Password-free Authentication for Smartphone Touchscreen Based on Finger Size Pattern

https://doi.org/10.3991/ijim.v14i19.17239

Yaser Ali Enaya, Mohammed Jawad Mohammed (✉),
Ghassan Abdulhussein Bilal
University of Technology, Baghdad, Iraq
mohammed.j.mohammed@uotechnology.edu.iq

Abstract—This study introduces a novel authentication methodology; it is based on pattern recognition of fingers size and pressure when users touch smartphone screen. By analyzing diagrams of these touches and applying data mining for the first time as an authentication technique, this paper presents three new approaches. First, an exact-range evaluation approach has been verified that size is more recognition consistency than pressure. Second, a pattern-range is a new technique reliance on size frequency position. At last, using a size-range has been facilitated the login. The association rules have been modified to work on finger touchscreen data files. To login, 94.1111% of 18 authorized users are succeeded and 98.9% of 20 unauthorized users are failed. Android device and Android studio are used. Size and pressure are normalized to 1; a training set is applied; the password is not considered.

Keywords—Data trace, support factor, confidence factor, training set, exact-range, size-range, pattern-range

1 Introduction

Authentication requirements are becoming a headache in the smart devices technology; this problem becomes more complicated because of the technology exponential development [1-2]. Focusing on smartphone, using password is inefficient due to the touchscreen limitation comparing to finger sizes, especially fat fingers [3]. As consequences, users are mostly leaning towards using 4-digit pin and reducing password length making smartphones more vulnerable than other devices [4]. In addition, smartphone is differed from other electronic devices by the numerous usages, reaching hundred times of daily interaction [5]. Therefore, users prefer a semi-blind touchscreen with intuitive use in order to not interrupt their main tasks [5]. One of the most interesting solution produced by Apple's and applied on iPhone is using fingerprint [6]. However, many users are unwilling to use fingerprint authentication due to the high cost of additional hardware and compromising fingerprint by saving its information in the smartphone memory [7]. This paper proposes a new direction that considers fingers' touchscreen information such as size and pressure as a gold mining

needed someone to dig it. Before this point, all researches dealt with this information as a black box. Therefore, they feed this information blindly to the machine learning without involving in observing the information [8]. Since smartphone sensors are electronic devices, a decent amount of information can be collected in a few seconds due to sensors' high speed. Therefore, this study deals with this information as a database because of the large amount of data and applied one of its tools, data mining, for the first time to our knowledge. Data mining can be defined as a number of processes to discover useful hidden patterns by finding relations between database attributes [9]. In this study, association rules that are one of data mining approaches are applied on finger size and pressure when touch smartphone screen. The popular example of association rules power is finding the relation between diapers and beers in super market database since often wives tell husbands to buy diapers when they go to shop beers and that gives an idea for managers to put diapers and beers in the same aisles [9]. The challenge that faces this work is that association rules are working on attributes in the same database and this study deals with multiple touches that every touch represents one database. Therefore, a modification on association rules to work with attributes in different databases has been made. By association rules assistance and analyzing finger size and pressure diagrams, a new pattern with strong user recognition is presented in this study. The method was applied on Android smartphones and IDE (Android studio) was used to build the code, in addition of enrolling 40 users. The result was promising, since it detects size pattern that is supporting authentication 98.9 %. The aim of this work is to facilitate using specific devices especially smartphones that users need to login many times a day by discarding the password without weakening the authentication through finding a powerful user recognition pattern. Our experiment was applied in laboratory environment; later work is making an Android app for the experiment.

2 Related Works

To the best of our knowledge, there is no literature dealt with information collected from the smartphones as database and analyzed by its tools. the most powerful and closest work to this research is Ref. [10] since they are using adaptive machine learning, such as neural network (NN) that is increasing the authentication efficiency through using training set. Ref. [11] is another study where they handled distinguishing between soft and hard finger pressure, based on users' features such as small fingers and speed. [12] proposes another powerful Android software development framework that uses OpenCV library for real-time face recognition.

3 Theoretical Work

In the past ten years, the smartphone password has become an increasingly important segment of the market [13]. Researches have focused on the relationship between flexibility, and efficiency of smartphone passwords depending on user's physical finger, but there have been little works exploring pattern of these fingers

such as pressure, size, etc. This paper is the first attempt exploring this field by trying to find out a pattern between finger's size and pressure and in order to more understand them, plotting data traces is applied. Because of large number of users that each one has multiple touches and every touch has multiple values of size and pressure needed to represent in one coordinate, a stochastic method, variance, is applied to convert them into one value. Variance equation is:

$$Variance = = \frac{1}{N}\sum_{i=1}^{N}(X_i - \mu)^2$$

Where

$$\mu = \frac{x1+x2+\cdots.xn}{n} \ldots (Mean)$$

N: Population Size [14].

