaction (HCI) is monitored by the program to obtain real data generated by keystroke and mouse operations in daily works; the study of human behavior is particularly meaningful in the field of HCI, because it can provide insight into human behavior [9]. This paper collects some volunteers' daily HCI data with the collection program developed by ourselves. Keystroke and mouse behavioral features are extracted from the collected raw data and fused by MKL (for more research on MKL, see Section 2.4) to achieve efficient and dependable authentication. The method proposed in this paper is named as user authentication based on MKL (UAMKL).

The main contributions of our work are summarized as follows.

(i) In Section 2, the researches of KD, MD, a combination of KD and MD in identity authentication are briefly reviewed, and the related research of MKL is summarized.

(ii) In Section 3, the framework of the proposed authentication method is first briefly described. Then, the methods of the data collection and feature extraction as well as the classification techniques used in this paper are introduced. Finally, the evaluation indicators and the specific implementation of experiments are described in detail.

(iii) Section 4 demonstrates and analyses the experiments' results.

(iv) The work done in this paper is summarized in Section 5 based on the research content of the previous parts, and the future research direction is proposed.

2. Related Research

2.1. KD. The researches on KD-based authentication technology started in the 1980s and have been developed for more than 30 years, and many researchers have proposed a large number of methods. Within KD literature, the keystroke features are mainly divided into two categories: static (fixed text) and dynamic (free-text), and both types of research have acquired a lot of results and made breakthrough progress.

In 1980, Gaines first proposed the method of user identity authentication based on the keystroke time series and the hypothesis test [10]. Seven users were selected in the experiment to type in three paragraphs of texts in two periods, each of which was input ten times, and then Gaines analyzed the time data of the entered letters. Although the data reliability and the experimental results were not ideal because of the simplicity of experiment and the small sample size, this research provided a new research direction for the application of keystroke behavioral features in the identity authentication. In 1990, Bleha et al. [11] presented a keystroke behavior recognition method based on Bayesian statistical classification, which further promoted the development of KD in the identity authentication, and the experiment obtained 2.8% false accept rate (FAR) and 8.1% false reject rate (FRR). Leggett et al. [12] designed a keystroke behavior detection system based on the principle of continuous statistics and compared the reference data with the test data in 1991. The experimental results were found to be acceptable for users with more than 60% effective data, while users with less than 60% chose to reject, and sum of illegal pass rate and legal reject rate was 24%. The identity recognition system was not practical, due to the high illegal pass rate and the limitation of the data quantity. Brow et al. [13] presented the approach for classification by Neural Network (NN), which greatly improved the authentication accuracy in 1993.

In the following years, many new methods were continuously proposed and quickly applied to the authentication research field based on keystroke features. Enzhe et al. [14] conducted a comprehensive analysis of key problems and applications in keystroke recognition in 2004 and proposed a recognition method based on Support Vector Machine (SVM) combined with Genetic Algorithm (GA). Recognition accuracy was improved, but it suffered from high computational complexity and the optimal parameters were unable to be found. Ahmed et al. [15] studied the time information of keystroke features of 17 test users, and identification was obtained with NN. The results showed that the average error rate (EER) was 2.46%. Although this method obtained considerable results, its classification and prediction took a long time. Morales et al. [16] used the scoring normalization technique to effectively improve the authentication accuracy of the KD authentication system. Li et al. [17] presented authentication approach by incorporating the dynamics of both free-text keystroke latency features and statistical wrist motion patterns extracted from the wrist worn smartwatches, and dynamic trust model (DTM) was developed to fuse two one-vs-all Random Forest

Ensemble Classifiers (RFECs). The result was that an impostor or intruder was detected within no more than one sentence (average 56 keystrokes) with the FRR of 1.82% and the FAR of 1.94%. Monaro et al. [18] analyzed the unique KD features in keyboard input answers to the fixed questions. The experimental results showed that the accuracy of the keystroke analysis to distinguish between the impostors and real users reached 95%. Krishnamoorthy el al. [19] proposed the feature selection approach based on minimum redundancy maximum relevance (mRMR) to get the classification accuracy of 97.4% and found that touch pressure, touch size, and coordinates were effective in identifying each user. Lu el al. [1] propose a model of a recursive NN plus a convolutional NN to learn a sequence of individual keystroke vectors to obtain individual keystroke features for the identity authentication in 2019, and the best results of their model were 1.95% FRR, 4.12% FAR, and 3.04% EER.

2.2. MD. Everitt et al. [20] started the research on identity authentication based on mouse operation in 2003. Like keystroke authentication, the identity authentication process includes two types: static authentication [21] and continuous dynamic authentication [2]. Over the past decades, many researchers have proposed different methods for mouse authentication.

Pusara [21] selected mouse movement and mouse events as features and used Decision Tree (DT) to build user mouse behavior model. The experiment collected data of 18 users and obtained the results of 1.75% false match rate (FMR) and 0.34% false nonmatch rate (FNMR); the authentication time ranged from 1 minute to 15 minutes. Gamboa et al. [2] proposed an authentication method based on game, and each mouse feature was a 63-dimensional feature vector, including spatial parameters, such as angle and curvature, and time parameters, such as velocity and acceleration. The experiment collected 50 users' data and selected the greedy algorithm for the feature selection and obtained 0.7% EER in 100 keystrokes. In 2007, Ahmed et al. [22] implemented continuous monitoring based on MD. They collected data on the daily work of users, extracted mouse features, and used NN for the training and classification. The experimental results achieved 2.4649% FAR and 2.4614% FRR and verified the possibility of using mouse features to achieve authentication, but it took 13.55 minutes to realize the authentication. Nakkabi et al. [23] conducted further research by collecting data from 48 users and proposed a fuzzy classification based on learning algorithm for multivariate data analysis. They combined the fusion scheme with the corresponding biometric score and achieved 0% FAR and 0.36% FRR.

Zheng et al. [24] presented user authentication based on the angle of mouse movement and conducted classification with SVM. The experimental data came from 30 users (different ages, educational backgrounds, and occupations), and the experimental results showed that twenty mouse clicks produced 1.3% EER. Mondal et al. [3] studied the performance of continuous biometric recognition system under different analysis techniques and tried three different verification processes. All the different combinations of fusion, threshold setting, score lifting technologies, and static and dynamic trust models were tested. These technologies also were applied to other biometric recognition patterns.

In recent years, more methods have been continuously improved and remarkable achievements have been obtained. Shen et al. [25] proposed a continuous authentication system based on mouse interaction in 2012, which did not require training pseudonymous data. The best results obtained by using classifier (One-Class SVM) were 0.37% FAR and 1.12% FRR. Dimensionality reduction was proposed to stabilize the dynamic change of mouse behaviors [26], which further enhanced the performance in 2014. A recognition system based on multiple biometric combinations was designed in 2016 [27], including keystroke features, face features, and skin color. A mining method based on pattern growth was proposed to extract frequent behavioral fragments in 2017 [28]. This method obtained stable and differentiated mouse interaction features and 0.09% FAR and 1% FRR in experiments. To bridge the security gap between two one-time authentications on the computer, Li et al. [29] proposed a continuous authentication approach, which is based on a Random Forest Ensemble Classifier (RFEC) and the Sequential Sampling Analysis. By combining the device independent, angle-based mouse movement features, and the wrist motion features, the proposed approach reached the FAR of 1.46% and 4.69% for impostors and intruders, respectively, and the FRR of 0%. Mo et al. [30] collected experiment data from different websites. Random Forest (RF) constructed mouse behavior models by using inconsistent data from different data sources, which were very consistent with the actual situation. In terms of left-click features, the error rate was less than 3.36%, and, for the moving sequence features, the error rate was less than 4.21%. This research was important for the development of identity authentication by using behavioral biometric in uncontrolled environments.

