# Exploring How User Routine Affects the Recognition Performance of a Lock Pattern

Lisa de Wilde, Luuk Spreeuwers, Raymond Veldhuis

Faculty of Electrical Engineering, Mathematics and Computer Science
University of Twente
P.O. Box 217, 7500 AE Enschede, The Netherlands
r.n.j.veldhuis@utwente.nl

**Abstract:** To protect an Android smartphone against attackers, a lock pattern can be used. Nevertheless, shoulder-surfing and smudge attacks can be used to get access despite of this protection. To combat these attacks, biometric recognition can be added to the lock pattern, such that the lock-pattern application keeps track of the way users draw the pattern. This research explores how users change the way they draw lock patterns over time and its effect on the recognition performance of the pattern. A lock-pattern dataset has been collected and a classifier is proposed. In this research the best result was obtained using the x- and y-coordinate as the user's biometrics. Unfortunately, in this paper it is shown that adding biometrics to a lock pattern is only an additional security that provides no guarantee for a secure lock pattern. It is just a small improvement over using a lock pattern without biometric identification.

## 1 Introduction

Nowadays all Android smartphones can be unlocked by drawing a pattern in a grid of 3 x 3 points. A pattern is valid if it obeys three rules: the pattern connects at least four points, each point is used only once and when two points are connected by a straight line there is no unused point between them [AGM+10].

Unfortunately, it is easy for an attacker to trace the pattern of a user and unlock the smartphone by shoulder-surfing or smudge-attacks. With a shoulder-surfing attack an attacker records the user's pattern. A smudge-attack occurs when an attacker extracts information from the smudges left on the screen [SLS13]. The success chances of these attacks can be reduced by adding the user's biometrics as an authentication factor [AW12, JRP06].

During enrolment the user draws the pattern while the lock pattern application records the user's biometrics, here the location, pressure and contact area of the finger as functions of time. During verification, the user draws the pattern to unlock the screen. The application checks if the pattern is correct and compares the biometrics to the enrolled data.

In this research it is explored how the biometrics of the user evolve over time where the user repeatedly enters the same pattern. This is done by a data analysis on a dataset collected in a user study. In this study the application *Touch Signature* was used to keep track

of the way a user draws a lock pattern. It is also explored how the evolution of the way the user draws the lock pattern affects the recognition performance of the lock pattern. This is important in order to find out if the user can still access his smartphone when his drawing behaviour naturally changes. Next to that, imposters that know the owner's lock pattern should not be granted access to the smartphone.

This leads to the following research question: *How does user routine affect the recognition performance of a lock pattern?* and more specifically: *How do users change the way they draw lock patterns over time?* and *How will this affect the recognition performance of the lock pattern?*

The remainder of this paper is as follows. Section 2 discusses the methods used to answer the research questions. Section 3 presents the results of the analysis of the data that has been collected. Section 4 discusses the results and presents conclusions.

## 2 Methods

### 2.1 User study and dataset

People were asked to install the application *Touch Signature* on their Android smartphone[1]. The application asks to draw the same pattern (see Figure 1) ten times every day for eight days. The pattern starts at the last row's central point. While drawing, the application keeps track of where and when the finger touches the screen, the pressure from the finger on the screen and the area that is touched by the finger.

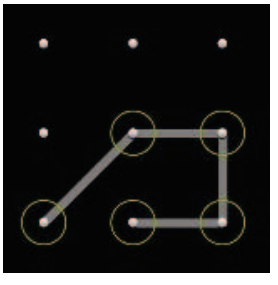

Figure 1: The lock pattern used in the user study.

In total 144 individuals participated in the user study. Their gender, age and handedness are in Table 1. In addition the application collected information about the device: manufacturer, model, screen dpi and screen resolution. In this research the screen dpi and resolution are not taken into account.

The collected dataset is used to explore how users draw their lock pattern over a course of time. At first, the data is validated: the results of individuals who participated more than one time to the experiment were discarded from the dataset. As stated before a total of 144 participants have participated in this study. In the best case there should be eight days with ten measurements per participant. But only 43,06% of the participants did measurements for eight days (see Table 2). Besides that 4.76% of the participants did not do exactly ten measurements per day.

