A SECURE AUTHENTICATION SCHEME USING LOCIMETRIC AND PRESS TOUCH CODE TECHNIQUES

NOOR ELYA AFIQAH BINTI CHE NORDIN

Bachelor Of Computer Science (Software Engineering) With Honours

UNIVERSITI MALAYSIA PAHANG

UNIVERSITI MALAYSIA PAHANG

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name	: NOOR ELYA AFIQAH BINTI CHE NORDIN
Date of Birth	: 9 JUN 1996
Title	: A SECURE AUTHENTICATION SCHEME USING LOCIMETRIC AND PRESS TOUCH CODE AND TECHNIQUES
Academic Session	: SEMESTER I 18/19

I declare that this thesis is classified as:

□ CONFIDENTIAL	(Contains confidential information under the Official Secret Act 1997)*
□ RESTRICTED	(Contains restricted information as specified by the organization where research was done)*
☑ OPEN ACCESS	I agree that my thesis to be published as online open access (Full Text)

I acknowledge that Universiti Malaysia Pahang reserves the following rights:

1. The Thesis is the Property of Universiti Malaysia Pahang
2. The Library of Universiti Malaysia Pahang has the right to make copies of the thesis for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by:

_______________________ (Student's Signature)

_______________________ (Supervisor's Signature)

____
960609-03-5026
Date: 10 January 2019

____
DR. MD SAIFUL AZAD
Date: 10 January 2019

NOTE : * If the thesis is CONFIDENTIAL or RESTRICTED, please attach a thesis declaration letter.

THESIS DECLARATION LETTER (OPTIONAL)

Librarian,
Perpustakaan Universiti Malaysia Pahang,
Universiti Malaysia Pahang,
Lebuhraya Tun Razak,
26300, Gambang, Kuantan.

Dear Sir,

CLASSIFICATION OF THESIS AS RESTRICTED

Please be informed that the following thesis is classified as RESTRICTED for a period of three (3) years from the date of this letter. The reasons for this classification are as listed below.

Author's Name
Thesis Title

Reasons (i)

(ii)

(iii)

Thank you.

Yours faithfully,

____
(Supervisor's Signature)

Date:

Stamp:

Note: This letter should be written by the supervisor, addressed to the Librarian, *Perpustakaan Universiti Malaysia Pahang* with its copy attached to the thesis.

Universiti
Malaysia
PAHANG
Engineering • Technology • Creativity

SUPERVISOR'S DECLARATION

I hereby declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Bachelor of Computer Science in Software Engineering with Honours.

____

(Supervisor's Signature)

Full Name : DR. MD SAIFUL AZAD

Position : SENIOR LECTURER

Date : 10 JANUARY 2019

UMP Universiti Malaysia PAHANG
Engineering • Technology • Creativity

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

____

(Student's Signature)

Full Name : NOOR ELYA AFIQAH BINTI CHE NORDIN

ID Number : CB15067

Date : 10 JANUARY 2019

A SECURE AUTHENTICATION SCHEME USING LOCIMETRIC AND PRESS TOUCH CODE TECHNIQUES

NOOR ELYA AFIQAH BINTI CHE NORDIN

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Bachelor of Computer Science (Software Engineering) with Honours

Faculty of Computer Science & Software Engineering
UNIVERSITI MALAYSIA PAHANG

JANUARY 2019

ACKNOWLEDGEMENTS

First of all, I would like to take this opportunity to dedicate my thankfulness to those persons who have kept on giving me support, advices, knowledge, understanding and contribution towards the successful in completing of this Bachelor Degree Project.

Besides, I would like to express my sincere gratitude and appreciation to my supervisor, Dr. Md Saiful Azad for encouragement, guidance, advices, suggestion and motivation during completing this research.

Furthermore, I would also like to thank to Ms. Nur Nadhirah Binti Ab Rasul for her guidance and care.

My sincere appreciation extends to all my undergraduate friends, especially member of batch 2015-2019 who have helped me and shared brilliant ideas throughout the whole year.

Last but not least, I would like to express my sincerest gratitude and deepest thankfulness to my parent Che Nordin Bin Yusoff and Rozzita Binti Yaakob for their love, support and encouragement that they had given to me.

