This is the Pre-Published Version.

Noname manuscript No.
(will be inserted by the editor)

DCUS: Evaluating Double-Click-based Unlocking Scheme on Smartphones

Wenjuan Li · Yu Wang · Jiao Tan · Nan Zhu ·

Received: date / Accepted: date

Abstract With the increasing capability of software and hardware, mobile devices especially smartphones are changing the way of peoples' communication and living styles. For the sake of convenience, people often store a lot of personal data like images on the device and use it for completing sensitive tasks like payment and financial transfer. This makes data protection more important on smartphones. To secure the device from unauthorized access, one simple and efficient method is to design a device or screen unlock mechanism, which can authenticate the identity of current user. However, most existing unlock schemes can be compromised if an attacker gets the correct pattern. In this work, we advocate that behavioral biometrics can be useful to improve the security of unlock mechanisms. We thus design DCUS, a double-click-based unlocking scheme on smartphones, which requires users to unlock the device by double clicking on the right location on an image. For user authentication, our scheme needs to check the selected images, image location and double-click patterns. In the evaluation, we perform a user study with 60 participants and make a comparison between our scheme and a similar unlock scheme. With several typical supervised classifiers, it is found that participants can perform well under our scheme.

Keywords User Authentication · Double Click · Smartphone Security · Behavioral Authentication · Touch Dynamics

A preliminary version of this paper has been presented at the 1st International Symposium on Emerging Information Security and Applications (EISA) in conjunction with SpaCCS 2020 [1].

Wenjuan Li
Institute of Artificial Intelligence and Blockchain, Guangzhou University, China and Department of Computing, Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong, China
E-mail: wenjuan.li@my.cityu.edu.hk

Yu Wang
Institute of Artificial Intelligence and Blockchain, Guangzhou University, No.230 Waihuaxi Road, Panyu. 510006, Guangzhou, China
E-mail: yuwang@gzhu.edu.cn

Jiao Tan
KOTO Research Center, Macao, China

Nan Zhu
KOTO Research Center, Macao, China

1 Introduction

Due to the wide adoption, smartphones have become one of the most ubiquitous and commonly used devices. The Deloitte report showed that up to 1.4 billion smartphones were shipped in 2019 [5]. Current smartphones can offer many functions, customers can use it for communication and perform different tasks. For this reason, users are usually store a lot of private and sensitive information on their smartphones such as photos, personal address, banking information, commercial applications and more. This makes smartphones a major target for cyber-attackers. In addition, with the increasing importance of data security and privacy (e.g., GDPR [14]), there is a great need to enforce access control and verify users on mobile devices.

For user authentication, password-based authentication should be the most widely adopted method, while such kind of authentication suffers known flaws in the aspects of security and usability. A typical example is that people are hard to remember complex or meaningless passwords for a long time, due to the memory limitation and the multiple password inference [31,

This version of the article has been accepted for publication, after peer review (when applicable) and is subject to Springer Nature's AM terms of use (https://www.springernature.com/gp/open-research/policies/accepted-manuscript-terms), but is not the Version of Record and does not reflect post-acceptance improvements, or any corrections. The Version of Record is available online at: http://dx.doi.org/10.1007/s11036-021-01842-1.

32]. Instead, they may choose a weak password for easy memory, but may greatly affect the system's security level [3,48]. In addition, passwords would be suffered from various attacks like recording attacks [35] - malware can record the phone screen, and charging attacks [29,30] - a kind of side channel attack that records the phone screen when the phone is charging.

Generally, password-based authentication includes both textual and graphical passwords. Different from textual passwords, graphical password (GP) requires users to generate their credentials by interacting with image(s). Android unlock pattern should be most widely known GP scheme, in which users can create a pattern to unlock their devices, within a grid of 3×3 [27, 28]. The motivation behind is that users can remember images better than textual strings [36]. However, graphical password may also suffer many issues similar to the traditional textual passwords, such as recording attacks and charging attacks. For example, the password space of Android unlock patterns is still vulnerable to brute-force attack (i.e., with only 389,112 possible patterns), and attackers can further reduce the password space by identifying the remained touch trails [2]. On the other hand, GP scheme needs to consider usability in practical usage, i.e., *PassPoints* [47] allows users to click on some locations on an image as credentials, but it may cause a high error rate for some users who are easy to confuse their selected locations.

In short, as long as attackers successfully obtain the correct patterns, GP schemes would become insecure. For example, cyber-attackers can launch charging attacks and obtain the unlock pattern from the recorded video clips [29,30]. To further improve the security of unlock mechanisms, there is a trend of involving behavioral biometrics with unlock mechanisms, aiming to verify user's identity based on their behavioral features. For instance, De Luca et al. [4] presented an idea of combining unlock patterns with behavioral features (e.g., touch coordinates) using dynamic time warping (DTW). The system needs to verify both the input pattern as well as how the user input their patterns. Then Meng et al. [28] introduced TMGuard, a touch movement-based scheme to enhance the Android unlock patterns, by verifying how users perform the touch movement. Li et al. [18,19] introduced SwipeVLock, a supervised unlocking mechanism with swipe action on mobile devices. The scheme can verify a user according to their unlock patterns and swipe features.

In this work, we advocate the current trend of integrating unlock mechanisms with behavioral biometric for a more secure authentication process. We then develop DCUS, a double-click-based unlocking scheme on smartphones, which requires users to unlock their device by using a double-click action to select the location on the selected image. The selection of double-click actions is due to its common usage, i.e., when most users are playing their phones. The contributions of our work can be summarized as below.