So, for every user involved in this experiment, two separated plots, size and pressure plots, has been sketched. Every coordinate in the plot represents multiple finger sizes or pressures of one touch. Based on these plots, a pattern evaluation has been made depend on coordinates frequency. So, plot with higher frequencies means that multi touches of the same user have the same sizes or pressures indicating pattern recognition that is assessment as an Exact Evaluation. Vice versa, plot with low frequencies is assessment as a Range Evaluation. According to that, finger size indicates pattern behavior higher than finger pressure. Furthermore, to support the study case, size and pressure distribution of one touch has been plotted where size or pressure frequencies is taken in consider and again indicates the same results. Finger size is not solid enough to be used as a password; therefore, one of data mining techniques that is association rules is used in order to raise up password efficiency. Association rules have modified to work on the same finger size or pressure in two data sets, touches, instead of multiple attributes of one database. Association rules have two factors, support and confidence, that calculate the ratio of relation between attributes [9, 15], size or pressure in our case, according to the below modified formulas:

Support Factor (Sup.) = No. of finger size in data set1 matches the same finger sizes in data set2 / Total No. of the same finger sizes in data set1

Confidence Factor (Con.) = No. of finger size in data set1 matches the same finger sizes in data set2 / Total No. of data set1elements (sizes)

Above formulas are applied first on finger size or pressure separately of two touches of the same user in order to find a pattern. On the other hand, the same procedures are applied again, but on two touches that each one belongs to different user to insure the inconsistency. Next, the exact above steps are repeated, but on finger size and pressure combination. Again, finger size proves among finger pressure and size and pressure combination that it is the highest pattern recognition. All above experiments guide this research to focus on the finger size rather than pressure or pressure and size. In addition, the huge amount of information of these experiments help to analysis finger size which led to discover a new feature, pattern. From experiments, single touch has multiple finger sizes that have different frequencies because fingers need time to settle on the touchscreen and to lift up from it. So, finger size at settlement time is the actual finger size and anything else is noise. Base on that, pattern is the

time to reach the finger size settlement point which is different from user to another. In the light of that, an application has been designed according to the Figure 1 flow charts.

4 Methodology

There are many related works as mentioned before such as the most successful IPhone finger print [16], but this paper differentiates by looking for pattern in users' behavior when they touch smartphone screen. This paper is about studying the potential of a new technique over touch screen that it is able to detect finger size or pressure pattern endeavor to cast the password. Therefore, information is collected from users' fingers for this purpose. This information has many parameters that are collected by Android around every 17 ms, where size and pressure are normalized to one. The experiment shows that size and pressure are changing between the time of fingers landing on the touchscreen to the time of lifting them up with different frequencies. Users without instructions tend to be random in their way of touching smartphone by their nature [17]. This randomness makes touch sizes and pressures for the same user different. On the other hand, randomness odds make finger sizes and pressures of different users compatible [18].

Therefore, 40 users were involved in this experiment to solve this problem where the number of users is multiplied based on [19] to get more accurate results. Users were told to touch the smartphone screen in the same way as best as they could. They kept the Android for two days and tried to touch the screen for more than 100 times. From each user, data traces that each consists of over 100 touch instances in time order are collected. Each instance represents the information of a specific touch. In this experiment, the size and pressure are the main topic, so two data sets, one for the size and the other for the pressure, are extracted from the information of each touch instance. Three experiments are applied; first one is a comparison of size and pressure to find out which one has better pattern using plotting to more understanding their features and to ease the analysis. Second experiment is to apply association rules for the first time as an authentication tool. In addition, it supports experiment one results. Last one, using the analyses and the new tool of experiments one and two to figure out a pattern in order to design an application based on machine learning. Next, results show that finger size is a promising pattern feature while pressure fails. Finally, conclusions cover any data that hasn't mentioned before in the paper.

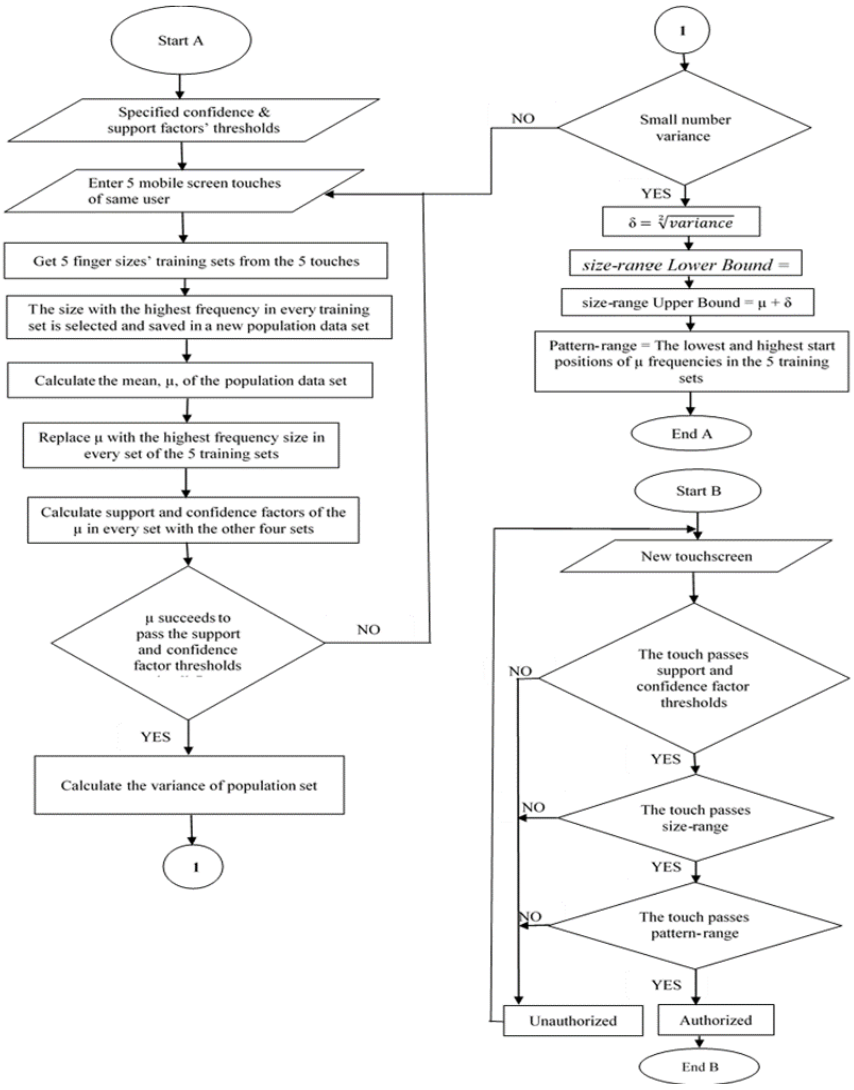

Fig. 1. A- Training set flowchart runs one time. B- Authorized flowcharts runs every time using the mobile

