JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 34, 961-976 (2018)
DOI: 10.6688/JISE.201807_34(4).0010

Jensen-Shannon Divergence Based Secure Authentication Method on Smart Phones

SHUANG-YUAN QIAO, YONG ZENG+, LING-JIE ZHOU,
ZHI-HONG LIU AND JIAN-FENG MA
School of Cyber Engineering
Xidian University
Xi'an, 710071 P.R. China
E-mail: {shyqiao; yzeng; ljzhou; zhhliu; jfma}@mail.xidian.edu.cn

Smart phones are widely used in our daily life on which there are much personal and sensitive information. To prevent information disclosure and to strengthen the authentication security for smartphones, implicit methods for authentication attract people's attention. Implicit authentication (IA) can continuously authenticate users by profiling their behavior using the variety of sensors prevalent. IA requires no explicit user action, which is much more user-friendly. In this paper, we focus on characteristic distribution probability evaluation for key-stroke dynamics and propose an authentication method based on Jensen-Shannon divergence (JS-divergence). Two phases, training phase and authentication phase, are used to identify the true user in our method. For authentication phase, the set of behavioral characteristics is preprocessed as the behavior characteristic distribution probability vector (BCDPV) to obtain the JS-divergence between two sets of behavioral characteristics. For training phase, a novel update strategy for training set based on sliding window is proposed, which can overcome the difficulties of retraining. The security of this method is estimated by False Rejection Rate (FRR), False Acceptance Rate (FAR) and Equal Error Rate (ERR). The result shows that the size of the training set (*i.e.* the size of the sliding window) is not the bigger the better and 5 for the best results. It also shows that our method based on JS divergence works better than that based on other measurement methods such as the cosine, chebyshev and correlation Euclidean.

Keywords: authentication, smart phones, JS-Divergence, security, behavior characteristic distribution probability vector (BCDPV)

1. INTRODUCTION

According to the IDC's China Quarterly Mobile Phone Tracker [1], as the development of the mobile communications industry, the demand for smart phones has increased dramatically. Smart phones are broadly used in daily life, including financial services, social relations, electronic information and even business, because of their portability and computing performance. There is no doubt that the emergence of smart phones greatly facilitates our lives. However, smart devices store sensitive and private data including bank accounts, passwords, contacts, emails, and photos, while their security has not gained enough attention.

To protect smart devices from misuse, traditional explicit authentication mechanisms such as PIN code, draw-a-secret, face recognition, fingerprint recognition, *etc*., are proposed, which is shown in Fig. 1 [2]. For PIN code, there are many people who don't

Received August 31, 2017; revised October 13, 2017; accepted December 15, 2017.
Communicated by Changqiao Xu.
+ Corresponding author.

have a passcode on their phone because it is not easy to recall the code for most people. Meanwhile the password is insecure because it can be shoulder peeped [3-6]. For drawing-a-secret, there are so many secret marks remaining on screen as shown in Fig. 2 (a) that we can see the secret with naked eyes or by light spectrum recovery [7-11]. Even though biometrics are much harder to be stolen than passwords, recent research [12] show that your fingerprint can be computed by your photographs as shown in Fig. 2 (b) [2], and then be forged. The leakage of fingerprint and face characteristics will make us in trouble.

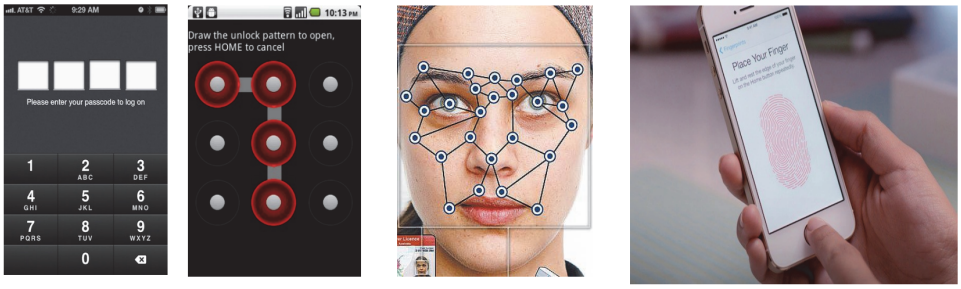
Recently, to enhance security and usability, implicit methods for authentication attract people's attention. Implicit authentication (IA) is a technique that allows the smart device to recognize its owner by being acquainted with his/her behaviors. For IA, research [2] have implemented them in an easily extensible open source framework for the Android operating system called Itus, which allows other researchers to iteratively improve on the existing mechanisms for performing IA. However, it is not yet clear which behavioral features and classification algorithms result in the best accuracy while also being measurable often enough to be useful. And profiles of actual users' everyday device usage are not easy to obtain. Meanwhile we also do not know which similarity distance can be used for authentication.

For the behavioral features IA can continuously authenticate users by profiling their behavior using the variety of sensors prevalent, such as walking style, swipe speed, location, trajectory, keystroke and physical layer noise. However, for walking style, swipe speed, location and trajectory, users have privacy concerns on these behaviors. As a result, the privacy-aware profiles of users' smart phones are hard to be obtained. The physical layer noise [13] may be used to implicit authentication. However, the tradeoff between energy efficiency and secrecy capacity/intercept probability under different fading environments is still an interesting and challenging open problem which is beyond the scope of this paper. The key stroke dynamics requires no explicit user action, which is much more user-friendly and privacy-aware. It can potentially enhance the user experience and further ensure security. It can also be deployed as a secondary defense mechanism on top of explicit authentication, providing layered security in the event of, for example, a shoulder-surfing compromising the smart phone's PIN code or an operating system vulnerability allowing its bypass [2]. As a result, this paper focuses on the keystroke dynamics for implicit authentication.