2.3. A Combination of KD and MD. The mouse and keyboard are the main devices for the interaction between users and computers. In order to prevent the impostors from using only one of the input devices of keyboard or mouse to avoid the detection and to improve the accuracy and practical application of identity authentication, Ahmed et al. [6] proposed for the first time that keyboard features and mouse features were combined to improve the accuracy of user authentication. This study provided a new research direction for the subsequent authentication. After that, some researchers [5, 7, 31–36] have added user-keyboard interaction data on the basis of user mouse interaction data and achieved remarkable experimental results in some related studies, most of which were conducted in the controlled environments with predefined tasks. However, there were few studies on combined keystroke behaviors and mouse behaviors for identity authentication compared with researches on one of keystroke and mouse, and Table 1 shows

Table 1: Summary of the related researches by using a combination of KD and MD.

Ref.	Year	Users	Method	Performance
[6]	2005	22	NN	FAR of 1.312% and FRR of 0.651%
[31]	2007	61	DT and SVM	Error rate of 1.5%
[32]	2009	20	Statistical analysis, feed-forward network with back-propagation, and *k*-nearest neighbour (k-NN)	Accuracy of 82.22–96.4%
[33]	2012	24	Bayesian network (BN)	EER of 8.21%
[34]	2014	31	BN, DT, and SVM	FAR of 2.10% and FRR of 2.24%
[5]	2015	67	Naive Bayes (NB) and SVM	FAR of 0.1% and FRR of 0.2%
[7]	2016	25	DT, Counter-Propagation Artificial Neural Network (CPANN), Artificial Neural Network (ANN), and SVM	Accuracy of 62.2%
[35]	2017	53	ANN, CPANN, and SVM	FRR of 5.7% and FAR of 0.1%
[36]	2018	41	RF, SVM, DT, and BN	Accuracy of 80.6%

the summary of these studies and their application methods and performance.

2.4. MKL. Because of the developments and applications of the SVM theory proposed by Boser et al. [37], many scholars have begun to pay attention to kernel method, which has been widely used in the field of the pattern recognition. Although the method has been applied practically and effectively to many fields, each kernel function has different performance, so the suitable application occasion of the kernel function is also explored. Particularly, when the sample features are heterogeneous or the sample size is large, it is very inappropriate to use single kernel to process the samples, while MKL can solve said problem [8].

Single-type feature is often difficult to fully express the sample information, and excessive features will lead to redundancy, which may result in overfitting and reduce the recognition rate. For these problems, the applications of MKL can achieve better results. So far, MKL has found high utilization in all fields, for instance, feature extraction [38], pattern classification [39] and regression [40], and multiclassification target detection and recognition [41], providing a wider application prospect for MKL.

MKL is a feature fusion method. When the target presents multiple features, each feature is mapped to an appropriate kernel function, and then different kernels are combined into a new kernel, which is applied to classifier. The effect of MKL is often better than single kernel learning, but MKL pays a high cost of time and space complexity, so researchers focused on how to optimize the combination of kernel functions and improve the operation efficiency of multikernel models, and many effective methods have been proposed to solve these problems. For example, Bach et al. [42] presented an algorithm based on sequence minimization optimization to improve computational efficiency. Sonnenbrug et al. [43] transformed the MKL problem to Semi-Infinite Linear Programming (SILP). The main idea of the algorithm was to use two-level loops to alternately optimize the combination coefficients and single kernel parameters, which further improved the efficiency and provided an effective solution for large-scale problems. To further improve the computational efficiency, Rakotomamonjy et al. [44] proposed a gradient descent method, Gehler et al. [45] proposed a method based on infinite kernel, Xu [46] proposed a method based on Least Absolute Shrinkage and Selection Operator (LASSO), and EasyMKL [47] was also proposed to improve the classification accuracy.

3. Proposed Approach

3.1. Authentication Architecture. User authentication in uncontrollable environment, which is closer to actual situation, is an important research direction. In order to improve the practicability of the recognition system, an authentication method is proposed in this paper. As Figure 1 shows, the proposed method includes data collection, feature extraction, feature mapping, and classification modules. Keyboard and mouse of HCI data are involved and the MKL is adopted for the keystroke and mouse feature fusion. Firstly, data acquisition is carried out by using the method introduced in 3.2, and then feature extraction and feature selection are performed according to the keyboard and mouse features defined in 3.3. Then, the MKL introduced in 3.4 performs the feature mapping, and finally user authentication is modeled by using the classifier.

3.2. Dataset Description. In order to collect experimental data more authentically, volunteers gathered data through a C++ monitoring program written with global keyboard and mouse hook technology. Four Hooks were WH_CALLWNDPROC, WH_GETMESSAGE, WH_KEYBOARD and WH_MOUSE used for the information collection. WH_GETMESSAG is mainly applied to the communication with the system. Keyboard data are obtained by WH_KEYBOARD and mouse data are collected through WH_MOUSE. Participants can run the two acquisition programs in the background, which are transparent to users without affecting the regular manipulation of users, and the operations of users are not restricted. The collected data are keyboard and mouse in the daily works of users. Finally, The participants' initial population was 21 volunteers and the final sample consists of 21 end-users. The number of users is about the same as the studies [15, 21, 32].

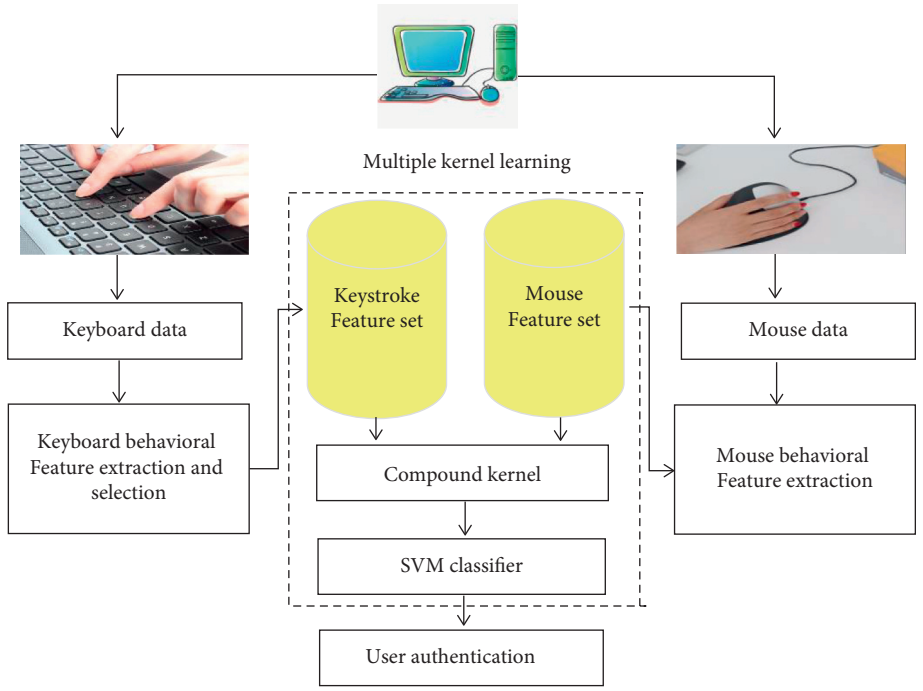

Figure 1: UAMKL method block diagram.

There were no significant age and expertise differences among the participants. Ten hours of real data generated by the operation are selected, and data processing and feature extraction are carried out according to time-slice [34], which has influences on the integrity of describing subject features. For example, an hour's data can be processed into 60 samples by one-minute processing and 30 samples by two-minute processing. The data sample sizes after being processed by time-slice are shown in Table 2.