5 Experiments and Results

This research is partitioned to three experiments; each experiment related to others and each one leads to the next one. First experiment is to compare between finger size and pressure properties in order to find out their suitability with pattern recognition. Second, the data mining approach association rules is modified to be a pattern recognition tool, then to apply on finger size and pressure of different users. Third experi-

ment is adding a new pattern that is more related to human behavior to leverage success percentage.

5.1 Experiment 1

The purpose of this experiment is to collect data traces. and, plotting them which is the best way to discover patterns.

Variance: Information of three random users A, B and C were chosen as an example to explain the results of this experiment. For each finger touch, there are two sets, size and pressure data set. Each data set represents one coordinate on Figures 2, 3 and 4.

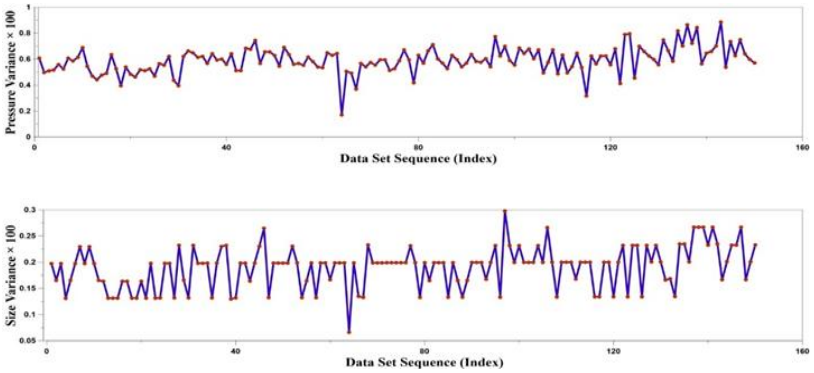

Fig. 2. Pressure and size variances of touches over time (user A)

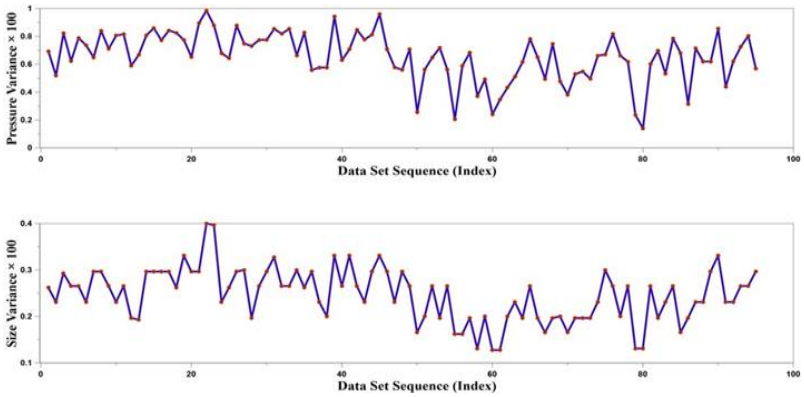

Fig. 3. Pressure and size variances of touches over time (user B)

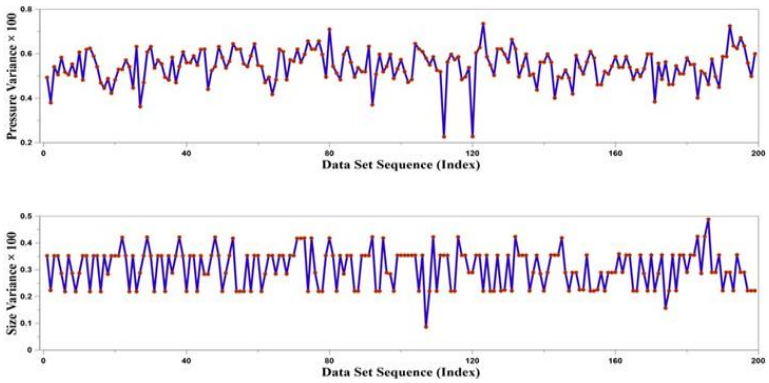

Fig. 4. Pressure and size variances of touches over time (user C)

In example 1, a pressure data set was selected randomly from more than 100 data sets that belong to user B's finger:

Pressure data set = {0.1666667:6, 0.3333336:5, 0.3:10, 0.4:4, 0.4333337:5, 0.3666667:12, 0.2666667:3}. Where, Pressure Data Set = {Finger Pressure Value: Frequency, …, P: F}. To get one coordinate in Figure 3 that represents all pressure values in the data set, the variance equation applied and the result is: Population size = 45, μ = 0.3251852 and Variance = 0.0059829.

Exact-range evaluation: This work applies an origin exact-range evaluation approach on diagrams, for example, size variance diagram of Figure 4 has four values with highest four frequencies as shown in Table1. Therefore, it can say that user C's finger size variance equal exactly (0.225374, 0.286227, 0.35, or 0.412372). On the other hand, it cannot say the same thing on pressure variance since its points in the diagram are scattering and have less frequency.