ABSTRAK

Kata laluan digunakan untuk mengawal akses hampir pada semua peralatan digital dan pengkomputeran. Umumnya, kata laluan terdiri daripada abjad atau beberapa huruf dan nombor yang digunakan untuk mengesahkan identiti pengguna untuk mendapatkan akses. Kata laluan yang sedia ada mempunyai beberapa kelemahan seperti serangan kamus, serangan tompokan dan melayari bahu. Oleh kerana pengguna mempunyai kebimbangan yang rendah pada pengesahan pengguna, skema pengesahan menggunakan grafik yang berasaskan Android, dicadangkan dalam projek ini untuk menyelesaikan masalah tersebut. Locimetrik dan peta Malaysia akan digunakan bersama dengan Press Touch Code.

Terdapat banyak teknik yang telah dicadangkan untuk mengatasi masalah tersebut. Untuk kajian ini, kami menggabungkan teknik Locimetric dan Press Touch Code untuk membuat skim pengesahan yang baru supaya lebih selamat. Tujuan penyelidikan ini adalah untuk merekabentuk skim pengesahan hibrid yang selamat menggunakan dua teknik yang disebutkan di atas yang bergantung kepada saiz resolusi skrin dan menguji keberkesanan skim pengesahan yang dicadangkan pada sistem pengendalian berasaskan Android.

Berdasarkan kajian sebelum ini, kami akan membincangkan lebih banyak maklumat tentang skema pengesahan dan konsep Locimetric dan Press Touch Code. Beberapa bahagian dari kaedah Passpoint Locimetric bersama dengan Press Touch Code dan konsep grid akan digunakan dalam penyelidikan ini. Projek ini terdiri daripada perkakasan dan perisian.

ABSTRACT

A password is one of the most used access control procedures applied in virtually all digital and computing appliances. Generally, a password is a word or a string of characters used for user authentication to prove identity or access approval to gain access to a resource, which is to be kept secret from those not allowed access. The current existing password has some drawbacks such as smudge attack and shoulder surfing attack. Due to lower concern on user authentication, an Android based graphical authentication scheme is proposed in this research to solve the problem. Locimetric and the Malaysia map will be utilized in conjunction with the Press Touch Code.

There are many techniques that have been proposed to overcome those limitations. For this research, we combine the Locimetric and Press Touch Code techniques to make the newly proposed authentication scheme is more secure. The purpose of this research is to design a secure hybrid authentication scheme using the two techniques mentioned above which is dependent to screen resolution size and test the effectiveness of the proposed authentication scheme on Android based operating system.

From the literature review, we will discuss more details on the authentication scheme and the concept of Locimetric and Press Touch Code. Some part of the Passpoint Locimetric method together with the Press Touch Code and grid concept will be utilize in this research. This research consists of hardwares and softwares.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

PTFA	Press Touch Finding Algorithm

LIST OF ABBREVIATIONS

PTFA	Press Touch Finding Algorithm

CHAPTER 1

INTRODUCTION

1.1 Background of Study

A password or authentication scheme adds a big measure of security and convenience to the users. A password is used to restrict access to a system, application or service to only those users who are authorized to use it. With the rapid development of wireless technology, passwords are a vital component of system security, which usually controlled by the small size pocket computer which is the smartphones.

Authentication is defined as the process of determining someone or something as they are declared to be (Margaret Rouse, 2015). The process involves in comparing the data saved in the database of authorized user information in the authentication server. If the identity is verified, the process of authentication is deemed complete and the user gets access to the system.

The existing passwords have some limitations. Text-based password is a system where memorability will affect the security of passwords. Most of the users tend to choose weak texts as passwords to make it easy for them to remember. A weak password is easy to remember, but giving lower or no security since the password are easy to guess and break. Besides, the voice recognition and face recognition has its own drawback which is those data is easy to get by forgery the voice, data or holding up a photo of authenticated user to break the door security system. The fingerprint does not preferable since some people do not like keeping their fingerprints and facial images in a file that can be accessed by others (Jing Teng et al., 2010).