3.3. Feature Extraction

3.3.1. Keystroke Features. For the keystroke behaviors of users, the keystroke timing features are mainly determined by two time points: the pressing time point of a key and the releasing time point of a key. Keystroke time series are composed by selecting the keystroke time points of the user. The key values involved in this paper are shown as Table 3, and two types of keyboard features are defined by referring to [6].

Let $D_1 = \{(x_{11}, \ldots, x_{1l}), \ldots, (x_{m1}, \ldots, x_{ml})\}$ be the KD example matrix, where m is the total number of KD examples and is determined by the time-slice; l is the number of KD feature attributes:

(1) Single key feature is the key hold time (the time between first key press and first key release) of a given key

(2) Key digraph features include the following:

(i) Release-Press Time (denoted as R-PT) indicates the time between first key release and second key press

(ii) Press-Release Time (denoted as P-RT) indicates the time between the first key press and second key release

(iii) Press-Press Time (denoted as P-PT) indicates the time between first key press and second key press

(iv) Release-Release Time (denoted as R-RT) indicates the time between the first key release and the second key release

Figure 2 is the graphical representation of KD feature extraction process. 110 key values are adopted as shown in Table 3, and the combination features are $110 \times 110 \times 4 = 48,400$ dimensions and so $l = 48{,}400$. Because the number of keyboard features is much larger than the number of samples, which is easy to cause dimension disasters, and the modeling time is very long, it is necessary to conduct the feature selection. This paper adopts Least Absolute Shrinkage and Selection Operator (LASSO), an embedded feature selection method proposed by Tibshirani [48], and the number of features corresponding to the time-slice is shown in Table 4 after the feature selection.

3.3.2. Mouse Features. The mouse features extracted in this paper refer to [23], which defines the following four mouse behaviors:

(i) Mouse-Move (denoted as MM) represents normal mouse movement behavior

(ii) Drag-and-Drop (denoted as DD) represents the dragging behaviors of the left mouse button

Table 2: Samples after processing per time-slice.

Time-slice	One min	Two mins	Three mins	Four mins	Five mins	Six mins
Samples	12600	6300	4200	3150	2520	2100

Table 3: Key value used.

Key value	Counts
A ~ Z	26
0~9	10
Number keyboard 0~9	10
Number keyboard * + enter − /	6
F1~F15	15
Backspace; tab; enter; clear; L-Shift; R-Shift; L-Control; R-Control; L-Alt; R-Alt	10
Pause; CapsLock; L-Windows; R-Windows; TextKey; Esc; SPACE	7
Page up; page down	2
End; Home	2
LeftArrow; UpArrow; RightArrow; DownArrow	4

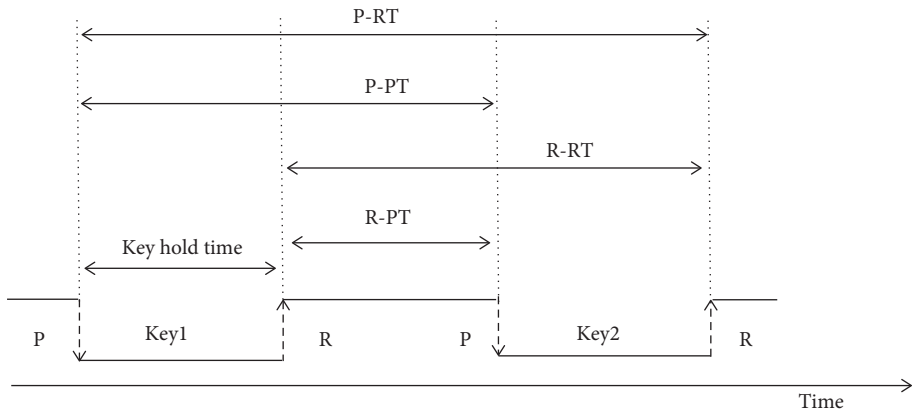

Figure 2: Keystroke dynamics features.

Table 4: KD features quantities after selection per time-slice.

Time-slice	One min	Two min	Three min	Four min	Five min	Six min
KD features quantities after selection	3154	2636	3148	2699	2646	2532

(iii) Point-and-Click (denoted as PC) represents the click and double-click behaviors of the left or right mouse button

(iv) Silence means no action occurs

The original features of each user can be collected by the acquisition program including the type of mouse actions, time-stamps, and coordinates. In order to explore the user behavior characteristics in the moving direction, this paper proposes a direction partition method on the plane by referring to [23]. The 360°of the plane is evenly divided into eight directions, numbered 1–8, and each direction accounts for 45°. Default user action start and end line is the movement direction of the action; the specific direction is divided as in Figure 3. On the basis of raw features, this paper extracts the following seven types of features, a total of 49 dimensions, let $D_2 = \{(x_{11}, \ldots, x_{1k}), \ldots, (x_{m1}, \ldots, x_{mk})\}$ be the MD example matrix, where m is the total number of MD examples and is determined by the time-slice, k is the number of MD feature attributes, and $k = 49$:

(i) Movement speed compared to traveled distance (MSD) indicates the average operation speed of user mouse behaviors in different distance ranges. Distance is divided into eight segments, the first segment is 1 to 100, the interval is 150 pixels, and the length of MSD vector is 8.

(ii) Average movement speed per movement direction (MDA) indicates the average operation speed of user mouse behaviors in different directions, and the length of MDA vector is 8.

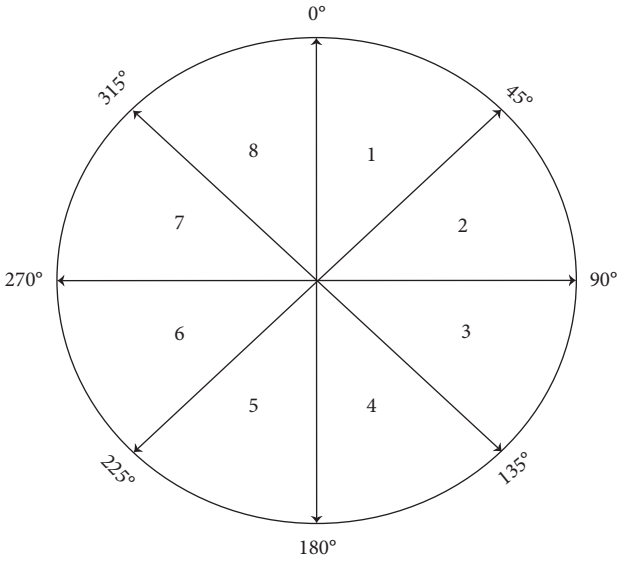

Figure 3: Direction of the mouse movements [23].

(iii) Movement direction histogram (MDH) indicates the proportion of mouse actions of users in different directions, and the length of MDH vector is 8.

(iv) Traveled distance histogram (TDH) indicates the proportion of user operations in different distance ranges, and the length of the TDH vector is 8.

(v) Motion elapsed time histogram (MTH) indicates the proportion of user operations in different duration ranges, divided into 10 segments. Each segment lasts 300 ms, and the length of MTH vector is 10.

(vi) Average movement speed per types of actions (ATA) indicates the average operation speed of different mouse action types, and the length of ATA vector is 4.

(vii) The histogram of per types of actions (ATH) indicates the proportion of user operation number of different mouse action types, and the length of ATH vector is 3.