Thus, it can say that user C's finger pressure variance range is almost (0.38-0.66) since most points are incident in this range. Table 2 shows Figures 2, 3, and 4 evaluations using exact-range approach. The conclusion is that size is more organizing or less random than pressure. This is manifested in Figure 4, a little less in Figure 2 and even lesser in Figure 3.

Table 1. Size values and their frequencies from Figure 4.

Size	Frequency
0.225374	56
0.286227	37
0.35	76
0.412372	19

Table 2. Diagrams Evaluation of Figures 2, 3, and 4 Using Exact-Range Approach

Data Trace	Size	Pressure
A	Exact	Range
B	Exact to Range	Range
C	Exact	Range

However, Figure 4, even with its best result, has additional 3 random low frequency values and user B size variance is almost range evaluation indicating low accuracy.

Size and pressure distribution in one touch: For more analysis, diagrams are plotted for 3 touch instances that are selected randomly from over 500 touch instances of A as well as B and C data traces. As shown in Figure 5, size distributions in A, B, and C diagrams are more organizing than pressure distributions since they have fewer values with higher frequencies. As a consequence, we are going to focus on the size more than pressure since organizing converges a step towards pattern.

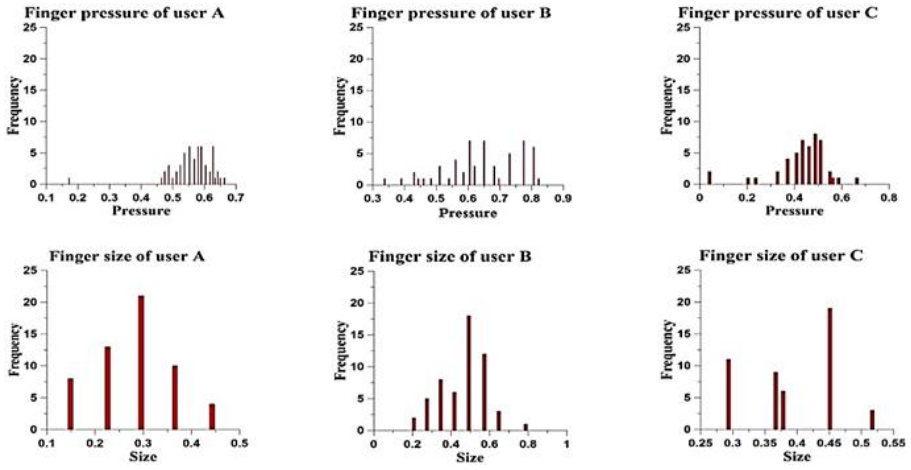

Fig. 5. Histograms of Single Pressure and Size Trace Instants of Users A, B and C Consequently

Despite of promising results, this experiment detected inconsistency problem of size and pressure when users try to login smartphone more than one time. In order to discover pattern recognition, data mining is applied in this work.

5.2 Experiment 2

In this experiment, a database technique, data mining, is used for the first time as an authentication tool. Data mining is a number of processes to discover useful hidden patterns in random data by finding relations between its attributes [9, 15]. In order to more understand user behaviours and find a unique pattern in fingers size and pressure, one of the data mining approaches was applied that is association rules.

Association rules: Modified association rules equations are applied on two sizes or two pressures of two touches coming from one user for the same finger index. Next, apply them again on the same finger index of two touches coming from two different users. The purpose is to be sure there is no consistency between touches to secure the user from others. Table3 is the results of applying association rules on two touches of the same user, User1.

Table 3. Comparing Two Touchscreens of the Same User (User1-User1)

Fingers	Finger Size Frequency	No. of Hits	Support Fact	Confidence Fact
Finger 1	15	11	0.7333	0.3793
Finger 2	8	7	0.875	0.2592
Finger 3	5	5	1	0.318919

In Table3 a specific size of finger index1 is appeared in data set1 15 times which is the frequency and the same size is appeared in data set2 11 times. Therefore, the number of size frequency in data set1 that is matching the same size in data set2 is 11. The support factor for the finger index1 in data set1 is 0.7333, which means that 73% of finger index1 frequency in data set1 has match with the same finger in data set2. The confidence factor for the same finger size is 0.3793 which means that 38% of total items in data set1 has match. Example 2 is an explanation in numbers.

In example 2, Data Sets 1 & 2 are size sets of finger index 1 from two touchscreens of the same user, USER1:

Data Set1 = {0.355557:4, 0.344444:6, 0.466666:9, 0.433333:6, 0.366666:3, 0.333333:1}.

Data Set2 = {0.322222:2, 0.344444:4, 0.333336:5, 0.466666:7, 0.3:6}.

There are two sizes, 0.344444 & 0.466666, from data Set1 have matches with data Set2.

In Data Set1, total 0344444 frequencies are 6 + total 0.466666 frequency is 9 = 15, In Data Set2: total 0344444 frequencies are 4 + total 0.466666 frequency is 7 = 11. So, total frequency matches are 11 (the less frequency between the two sets). So, support factor = number of frequency matching btw. set1 & set2 / Total frequency number in set1 = 11/15 = 0.7333. Confidence factor = number of frequency matching btw. set1 & set2 / total number of data set1 items = 11/29 = 0.3793. Table4 is representing the exact information of Table 3, but the two touches are belonging to two different users, USER1-USER2.