- We develop DCUS, a double-click-based unlocking scheme on smartphones for authenticating users based on their double-click action. There is a two-step registration process: users first have to select a background image and then perform a double-click action on the selected location. A successful login requires examining whether both image and action are correct. This mechanism is transparent and easy to implement.
- For DCUS, we extract some behavioral features such as pressure, finger size and time difference to describe how users perform a double-click action, and evaluate the scheme with some supervised learning algorithms such as Decision tree (J48), Naive Bayes, Support Vector Machine (SVM), K-nearest neighbours (IBK) and Back Propagation Neural Network (BPNN).
- In the evaluation, we perform a new user study (different from the previous work [1]) with 60 common phone users. We also compare the performance between our scheme and a similar scheme proposed by De Luca et al [4]. The results indicate that participants could work well under our DCUS in practice, through analyzing the statistics and users' feedback.

The remaining parts are organized as follows. Section 2 introduces related work on unlock mechanisms and behavioral authentication schemes. Section 3 introduces the design of DCUS with selected features. Section 4 describes our user study with 60 participants. We discuss some limitations in Section 5 and conclude our work in Section 6.

2 Related Work

This section introduces related work on unlocking mechanism on mobile devices and behavioral authentication schemes.

2.1 Unlocking Mechanism

To protect mobile devices from unauthorized access, the design of unlocking mechanisms is an effective solution. Amongst the current unlocking mechanisms, Android unlock patterns [4,28] are one widely used scheme on smartphones, allowing people to draw a pattern within a 3×3 grid. This Android unlock application is actually

an extension from *Pass-Go* [43], which requires users to create a pattern on an image.

Table 1 Unlocking schemes on mobile devices in the literature.

Research Work	Performance
Face Unlock [8]	90.5% (Success Rate)
OpenSesame [11]	11-15% (FNR and FPR)
Izuta et al. [12]	43% (FAR)
TMGuard [28]	2.12%-2.23% (FAR and FR)
WearLock [49]	90% (Success Rate)
Heartbeat [45]	3.51% (EER)
SwipeVlock [18,19]	98% (Success Rate)
Shape-based scheme [20]	93.3% (Success Rate)

In the literature, there are many unlocking schemes on mobile devices, as shown in Table 1. Findling and Mayrhofer [8] introduced a Face Unlock system by using both frontal and profile face information during a pan shot around the user's head, based on camera and movement sensor. They showed a success rate of around 90.5%, but face recognition also suffers some issues [16]. Guo et al. [11] introduced OpenSesame, which verifies users based on their shaking patterns for locking/unlocking. By using a support vector machine (SVM) classifier, they could reach an FNR of 11%, with a standard deviation of 2.0%, and an FPR of around 15% with a standard deviation of 2.5%. Izuta et al. [12] presented a screen unlocking system on phones based on an accelerometer and pressure sensor arrays. They considered users' behavioral features when taking a mobile phone from the pocket and the pressure distribution when gripping the mobile phone, i.e., a taking-out action. In the evaluation, an FAR of around 0.43 was achieved at 30th trial with the training data from 18 objects. Meng et al. [28] introduced TMGuard, a touch movement-based security mechanism aiming to improve the security of Android unlock patterns. It requires users to input both correct pattern and touch movement for authentication. In the study with 75 participants, they could reach an FAR of 2.12% and FRR of 2.23%.

Yi et al. [49] introduced WearLock, which uses acoustic tones as tokens to automate the phone unlocking. The design includes signal detection using preamble identification, time synchronization using preamble and cyclic prefix, channel estimation, etc. They finally showed an average success rate of 90% among five participants. Wang et al. [45] introduced an unlocking scheme based on the built-in accelerometer to capture the heartbeat vibration. To unlock the device, users only have to press the device on their chest to collect heartbeat signals, and the system can identify the user within a few heartbeats. Their evaluation collected more than 110, 000 heartbeat samples from 35 participants, and reached an Equal Error Rate (EER) of 3.51% for user authentication when using five heartbeat cycles. Li et al. [18,19] introduced SwipeVLock, an unlocking mechanism that verifies users based on swiping action. Their results showed that participants could perform well with a success rate of 98% in the best case. Li et al. [20] introduced a simple shape-based behavioral scheme that requires users to draw some simple shapes for authentication. They found that SVM classifier could outperform other classifiers in their evaluation, and that participants preferred two-shape scheme by balancing both security and usability.

Basically, unlock mechanism can be considered as pure graphical password schemes or hybrid schemes with other elements [33,41]. For example, in order to enlarge the password space, recent schemes may consider involving world map so that users can create a password by selecting one or more locations on the map [38]. Meng [26] introduced *RouteMap*, which requires users to make a route on a world map. Sun *et al.* [42] presented *PassMap* in which two locations should be selected by users, while Thorpe *et al.* [44] showed *GeoPass* in which only one location is required to be selected by users. The number of locations may affect the scheme performance, while there is no significant difference between selecting one and two locations [33].

Similar to textual passwords, unlock patterns may also have the issue of multiple password interference, where users can be confused when they need to handle multiple credentials. Meng *et al.* [32] investigated this issue and considered six account scenarios between textual passwords and map-based passwords. Their study with 60 participants indicated that participants in the map-based graphical password scheme could perform better than the textual password scheme in both short-term (one-hour session) and long term (after two weeks) password memory tests.