1.2 Problem Statement

The most common problem that faced by the users is memorability. Most of the users tend to choose weak texts as passwords to make it easy for them to remember. A weak password is easy to remember, but giving lower or no security since they are easy to guess and break.

In addition, most of the password scheme that available today has a higher risk to shoulder surfing. This can be done by spying over the victim's shoulder to obtain information such as personal identification password and numbers. Thus, the attackers are able to unlock and access the victim smartphone.

Besides, alike the pattern based password, the oily residues from fingers sliding across the touch-screen surface. This smudge are then analyzed using standard computers running photo-editing software causing the attackers to easily break the password.

Therefore, in this research, a new hybrid authentication scheme is proposed which combines the Locimetric scheme along with Press Touch Code (Ranak et al., 2017). The advantage of this scheme is that it offers an authentication scheme that is screen resolution size dependent. Thereby, our proposed graphical password will provide a higher degree of security than the existing authentication scheme.

Table 1.1 : Problem statement summarization

Problem	Description	Effect
Low memorability	Users tend to choose weak texts as passwords to make it easy for them to remember	Weak password is easy to remember but giving lower or no security since they are easy to guess and break
Shoulder surfing attack	Spying over the victim's shoulder to obtain information such as personal identification numbers and password.	Attackers are able to unlock and access the victim's smartphone
Smudge attack	The oily residues from fingers sliding across the touch-screen surface.	This smudge are then analyzed using standard computers running photo-editing software causing the attackers to easily break the password.

1.3 Aim and Objectives

The goal of this research is to develop an Android mobile application for a secure hybrid authentication scheme. To attain this goal, following objectives is necessary to be acquired:

i. To design a secure hybrid authentication scheme using the Locimetric graphical password and Press Touch Code.
ii. To implement the authentication scheme on Android based OS.
iii. To test the effectiveness of the proposed authentication scheme.

1.4 Scope

The scope of this research is as follows:

i. The study focus on authentication scheme for smartphone security.
ii. The authentication scheme is only applicable and applied on Android smartphones.
iii. The authentication scheme is a combination of pressure intensity, grid and Locimetric graphical password.
iv. The authentication scheme is a screen resolution size dependent.

1.5 Significance

The significance of the research is as follows:

i. Ability to tap at a point of multiple time without lift up the finger. .
ii. The authentication scheme fit with the screen resolution size.

1.6 Structure of Thesis

This thesis consists of five chapters. Chapter 1 will be discussed in the introduction to the research, objective and goal of developing this hybrid authentication scheme, problem statement, scope of this research and the significance.

Recent work on concept and theory involve is discussed in the literature review, Chapter 2. This part is going to discuss and differentiate the method used for authentication. Besides, this chapter also will be discussing on which technique is more suitable to be used in developing this Android application.

The methodology will be discussed in Chapter 3. The purpose of this chapter is to present the software and hardware that will be used, as well as to introduce the strategy and the techniques applied for this research.

The research implementation, testing and discussion result will be discussed in Chapter 4. The last chapter, which is the Chapter 5 will be discussing summary of findings, and conclusion of this research.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Locimetric is a click-based graphical password technique which identifies the target points within an individual image. This scheme is based on loci method (Higbee et al., 1979). This scheme requires a user to choose or click any point or place in the given image as a password click point. Features are extracted from a selection which will be saved in the database for registration The successful authentication is determined based on the correct click on the sequence of click points in the same order as during the registration phase. Press Touch Code requires the user to click by pressing on the authentication region and then applying more pressure. This chapter will describe some of the related work that is relevant to this research.

2.2 Related Work

Some previous research has been done that is related to the click-based graphical password technique and Press Touch Code. Following this, some of the related work done regarding the technique used for authentication process and how the flow of the process will be discussed.

2.2.1 Locimetric

The first Locimetric is the Blonder technique and next was enhanced to other multiple techniques to make the scheme is more secure. The subsection below explains the details about the revolution of Locimetric.

2.2.1.1 Blonder technique

Blonder (Blonder G. E., 1996) proposed a graphical password scheme where a password is created that need the user to click on several locations on an image during the registration process. During authentication, the user must click on the previously determined areas of those locations. The image helps to assist the users to recall their passwords and therefore this method is considered more suitable than textual passwords. The drawback of this is memorable password space. The user cannot click where he wants because of predetermined tap regions. Also background of image is very simple thus easy for the attackers to break the password.