Table 4. Comparing Two Touchscreens of Different Users (User1-User2)

Fingers	Finger SizeFrequency	No. of Hits	Support Fact	Confidence Fact
Finger 1	5	5	1	0.2111
Finger 2	9	8	0.8999	0.2424
Finger 3	3	3	1	0.1304

The purpose of Table4 is to exam if the idea is fulfilled the second condition of pattern recognition that is no consistency between different users' touches, or not. On the contrary, Table3 is to exam if the idea is fulfilled the first condition of pattern recognition that demonstrates consistency between two touches of the same user. Table3 indicates promising results, which are notable in confidence factor column where all its values are larger than its values of the same column in Table4, but not sufficient for authentication purposes especially the results are very close in finger index2. Support factor job is to find matching between two sets. Looking at Table3 and Table4, surprisingly support factor of USER1-USER2 is higher than support

factor of USER1-USER1, but actually it is a good sign; Example3 will explain this contradiction.

In example 3, Suppose for the same size, the frequencies of USER1& USER2 are 15 and 5 consequently. Therefore, USER2 support factor = 5/5=1, so all size frequencies of USER2 find matches with size frequencies of USER1, since USER2 size frequency is the lower one. By reversing the procedures, USER1 support factor = 5/15 = 0.33333 since total size frequency number of USER2 equals 5 that only 5 matches are found out of 15. Example 3 proves that support factor is not sufficient without confidence factor and they are integrating each other. So, association rules work as two steps, first, finding matches that is support factor task. Second, find out if the matches are worthy that is confidence factor task. Confidence factor task is deciding if the result of support factor represents a phenomenon in the data set population, or not.

In example 4, Suppose data set1 length = 20 and finger size frequency = 1 in data set1. Moreover, the same size has frequency = 15 in data set2. Then the support factor = 1/1 = 1. This is a complete score in spite of that the size frequency is trivial in data set1, but support factor failed to discover it. Therefore, association rules calculate confidence factor to cover this defect: confidence factor = 1/20 = 0.05 which is lower than any threshold. Next section is to examine the pressure by association rules.

Using association rules with both size and pressure: In Tables 5 and 6, matching condition is of fingers size and pressure at the same time rather than just size. Also, if the finger matches the same finger in different events just in size or pressure, it will not consider. This approach is covered under Weka tool. The result was unpromising because the matching odds of two values, size and pressure, are lower than matching odds of one value such as just size or pressure.

Table 5. Comparing Finger Size and Pressure Between Two Touchscreens of the Same User (User1-User1)

Fingers	Finger Size Frequency	No. of Hits	Support Fact	Confidence Fact
Finger 1	19	1	0.0526316	0.02
Finger 2	17	1	0.0588235	0.02
Finger 3	15	13	0.866667	0.26

Table 6. Comparing Finger Size and Pressure Between Two Touchscreens of the Different Users (User1-User2))

Fingers	Finger Size Frequency	No. of Hits	Support Fact	Confidence Fact
Finger 1	17	1	0.0588235	0.0238095
Finger 2	14	0	0	0
Finger 3	1	4	0.333333	0.0952381

5.3 Experiment 3

This experiment applies a new idea to find a pattern.

A new feature (pattern): From Figure 6, Time vs Size Frequency, finger size frequency increases at the beginning and decreases at the end while it is set in the middle. This pattern is because in an idol touch, the user needs time to settle fingers

and during that, size and pressure are changing. Meanwhile, the Android keeps reading frequencies every 17 ms when the same size or pressure stay still. This process will be reversed when user lifts fingers up and it starts from the settlement point down to lift up all fingers. This is the reason that different sizes and pressures with different frequencies are read in one touch. It is noticeable that there is delay to reach the settlement point, which is the highest size frequency at the same time. This time delay is different from user to another and can be used as a pattern that recognizes the user. The settlement point does not necessarily represent largest size or pressure value; it represents the highest frequency of specific size or pressure among all sizes or pressures in one touch. So, all size or pressure values before and after settlement point are random. The advantage of time delay pattern is that even if there are two users have the same fingers' sizes or pressures, they will reach the settlement point at different times.

Steps of application: The system was applied on one finger in order to evaluate the technique strength, but it can be expanded. Pattern experiment processes are listed below:

1. Specifying a threshold for confidence factor. After analysing the data of 40 users, the practical threshold is found to be 0.3. This threshold is very reasonable considering people randomized nature. In other words, user settles finger 30% of whole time of touch verses 70% noise before and after the settlement. In addition, just 5% of unauthorized users passed this threshold.
2. Specifying a threshold for support factor. About 97.5% of authorized users and 30% unauthorized users passed the 70% threshold which makes it acceptable. Support factor task is to find matches between two touches and often it happens even with two different users because of their randomized nature. However, confidence factor task is to decide if this matching is just noise or genuine.
3. The training set is necessary for comparing in any machine learning. Therefore, the training set of this experiment includes 5 data sets, 5 touches, for each user. Below is an example of USER25's training sets:

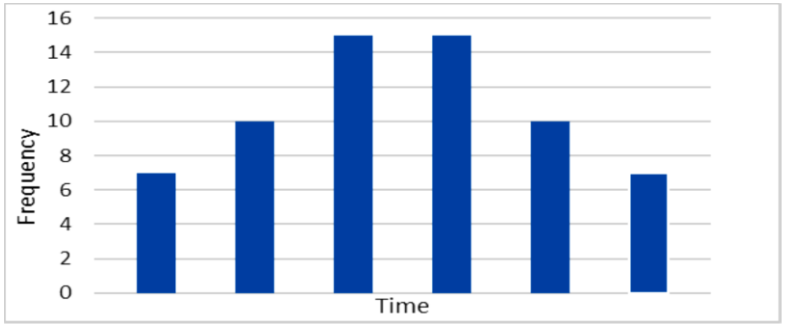

Fig. 6. Time VS Frequencies of finger sizes for one touch

Set 1 = {0.4666667:9, 0.5:11, 0.53333337:7}
Set 2 = {0.4666667:2, 0.40000004:3, 0.3666667:2, 0.43333337:3, 0.4666667:3, 0.48333333:12, 0.4666667:4}
Set 3 = {0.5:2, 0.53333337:1, 0.5666667:4, 0.6:2, 0.53333337:1, 0.5666667:1, 0.52222228:15, 0.4666667:2}
Set 4 = {0.43333337:9, 0.5666667:1, 0.53333337:2, 0.47777779:11, 0.4666667:1, 0.43333337:5, 0.40000004:3}
Set 5 = {0.40000004:7, 0.4333337:2, 0.5:14, 0.4666667:4}