2.2 Behavioral Authentication

With the rapid development of Internet-of-Things (IoT), there is a demand to design behavioral authentication schemes to provide implicit user verification on smart devices [13,22]. As most current phones are touch-enabled, many touch behavioral schemes have been studies. For instance, Fen *et al.* [7] introduced a user authentication scheme based on their finger gesture, and provided an FAR of 4.66% and an FRR of 0.13% using a random forest classifier. An early behavioral authentication scheme was proposed by Meng *et al.* [23]. They employed a total of 21 features and provided an average error rate of 3% using a hybrid algorithm called PSO-RBFN. Then

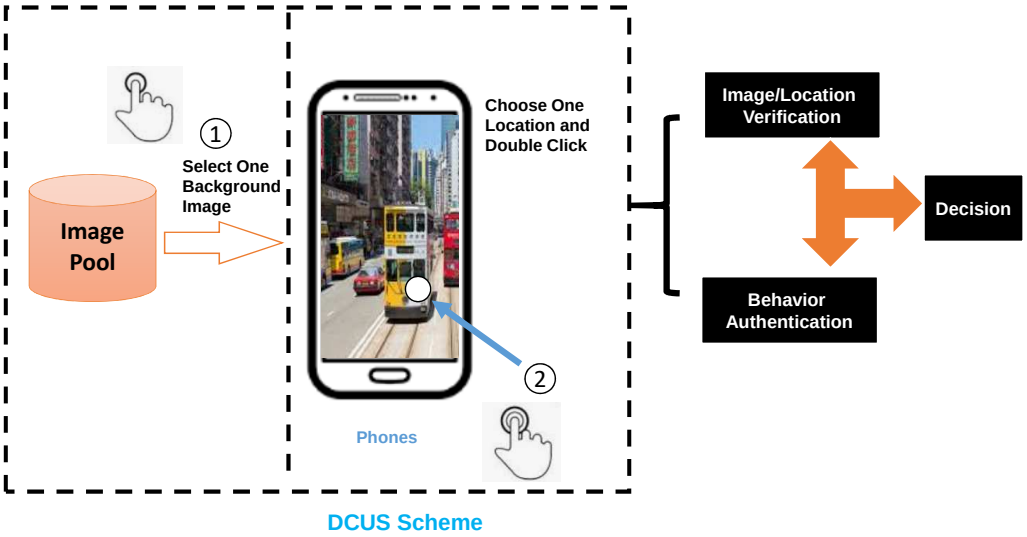

Fig. 1 DCUS scheme: (1) Step1: select one background image; and (2) Step2: choose one location on the image and double click.

Touchalytics was introduced by Frank *et al.* [9], with a number of 30 features. Their scheme could achieve a median equal error rate of around 4%.

To design a suitable behavioral authentication scheme, it is important to understand users' habits. The scheme of CD-GPS was introduced by [24], which explored the effect of multi-touch on creating graphical passwords in the aspects of security and usability. They found that by integrating the action of multi-touch, graphical passwords can be generally enhanced. Zheng *et al.* [50] investigated users' tapping habits on phones with passcode input. With a one-class algorithm, they could reach an averaged equal error rate of nearly 3.65%. Smith-Creasey and Rajarajan [37] believed that a stacked classifier could help address some prevalent issues, and introduced a set of meta-level classifiers. They showed an equal error rate of 3.77% for a single sample. Sharma and Enbody [40] explored users' habits when they play with the application interface, and studied an SVM-based ensemble classifier. Their results showed a mean equal error rate of 7% during the authentication. Shahzad *et al.* [39] focused on how participants input a gesture on phones and introduced a scheme with features like velocity, device acceleration, and stroke time. Li et al. [17] introduced three practical anti-eavesdropping password entry schemes on stand-alone smart glasses, named gTapper, gRotator and gTalker. This aims to break the correlation between the underlying password and the interaction observable to attackers. Li et al. [21] presented a study to investigate users' touch behavior within Email applications on smartphones, and found the behavioral deviation to be decreased during the Email usage.

Fang et al. [6] introduced HandiText, a handwriting recognition scheme for user authentication based on behavior and biometrics features. It captures the static biological features and dynamic behavior features when users are writing. With the algorithm of Long Short-Term Memory (LSTM), this scheme could reach a relatively low false positive rate and false negative rate. Meng and Liu [34] introduced a touch movement-based GP scheme on smartphones - TMGMap, which requires users to draw their secrets on a world map via touch movement events. Some more schemes can refer to some surveys like [10, 25].

3 Our Proposed Scheme

In the research community, many unlocking schemes have been studied by integrating with behavioral features. In this work, we advocate this advantage and introduce DCUS, a double-click-based unlocking scheme, which requires users to double click on a location on the selected image. Figure 1 depicts the scheme design with two major steps: 1) choosing one background image and 2) double-clicking on one location.

DCUS registration phase. Users should first choose one image from the image pool as the background image, and then select one location on the selected image to double click. The number and the themes of images can be adjusted according to the concrete application scenarios. In practice, there is a balance should be made between usability and security.