2.2.1.2 PassPoint technique

The "PassPoint" system enhanced the Blonder's idea by eliminating the boundaries and allowing the user to choose the images to be used (Wiedenbeck et. Al., 2015). As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of the chosen pixels.

2.2.1.3 VisKey

The PassPoints is commercialized as PocketPC for mobile devices is available from visKey for screen-unlock by tapping using a stylus or finger, on the correct sequence. The settings such as the size of the tolerance region and chosen image may define by users, so that it is easy to click on the exact spot.

2.2.1.4 Cued Click Point

Cued Click Points was designed (Chiasson et. al., 2008) to reduce the hotspots and pattern. The user need to identify and target previously selected locations within one or more images. The next image is based on the location of the previous click-point. The images act as memory cues (Tulving et. al., 1966) to aid recall. No evidence of patterns in Cued Click-Points based on the analysis and user testing, so pattern-based attacks seem not effective. Although the result showed that hotspots remain a problem (Dhapade et. al.,2013). Example systems include Pass Points (Wiedenbeck et. al., 2005) and Cued Click-Points (CCP).

2.2.1.5 Persuasive Cued Click Point

Persuasive Cued Click-Points scheme (Chiasson et. al., 2008) encourage users to select less likely to prefer images as a password. The main feature of PCCP is to allow the user to select a click point within the highlighted viewport of the image. The user is allowed to adjust the location of the viewport until the suitable location is found. During authentication the images are displayed normally without viewport. Although it reduces the hotspot effects, but shoulder surfing remain a problem.

Table 2.1 : Comparison of each Locimetric algorithms

Locimetric Algortihm	**Strength**	**Weakness**	**Security attack**
Blonder	Secure method since the scheme have millions regions to click	Need a longer password in order to be secure	Brute Force, Shoulder Surfing, Guessing
PassPoints	Several points on a picture is click in a particular order	Longer login time than alphanumerical method	Shoulder Surfing, Brute Force, Guessing
Viskey	Resolve the difficulty in pointing to the exact spots.	No input tolerance or need to be precise	Description, Dictionary

Cued Click Point	An authentication failure message is displayed after the final click-point, to protect against incremental guessing attacks	False accept and false reject	Shoulder Surfing, Guessing
Persuasive Cued Click Point	Influence the user preference to select more random passwords that are less likely to include hotspots	Easy to broken by capturing input sequence	Shoulder Surfing, Description

2.2.2 Press Touch Code

Press Touch Code is a new screen size independent password-based authentication scheme Since graphical password schemes are easily being attacked which is shoulder surfing (Chakraborty N et al.,2016), smudge attack (Aviv AJ et al., 2010), intersection attack (Debnath A et al., 2014), and reflection attack (Biddle R et al., 2014), this PTC is implemented in this proposed system.

2.2.3 Knock Code

Same as Press Touch Code, this Knock Code need to use a fingertip instead of a fingernail to tap the screen to turn the screen on. If your Lock screen unlock sequence is set to a Knock Code, tap your Knock Code on the darkened screen to automatically turn the screen on and unlock it at the same time. Knock Code perform poorly than PTC. The reason behind this is that knocks are recognizable even from a long distance, but the presses are seldom recognizable from that distance(Ranak et al., 2017).

2.3 Conclusion

Both Locimetric and Press Touch Code will be implemented in this research in order to make the hybrid authentication scheme is more reliable

CHAPTER 3

METHODOLOGY

3.1 Overview

This chapter will explain the overall approach and framework that we have planned, which to implement in this research where the justified method, techniques, tools, instruments, framework, model that has been selected. The steps that should involve in order to develop this hybrid authentication scheme of combining Locimetric and Press Touch Code are elaborated in this chapter.

3.2 Methodology

This section discusses on technique and testing method that implemented in this proposed research.