In order to find a pattern that recognizes USER25, the size with the highest frequency in every set is selected and saved in a new population data set. Therefore, sizes 0.5, 0.48333333, 0.52222228, 0.47777779 and 0.5 have been selected from data sets 1, 2, 3, 4 and 5 consequently. Thus, the new data set is {0.5:11, 0.48333333:12, 0.52222228:15, 0.47777779:11, 0.5:14}. Next, finding the mean, μ, of the new data set and replaced it with all its sizes in their original sets to facilitate association rules calculation. μ = 0.49823634. So, the new 5 training data sets after replacing their highest frequency sizes with the μ = 0.49823634 is as below:

Set1 = {0.4666667:9, 0.49823634:11, 0.53333337:7}
Set2 = {0.4666667:2, 0.40000004:3, 0.3666667:2, 0.43333337:3, 0.4666667:3, 0.49823634:12, 0.4666667:4}
Set3 = {0.5:2, 0.53333337:1, 0.5666667:4, 0.6:2, 0.53333337:1, 0.5666667:1, 0.49823634:15, 0.4666667:2}
Set4 = {0.43333337:9, 0.5666667:1, 0.53333337:2, 0.49823634:11, 0.4666667:1, 0.43333337:5, 0.40000004:3}
Set5 = {0.40000004:7, 0.4333337:2, 0.49823634:14, 0.4666667:4}

Next step is calculating support and confidence factors of the μ in every set with the other four sets as shown in Table7. From Table7, Size 0.49823634, μ, succeeded to pass the support and confidence factor thresholds in all five training sets. Consequently, the training set gets the approval that it represents USER25 finger size.

Table 7. Support and Confidence Factors of the μ = 0.49823634 in every set

Size 0.49823634	**Set1**		**Set2**		**Set3**		**Set4**		**Set5**	
	Sup.	***Con.***	***Sup.***	***Con.***	***Sup.***	***Con.***	***Sup.***	***Con.***	***Sup.***	***Con.***
Set1	-	-	1	0.4074	1	0.4074	1	0.4074	1	0.4074
Set2	0.9166	0.3793	-	-	1	0.4137	0.9166	0.3793	1	0.4137
Set3	0.7333	0.3928	0.8	0.4285	-	-	0.7333	0.3928	0.9333	0.5
Set4	1	0.3437	1	0.3437	1	0.3437	-	-	0.5	0.3437
set5	0.7857	0.44	0.8571	0.48	1	0.56	0.7857	0.44	-	-

Next step is to find the variance of the highest frequency set for two purposes. First, since training set is coming from five touches of the same user, then it reflects the quality of the user touches that if the user follows the instructions or not. Therefore, if the variance is a small number, the training set quality is high, otherwise it is low. In other words, if the highest frequency set elements are closed, the variance number is a small and vice versa. Second, using variance to calculate the deviation, δ,

in order to use it for specifying the lower and upper bounds of size-range. So, the variance of the highest frequency data set:

variance = 0.000536018 … USER25' training set quality is very high

$\delta = \sqrt[2]{variance}$

$\delta = \sqrt[2]{0.000536018}$ = 0.01592488

Lower Bound = μ - δ

= 0.49823634 - 0.01592488 = 0.48231146

Upper Bound = μ + δ

= 0.49823634 + 0.01592488 = 0.51416122 [14].

Therefore, the size-range of USER25's finger is = (upper bound-lower bound) = (0.48231146 - 0.51416122) and for any new touch, its size value with highest frequency should be incident in this range, otherwise the touch is failed. To determine the pattern range, the lowest and highest start positions of size 0.48923634 frequencies in the 5 data sets are taken. From Table8, the pattern-range is (10-14).

Table 8. Start positions of size 0.48923634 frequency in all five sets

Set	position
Set1	10
Set2	14
Set3	12
Set4	13
Set5	10

1. The task of the training set is finishing after finding pattern-range, the highest frequency size, and the size-range; therefore, training set is discarded after that. So, the results from USER25's training set are Highest size frequency = 15, size-range = 0.48231146 - 0.51416122 and Pattern-range = 10-14. In example 5, Suppose both new two touches, setA (item number (length) = 26) and setB have equal size = 0.5 with frequencies 1 and 45 consequently. From the training set of USER25, size 0.5 is incident in the size-range (0.48231146 - 0.51416122), setA support factor $\frac{1}{1}$ = 1, and setA confidence factor $\frac{1}{26}$ = 0.0384 failed to pass the threshold 0.3. Therefore, choosing frequency 15 does not affect discovering noise. On the other hand, setB support factor = $\frac{15}{45}$ = 0.3333 since the training set size frequency of USER25 is equal 15. Again, the noise is discovered since the support factor is failed to pass the threshold, 0.7. Conclusion, the perfect frequency from training set is the highest one since it leverages the probability of accepting high frequency without impacting to discover noise, too high or too low frequency.
2. Now, any new finger touch should be passing the size-range, two thresholds and the start position of the highest size frequency should be incident in the pattern range. Below are 3 examples of rejecting touches. In example 6, USER25 new touch's set25 = {0.43333337:7, 0.4666667:6, 0.48666666:23, 0.4666667:2, 0.43333337:4}, size 0.48666666 with the highest frequency = 23 is incident in the size-range (0.48231146 - 0.51416122). Start frequency position of size 0.48666666 = 14 is incident in pattern-range (10-14). Confidence factor = $\frac{15}{42}$ = 0.3571 passes