There has been an IA based on Jensen-Shannon divergence (JS-divergence) [14] as the similarity distance for keystroke dynamics [15]. It pays attention to how to determine the best retraining frequency when updating the user behavior model, and how to dynamically degrade user privilege, when authentication fails to identify legitimate users. The results show that this method can successfully detect the degradation of accuracy of the user behavior model, as well as automatically determine and adjust to the best retraining frequency. It is also shown that the dynamic privilege-based access control reduces the impact of false negatives on legitimate users and enhances system reliability and user experience compared with the traditional lock-only method in case of authentication failure. However, the retraining frequency in this paper is still some high.

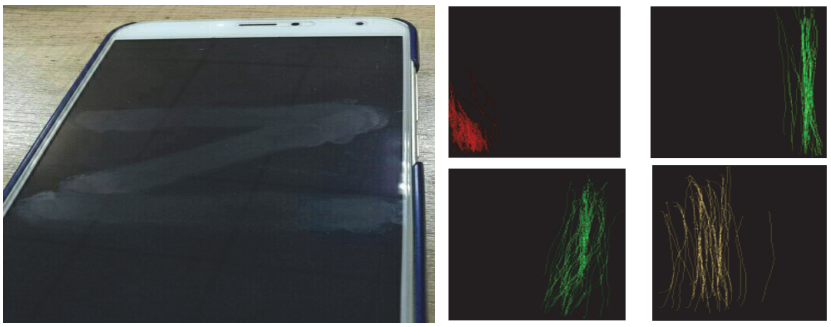
In this paper, we focus on characteristic distribution probability evaluation for keystroke dynamics using JS divergence. Two phases, training phase and authentication phase, are used to identify the true user in our method. For authentication phase, the set

of behavioral characteristics is preprocessed as the behavior characteristic distribution probability vector (BCDPV) to obtain the JS-divergence between two sets of behavioral characteristics. For training phase, a novel update strategy for training set based on sliding window is proposed, which can overcome the difficulties of retraining. A battery of related experiments is designed and carried out in this paper. The security of this method is estimated by False Rejection Rate (FRR), False Acceptance Rate (FAR) and Equal Error Rate (ERR). The result shows that the size of the training set (*i.e.* the size of the sliding window) is not the bigger the better and 5 for the best results. It also shows that our method based on JS divergence works better than that based on other measurement methods such as the cosine, chebyshev and correlation Euclidean.

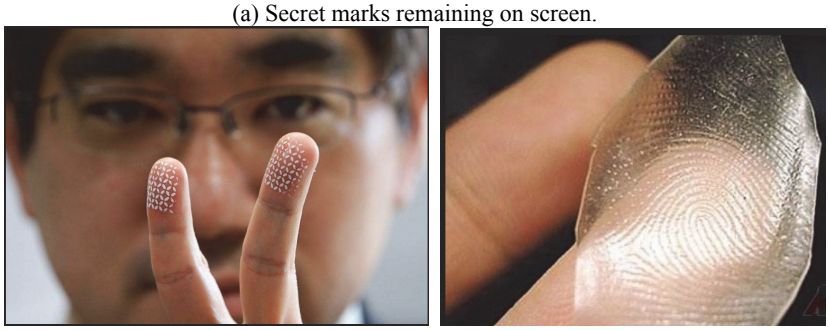


(a) PIN code. (b) Draw-a-secret. (c) Face recognition. (d) Fingerprint recognition.

Fig. 1. Explicit authentications.



(a) Secret marks remaining on screen.



(b) Photo fingerprint hacking.

Fig. 2. The limitations of explicit authentications.

2. PRELIMINARIES

2.1 Jensen-Shannon Divergence

The similarity between two BCDVs based on the JS differences that are rarely used in smartphone authentication is calculated in our paper.

A common method of measuring the similarity between the two states is to compute the KL-deviation between them. The KL-divergence between random probability distributions P and Q is:

$$D_{KL}(P,\ Q)=\sum_{i=1}^{n} p(x_i)\log\frac{p(x_i)}{q(x_i)}. \tag{1}$$

The KL-divergence is zero, as there are equal distributions. However, KL-divergence does not apply to distance measurements due to its asymmetry. Thus, we construct a symmetric formula $J(P, Q)$, shown in Eq. (2).

$$J(P,\ Q)=D_{KL}(P,\ Q)+D_{KL}(Q,\ P)=\sum_{i=1}^{n}\left(p(x_i)-q(x_i)\right)\log\frac{p(x_i)}{q(x_i)} \tag{2}$$

However, there is no upper bound in the Eq. (2) so we further construct one with upper bound, which is shown in Eq. (3).

$$K(P,\ Q)=\sum_{i=1}^{n} p(x_i)\log\frac{p(x_i)}{\frac{1}{2}p(x_i)+\frac{1}{2}q(x_i)} \tag{3}$$

Obviously, Eqs. (2) and (3) constructed above cannot be symmetrical and have the upper bound at the same time. In order to make the formula both symmetric and have upper bound, we construct the formula $L(P, Q)$, as shown in Eq. (4).