3.4. Feature Fusion Based on MKL. At present, multikernel learning method is suitable for both single and multiple features from different sources. This paper constructs a multikernel model based on keyboard and mouse features. Mouse and keyboard data come from different operating devices, and the extracted features perform otherness. Keyboard and mouse features value distribution scatter maps are obtained by random sampling method shown in Figures 4 and 5. From Figures 4 and 5, it can be seen that both keyboard and mouse feature matrices are sparse. The zero value of keyboard feature matrix is 92% and that of mouse feature matrix is 21.7%. This sparsity is closely related to the user operation behavior during acquisition. Keystroke feature values are concentrated between 0 and 800 excluding zero feature value, while mouser feature values are

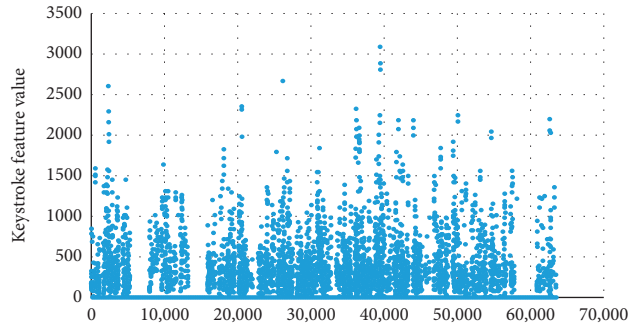

Figure 4: Keystroke feature value distribution scatter diagram.

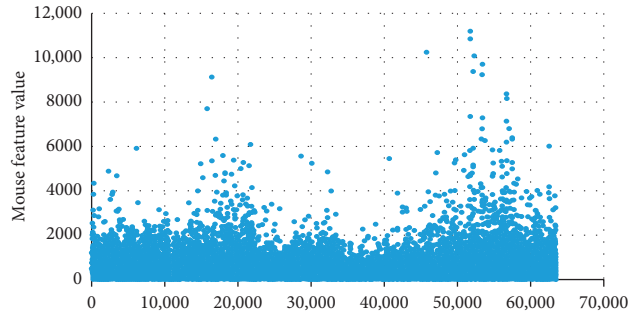

Figure 5: Mouse feature value distribution scatter diagram.

concentrated between 0 and 2000, and a few values are much larger than 2000. The difference between the two types of feature value distribution can be explained as follows: keyboard features are extracted by keystroke time points and the time intervals of user keystrokes are generally shorter, and the combination keys involved in a short time period are fewer, while mouse features mainly include frequency data and counting data. Mouse is a mobile device, which results in a wide range of eigenvalues.

From the above analysis, it can be concluded that the distributions of keyboard and mouse features belong to heterogeneous feature spaces, and the two kinds of features from different sources can provide useful information to vary degrees. The choice of MKL fusion is conducted to improve the authentication accuracy, and each type of features corresponds to a kernel function. The selection of weight coefficient of basic kernel becomes the key problem under the framework of multikernel. The multikernel algorithm for the feature fusion in this paper chooses AverageMKL that the average for kernel learning is the arithmetic average [49]. Although this algorithm is simple, it is a strong algorithm that is often better than other more advanced techniques and can achieve advantageous results [50]. The AverageMKL defined partial or base kernel K_i on a finite collection of input spaces [49]. The keyboard and mouse features in this paper correspond to two different kernels; their combined kernel is defined in the following equation:

$$\begin{aligned} \text{NewK} &= M_q^{\alpha}\left(K_1\left(r_1, r_1^*\right), K_2\left(r_2, r_2^*\right)\right) \\ &= \left(\alpha_1\left(K_1\left(r_1, r_1^*\right)\right)^q + \alpha_2\left(K_2\left(r_2, r_2^*\right)\right)^q\right)^{1/q}, \end{aligned} \tag{1}$$

where $q \in R$, $\alpha_1, \alpha_2 > 0$, and $\sum_{i=1}^{2} \alpha_i = 1$, α_i coefficients perform the explicit feature selection process. $r_1, r_1^* \in D_1$ and $r_2, r_2^* \in D_2$; NewK is a new compound kernel.

In this paper, the keyboard feature dimension extracted by a user is much larger than the number of samples. In this case, dataset is easy to be linearly separable; we choose the linear kernel for the keyboard features to improve the efficiency of modeling, while the mouse feature dimension is much smaller than the sample size; the RBF kernel mapping low-dimensional features to high-dimensional spaces is selected for the modeling of the mouse features. Mouse and keyboard behavioral features are mapped to the appropriate kernel functions, so the linear kernel function and RBF kernel function in this paper correspond to equations (2) and (3), respectively.

$$K_1(r_1, r_1^*) = r_1^T r_1^*, \quad r_1, r_1^* \in D_1, \tag{2}$$

$$K_2(r_2, r_2^*) = \exp\left(-\frac{\|r_2 - r_2^*\|}{2\delta^2}\right), \quad \delta > 0, r_2, r_2^* \in D_2. \tag{3}$$

In equation (3), δ is the width of RBF kernel and controls the adaption performance of kernel function.

3.5. Evaluation and Procedures. The accuracy obtained by using multiclassification is not ideal [7], so the multiclassification problem is transformed into a two-classification problem in this paper. The training and testing data that we used in the experiment are all from the data we collected. Each user data was divided into training set and testing set, and the ratio of each training set to each test set is 4 : 1. Firstly, for each user i $(1 \le i \le N)$ marked as a legitimate user, N represents the numbers of users, we have 19 users, and the training samples are marked as positive samples, while the remaining $N-1$ users are marked as illegal, and their training samples are marked as negative samples. In order to keep the balance between positive and negative samples, the negative samples with the same proportion as the positive samples are selected from the negative samples by downsampling method. Next, the experiment is repeated until every remaining user j $(1 \le j \le N-1, i \ne j)$ is marked as a legitimate user. Then, we take the time-slice from 1 to 6 different values and repeat the above steps, so we have $N \times 6 = 90$ different classifier models of different classification algorithms for each experimental group. Otherwise, traditional performance evaluation indicators used for our experiments are as follows: T_i represents the test set of legitimate users, TP_i represents the test set of the correctly classified by the legitimate user, T_j represents the test set of illegal users, and TP_j represents the test set of the correctly classified by illegal user.

(i) Accuracy (denoted as Acc) represents the overall judgment accuracy of each legitimate user in test, as equation (4)

(ii) FAR represents the probability that the system accepts an illegal intruder incorrectly, while user i is marked as an illegitimate user, as equation (5)

(iii) FRR represents the probability that the system mistakenly rejects a legitimate user, while user i is marked as a legitimate user, as equation (6)

$$\mathrm{Acc}_i = \frac{\mathrm{TP}_i + \mathrm{TP}_j}{T_i + T_j}, \tag{4}$$

$$\mathrm{FAR}_i = \frac{T_j - \mathrm{TP}_j}{T_j}, \tag{5}$$

$$\mathrm{FRR}_i = \frac{T_i - \mathrm{TP}_i}{T_i}. \tag{6}$$

Besides, we also adopt Average Accuracy (denoted as AAcc), Average False Accept Rate (denoted as AFAR) and Average False Reject Rate (denoted as AFRR) as evaluation indicator so as to reflect the overall classification effect. The corresponding evaluation formulas are equations (7)–(9). In addition, Stdevp is used to reflect the degree of dispersion of the overall user recognition accuracy relative to the average under different algorithms, as defined in equation (10).

$$\mathrm{AAcc} = \frac{\sum_{i=1}^{N} \mathrm{Acc}_i}{N}, \tag{7}$$

$$\mathrm{AFAR} = \frac{\sum_{i=1}^{N} \mathrm{FAR}_i}{N}, \tag{8}$$

$$\mathrm{AFRR} = \frac{\sum_{i=1}^{N} \mathrm{FRR}_i}{N}, \tag{9}$$

$$\mathrm{Stdevp} = \sqrt{\frac{\sum_{i=1}^{N} (\mathrm{Acc}_i - \mathrm{AAcc})^2}{N}}. \tag{10}$$

4. Experimental Result Analysis

DT, RF, NB, One-Class SVM, and SVM are selected to classify mouse data and keyboard data in this paper, in which DT, RF, NB, One-Class SVM, and SVM are used as the control group. It is worth noticing that it is difficult to repeat and compare all experiments in previous studies because of some experimental differences, such as the limited environments and datasets, so we selected the state-of-art classifiers used by other studies as the basis concise reference in the work described. The experimental group selects MKL to fuse features, which combines different characteristics of kernel functions to obtain the advantages of each type of kernel functions, and also fuses different features to avoid the loss of important information. Keyboard features and mouse features in this paper are commonly used biological features. Users may operate one or two input devices at a certain time in daily work; higher accuracy can be obtained by using MKL to fuse two kinds of behavior features (see 3.4 for the fusion method). Each algorithm used in this paper adopts fivefold cross validation, and the difference between

maximum and minimum values is too great; it is essential that all data is normalized before the experiment.