the threshold 0.3. Support factor = $\frac{15}{23}$ = 0.6521 fails to pass the threshold 0.7. So, even though the training set belongs to the same user, USER25, the user could not login because the user kept the finger for long time on the touchscreen and did not use a regular touch leading to too high frequency, 23. In example 7, USER10 touch's set10 = {0.4666667:2, 0.5:10, 0.53333336:8, 0.5666667:10, 0.4666667:3}, both sizes 0.5 and 0.5666667 have highest frequencies = 10. Size 0.5 passes USER25's size-range while size 0.5666667 fails. Start position of size 0.5 frequency = 3 fails passing USER25's pattern-range (10-14). Confidence factor = $\frac{10}{30}$ = 0.3333 passes the 0.3 threshold. Support factor = $\frac{10}{10}$ = 1 passes the 0.7 threshold.

In example 8, USER36 touch's set36 = {0.20000006:5, 043333337:5, 0.3666667:1, 0.43333337:2, 0.51222228:9, 0.4666667:5, 0.36666667:7, 0.5:9, 0.23333336:2}, both sizes 0.51222228 and 0.5 with highest frequencies = 9 pass USER25's size-range. Start position of size 0.512222228 frequency = 14 passes USER25's pattern-range (10-14) while start position of size 0.5 frequency = 35 fails. For size 0.512222228, confidence factor = $\frac{9}{45}$ = 0.2 does not pass the 0.3 threshold; support factor = $\frac{9}{9}$ = 1 passes the 0.7 threshold. For size 0.5, confidence factor = $\frac{9}{45}$ = 0.2 does not pass the 0.3 threshold; support factor = $\frac{9}{9}$ = 1 passes the 0.7 threshold. The results are too hard to break the two factors with size-range and pattern-range supporting. In addition, size-range gives higher login tolerant than exact size.

Success percentage: In this work, two users' success percentages were 0% and 45% consequently; this is because of not following the instructions since their training sets were inaccurate, which are the base of the system. one user lifted up one of fingers and put it back during the training set time, while the other user thought that it should touch the screen in irregular manner. To avoid such problems, users must follow simple instructions as any other system does, as shown below:

1. User touches should be stable for at least 2-3 seconds, so the system can recognize the actual finger size and pressure from the noise; otherwise, the touch is only noise.
2. The system is looking for a pattern in the period between the finger landing and lifting up time and any interrupting such as lifting fingers up and putting them back during this process leads to lose the pattern.
3. Users should touch the screen in their regular way since the system is testing different touches, training set, for the same user to get the pattern.
4. After excluding information of above two users, results showed 94.1111% of 18 authorized users successfully login and 98.9% of 20 unauthorized users failed to login. 1.1% of total times unauthorized users enabled to break the system and this is back to probability and system defect. This problem will be conducted by involving pressure.

6 Conclusion

The following conclusions can be drawn from this work:

1. Authentication based on size or pressure is highly randomized and very weak due to the multi values in a single touch which rises up correspondence odds of different users.
2. Without supporting pattern-range, using finger size-range is minimizing the authentication efficiency. While exact finger size is maximizing authentication efficiency since it is only one number rather than multi numbers such as size-range leading to reduce matching probability, though it is less toleration.
3. Involving size frequency positions in pattern-range technique minimize randomness by about 90%. Therefore, pattern-range changes authentication based on size from randomness to organizing.
4. Data mining can work out of classic database field to be used as a part of machine learning.
5. Intruders' finger size frequencies are always lower than authorized ones which oriented this study towards pattern recognition.

7 Future Work

Future work is involving pressure hoping to increase efficiency [20]. However, pressure is not the only way since it can utilize other works such as adding recognition to different fingers or parts of fingers allowing them to be mapped to different authentication functions [21, 22]; or adding a new concept called finger-aware interaction system which enables to recognize fingers' touches on whole smartphone's surface [23].

8 References

[1] Hosam El-Sofany, A Novel Model for Securing Mobile-based Systems against DDoS Attacks in Cloud Computing Environment, International Journal of Interactive Mobile Technologies (iJIM) vol 13 No 1, 2019. https://doi.org/10.3991/ijim.v13i01.9900

[2] Amir H. Alavi, An Overview of Smartphone Technology for Citizen-Centered, Real-time and Scalable Civil Infrastructure Monitoring, Future Generation Computer Systems Journal, 93 pp. 651-672, 2019. https://doi.org/10.1016/j.future.2018.10.059

[3] Chun Yu, HandSee: Enabling Full Hand Interaction on Smartphone with Front Camera-based Stereo Vision. CHI Conference on Human Factors in Computing Systems, p. 705. ACM. 2019. https://doi.org/10.1145/3290605.3300935

[4] Noman Ranak, Press touch code: A finger press-based screen size independent authentication scheme for smart devices. https://www.doi.org/10.1371/journal.pone.0186940. October2017. https://doi.org/10.1371/journal.pone.0186940

[5] Ashley Colley, Extending Mobile Touchscreen Interaction. Academic dissertation, Art and Design at the University of Lapland. June 2017.