To get a first view of the measurement four 2d-plots were created (see Figure 2). Each plot contains the measurements of day one (blue lines) and day eight (dashed red lines)

[1]This application was developed by the students Stijn van Winsen, Joep Peeters, and Ties de Kock who are kindly acknowledged for this work.

Table 1: Partition of gender, age and handedness among participants.

| | **Amount** | **Percentage** |
|---|---|---|
| **Gender** | | |
| Female | 25 | 17,36% |
| Male | 119 | 82,64% |
| **Age** | | |
| 0 - 19 | 42 | 29,17% |
| 20 - 39 | 96 | 66,67% |
| 40 - 59 | 4 | 2,78% |
| 60 - 79 | 1 | 0,69% |
| 80 - 100 | 1 | 0,69% |
| **Handedness** | | |
| Left | 12 | 8,33% |
| Right | 125 | 86,81% |
| Not sure | 7 | 4,86% |

Table 2: Partitioning of number of measurement days among participants.

| **Days** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|
| **Number** | 43 | 5 | 5 | 3 | 2 | 7 | 11 | 62 | 5 | 1 |
| **Percentage** | 30% | 4% | 4% | 2% | 1% | 5% | 8% | 43% | 4% | 1% |

from one specific individual, whereby both days consists of ten measurements. The plots visualizes the x-coordinate versus time, y-coordinate versus time, pressure versus time and area touched by the finger versus time. The measurements of this individual in these plots represents the most of the measurements of other individuals.

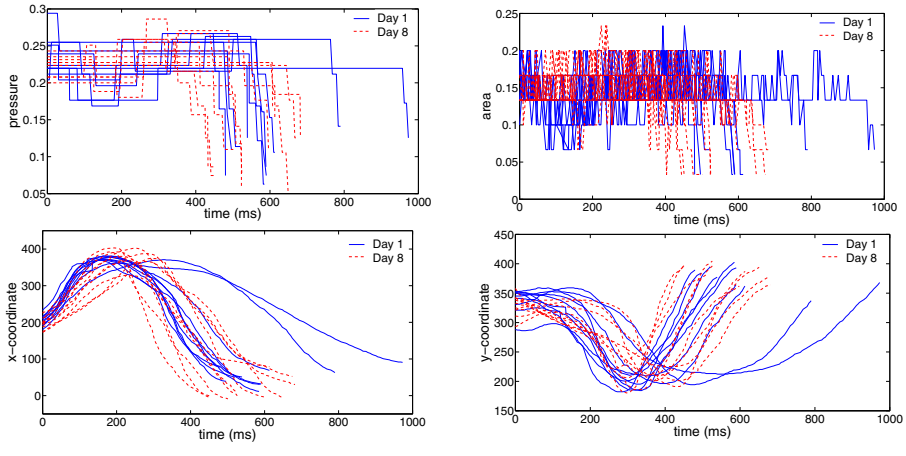


Figure 2: Top left: pressure versus time; top right: area touched by the finger versus time; bottom left: x-coordinate versus time; bottom right y-coordinate versus time.

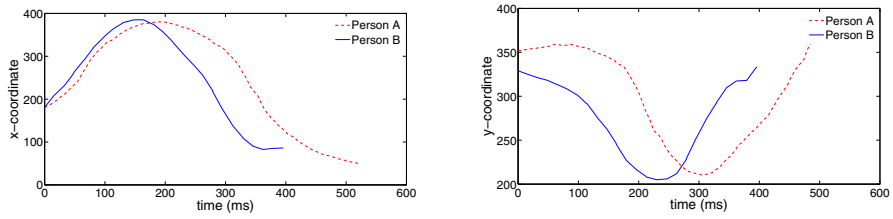


Figure 3: Left: x-coordinate versus time of two persons; right: y-coordinate versus time of two persons.