In this paper, the size of time-slices has a great impact on the integrity of expression features, thus affecting the results of different classification algorithms. The size of time-slices ranges from 1 min to 6 min in this work. Different classification algorithms have distinct effects for the single feature and fusion feature extracted by time-slices. To illustrate the efficient of the proposed method, this paper carries out three groups of experiments, and the results of the three groups of experiments are analyzed. For more detailed experimental steps, see 3.5.

4.1. Experiment A. In order to verify the validity of the proposed algorithm for mouse feature classification, only mouse features are selected in this part of the experiment. From Figure 6, the AAcc of UAMKL is always higher than algorithms of control group from 1 min to 6 mins and achieves the maximum AAcc of 84.5%, when the time-slice is 5 min. SVM, RF, and One-Class SVM achieve their highest AAcc of 77.9%, 78%, and 76.5%, when the time-slice is 5 min. Individually, DT and NB achieve the best results: AAcc of 70.5% and 66.2% at 3 min. Figure 7 shows that each algorithm from 1 min to 6 min achieves the best AAcc corresponding to the AFAR and AFRR, the AFR and AFRR for UAMKL are far lower than other algorithms, and NB classification effect is the worst. It can be seen that the proposed UAMKL has a significant classification effect for the mouse features.

4.2. Experiment B. Similar to Experiment A, in order to verify the effectiveness of the proposed algorithm for keystroke feature classification, this part of the experiment chooses keystroke features. The experimental results show that the proposed UAMKL shows advantages over algorithms of control group for keystroke feature classification. It can be seen from Figure 8 that UAMKL from 1 min to 6 min has little difference with other algorithms but is always better than other algorithms in terms of AAcc, no matter what size the time-slice takes, and achieves the maximum AAcc of 80.2%, when the time-slice is taken for 5 min. SVM and NB achieve their highest AAcc of 77.4% and 70.9%, respectively; RF, One-Class SVM, and DT achieve the best results of AAcc of 77.8%, 75.6%, and 75.4%, when the time-slice is 6 min. Figure 9 shows that the best AAcc corresponds to the AFAR and AFRR for each algorithm; we can conclude that the AFRR for UAMKL is far lower than other algorithms, and the AFRR for UAMKL and NB is the lowest, but its AFRR of NB is too high, and the classification effect is the worst in terms of AAcc, UAMKL still has obvious advantages.

4.3. Experiment C. In this experiment, keystroke and mouse fusion features are selected. Keystroke and mouse features are mapped to different kernels by UAMKL, and then their features are fused for classifier classification. Figure 10 shows that the AAcc of UAMKL increases at first, reaches the maximum AAcc of 89.6%, when the size of time-slice is 5 minutes, and then decreases. Figure 11 is the accuracy of each user under various algorithms, when the time-slice value is 5 min. It can be found that the classification effect of this algorithm for each user is higher than that of other algorithms from control group. Table 5 shows when UAMKL classification is adopted, Stdevp, AFAR, and AFRR are the lowest, which shows that the accuracy gap between users is not large and high, while the accuracy of users using other algorithms is very unstable, which verifies the effectiveness and stability of user authentication based on MKL.

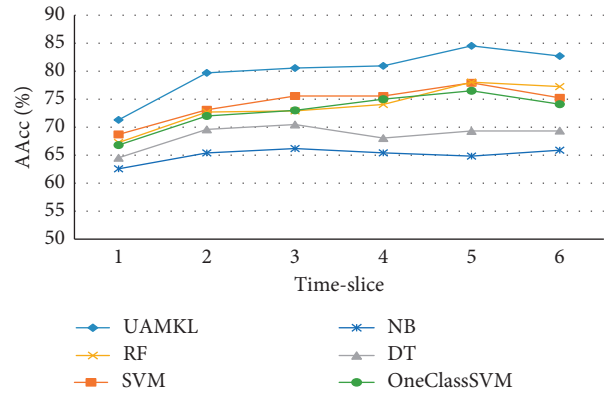

Figure 6: The AAcc of different algorithms per time-slice for mouse feature.

4.4. Comparison. According to Experiment A, Experiment B, and Experiment C, when the time-slice is selected for 5 minutes, the performance of keystroke features, mouse features, and fusion features by using the proposed algorithm can reach the maximum values, which are 80.2%, 84.5%, and 89.6% AAcc, respectively, as shown in Figure 12. It can be concluded intuitively from experimental results that the proposed algorithm is more effective than other algorithms for the classification of single feature extracted by different time-slices. The best results by synthesizing the three experiments are the AAcc of 89.6%, the AFAR of 8.8%, and the AFRR of 11.9% obtained by the proposed algorithm, when the time-slice is 5 min (average 109 keystroke and 1515 mouse behaviors). The results show that double-index composite identity authentication can improve the recognition rate of the system identity to a certain extent, thereby preventing information leakage or money loss caused by the identity of the system. The results of this paper are better than those of the typical methods [7, 36] and have no better effect than other methods [5, 6, 31–35]. However, the reader should bear in mind that performance figures cannot be fairly compared, because every study has used different experimental setups. In addition, some devices may have only one input device, such as a mouse, while other related works shows that their dual-indicator authentication does not take this into account.

From Figure 12, we know that the proposed algorithm is also applicable to the case of missing an index. Although the effect of index authentication is not as good as that of

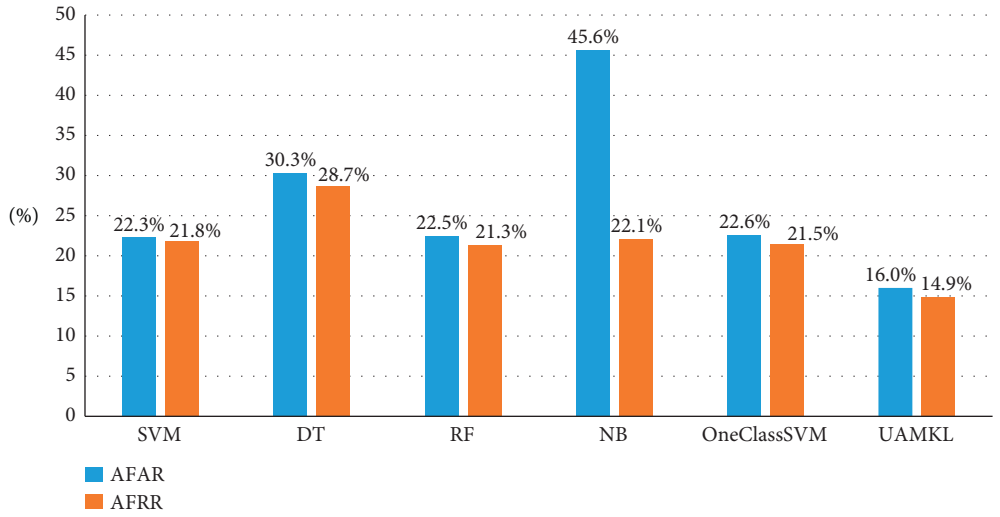

Figure 7: The best result in AFAR and AFRR for different algorithms for mouse feature.