DCUS authentication phase. To authenticate and unlock the phone, users have to choose the same image

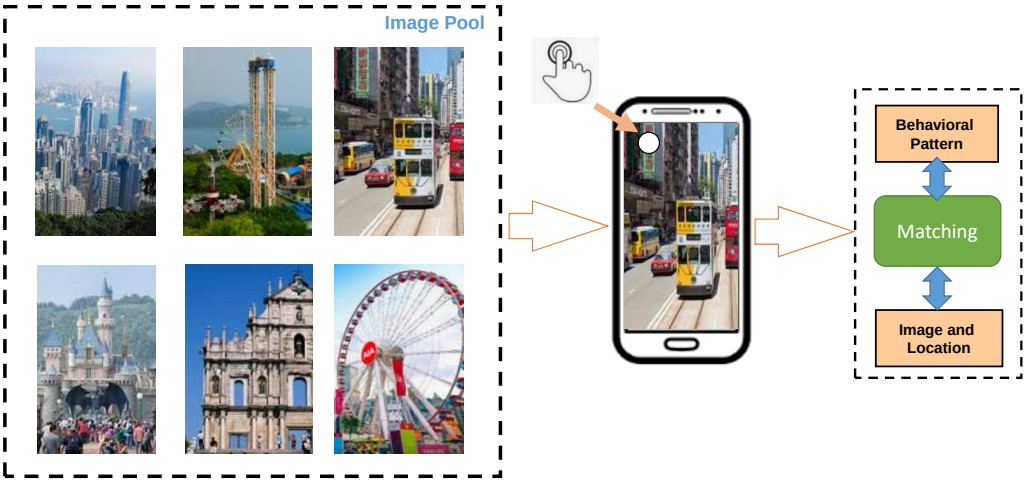

Fig. 2 A case implementation of DCUS in our user study.

from the image pool, and double click on the same (pre-selected) location. A successful trial requires all the selected background image, location and double-clicking to be matched with the stored data.

Scheme implementation. Figure 2 shows an implementation case of DCUS. There are a total of six images in the image pool (including buildings, ferris wheel, playground and public transportation), and users need to select one image and double click on a location to unlock the phone. To decide whether current user is legitimate, our scheme should compare image & location selection and double-click behavior with the pre-stored information. For image and location matching, we only need to compare the input with the stored pattern. For behavioral verification, our scheme can build a normal profile and make a decision, by using various machine learning algorithms like SVM, decision tree, neural networks, etc.

To make the scheme usable in practice, we set the error tolerance to a 21×21 pixel box around the selected location. The setting is selected based on the previous work [18,33], i.e., these work demonstrated that it is usable to adopt an error tolerance of 21×21 pixel in practical GP design and implementation.

Double-click features. To model users' double click actions, this work considers some popular and common behavioral features such as time difference between two touches, touch pressure, touch duration and acceleration. The effectiveness of these features has been validated by previous studies. The coordinates of touches would be examined by location matching process.

- *Time difference between two touches.* Our scheme records the time difference between the first touch and the second touch. Intuitively, phone users should perform the double-click action differently.
- *Touch pressure.* Most smartphones are able to record touch pressure values, which can be utilized to model a user's touch behavior.
- *Touch duration.* This feature is used to measure the time difference between a touch press and touch release, which can be used to distinguish users. For our scheme, this feature contains two vectors: the touch duration for the first click, and the touch duration for the second click.
- *Touch acceleration.* Similar to the previous work [50], this work considers touch acceleration with three vectors, such as the magnitude of acceleration when the touch is pressed down; the magnitude of acceleration when the touch is released; and the average value of magnitude of acceleration during touch-press to touch-release.

4 User Study

To investigate the performance of DCUS, we involve a total of 60 participants in an approved user study, which is a new study than the one in the previous work [1]. In particular, 50% of them are Android phone users, 30% of them are iPhone users, and the rest are using both types of phones. Table 2 describes the basic information of participants about their occupation and gender. We have 29 males and 31 females who aged from 21 to 50, including business people, students, university researchers, staff and faculty members. Each participant could get a $20 gift voucher after the study.

Supervised machine learning. Similar to previous work [1,18], we mainly consider some typical learning

Table 2 Participants information in the user study.

Information	Male	Female	Occupation	Male	Female
Age < 25	14	15	Students	16	19
Age 25-35	10	11	University Faculty&Staff	9	7
Age 35-50	5	5	Business People	4	5

algorithms to model users' click actions such as Decision tree (J48), Naive Bayes, Support Vector Machine (SVM), K-nearest neighbours (IBK) and Back Propagation Neural Network (BPNN). These classifiers can be easily implemented on smart devices, and are popular in other relevant studies.

- The decision tree classifier can label instances based on the pre-trained tree-like structure.
- Naive Bayes algorithms are developed based on Bayes' theorem with the assumption of conditional independence between every pair of features given the value of the class variable.
- K-nearest neighbours classifier is simple and easy to implement, in which an instance is classified by a majority vote of its neighbors. There is no need to build a model and tune several parameters.
- Back-propagation neural network fine-tunes the weights of a neural net based on the error rate obtained in the previous iteration, by making the model reliable by increasing its generalization.
- Support Vector Machine (SVM) [15] can plot each data item as a point in a n dimensional space, in which each feature is being the value of a particular coordinate, and then it finds the hyper-plane to distinguish the two classes.

To avoid implementation bias, we extract these classifiers from the WEKA platform [46], which provides an open-source collection of many machine learning algorithms in Java. In the evaluation, we use the default settings for all classifiers, which is often adopted by other relevant work. To judge the performance, we use the following two typical metrics.

- False Acceptance Rate (FAR): shows the rate of how many intruders are classified as legitimate users.
- False Rejection Rate (FRR): shows the rate of how many legitimate users are classified as intruders.

Similar to other studies like [18,19], we also adopt a metric of average error rate, which is an average value of FAR and FRR.

Algorithm performance. In our previous work [1], the study with 40 participants have demonstrated that SVM could achieve the best performance. To facilitate the comparison with previous studies, we used 60% of trials as training data and the rest as testing data, with a 10-fold cross-validation mode. Table 3 indicates that SVM could achieve better performance than other classifiers, i.e., it could achieve an average error rate (AER) of 3.8%, as compared with J48 8.9%, NBayes 12.05%, IBK 7.95%, and BPNN 8.15%. Hence in this work, we used SVM for user authentication in the new user study.