Ideally, different measurements of one individual should be (almost) the same, so the deviation between the different lines in the plots should be small. Unfortunately, it is clearly visible that there is a large deviation of the pressure and the area touched by the finger at different measurements. On the other hand the x-coordinate and y-coordinate seem more consistent and have a small deviation. For that reason, only the x- and y-coordinate and time are used to analyse the measurements and to answer the research questions. Figure 3 shows the x- and y-coordinate over time of two individuals. Each line represents one measurement. The lines are far apart from each other, which means that person B has drawn the pattern faster than person A. This suggests that the measurements of different persons are different and that these biometrics could be used to distinguish different individuals.

### 2.2 Classification

To compare the different measurements per individual a likelihood-ratio based classifier [SVSD14] is used. This classifier compares the biometric features of two lock patterns and produces a similarity score. The score increases with the similarity of the patterns. The score is compared with a threshold. If it is higher than the threshold the classifier decides that the lock patterns are from the same individual. Otherwise it decides that the lock patterns are from different individuals. In order to use this classifier every measurement must have the same amount of measuring points. This is achieved by inter- and extrapolating the measuring points of the dataset to 93 equidistant points, 93 being the median of the measuring points of the dataset. The classifier is based on transforming the data using two transformations. The first is called principle component analysis (PCA) and has the purpose of reducing the dimensionality of the data such that noisy components are removed. The second is called linear discriminant analysis (LDA) and retains only discriminative components. Hence, the classifier has two parameters that need to be tuned to the data: the number of PCA coefficients and the number of LDA coefficients. Given these parameters, the transformations are learned from a a part of the data that is set aside as a training set. There is no overlap between individuals in this training set and the remaining test set. The dataset is split based on the characteristics of the participants and their smartphones. The training set consists of data of 96 individuals and the test set contains data of

Table 3: Results of the comparison of all measurements.

| **Dataset** | **TMR@FMR=0,1** | **TMR@FMR=0,01** | **EER** |
|---|---|---|---|
| x- and y-coordinate and time | 53,1% | 8,6% | 19,0% |
| x- and y-coordinate | 58,0% | 6,5% | 16,9% |
| x- and y-coordinate and time/time$_{max}$ | 54,8% | 12,2% | 18,2% |

Table 4: Results of the comparison of the second and last day.

| **Dataset** | **TMR@FMR=0,1** | **TMR@FMR=0,01** | **EER** |
|---|---|---|---|
| x- and y-coordinate and time | 36,3% | 3,9% | 23,7% |
| x- and y-coordinate | 52,6% | 6,4% | 18,7% |
| x- and y-coordinate and time/time$_{max}$ | 45,6% | 11,1% | 20,3% |

48 individuals.

The classifier calculates a score matrix using the test set, containing the comparison scores of all pairs of individuals in the test set. The score matrix consists of two types of scores, namely the so-called genuine scores resulting from comparisons of individuals with themselves and the impostor scores resulting from comparing individuals with other individuals. These scores are used to plot a receiver operating characteristic (ROC)-curve which plots the true match rate (TMR) as a function of the false match rate (FMR). The closer the curve is to the upper left corner, the higher the overall accuracy of the classifier [Rev08]. To get closer to the upper left corner the numbers of PCA and LDA coefficients are optimised.

In addition to the dataset with the x-coordinate, y-coordinate and time, the analysis above is also done with two other datasets. One dataset only contains the x-coordinate and y-coordinate. The other dataset contains also the x-coordinate, y-coordinate and normalised time, which is time divided by the maximum time of that measurement (time/time$_{max}$).

To get a better view of how biometrics of the user's lock pattern changes with, ROC-curves were created using only the second and last measurement day. The first day is not used, because that was the first day the participants have drawn the pattern and could contain some large differences in the way of drawing. The last day should be day eight, but not every participant completed exactly eight measurement days. For that reason the last day in the ROC-curve is the last day the participant has drawn the pattern, this day varies from day 5 to day 9. In the test set, there were 26 participants who did measurements on the second day and day 5 or higher (2x day 9, 15x day 8, 4x day 7, 4x day 6 and 1x day 5). To create new ROC-curves containing only measurements of the second and last day, a new score matrix is created. This is done by extracting the scores of these days from the original score matrix.