$$L(P,\ Q)=K(P,\ Q)+K(Q,\ P)=2H\left(\frac{P+Q}{2}\right)-H(P)-H(Q) \tag{4}$$

The formula shown in Eq. (5) can be derived by extending the Eq. (4).

$$D_{JS}(p_1,\ p_2,\ \ldots,\ p_n)=H\left(\sum_{i=1}^{n}\pi_i p_i\right)-\sum_{i=1}^{n}\pi_i H(p_i), \tag{5}$$

where π_i ($\pi_i \geq 0$) is the weight of the random probability distribution q_i and the sum of π_i is 1. If there are only two probability distributions P_1 and P_2 whose corresponding weights are π_1 and π_2, then the JS divergence is

$$D_{JS}(p_1,\ p_2)=H(\pi_1 p_1+\pi_2 p_2)-\pi_1 H(p_1)-\pi_2 H(p_2). \tag{6}$$

In particular, when $\pi_1 = \pi_2 = 1/2$, the JS-divergence is obtained as follows according

to the information entropy.

$$D_{JS}(P,\ Q) = \frac{1}{2} D_{KL}(P,\ M) + \frac{1}{2} D_{KL}(Q,\ M), \tag{7}$$

where $M = 0.5(P + Q)$. It can be found that the more similar P is to Q, the smaller the JS-divergence is. Similarly, the JS-divergence will be zero, when the distributions are equal.

2.2 The Properties of JS Divergence

The properties of JS Divergence can be clearly seen by Eq. (7). Next we will explain the properties of JS divergence in detail. The properties of JS divergence are as follows:

(1) Nonnegative: The value of the JS divergence is nonnegative, as shown in Eq. (8). If and only if P and Q are identical, the equal sign holds.

$$D_{JS}(P,\ Q) \geq 0 \tag{8}$$

(2) Symmetric: The JS divergence is symmetrical about P and Q, that is, the JS divergence between P and Q is equal to the that between Q and P.

$$D_{JS}(P,\ Q) = D_{JS}(Q,\ P) \tag{9}$$

(3) Triangle inequality: The JS divergence satisfies the trigonometric inequality, which can be used as a distance to measure the similarity between the two probability distributions.

$$D_{JS}(P,\ Q) < D_{JS}(P,\ R) + D_{JS}(R,\ Q) \tag{10}$$

(4) Bounded: JS divergence has an upper bound and the maximum value is not greater than 1.

$$D_{JS}(P,\ Q) \leq 1 \tag{11}$$

It can be seen from the above properties that JS-divergence can meet all the requirements of similarity distance. It can be used as a distance to measure the similarity between the two probability distributions.

3. AUTHENTICATION METHOD

3.1 Behavior Characteristic Distribution Probability Vector

In this paper, we focus on characteristic distribution probability evaluation for keystroke dynamics. Specifically, the behavioral characteristics shown in Fig. 3 include Key

hold time (*H*), Down-down time (*DD*), Up-down time (*UD*), Key press pressure (*P*), Finger Area (*FA*) and so on.

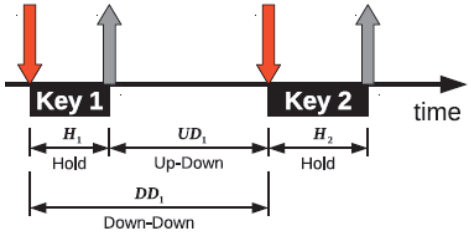


Fig. 3. The schematic of behavioral characteristics *H*, *DD*, *UD*, *P*, *FA*.

Since the JS divergence measures the similarity between the probability distributions of two random variables, the data needs to be processed before the similarity is calculated. To obtain the probability distributions of behavior characteristics, the data need to be pre-processed as behavior characteristic distribution probability vector (BCDPV).

The specific process of data preprocessing is as follows:

(1) Time sequence: A characteristic sequence *S* is ordered, that is, the value inside is arranged in order. The ordered sequence is recorded as

$$S_L = \{x_1, x_2, \ldots\}. \tag{12}$$

For instance, if the user enters three keys, then *S* will contain three Key hold time (H_1, H_2, H_3), two Down-down time (DD_1, DD_2) and two Up-down time (UD_1, UD_2). The ordered sequence S_L is $\{H_1, DD_1, UD_1, H_2, DD_2, UD_2, H_3\}$.

(2) Normalizing: Firstly, the maximum value and the minimum value of all characteristics values in a behavioral characteristics sequence are computed. Next, each characteristics value in a behavioral characteristics sequence is normalized using the formula shown in Eq. (12). The normalized feature sequence is denoted as S_L^*.

$$x_i^* = \frac{x_i - \min}{\max - \min} \tag{13}$$

For instance, if the *SL* mentioned in the last step is {2, 10, 8, 3, 12, 9, 2}, then the maximum value is 12 and the minimum value is 2. Consequently, S_L^* = {0, 0.8, 0.6, 0.1, 1, 0.7, 0}.

(3) Intervals partition: In order to facilitate the statistics and obtain the behavioral characteristic probability distribution, the interval is first divided. Since the values of normalized characteristics sequence are in the range of [0,1], we divide [0,1] into *N* intervals, that is,

$$intervalwidth = \frac{1}{N}. \tag{14}$$

It is worth noting that the size of *N* for each user is the same.