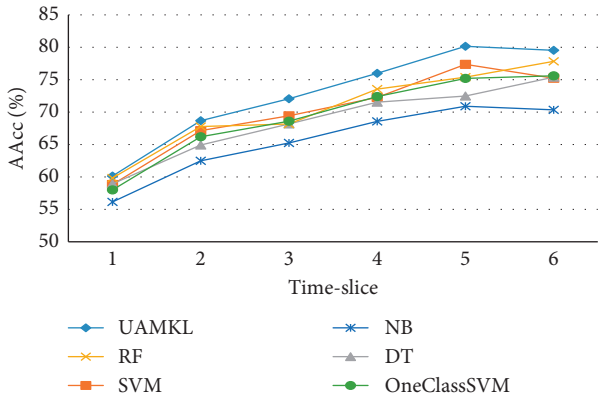

Figure 8: The AAcc of different algorithms per time-slice for keystroke feature.

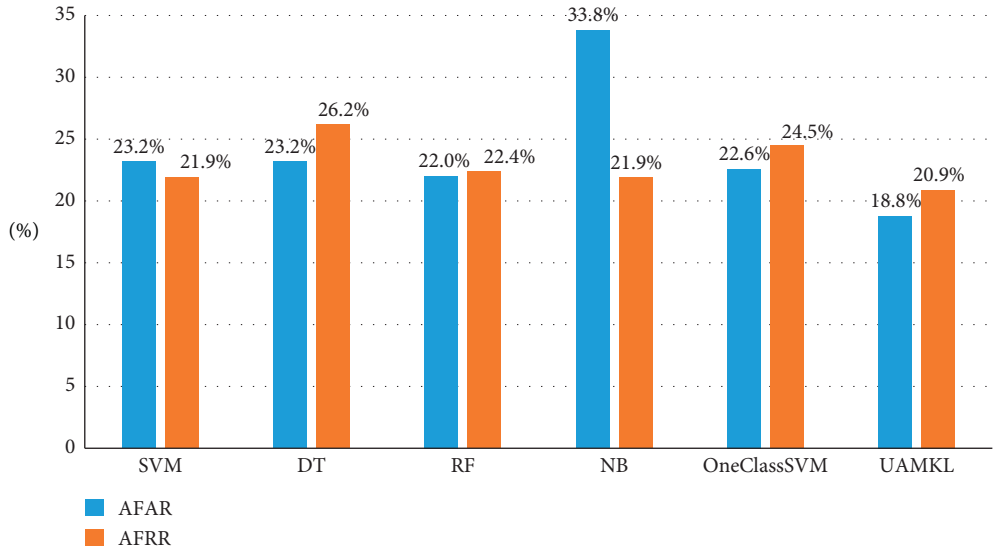

Figure 9: The best result in AFAR and AFRR for different algorithms for keystroke feature.

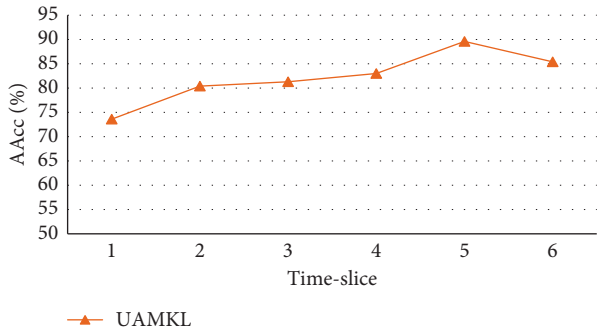

Figure 10: The AAcc of UAMKL per time-slice for fusion feature.

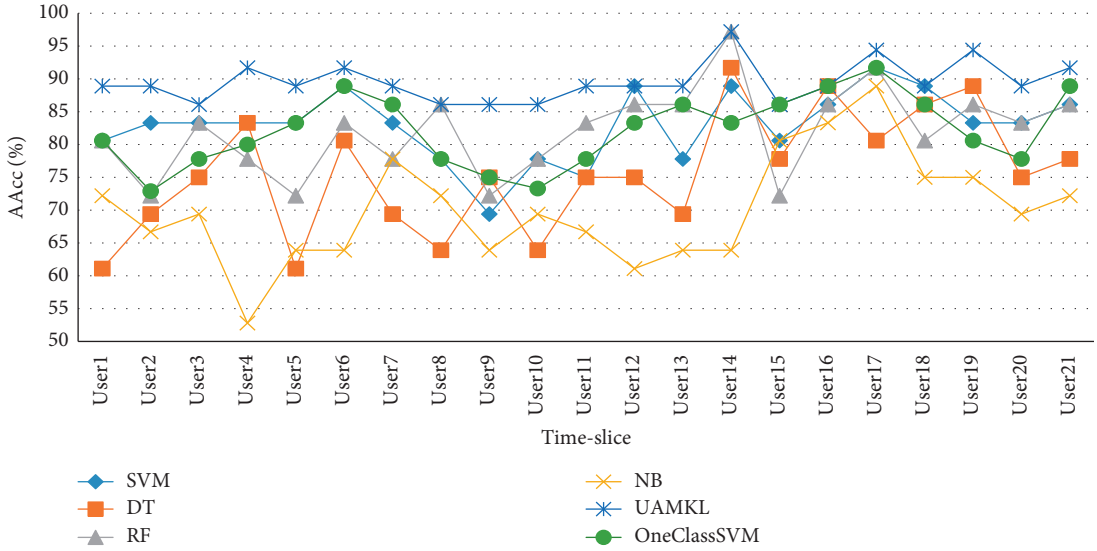

Figure 11: The AAcc of different algorithms per users for fusion feature extracted by 5 min.

Table 5: Comparison of results for different algorithms in 5 min.

Evaluation	SVM (%)	DT (%)	RF (%)	BN (%)	One-Class SVM (%)	UAMKL (%)
Stdevp	5.2	8.9	6.5	8	5.3	**3**
AFAR	18.5	27.1	20.6	37.2	18.2	**8.8**
AFRR	15.4	21.5	15.2	22.5	15.9	**11.9**
AAcc	82.9	75.7	82	70.1	82.2	**89.6**

double-index authentication, the accuracy of fusion of similar features is generally higher than that of other machine learning algorithms, which indicates that some machine learning algorithms are not suitable for heterogeneous information problems in free environments. Compared with some previous research works for single index authentication, the experimental results of this paper may not show obvious advantages, probably because it is the data collected in the real environment that does not control more environmental factors, and such an environment is more realistic, and the overall effect shows that this method is suitable for user identification requirements in free environments. On this basis of this study, we will further study more robust methods to apply to both single feature and double indices. In this paper, we build a model for each user. The results reflect the overall effect of users, and Figure 13 shows that the mean results are similar presenting no very great relevant correlation with the number of users, and previous study [2] for mouse behavior obtained a similar conclusion. Considering that there are relatively few available instances in the user set, the overall ideal results encourage us to continue our research in this direction.