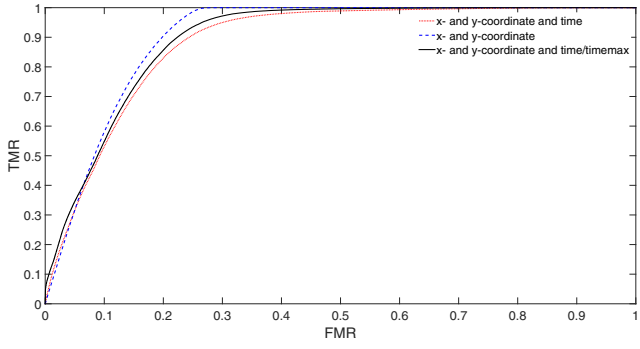


Figure 4: ROC-curves for different features. Dashed blue: x- and y-coordinate (PCA 50 and LDA 49); solid red: x- and y-coordinate and time (PCA 50 and LDA 49, solid black: x- and y-coordinate and time/time$_{max}$(PCA 7 and LDA 4).

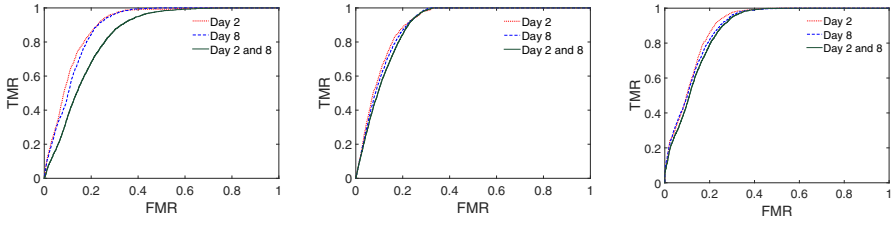


Figure 5: ROC-curves for different features across time. Left: x- and y-coordinate and time; centre: x- and y-coordinate; right: x- and y-coordinate and time/time$_{max}$.

## 3 Results

ROC-curves where created with the dataset containing the x-coordinate, y-coordinate and time. The deviation between different numbers of PCA and LDA coefficients was small. The best result was achieved using 50 for the PCA and 49 for the LDA (see Fig 4, red curve). For the ROC-curve with the dataset with the x-coordinate and y-coordinate the same PCA and LDA coefficients were the best choice (see Figure 4, dashed blue curve). Finally, the dataset with x-coordinate, y-coordinate and time/time$_{max}$ was used to create ROC-curves. In this case PCA 7 and LDA 4 yielded the best result (see Figure 4, black curve). These curves show the true match rate (TMR) as a function of the false match rate (FMR). It is assumed that the owner of the smartphone and the imposter who impersonate the user's biometrics always draw the correct pattern. Table 3 shows the chances that the owner of the smartphone can get access to his smartphone when the chances that an imposter can get access to the smartphone is 10% or 1%. The higher TMR, the more secure the lock pattern and the better the dataset. Next to that, the best description of the error rate, the equal error rate (EER) is given (see Table 3). The biometrics of the dataset with the lowest EER contains the least errors and are the most secure to use.

The three plots with the comparison of the second and last day (see Figure 5) are made to explore how users change the way they draw lock patterns over a course of time. The smaller the distance between the different lines, the smaller the changes in the way of drawing the lock pattern. The leftmost plot is created using the x-coordinate and y-coordinate and time and has a small deviation between the second and the last day and the curve of comparison of the second and last day has a larger deviation and is slightly more to the right. The centre plot is created using only the x-coordinate and y-coordinate has all three ROC-curves close to each other and they are more to the upper left corner than the curves of the first plot. Finally, the ROC-curves in the rightmost plot using the x-coordinate and y-coordinate and time/$\text{time}_{\text{max}}$ are also close to each other, but is less close to the upper left corner than the centre plot.

For the ROC-curves of the comparison of the second and last day the TMRs are given as well for a FMR of 10% and 1% for the three different datasets (see Table 4). Besides that, the EER is calculated for all three datasets (see Table 4). The biometrics used in the dataset with the highest TMR and lowest EER are the most secure over a course of time.