(4) Frequency count: Statistic the quantity of characteristic values in each interval ac-

cording to the intervals partition for each normalized characteristics sequence. The set of frequency count is denoted as

$$freNum = \{freNum_1, freNum_2, \ldots\}. \tag{15}$$

For instance, if N is 4, then the *intervalwidth* is 0.25. Hence the *freNum* of S_L^* mentioned in step 2) is {3, 0, 2, 2}.

(5) BCDPV: It is supposed that the length of a behavioral characteristics sequence is L, that is to say, the number of characteristics value in a behavioral characteristics sequence is L. According to the frequency count, the behavior characteristic distribution probability vector can be gotten as

$$X = \frac{freNum}{L}. \tag{16}$$

3.2 Authentication and Update Strategy for Training Set

Now given two BCDPVs $X_1 = \{p_{11}, p_{12}, \ldots, p_{1N}\}$ and $X_2 = \{p_{21}, p_{22}, \ldots, p_{2N}\}$, we can get the JS distance between them:

$$DJS(X1 \| X2) = \frac{1}{2}[\sum_{n=1}^{N} p_{1n} \log \frac{p_{1n}}{\frac{1}{2}(p_{1n} + p_{2n})} + \sum_{n=1}^{N} p_{2n} \log \frac{p_{2n}}{\frac{1}{2}(p_{1n} + p_{2n})}]. \tag{17}$$

To verify the legitimacy of the user input, we first determine whether the password is wrong. If the password is correct, user's behavior characteristics will be identified.

The matching of user characteristics involves the calculation of two mean feature similarities. Assuming that X_{n+1} is the BCDPV to be matched and $\{X_n, X_{n-1}, \ldots\}$ is the ordered set whose elements have been matched successfully. As shown in the solid box in Fig. 2, k BCDPVs which have recently been matched are selected as the training set. As the size of the training set is k, there are $k(k-1)$ JS distances between two elements in this set. Since the JS divergence is symmetrical, the average of these distances can be gotten as:

$$\overline{\overline{D_{JS}}} = \frac{2 \times \sum_{i=1}^{k} \sum_{j=i+1}^{k} D_{JS}\left(X_{n-i+1} \| X_{n-j+1}\right)}{k(k-1)}. \tag{18}$$

Then the JS-divergence between X_{n+1} and each X_i in the training set should be computed and the average of these values is

$$\overline{D_{JS}} = \frac{\sum_{i=1}^{k} D_{JS}\left(X_{n-i+1} \| X_{n+1}\right)}{k}. \tag{19}$$

If the two mean values meet the conditions shown in Eq. (20), then the certification is successful.

$$\frac{\left|\overline{D_{JS}} - \overline{\overline{D_{JS}}}\right|}{\overline{\overline{D_{JS}}}} \leq \sigma \tag{20}$$

where σ is the authentication threshold.

Training set

Fig. 4. The training set.

In addition, the elements of the training set are not static. In order to capture the dynamic changes in the behavior of the user, a new update strategy for training set based on sliding window is proposed, in which the training set is dynamically changing. As shown in Fig. 2, once the matching BCDPV X_{n+1} matches successfully, the solid line box moves to the position of the dashed box, which means that the newly entered X_{n+1} replaces the previous X_{n-j+1}. This is like the sliding window mechanism and the window is constantly moving forward with the addition of matched BCDPV. As time goes by, the new matched BCDPV is constantly added, which can capture the dynamic changes in user behavior. This strategy overcome the difficulties of retraining and avoids the determination of the best retraining frequency when updating the user behavior model.

3.3 Authentication Framework

There are two stages in the authentication process of this method, which is shown in Fig. 5.

In the training phase, to form the training set, the corresponding behavioral feature sequence and the user authentication password are recorded at first. For each sequence of behavioral features in the training set, BCDPV is obtained as described in Section 3.2. Then BCDPV is combined into a combination called BCDPV-set (*i.e.* the training set). Finally, the similarity between two BCDPVs in BCDPV-set is calculated to establish the user characteristic model (*i.e.* the value shown in Eq. (18)). At the same time, we set the default authentication threshold.

In the authentication phase, we collect the user's corresponding behavior feature sequence and its current authentication password. If the current authentication password matches successfully, then we reconstruct and normalize the current behavior sequence to get the current BCDPV. Otherwise, re-enter the authentication password and re-collect the corresponding record feature sequence. Then compute the similarity between the current BCDPV and each one in BCDPV-set to obtain the current average feature similarity, which is used for authenticating the user's identity. If the difference between the user characteristic model and the value is less than the authentication value, the authentication succeeds. At this point, the current BCDPV is added to update the BCDPV-set, and the oldest BCDPV is replaced to capture the dynamic changes in the behavior of the user. Otherwise, authentication fails.

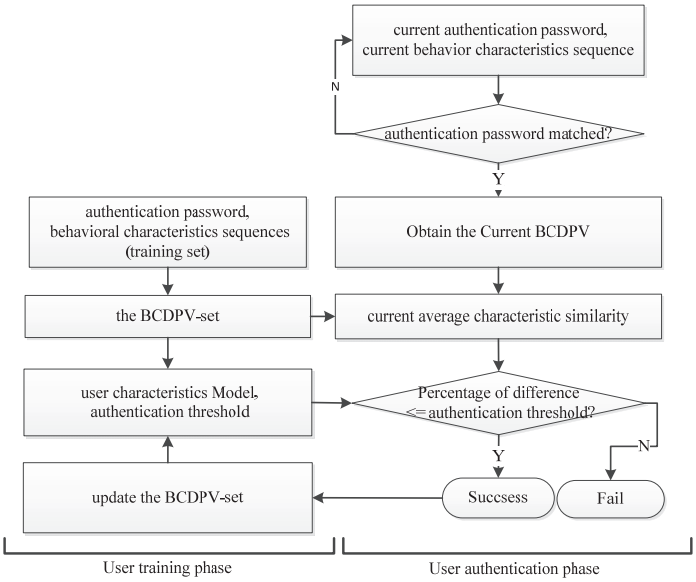


Fig. 5. Authentication process.