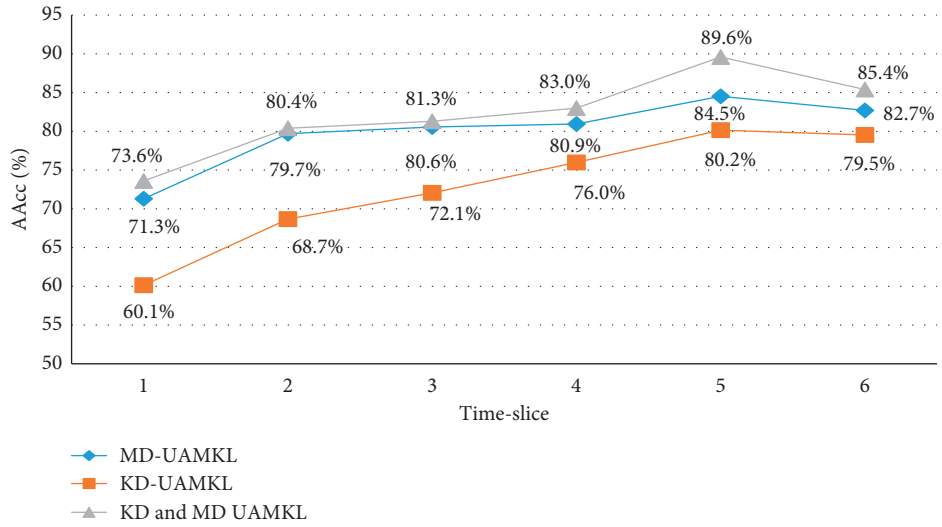

Figure 12: The AAcc of different features per time-slice.

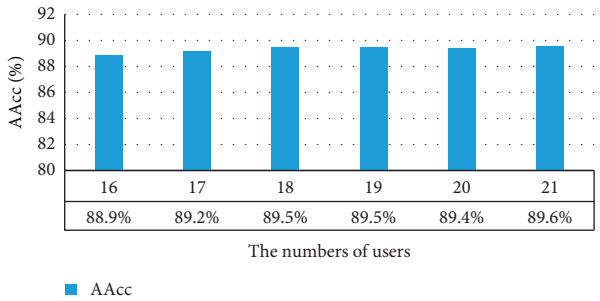

Figure 13: The AAcc of different numbers of users for UAMKL in 5 min.

5. Conclusion Remarks

5.1. Summary. In this paper, a linear multikernel identity authentication method named UAMKL is proposed based on two kinds of features: keyboard and mouse. This method maps the different kernel functions corresponding to two kinds of keyboard and mouse features, and different kernel functions are combined into a new kernel function, and then the kernel function is applied to the classifier. The mouse and keyboard features in identity authentication are suitable for different kernel functions, due to their heterogeneity, and the appropriate kernel function mapping and combination can effectively achieve dual-index authentication and greatly improve the authentication accuracy and other performances. Moreover, the proposed method is applied to single index authentication, and the authentication accuracy is higher than other algorithms. In this paper, three groups of experiments are carried out for mouse features, keyboard features, and fusion features.

The experimental analysis shows that the results are radically different based on the time-slice of segmentation. The best time-slice selection of mouse features, keyboard features, and fusion features is 5 min. In addition, compared with other algorithms, no matter using a single index or a combination of mouse and keyboard features, the method proposed in this paper has higher authentication accuracy, and the overall accuracy standard deviation of users is lower. Through the comparison of several groups of experiments, the best experimental results come from the algorithm proposed in this paper; the result of the accuracy is 89.6%, which is much higher than the best effect of other methods.

5.2. Future Work. Generally, few studies have applied the dual features of mouse and keyboard to user authentication. The proposed method has achieved impressive results; there are many shortcomings in this experiment, which do not take into account more external environmental factors, but the method of feature recognition in this paper has satisfactory recognition requirement, although these biometric recognition techniques are generally considered to be not suitable for identifying people. We believe that the proposed method has effectiveness and strong expansibility when we fuse more biological features by a new kernel, but it needs further improvement to be applied to practice. The future optimization direction will focus on commercial applications, for instance, considering that different models can be established for different types of active windows, because the operations of users in different scenarios are very different, considering combining with newer intelligent devices, such as voice control devices, and evaluating the impacts of personality on the generation model to complete the certification accurately and quickly. In conclusion, it is hoped that the results of this paper can promote further research and realize the wide applications of mouse and keyboard features as soon as possible.

Data Availability

The metadata used to support the findings of this study have not been made available because no agreement was obtained from the data participants.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was financially supported by the National Key R&D Program of China (Grant no. 2017YFB0802703), Beijing Natural Science Foundation (Grant no. 4202002), and the research project of the Department of Computer Science in BJUT (Grant no. 2019JSJKY004).

References

[1] X. Lu, S. Zhang, and S. Yi, "Continuous authentication by free-text keystroke based on CNN plus RNN," *Procedia Computer Science*, vol. 147, pp. 314–318, 2019.

[2] H. Gamboa and A. Fred, "A behavioral biometric system based on human-computer interaction," *Proceedings of SPIE*, vol. 5404, pp. 381–392, 2004.

[3] S. Mondal and P. Bours, "A computational approach to the continuous authentication biometric system," *Information Sciences*, vol. 304, pp. 28–53, 2015.

[4] V. Matyas and Z. Riha, "Toward reliable user authentication through biometrics," *IEEE Security and Privacy*, vol. 1, no. 3, pp. 45–49, 2003.

[5] L. Fridman, A. Stolerman, S. Acharya et al., "Multi-modal decision fusion for continuous authentication," *Computers and Electrical Engineering*, vol. 41, pp. 142–156, 2015.

[6] A. A. E. Ahmed and I. Traore, "Anomaly intrusion detection based on biometrics," in *Proceedings of the Sixth Annual IEEE SMC Information Assurance Workshop*, pp. 452-453, West Point, NY, USA, June 2005.

[7] S. Mondal and P. Bours, "Combining keystroke and mouse dynamics for continuous user authentication and identification," in *Proceedings of the 2016 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)*, pp. 1–8, Sendai, Japan, February 2016.

[8] T. Sun, L. Jiao, F. Liu, S. Wang, and J. Feng, "Selective multiple kernel learning for classification with ensemble strategy," *Pattern Recognition*, vol. 46, no. 11, pp. 3081–3090, 2013.

[9] T. Katerina and P. Nicolaos, "Mouse behavioral patterns and keystroke dynamics in end-user development: what can they tell us about users' behavioral attributes?" *Computers in Human Behavior*, vol. 83, pp. 288–305, 2018.

[10] R. S. Gaines et al., "Authentication by keystroke timing: some preliminary results," p. 52, 1980, Rand Report R-256-NSF.

[11] S. Bleha, C. Slivinsky, and B. Hussien, "Computer-access security systems using keystroke dynamics," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 12, no. 12, pp. 1217–1222, 1990.

[12] J. Leggett, G. Williams, M. Usnick, and M. Longnecker, "Dynamic identity verification via keystroke characteristics," *International Journal of Man-Machine Studies*, vol. 35, no. 6, pp. 859–870, 1991.

[13] M. Brown and S. J. Rogers, "User identification via keystroke characteristics of typed names using neural networks," *International Journal of Man-Machine Studies*, vol. 39, no. 6, pp. 999–1014, 1993.

[14] E. Yu and S. Cho, "Keystroke dynamics identity verification-its problems and practical solutions," *Computers and Security*, vol. 23, no. 5, pp. 428–440, 2004.

[15] A. A. Ahmed and I. Traore, "Biometric recognition based on free-text keystroke dynamics," *IEEE Transactions on Cybernetics*, vol. 44, no. 4, pp. 458–472, 2014.

[16] A. Morales, E. Luna-Garcia, J. Fierrez, and J. Ortega-Garcia, "Score normalization for keystroke dynamics biometrics," in *Proceedings of the 2015 International Carnahan Conference on Security Technology (ICCST)*, pp. 223–228, Taipei, Taiwan, September 2015.