3.2.1 Locimetric

In Locimetric scheme, a user has to identify the target points within an individual image. Another term of Locimetric is passpoints and persuasive cued click points. This research will utilize a Locimetric authentication scheme in order to authenticate the user and to control the access of the Android smartphones. Users create their passwords by selecting specific areas of the image, in a specific order. For authentication, the user clicks on the predetermined areas of the locations in a particular sequence. If he manages to click on correct areas, he is able to authenticate.

This technique is chosen because human users were able to recognize 98.5% images accurately after 60mins delay, which was not possible with letters, texts, and sentences (Roger N. Shepard, 1967). Graphical passwords are claimed to make remembering passwords easier, thus allowing more secure passwords to be produced and reducing the temptation for users to create unsafe passwords (Ian Jermyn et al., 1999).

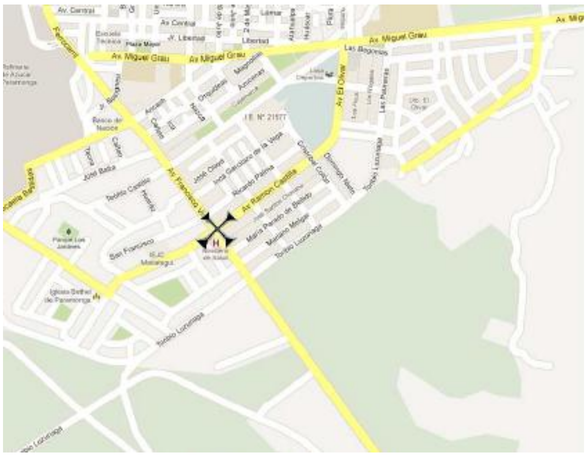


Figure 3.1 : The X-maker show the user password

3.2.2 Press Touch Code

When a user places a finger within the given box on the screen, data acquisition is occurring. The box is given to solve any confusion that may occur in deciding where to press. The data acquisition process keeps acquiring press intensity values after every different of time unit and stores them in a vector. The user must be quick and sharp. If the user fails to do so, noise will be introduced due to finger movement. To stop the process of the data acquisition, a user must remove his finger from attached to the screen. Once all the data are acquired, they are cleaned and processed later to extract the PTC. The user need to press the confirmation button to continue to the next phase.

```
Down = 0
Taken = 1
for    i = 0 to Pressure.size - 1 do
    if Pressure (i) > Pressure (i+1) do
        Down = 1
    Else
        Down = 0
        Taken = 1
    if i = Pressure.size - 2
        Down = 1
    end if

    if Down && Taken do
        Total + 1
        Taken = 0
    end if
end for
return Total
```