4. EVALUATION AND EXPERIMENTS

4.1 Datasets and Measures

The security of the authentication method proposed in this paper was evaluated. We compare and analyze the impacts on the authentication results based on the above experimental results from the following aspects: the size of the training sample set, the number of intervals partition as well as the different distance measurement methods. Since the behavior characteristics' sequence length plays an important role and we need a longer one, we choose available datasets [16] with longer sequence length of each behavior characteristic instead of those collected by ourselves used in the experiments to obtain more effective authentication results. The results are presented using FRR, FAR and ERR. Fig. 6 shows the curves of FRR, FAR and ERR. FRR and FAR are contradictory when a is increasing. ERR is the intersection of the curve FRR and FAR. The smaller ERR is the better performance.

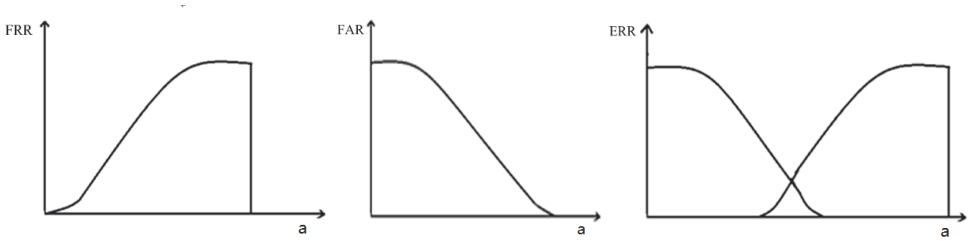


Fig. 6. The curves of FRR, FAR and ERR.

Data acquisition: The entire available online data collection process took 2 weeks and are, and the equipment used were Android operating system. There are 42 people, 24 boys, 18 girls, totally involved in data collection. A uniform password was tested 60 times for all participants, so that data of each user can be used as illegal data in addition to legitimate data during the test process. The password requires 14 entries, including 8 letters, 1 number, 1 English period, 2 alphanumeric conversions, 2 case conversions. Thus, the collected behavioral characteristics include several contents: 14 Key hold time (*H*), 13 Down-down time (*DD*), 13 Up-down time (*UD*), 14 Key press pressure (*P*), 14 Finger Area (*FA*), 1 Average time (*AH*), 1 Average pressure (*AP*), 1 Average finger area (*AFA*).

Dataset: Tables 1, 2 and 3 show the datasets used in these experiments. The first dataset (dataset1) contains all features while the second dataset (dataset2) has 17, which contains the 14 *H* and the means of the *H*, *P* and *FA*. The second dataset, which is used for historical reason, holds time features perform the best in comparison to the other time-based features [17]. The participants selected 50 valid behavioral characteristics sequence samples. That is, both of dataset1 and dataset2 have a set of 42 * 50 = 2100 behavioral characteristics sequences samples.

Table 1. Dataset1.

Characteristics	Count
Key hold time (*H*)	14
Down-down time (*DD*)	13
Up-down time (*UD*)	13
Key press pressure(*P*)	14
Finger area	14
Average Key hold time	1
Average pressure (*AP*)	1
Average finger area (*AFA*)	1

Table 2. Dataset2.

Characteristics	Count
Key hold time (*H*)	14
Average hold time (*AH*)	1
Average pressure (*AP*)	1
Average finger area (*AFA*)	1

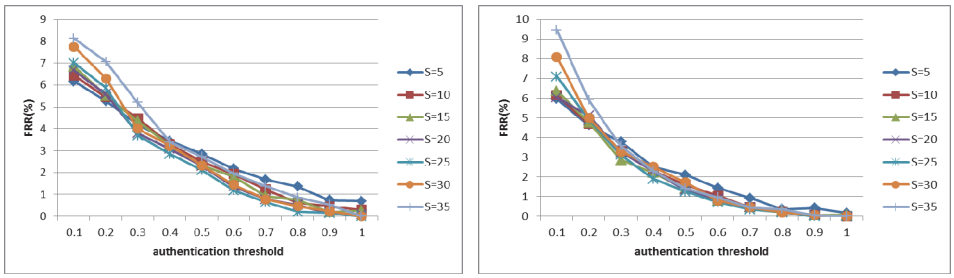
Table 3. Dataset and description.