Table 3 The performance of different classifiers obtained from the previous work [1].

Metric	J48	NBayes	SVM	IBK (k=3)	BPNN
FAR (%)	8.3	11.8	3.5	8.4	7.6
FRR (%)	9.5	12.3	4.1	7.5	8.7
AER (%)	8.9	12.05	3.8	7.95	8.15

Study steps. Before the study, we first introduced our objectives to all participants, and explained what kind of data would be collected and how to ensure the data privacy. We also provided a paper note with the same guidelines for all participants. Different from the previous work [1], in this new study, we required participants to complete both our scheme and a similar scheme of DeLucaUnLock, which was proposed by De Luca et al [4]. Their scheme authenticates users by checking both unlock pattern and behavioral biometrics. The scheme to be started first would be selected randomly, and there would be a 15-minute rest between two schemes.

Each participant could have three trials to get familiar with the scheme, when they got the Android phone (Samsung Galaxy Note). All participants performed the study in our lab environment. The detailed steps for each scheme are shown as below.

- DCUS scheme
  - Step 1. Creation phase: participants need to register their credentials according to DCUS steps.
  - Step 2. Confirmation phase: participants have to confirm the DCUS credentials by verifying both the image, location and double-click behavior for 5 times. Participants can change their credentials if they fail or want to create a new one.
  - Step 3. Distributed memory: participants are given one paper-based finding tasks to distract them for 10 minutes.
  - Step 4. Login phase: participants should unlock the phone with their credentials for 5 trials.

Table 4 Success rate in the login and retention phase for DCUS and DeLucaUnlock.

Success rate	DCUS	DeLucaUnLock
Confirmation	275/300 (91.7%)	268/300 (89.3%)
Login	287/300 (95.7%)	288/300 (96.0%)
Retention	243/260 (93.4%)	240/260 (92.3%)

  - Step 5. Retention. After three days, participants are invited to unlock the phone for 5 times in our lab.
- DeLucaUnLock
  - Step 1. Creation phase: participants need to register their credentials according to DeLucaUnLocksteps.
  - Step 2. Confirmation phase: participants have to confirm the DeLucaUnLock secrets by verifying both the pattern and behavioral features for 5 times. Participants can change their credentials if they fail or want to create a new one.
  - Step 3. Distributed memory: participants are given one paper-based finding tasks to distract them for 10 minutes.
  - Step 4. Login phase: participants should unlock the phone with their DeLucaUnLock credentials for 5 trials.
  - Step 5. Retention. After three days, participants are invited to unlock the phone for 5 times in our lab.

After each participant completed two schemes and the retention phase, they would be given one feedback form with a set of questions (with totally two feedback forms during the study).

Study results. In the study, we could collect a total of 300 trials in the confirmation phase and 300 trials in the login phase for each scheme. Table 4 depicts the authentication performance between DCUS and DeLucaUnlock scheme.

- *Confirmation phase.* It is found that participants could reach a success rate of 91.7% and 89.3% for DCUS and DeLucaUnlock scheme, respectively. For DCUS, the errors were mainly caused by behavioral matching with two main error types: 1) a double-click action is too fast or slow than the registered one, and 2) the touch acceleration is not matched. For DeLucaUnlock, the errors are similarly caused by behavioral matching, i.e., participants touch action suffered a deviation from the normal profile.
- *Login phase.* In this phase, it is found that participants could perform better than the confirmation phase, with a success rate of 95.7% and 96% for DCUS and DeLucaUnlock scheme, respectively. This means that participants got to be more familiar with the scheme. The error types were similar to the confirmation phase for both schemes.
- *Retention phase.* Participants were invited to come back for a retention test after three days, and 52 of them were successfully returned. It is found that a success rate of 93.4% and 92.3% could be achieved for DCUS and DeLucaUnlock scheme, respectively. The rate of DCUS is a bit higher than DeLucaUnlock scheme, and the errors were caused by behavioral deviation for both schemes. While only three participants made an error due to the selection of a wrong location for DCUS.

Based on the collected data, it validated the observation in former work that few errors were made due to the image and location selection. This implies two points: 1) the selected error tolerance is usable, and 2) users can remember the image and location well. For the errors occurred in the behavioral matching process, performing more practice should be an option to improve the authentication performance, according to the observation from previous studies like [28]. Table 4 shows that the authentication performance is similar between our DCUS and the DeLucaUnlock scheme. As the DeLucaUnlock scheme is believed to be usable by the literature, our DCUS is implied to be viable and usable as well.

User feedback. During the user study, two feedback forms were given to each participant regarding the scheme usage, in the aspects of both security and usability. Ten-point Likert scales are used for each question, where 1-score indicates strong disagreement and 10-score indicates strong agreement. The major questions and scores are shown in Table 5.

- *The first feedback form.* For the first two questions, it is found that participants overall satisfied the usage of both schemes, i.e, DCUS got a higher score of 9.1 versus a score of 8.8 for DeLucaUnlock. Most participants also satisfied with the time consumption, i.e., both schemes received a score of above 8: a score of 8.6 and 8.3 for DCUS and DeLucaUnlock each. Then, we ask whether participants would like to use DCUS or DeLucaUnlock as compared with textual passwords in practice, where more than half participants were willing to try DCUS, and almost half of them were willing to try DeLucaUnlock. We informally interviewed some participants, and found that most participants believed they could complete DCUS faster than DeLucaUnlock. This is the main reason why they would like to try DCUS. The 7th question echoed to this feedback that most participants prefer DCUS than DeLucaUnlock. While the

Table 5 Major questions and average scores from the participants.