[6] Choonsung Nam, Force-touch measurement methodology based on user experience. International Journal of Distributed Sensor Networks Vol. 14(4). DOI: 10.1177/1550147718767794. journals.sagepub.com/home/dsn. 2018.
[7] Yunpeng Song, Multi-touch authentication using hand geometry and behavioural information. IEEE Symposium on Security and Privacy (SP), pp. 357-372. May 2017. https://doi.org/10.1109/sp.2017.54
[8] Shuo Gao, High Three-Dimensional Detection Accuracy in Piezoelectric-Based Touch Panel in Interactive Displays by Optimized Artificial Neural Networks. Sensors, 19(4):753. Jan 2019. https://doi.org/10.3390/s19040753
[9] Yaser Ali, Genetic Algorithm for Attribute-Oriented Induction Mining by Using Association Rules as a Fitness Function. Dissertation of Master of Science, University of Technology, Iraq-Baghdad, 2004.
[10] Sven Mayer, Estimating the Finger Orientation on Capacitive Touchscreens Using Convolutional Neural Networks. ACM International Conference on Interactive Surfaces and Spaces, pp. 220-229. ACM. 2017. https://doi.org/10.1145/3132272.3134130
[11] Toan Nguyen, Kid on the phone! Toward automatic detection of children on mobile devices. Computers & Security, 84, pp.334-348. 2019. https://doi.org/10.1016/j.cose.2019.04.001
[12] Laxmisha Rai, Software Development Framework for Real-Time Face Detection and Recognition in Mobile Devices, International Journal of Interactive Mobile Technologies (iJIM) vol 14 No 4, 2020. https://doi.org/10.3991/ijim.v14i04.12077
[13] Satwinderjit Singh, New Wave in Mobile Commerce Adoption via Mobile Applications in Malaysian Market: Investigating the Relationship Between Consumer Acceptance, Trust, and Self Efficacy, International Journal of Interactive Mobile Technologies (iJIM) vol 12 No 7, 2018. https://doi.org/10.3991/ijim.v12i7.8964
[14] Uri Bram, Thinking Statistically. Book, ISBN-10: 0995529523 ISBN-13: 9780995529526, Publisher: Capara Books, 2017-07-07.
[15] Dhamea A, Deep image mining for convolution neural network. Indonesian Journal of Electrical Engineering and Computer Science. http://doi.org/10.11591/ijeecs.v20.i12020.
[16] Philipp Markert, This PIN Can Be Easily Guessed: Analysing the Security of Smartphone Unlock PINs, IEEE Symposium on Security and Privacy (SP), 2020. https://doi.org/10.1109/sp40000.2020.00100
[17] Dimitrios Iakovakis, Touchscreen typing-pattern analysis for detecting fine motor skills decline in early-stage Parkinson's disease. Scientific reports 16:8(1): pp. 7663. May 2018. https://doi.org/10.1038/s41598-018-25999-0
[18] Siao Toh, The associations of mobile touch screen device use with musculoskeletal symptoms and exposures: A systematic review. PloS one, 7;12(8): e0181220. Aug 2017. https://doi.org/10.1371/journal.pone.0181220
[19] Eunyong Cheon, Gesture Authentication for Smartphones: Evaluation of Gesture Password Selection Policies, IEE Computer Society, Volume: 1, Pages: 249-267, 2020. https://doi.org/10.1109/sp40000.2020.00034
[20] Paul Strohmeier, Optimizing Pressure Matrices: Interdigitation and Interpolation Methods for Continuous Position Input. In Proceedings of the Thirteenth International Conference on Tangible, Embedded, and Embodied Interaction, pp. 117-126. ACM, 2019. https://doi.org/10.1145/3294109.3295638
[21] Ashley Colley, Exploring finger specific touch screen interaction for mobile phone user interfaces. In Proceedings of the 26th Australian Computer-Human Interaction Conference on Designing Futures: The Future of Design. pp. 539-548. ACM. December 2014. https://doi.org/10.1145/2686612.2686699

[22] Huy Le, PalmTouch: Using the Palm as an Additional Input Modality on Commodity Smartphones. CHI Conference on Human Factors in Computing Systems, p. 360. ACM, 2018. https://doi.org/10.1145/3173574.3173934

[23] Huy Le, InfiniTouch: Finger-Aware Interaction on Fully Touch Sensitive Smartphones. In The 31st Annual ACM Symposium on User Interface Software and Technology, pp. 779-792. ACM. October 2018. https://doi.org/10.1145/3242587.3242605

9 Authors

Yaser Ali Enaya is a lecturer at University of Technology, Baghdad, Iraq (UOT) where he taught subjects like network, processor, computer architecture, expert system and security related subjects. He received his B.Sc, M.Sc, (Computer Science) from UOT. He is active in Network Research. He also does Secure Coding, Android, data mining, and multi objective. He loves gadgets and enjoys exploring new things related to security.

Mohammed Jawad Mohammed is Associated Editor in International Journal of Advance Control and Automation System (IJACAS). Currently, he is Assist. Prof. Dr. in University of Technology in Iraq and interested by Electromechanical Devices and Instrumentation, Actuators and Sensors, System Identification and Dynamic Modelling, in addition to Traditional and Intelligent Control and optimization Techniques.

Article submitted 2020-07-23. Resubmitted 2020-09-03. Final acceptance 2020-09-03. Final version published as submitted by the authors.