Name	Description
dataset1	71 characteristics
dataset2	17 characteristics: 14 *H* + the means of the *H*, *P* and *FA*

4.2 The Size of the Training Set

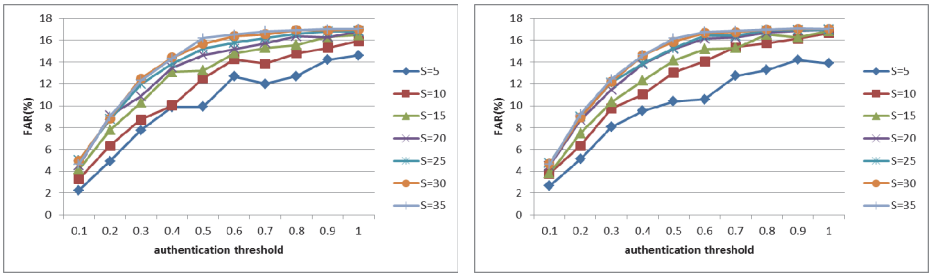
The user characteristic model of the suggested safety authentication method is gotten by Eq. (18). As the limitations of the performance of smart phones and the acquisi-

tion of data in practical application, the larger the sample set is, the greater the trouble of the collection of data is, as well as the cost of computing. Therefore, to verify the effect of the size of the training set, the experiments with the value of intervals N is 10 are carried out. The average FRR and FAR of all participants at different thresholds are obtained and shown in Figs. 6-8. Note that the results of $s < 5$ are not shown in the figure, as the size of the training set is too small to recognize its owner adequately.



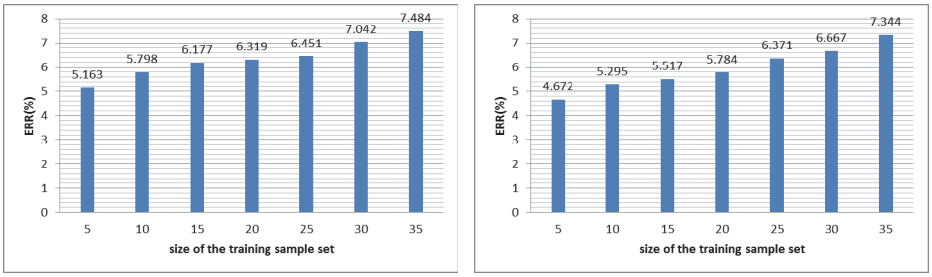
(a) Dataset1 (b) Dataset2

Fig. 7. The FRR of different size of the training sample set and different dataset.



(a) Dataset1 (b) Dataset2

Fig. 8. The FAR of different size of the training sample set and different dataset.



(a) Dataset1 (b) Dataset2

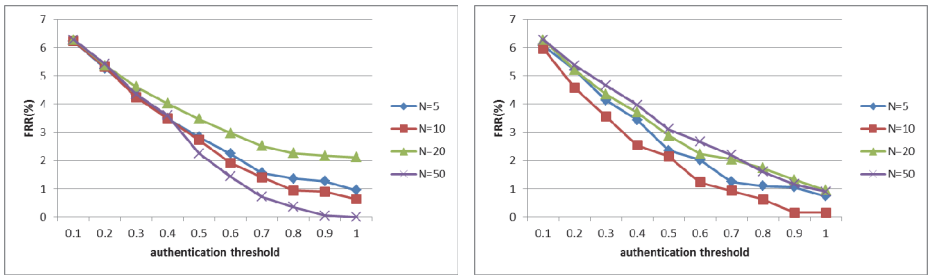
Fig. 9. The ERR of different size of the training sample set and different dataset.

4.3 The Number of Intervals Partition

To study the influence of the number of interval partition which takes an important role in the characteristics reconstruction process on authentication results, the experi-

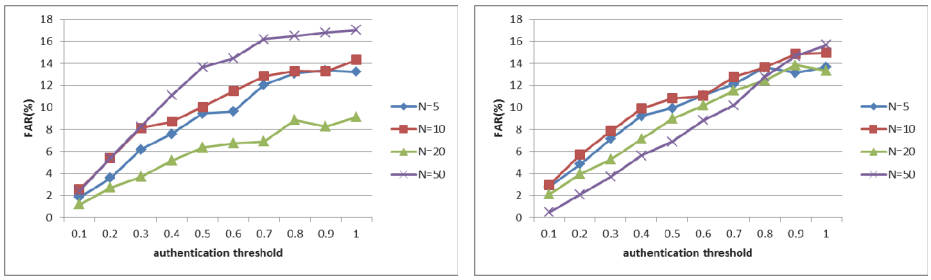
ments dividing each training sample to different number of interval partition are carried out, then the BCDPV and the authentication result with the size of training sample set is 5 are obtained. The average FRR and FAR of all participants at different thresholds are obtained and shown in Figs. 10-12 (a)-(b).

It can be seen from Figs. 10-12 (a)-(b) that the number of intervals partition has an impact on the authentication result. In the two datasets, ERR is the lowest, 4.71% and 4.68% respectively, as the number of intervals partition is 20. It can be also shown that too little or too much intervals partition may make the BCDPV not reflect the specificity of a user' behavior characteristic. And it further influences the authentication results. Therefore, we can choose the appropriate number of interval partitions to achieve better certification results.



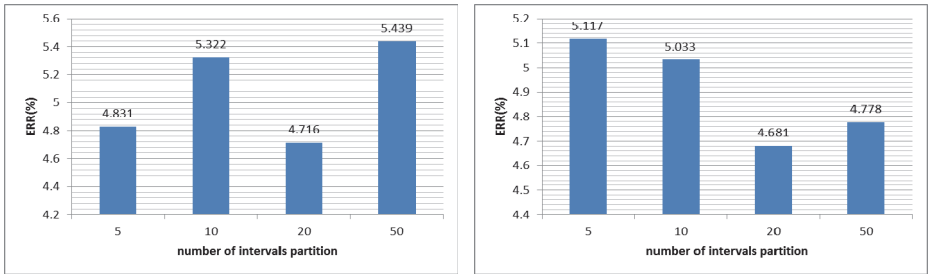
(a) Dataset1 (b) Dataset2

Fig. 10. The FRR of different number of interval partition and different dataset.