Questions (Login Phase)	Average Scores
1. I could easily create a credential under DCUS	9.1
2. I could easily create a credential under DeLucaUnlock	8.8
3. The time consumption is acceptable for DCUS	8.6
4. The time consumption is acceptable for DeLucaUnlock	8.3
5. I prefer textual passwords than DCUS	4.4
6. I prefer textual passwords than DeLucaUnlock	5.1
7. I prefer DeLucaUnlock than DCUS in practical usage	3.6
8. I prefer Android unlock pattern than DCUS	5.5
Questions (Retention Phase)	**Average Scores**
1. I could easily log into DCUS	8.7
2. I could easily log into DeLucaUnlock	8.4
3. I can remember my selected image	8.8
4. I can remember my selected location on the image	9.1
5. I can remember how to input DeLucaUnlock	8.1
6. I prefer textual passwords than DCUS	4.5
7. I prefer textual passwords than DeLucaUnlock	5.2
8. I prefer DeLucaUnlock than DCUS	4.1

last question shows that most participants were still more familiar with Android unlock pattern.

– *The second feedback form.* This form is a bit different from the first one, while most participants considered both schemes are easily to use, with a score of 8.7 and 8.4 each. For DCUS, most participants could remember the selected image and location, with a score of 8.8 and 9.1, respectively. Also, most participants reflected that they could remember how to input DeLucaUnlock with a score of 8.1, though the score is lower than DCUS. As compared with the traditional textual password, the feedback was similar to the first form. That is, more than half participants were willing to try DCUS, while less than half participants were willing to try DeLucaUnlock. Most participants were more likely to use DCUS in practice, as they could perform faster in the authentication.

Previous study. For the feedback from previous study [1], most participants felt positive on the scheme usage, i.e., they believe it is easy to create the password, and the time consumption is acceptable. When compared DCUS with PIN-code, it is found that most participants believed DCUS is more secure than 4-digit PIN codes, but may be less secure than 8-digit PIN codes. This is because they considered DCUS seemed simpler than 8-digit PIN codes, with only one double-click action. For the retention phase, the score is still similar to the first form, but nearly half participants believed that DCUS might have a similar security level as 8-digit PIN codes (they realized that behavioral authentication could provide additional protection). At last, most participants accepted the time consumption required by DCUS with a score of 8.4.

Current study. The collected feedback validated the observations on DCUS from the previous study. Most participants are positive on the usage of DCUS and DeLucaUnlock. While most of them preferred DCUS as it is easy to use without causing much time consumption in the login phase. Thus most of them were willing to try DCUS in a practical scenario.

5 Discussion

The current results and feedback on DCUS are mostly positive, but DCUS needs to be further improved to address some usability and security issues.

– *Usability aspect.* As an example implementation, this work considers six images in the image pool, but it is an open question on how to select the number and image themes. Usability studies can be performed on our scheme. Then, this work does not consider multiple password interference [31,32], which means that different passwords may confuse users' memory and input a wrong password. To investigate this issue, we plan to conduct another study that requires participants to create more than one DCUS credential. It is also an interesting topic to explore the impact of different phone types on scheme performance, and investigate the difference between right handed and left handed participants.

– *Security aspect.* Some participants reflected that DCUS might be less secure than a 8-digit PIN code due to the use of only one double-click action. To address this concern, one option is that DCUS can examine users' swiping behavior when they select images. This can be considered as a combination of

DCUS with SwipeVLock [18,19]. In addition, the selection of images and locations may be biased, and it is an interesting topic to study 'hot-spot' issue, which is commonly happened in graphical password generation and usage [23]. To further enhance the scheme, we can also consider more touch behavioral features for user authentication.

- *Scheme evaluation.* In this work, we involved 60 participants, and we plan to recruit more participants to validate our obtained results. It is the same to our evaluated machine learning schemes, our future work plans to consider more learning algorithms like deep learning, which is inspired by the structure and function of the brain called artificial neural networks. In addition, transfer learning is an interesting topic that explores how a learning model can be applied into different scenarios.
- *Adversarial scenario.* This work does not consider adversarial scenarios, where an attacker can get the phone and try to compromise the unlocking mechanism. Our future work also plans to investigate some attacks, e.g., mimic attack, to examine the scheme security in practice.
- *Background image.* In practice, users can define their own background image according to the requirements. The self-selected images can benefit users' memory, but may open a hole for attackers to explore, i.e., attackers can analyze users' habits and identify the potential images and locations. This is an interesting topic in future work.

6 Conclusion

With smartphones becoming popular, there is an increasing need to design proper unlocking mechanisms to enforce access control and examine the legitimacy of current phone users. The current unlock schemes like Android unlock patterns are vulnerable to various attacks, there is a trend of combining unlocking mechanisms with behavioral biometrics. Motivated by this, we introduce DCUS, a double-click-based unlocking scheme, which allows users to unlock the phone by double clicking on the location on the selected image. A successful login requires to check the selected image, image location and double-click action. In the study, we involved 60 participants and examined the scheme performance as compared with a similar scheme of DeLucaUnlock, according to success rate and users' feedback. In the study with the SVM classifier, we found that most participants could provide positive feedback and work well with DCUS, and that most of them were willing to use DCUS in a practical scenario.

7 Compliance with Ethical Standards

Conflict of Interest: All authors declare that they have no conflict of interest.

Acknowledgements We would like to thank the participants for their hard work in the user study. This work was partially supported by National Natural Science Foundation of China (No. 61802080 and 61802077).