[17] B. Li, H. Sun, Y. Gao, V. V. Phoha, and Z. Jin, "Enhanced free-text keystroke continuous authentication based on dynamics of wrist motion," in *Proceedings of the 2017 IEEE Workshop on Information Forensics and Security (WIFS)*, pp. 1–6, Rennes, France, December 2017.

[18] M. Monaro, C. Galante, R. Spolaor et al., "Covert lie detection using keyboard dynamics," *Scientific Reports*, vol. 8, no. 1, p. 1976, 2018.

[19] S. Krishnamoorthy, L. Rueda, S. Saad, and H. Elmiligi, "Identification of user behavioral biometrics for authentication using keystroke dynamics and machine learning," in *Proceedings of the 2018 2nd International Conference on Biometric Engineering and Applications (ICBEA)*, pp. 50–57, Amsterdam, Netherlands, May 2018.

[20] R. A. J. Everitt and P. W. McOwan, "Java-based Internet biometric authentication system," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 9, pp. 1166–1172, 2003.

[21] M. Pusara and C. E. Brodley, "User re-authentication via mouse movements," in *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, pp. 1–8, Washington, DC, USA, October 2004.

[22] A. A. E. Ahmed and I. Traore, "A new biometric technology based on mouse dynamics," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 3, pp. 165–179, 2007.

[23] Y. Nakkabi, I. Traore, and A. A. E. Ahmed, "Improving mouse dynamics biometric performance using variance reduction via extractors with separate features," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 40, no. 6, pp. 1345–1353, 2010.

[24] N. Zheng, A. Paloski, and H. Wang, "An efficient user verification system via mouse movements," in *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 139–150, Chicago, IL, USA, October 2011.

[25] C. Shen, Z. Cai, and X. Guan, "Continuous authentication for mouse dynamics: a pattern-growth approach," in *Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012)*, pp. 1–12, Edinburgh, UK, June 2012.

[26] Z. Cai, C. Shen, and X. Guan, "Mitigating behavioral variability for mouse dynamics: a dimensionality-reduction-based approach," *IEEE Transactions on Human-Machine Systems*, vol. 44, no. 2, pp. 244–255, 2014.

[27] C. Shen, Z. He, Y. Zhenyu et al., "Modeling multimodal biometric modalities for continuous user authentication," in *Proceedings of the 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 001894–001899, Budapest, Hungary, October 2016.

[28] C. Shen, Y. Chen, X. Guan, and R. Maxion, "Pattern-Growth based mining mouse-interaction behavior for an active user authentication system," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 2, pp. 335–349, 2020.

[29] B. Li, W. Wang, Y. Gao, V. V. Phoha, and Z. Jin, "Hand in motion: enhanced authentication through wrist and mouse movement," in *Proceedings of the 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–9, Los Angeles, CA, USA, October 2018.

[30] F. Mo, S. Xiong, S. Yi, Q. Yi, and A. Zhang, "Authentication using users' mouse behavior in uncontrolled surroundings," *Intelligent Computing and Internet of Things*, in *Proceedings of the from First International Conference on Intelligent Manufacturing and Internet of Things and 5th International Conference on Computing for Sustainable Energy and Environment (IMIOT and ICSEE 2018)*, pp. 121–132, Chongqing, China, September 2018.

[31] M. Pusara, *An Examination of User Behavior for User Re-authentication*, ETD Collection for Purdue University, 2007.

[32] H. Jagadeesan and M. S. Hsiao, "A novel approach to design of user re-authentication systems," in *Proceedings of the IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems*, pp. 1–6, Washington, DC, USA, 2009.

[33] I. Traore, I. Woungang, M. S. Obaidat, Y. Nakkabi, and I. Lai, "Combining mouse and keystroke dynamics biometrics for risk-based authentication in web environments," in *Proceedings of the 2012 4th International Conference on Digital Home*, pp. 138–145, Guangzhou, China, 2012.

[34] K. O. Bailey, J. S. Okolica, and G. L. Peterson, "User identification and authentication using multi-modal behavioral biometrics," *Computers and Security*, vol. 43, pp. 77–89, 2014.

[35] S. Mondal and P. Bours, "A study on continuous authentication using a combination of keystroke and mouse biometrics," *Neurocomputing*, vol. 230, pp. 1–22, 2016.

[36] S. Salmeron-Majadas, R. S. Baker, O. C. Santos, and J. G. Boticario, "A machine learning approach to leverage individual keyboard and mouse interaction behavior from multiple users in real-world learning scenarios," *IEEE Access*, vol. 6, pp. 39154–39179, 2018.

[37] B. E. Boser, I. M. Guyon, and V. N. Vapnik, "A training algorithm for optimal margin classifiers," in *Proceedings of Annual ACM Workshop on Computational Learning Theory*, vol. 5, pp. 144–152, New York, NY, USA, July 1992.

[38] B. Mak, J. T. Kwok, and S. Ho, "A study of various composite kernels for kernel eigenvoice speaker adaptation," in *Proceedings of the 2004 IEEE International Conference on Acoustics, Speech, and Signal Processing*, pp. I–325, Montreal, Quebec, Canada, May 2004.

[39] A. Bosch, A. Zisserman, and X. Munoz, "Representing shape with a spatial pyramid kernel," in *Proceedings of the ACM International Conference on Image and Video Retrieval*, pp. 401–408, New York, NY, USA, October 2007.

[40] A. Ben-Hur and W. S. Noble, "Kernel methods for predicting protein-protein interactions," *Bioinformatics*, vol. 21, no. 21, pp. i38–i46, 2005.

[41] T. Damoulas and M. A. Girolami, "Probabilistic multi-class multi-kernel learning: on protein fold recognition and remote homology detection," *Bioinformatics*, vol. 24, no. 10, pp. 1264–1270, 2008.

[42] F. R. Bach and G. R. G. Lanckriet, "Multiple kernel learning, conic duality, and the SMO algorithm," in *Proceedings of International Conference on Machine Learning*, pp. 6–13, Shanghai, China, August 2004.

[43] S. Sonnenburg, "Large scale multiple kernel learning," *Journal of Machine Learning Research*, vol. 7, no. 2006, pp. 1531–1565, 2006.

[44] A. Rakotomamonjy, F. R. Bach, S. Canu, and Y. Grandvalet, "SimpleMKL," *Journal of Machine Learning Research*, vol. 9, pp. 2491–2521, 2008.

[45] P. V. Gehler and S. Nowozin, "Infinite kernel learning," in *Proceedings of the NIPS 2008 Workshop on "Kernel Learning: Automatic Selection of Optimal Kernels,"* pp. 1–4, Whistler, Canada, December 2010.

[46] Z. Xu, R. Jin, J. Ye, I. King, and M. R. Lyu, "Simple and efficient multiple kernel learning by group Lasso," *Proceedings of the International Conference on Machine Learning*, pp. 1175–1182, 2010.

[47] F. Aiolli and M. Donini, "EasyMKL: a scalable multiple kernel learning algorithm," *Neurocomputing*, vol. 169, pp. 215–224, 2015.

[48] R. Tibshirani, "Regression shrinkage and selection via the Lasso," *Journal of the Royal Statistical Society: Series B (Methodological)*, vol. 58, no. 1, pp. 267–288, 1996.

[49] L. A. Belanche and A. Tosi, "Averaging of kernel functions," *Neurocomputing*, vol. 112, pp. 19–25, 2013.

[50] X. Xu, I. W. Tsang, and D. Xu, "Soft margin multiple kernel learning," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 24, no. 5, pp. 749–761, 2013.