(a) Dataset1 (b) Dataset2

Fig. 11. The FAR of different number of interval partition and different dataset.

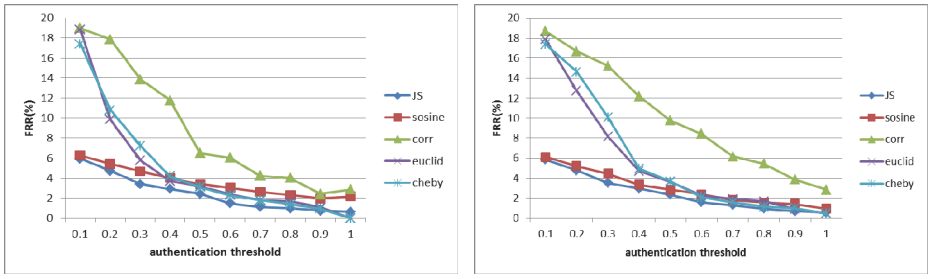


(a) Dataset1 (b) Dataset2

Fig. 12. The ERR of different number of interval partition and different dataset.

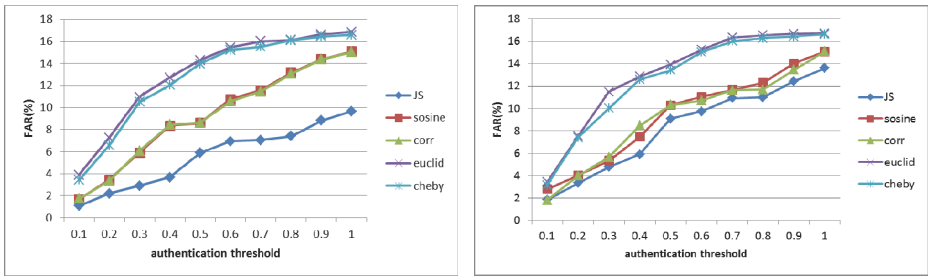
4.4 The Different Distance Measurement Methods

We use different similarity measurement methods including JS-divergence, cosine distance, correlation distance, Euclidean distance, and Chebyshev distance to calculate the similarity. The results for the five similarity measurement methods in two datasets are shown in Figs. 13-15 (a)-(b):



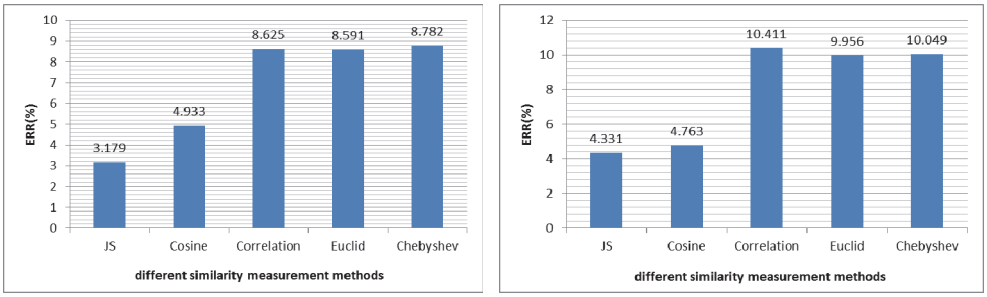
(a) Dataset1 (b) Dataset2

Fig. 13. The FRR of different similarity measurement methods and different dataset.



(a) Dataset1 (b) Dataset2

Fig. 14. The FAR of different similarity measurement methods and different dataset.



(a) Dataset1 (b) Dataset2

Fig. 15. The ERR of different similarity measurement methods and different dataset.

The proposed authentication method based on JS-divergence is better than other four similarity measurement methods including the cosine, correlation Euclidean and Chebushev. As can be seen from Figs. 12 (a) and (b), for FRR, the values based on JS-

divergence are all very small, and the maximum belongs to dataset1 when the authentication threshold is equal to 0.1, which is 5.955%. Except the cosine, the similarity based on the rest measurement methods differs greatly from that based on the JS-divergence, especially when the authentication threshold is less than 0.4. The results of FAR are shown in Figs. 13 (a) and (b), and compared with other similarity measurement methods the proposed authentication method based on JS-divergence also dose the best. As is shown in Figs. 14 (a) and (b), the ERR based on JS-divergence on dataset1 is 3.179% and 4.331% on dataset2, which is the smallest on both two datasets, and differs significantly form the correlation coefficient, Euclidean, Chebyshev. It can be seen that our method based on JS-divergence is the best in identity authentication and it has high security.

5. CONCLUSIONS

In this work, we propose an authentication method based on JS-divergence, which uses behavior of user entering password by touching screen. It is found from the experiment that this method is feasible and the security of that with ERR is very high under 3.719% for dataset1 and 4.331% for dataset2. In general, the behavioral characteristics can be reconstructed and normalized based on JS-divergence, so that BCDPVs, an aided authentication beyond passwords to strengthen the security of touch authentication, can be obtained.