References

1. W. Li, J. Tan, N. Zhu, and Y. Wang. Designing Double-Click-based Unlocking Mechanism on Smartphones. In: Proceedings of the First International Symposium on Emerging Information Security and Applications (EISA), Springer, 2020.
2. A.J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J.M. Smith. Smudge attacks on smartphone touch screens. In: Proceedings of the 4th USENIX Conference on Offensive Technologies, pages 1–7, USENIX Association, 2010.
3. Bonneau, J.: The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In: Proceedings of the 2012 IEEE Symposium on Security and Privacy, pp. 538-552 (2012)
4. 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 CHI, pages 987–996, ACM, 2012.
5. Deloitte's 2019 global mobile consumer survey. `https://www2.deloitte.com/content/dam/insights/us/articles/glob43115_2019-global-mobile-survey/DI_2019-global-mobile-survey.pdf`
6. L. Fang, H. Zhu, B. Lv, Z. Liu, W. Meng, Y. Yu, S. Ji, Z. Cao. HandiText: Handwriting Recognition based on Dynamic Characteristics with Incremental LSTM. ACM Transactions on Data Science, In Press, ACM. `https://doi.org/10.1145/3385189`
7. Feng, T., Liu, Z., Kwon, K.-A., Shi, W., Carbunary, B., Jiang, Y., Nguyen, N.: Continuous mobile authentication using touchscreen gestures. In: Proceedings of the 2012 IEEE Conference on Technologies for Homeland Security (HST), pp. 451-456, IEEE, USA (2012)
8. R.D. Findling, R. Mayrhofer: Towards face unlock: on the difficulty of reliably detecting faces on mobile phones. MoMM 2012: 275-280
9. Frank, M., Biedert, R., Ma, E., Martinovic, I., Song, D.: Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication. IEEE Transactions on Information Forensics and Security 8(1), 136-148 (2013)
10. M. Gomez-Barrero, J. Galbally: Reversing the irreversible: A survey on inverse biometrics. Comput. Secur. 90: 101700 (2020)
11. Y. Guo, L. Yang, X. Ding, J. Han, Y. Liu: OpenSesame: Unlocking smart phone through handshaking biometrics. INFOCOM 2013: 365-369
12. R. Izuta, K. Murao, T. Terada, T. Iso, H. Inamura, M. Tsukamoto: Screen Unlocking Method using Behavioral Characteristics when Taking Mobile Phone from Pocket. MoMM 2016: 110-114