## 4 Discussion and conclusions

To collect a dataset a user study has been done with use of the application "Touch Signature". This application kept track of five of the user's biometrics: the location of the finger (x- and y-coordinate), the time to draw the pattern (in milliseconds), the pressure of the finger and the area touched by the finger. During this research it was concluded that the pressure and the area touched by the finger deviated too much to use for this research. The other three biometrics (x- and y-coordinate and time) were used in three different datasets to classify the measurements. The first dataset contains all three biometrics and the second only the x- and y-coordinate. Finally, the third dataset contains next, to the x-coordinate and y-coordinate, the normalized time which is: time/$\text{time}_{\text{max}}$.

The best dataset is determined by the height of the TMR when the FMR is 10% or 1% and the EER. The higher the TMR and the lower the EER, the more secure the lock pattern is. When a FMR of 10% is desirable the dataset using the x- and y-coordinate has the highest TMR, thus is the best dataset (see Table 3 and 4). The TMR for this dataset is 58,0% for all measurements together and 52,6% for the comparison of the second and last day. Thereafter the dataset using the x- and y-coordinate and time/$\text{time}_{\text{max}}$ is the best and at last the dataset using the x- and y-coordinate and time. This order is also the best for the EER, whereby the highest EER of 16,9% for all measurements together and 18,7% for the comparison of the second and last day using the x- and y-coordinate (see Table 3 and 4).

According to a FMR of 1%, the dataset using the x- and y-coordinate and time/$\text{time}_{\text{max}}$ is the best dataset with a FMR of 12,2% for all measurements and 11,1% for the comparison of the second and last day. In this case the dataset using the x- and y-coordinate is the second best dataset to use (see Tables 3 and 4).

In conclusion, the way users draw their pattern over a course of time changes the most using the dataset with the x- and y-coordinate and time. In other words the time in which

a user draws a pattern differs relatively more per drawing than the location of the finger. The normalized time gives a better result than just the time to draw a pattern. Still, the way users draw their lock pattern over a course of time changes the least using a lock pattern with the location of the finger as user's biometric. Thus, the lock pattern using the x- and y-coordinates can be used best. However, when a FMR of 1% is desired, the biometric time/$\text{time}_{\text{max}}$ should be added to the lock pattern application.

Finally, the less the user's biometrics changes, the higher the TMR and the lower the EER, with the consequence that the recognition performance of the lock pattern will be higher. Unfortunately, the TMR is still too low and the EER is still too high to give reliable results. In other words, an imposter can still access the smartphone easily when he knows the pattern, however it is made more difficult due the addition of the user's biometrics. Concluding, the lock pattern using user's biometrics can be used as an additional security, but provides no guarantee for a secure lock pattern.

## References


[AGM+10] Adam J Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M Smith. Smudge Attacks on Smartphone Touch Screens. *Proceedings of the 4th USENIX Conference on Offensive Technologies, WOOT'10*, 10:2, 2010.

[AW12] Julio Angulo and Erik Wästlund. Exploring Touch-Screen Biometrics for User Identification on Smart Phones. In *Privacy and Identity Management for Life*, volume 375 of *IFIP Advances in Information and Communication Technology*, page 139. 2012.

[JRP06] AK. Jain, A Ross, and S. Pankanti. Biometrics: a tool for information security. *Information Forensics and Security, IEEE Transactions on*, page 125, 2006.

[Rev08] Kenneth Revett. *Behavioral biometrics: a remote access approach*. John Wiley & Sons, 2008.

[SLS13] Muhammad Shahzad, Alex X. Liu, and Arjmand Samuel. Secure Unlocking of Mobile Touch Screen Devices by Simple Gestures: You Can See It but You Can Not Do It. In *Proceedings of the 19th Annual International Conference on Mobile Computing & Networking*, MobiCom '13, page 39, 2013.

[SVSD14] L. J. Spreeuwers, R. N. J. Veldhuis, S. Sultanali, and J. Diephuis. Fixed FAR Vote Fusion of regional Facial Classifiers. In C. Busch and A. Brömme, editors, *BIOSIG 2013: Proceedings of the 13th International Conference of the Biometrics Special Interest Group, Darmstadt, Germany*, Darmstadt, September 2014. Gesellschaft für Informatik.