ACKNOWLEDGMENT

We would like to thank the anonymous reviewers for their insightful comments. This work was sponsored in part by the National Key Research and Development Program of China (2016YFB0800601), China 111 Project (B16037), the National Natural Science Foundations of China (U1405255), and the Fundamental Research Funds for the Central Universities(BDZ011402).

REFERENCES

1. http://www.idc.com/getdoc.jsp?containerId=prCN24688114 2014/2/19 IDC: 2014 Technology Outlook for China's Growing Mobile Phone Industry.
2. A. Atwater, H. Khan, and U. Hengartner, "Poster: when and how to implicitly authenticate smartphone users," in *Proceedings of ACM SIGSAC Conference on Computer and Communications Security*, 2014, pp. 1415-1417.
3. A. Bianchi, I. Oakley, and D. S. Kwon, "The secure haptic keypad: a tactile password system," in *Proceedings of ACM SIGCHI Conference on Human Factors in Computing Systems*, 2010, pp. 1089-1092.
4. A. de Luca, E. von Zezschwitz, and H. Hußmann, "Vibrapass: secure authentication based on shared lies," in *Proceedings of ACM SIGCHI Conference on Human Factors in Computing Systems*, 2009, pp. 913-916.
5. V. Roth, K. Richter, and R. Freidinger, "A pin-entry method resilient against shoulder surfing," in *Proceedings of the 11th ACM Conference on Computer and Commu-*

nications Security, 2004, pp. 236-245.
6. L. Wu, X. Du, and X. Fu, "Security threats to mobile multimedia applications: camera-based attacks on mobile phones," *IEEE Communications Magazine*, Vol. 52, 2014, pp. 80-87.
7. A. J. Aviv, K. L. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," *Woot*, Vol. 10, 2010, pp. 1-7.
8. A. de Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, "Touch me once and I know it's you!: implicit authentication based on touch screen patterns," in *Proceedings of ACM SIGCHI Conference on Human Factors in Computing Systems*, 2012, pp. 987-996.
9. Y. Zhang, P. Xia, J. Luo, Z. Ling, B. Liu, and X. Fu, "Fingerprint attack against touch-enabled devices," in *Proceedings of the 2nd ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, 2012, pp. 57-68.
10. E. Von Zezschwitz, A. Koslow, A. De Luca, and H. Hussmann, "Making graphic-based authentication secure against smudge attacks," in *Proceedings of ACM International Conference on Intelligent User Interfaces*, 2013, pp. 277-286.
11. K. Airowaily and M. Alrubaian, "Oily residuals security threat on smart phones," in *Proceedings of the 1st IEEE International Conference* on *Robot*, *Vision and Signal Processing*, 2011, pp. 300-302.
12. T. Feng, J. Yang, Z. Yan, E. M. Tapia, and W. Shi, "Tips: Context-aware implicit user identification using touch screen in uncontrolled environments," in *Proceedings of the 15th ACM Workshop on Mobile Computing Systems and Applications*, 2014, p. 9.
13. L. Zhou, D. Wu, B. Zheng, and M. Guizani, "Joint physical-application layer security for wireless multimedia delivery," *IEEE Communications Magazine*, Vol. 52, 2014, pp. 66-72.
14. J. Lin, "Divergence measures based on the shannon entropy," *IEEE Transactions on Information Theory*, Vol. 37, 1991, pp. 145-151.
15. Y. Yang, J. S. Sun, C. Zhang, and P. Li, "Retraining and dynamic privilege for implicit authentication systems," in *Proceedings of the 12th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, 2015, pp. 163-171.
16. M. Antal, L. Z. Szabó, and I. László, "Keystroke dynamics on android platform," *Procedia Technology*, Vol. 19, 2015, pp. 820-826.
17. P. S. Teh, S. Yue, and A. B. Teoh, "Feature fusion approach on keystroke dynamics efficiency enhancement," *International Journal of Cyber-Security and Digital Forensics*, Vol. 1, 2012, pp. 20-31.

Shuang-Yuan Qiao (乔双媛) received her B.Sc. and M.S. degrees from Xidian University, China, in 2014, 2017.

Yong Zeng (曾勇) received his B.Sc., M.S., and Ph.D. degrees from Xidian University in 2000, 2003, and 2008, respectively. Since 2007 he has been with Xidian University as an Associate Professor. His research interests include cryptography, physical-layer security, and complex networks.

Ling-Jie Zhou (周灵杰) received her M.S. degree from Xidian University, China, in 2016. From 2016 to now, she attended Xidian University, majoring in Computer Science and Technology.

Zhi-Hong Liu (刘志宏) received his B.Sc. degree from National University of Defense Technology, China, in 1989, his M.S. degree in Computer Science from Air Force Engineering University, China, in 2001, and his Ph.D. degree in cryptography from Xidian University in 2009. Now he is with the School of Cyber Engineering at Xidian University. His research areas include mobile computing and information security.

Jian-Feng Ma (马建峰) received his B.Sc. degree from Shaanxi Normal University, China, in 1985, and his M.Sc. and Ph.D. degrees in Computer Software and Communications Engineering from Xidian University in 1988 and 1995, respectively. He is currently a Professor and Ph.D. supervisor at the School of Computer Science and Technology, Xidian University. His current research interests include information and network security and computer networks. He has published more than 200 refereed articles in these areas and coauthored more than 10 books. He is a Senior Member of the Chinese Institute of Electronics.