13. L. Jiang, W. Meng: Smartphone User Authentication Using Touch Dynamics in the Big Data Era: Challenges and Opportunities. Biometric Security and Privacy - Opportunities & Challenges in The Big Data Era (Book), Springer, pp. 163-178, 2016.
14. X. Larrucea, M. Moffie, Sigal. Asaf, I. Santamaria: Towards a GDPR compliant way to secure European cross border Healthcare Industry 4.0. Comput. Stand. Interfaces 69: 103408 (2020)
15. LIBSVM – A Library for Support Vector Machines. https://www.csie.ntu.edu.tw/~cjlin/libsvm/.
16. Y. Li, Z. Wang, Y. Li, R.H. Deng, B. Chen, W. Meng, H. Li: A Closer Look Tells More: A Facial Distortion Based Liveness Detection for Face Authentication. AsiaCCS 2019: 241-246
17. Y. Li, Y. Cheng, W. Meng, Y. Li, R.H. Deng. Designing Leakage-Resilient Password Entry on Head-Mounted Smart Wearable Glass Devices. IEEE Transactions on Information Forensics and Security, vol.16, pp. 307-321, 2021.
18. W. Li, J. Tan, W. Meng, Y. Wang, J. Li. SwipeVLock: A Supervised Unlocking Mechanism Based on Swipe Behavior on Smartphones. The 2nd International Conference on Machine Learning for Cyber Security (ML4CS), pp, 140-153, September 2019.
19. W. Li, J. Tan, W. Meng, Y. Wang. A Swipe-based Unlocking Mechanism with Supervised Learning on Smartphones: Design and Evaluation. Journal of Network and Computer Applications, vol. 165, 102687, Elsevier, 2020.
20. W. Li, Y. Wang, J. Li, Y. Xiang. Towards Supervised Shape-based Behavioral Authentication on Smartphones. Journal of Information Security and Applications, volume 55, 102591, 2020.
21. W. Li, W. Meng, S. Furnell. Exploring Touch-based Behavioral Authentication on Smartphone Email Applications in IoT-enabled Smart Cities. Pattern Recognition Letters, In press, Elsevier. https://doi.org/10.1016/j.patrec.2021.01.019
22. Z. Lin, W. Meng, W. Li, D.S. Wong. Developing Cloud-based Intelligent Touch Behavioral Authentication on Mobile Phones. Deep Biometrics (Book), Richard Jiang (eds), Springer, July 2019.
23. Meng, Y.: Designing Click-Draw Based Graphical Password Scheme for Better Authentication. In: Proceedings of the 7th IEEE International Conference on Networking, Architecture, and Storage (NAS), pp. 39-48 (2012)
24. Meng, Y., Li, W., Kwok, L.-F.: Enhancing Click-Draw based Graphical Passwords Using Multi-Touch on Mobile Phones. In: Proceedings of the 28th IFIP TC 11 International Information Security and Privacy Conference (IFIP SEC), IFIP Advances in Information and Communication Technology 405, pp. 55-68 (2013)
25. Meng, W., Wong, D.S., Furnell, S., Zhou, J.: Surveying the development of biometric user authentication on mobile phones. IEEE Communications Surveys and Tutorials 17(3), pp. 1268-1293 (2015)
26. Meng, W.: RouteMap: A Route and Map Based Graphical Password Scheme for Better Multiple Password Memory. In: Proceedings of the 9th International Conference on Network and System Security (NSS), pp. 147-161 (2015)
27. Meng, W.: Evaluating the Effect of Multi-Touch Behaviours on Android Unlock Patterns. Information and Computer Security, vol. 24, no. 3, pp. 277-287, Emerald (2016)
28. Meng, W., Li, W., Wong, D.S., Zhou, J.: TMGuard: A Touch Movement-based Security Mechanism for Screen Unlock Patterns on Smartphones. In: Proceedings of the 14th International Conference on Applied Cryptography and Network Security (ACNS), pp. 629-647 (2016)
29. Meng, W., Lee, W.H., Liu, Z., Su, C., Li, Y.: Evaluating the Impact of Juice Filming Charging Attack in Practical Environments. In: Proceedings of ICISC, pp. 327-338 (2017)
30. Meng, W., Fei, F., Li, W., Au, M.H.: Harvesting Smartphone Privacy Through Enhanced Juice Filming Charging Attacks. In: Proceedings of ISC, pp. 291-308 (2017)
31. Meng, W., Li, W., Kwok, L.-F., Choo, K.-K.R.: Towards Enhancing Click-Draw Based Graphical Passwords Using Multi-Touch Behaviours on Smartphones. Computers & Security, vol. 65, pp. 213-229 (2017)
32. Meng, W., Li, W., Lee, W., Jiang, L., Zhou, J.: A Pilot Study of Multiple Password Interference between Text and Map-based Passwords. In: Proceedings of the 15th International Conference on Applied Cryptography and Network Security (ACNS), pp. 145-162 (2017)
33. Meng, W., Lee, W., Au, M.H., Liu, Z.: Exploring Effect of Location Number on Map-Based Graphical Password Authentication. In: Proceedings of the 22nd Australasian Conference on Information Security and Privacy (ACISP), pp. 301-313 (2017)
34. W. Meng, Z. Liu. TMGMap: Designing Touch Movement-based Geographical Password Authentication on Smartphones. In: Proceedings of the 14th International Conference on Information Security Practice and Experience (ISPEC), pp. 373-390, 2018.
35. Nyang, D., Kim, H., Lee, W., Kang, S., Cho, G., Lee, M.K., Mohaisen, A.: Two-Thumbs-Up: Physical protection for PIN entry secure against recording attacks. Computers & Security 78, pp. 1-15 (2018)
36. Shepard, R.N.: Recognition memory for words, sentences, and pictures. Journal of Verbal Learning and Verbal Behavior, vol. 6, no. 1, pp. 156-163 (1967)
37. Smith-Creasey, M., Rajarajan, M.: A continuous user authentication scheme for mobile devices. In: Proceedings of the 14th Annual Conference on Privacy, Security and Trust (PST), pp. 104-113 (2016)
38. Spitzer, J., Singh, C., Schweitzer, D.: A Security Class Project in Graphical Passwords. Journal of Computing Sciences in Colleges 26(2), pp. 7-13 (2010)
39. Shahzad, M., Liu, A.X., Samuel, A.: Behavior Based Human Authentication on Touch Screen Devices Using Gestures and Signatures. IEEE Transactions on Mobile Computing 16(10), pp. 2726-2741 (2017)
40. Sharma, V., Enbody, R.: User authentication and identification from user interface interactions on touch-enabled devices. In: Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), pp. 1-11 (2017)
41. Suo, X., Zhu, Y., Owen, G.S.: Graphical Passwords: A Survey. In: Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC), pp. 463-472. IEEE Computer Society, USA (2005)
42. Sun, H., Chen, Y., Fang, C., Chang, S.: PassMap: A Map Based Graphical-Password Authentication System. In: Proceedings of AsiaCCS, pp. 99-100, 2012.
43. Tao, H., Adams, C.: Pass-Go: A Proposal to Improve the Usability of Graphical Passwords. International Journal of Network Security 2(7), pp. 273-292 (2008)
44. Thorpe, J., MacRae, B., Salehi-Abari, A.: Usability and Security Evaluation of GeoPass: a Geographic Location-Password Scheme. In: Proceedings of the 9th Symposium on Usable Privacy and Security (SOUPS), pp. 1-14 (2013)

45. L. Wang, K. Huang, K. Sun, W. Wang, C. Tian, L. Xie, Q. Gu: Unlock with Your Heart: Heartbeat-based Authentication on Commercial Mobile Phones. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 2(3): 140:1-140:22 (2018)
46. Weka: Machine Learning Software in Java. `https://www.cs.waikato.ac.nz/ml/weka/`,
47. Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., Memon, N.: Passpoints: Design and Longitudinal Evaluation of A Graphical Password System. International Journal of Human-Computer Studies 63(1-2), 102-127 (2005)
48. Weir, M., Aggarwal, S., Collins, M., Stern, H.: Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords. In: Proceedings of CCS, pp. 162-175 (2010)
49. S. Yi, Z. Qin, N. Carter, Q. Li: WearLock: Unlocking Your Phone via Acoustics Using Smartwatch. ICDCS 2017: 469-479
50. Zheng, N., Bai, K., Huang, H., Wang, H.: You are how you touch: User verification on smartphones via tapping behaviors. In: Proceedings of the 2014 International Conference on Network Protocols (ICNP), pp. 221-232 (2014)