Figure 3.2 : Algorithm for finding the peak of pressure

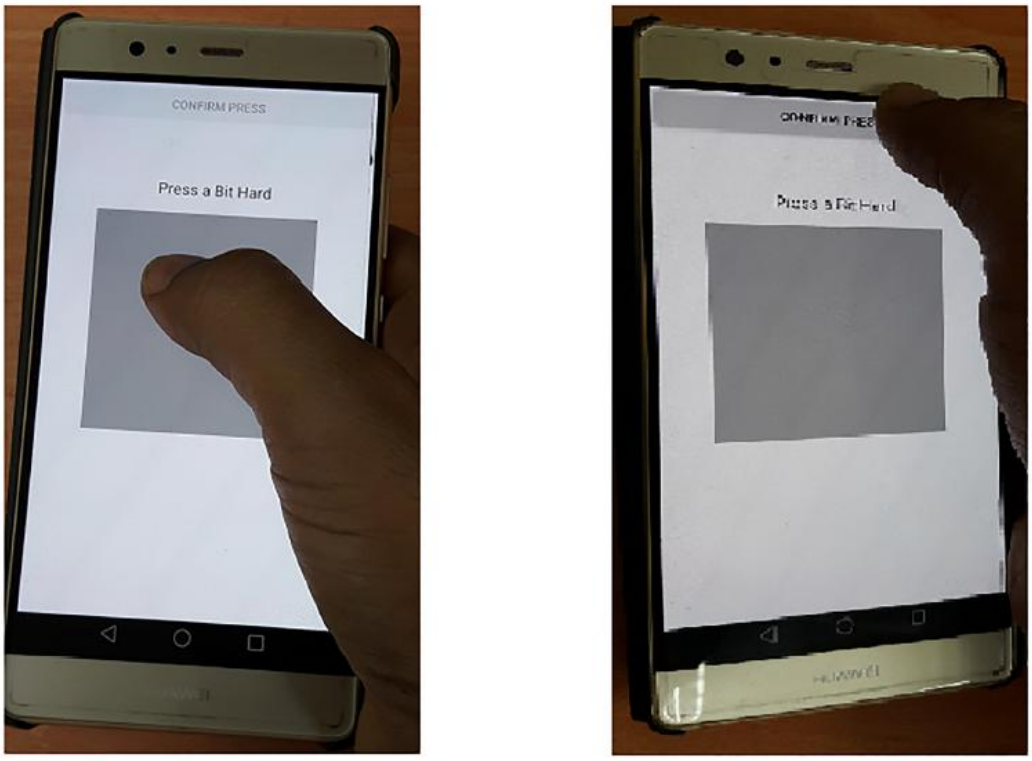


Figure 3.3 : Before and after data acquisition

3.2.3 Instruction for registration and authentication

A user has to register a signature first. The user has to open the application and after then the user need to point his finger to the box on the screen. When the first cycle is done, the user must lift the finger from the screen.

Next, the acquired data is processed to extract the signature of the particular user and would be saved in database. Later on, the user has to validate himself through an authentication session where he need to enter the provided signature during the registration session.

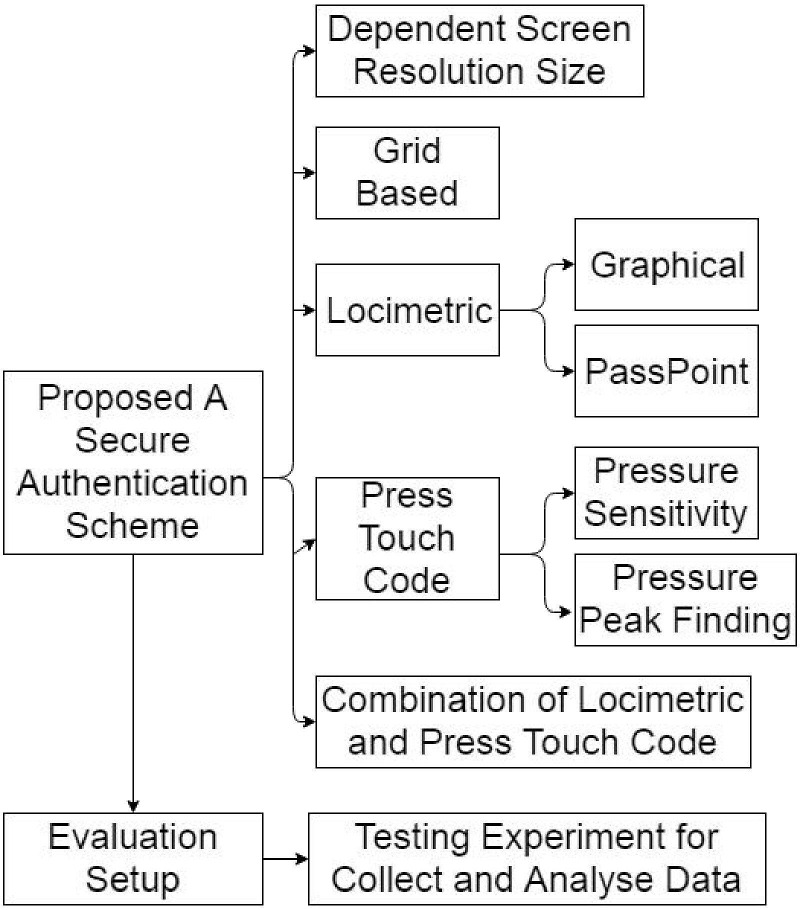

Dependent Screen Resolution Size
Grid Based
Locimetric
Graphical
PassPoint
Proposed A Secure Authentication Scheme
Press Touch Code
Pressure Sensitivity
Pressure Peak Finding
Combination of Locimetric and Press Touch Code
Evaluation Setup
Testing Experiment for Collect and Analyse Data

Figure 3.4 : Methodology Process Flow

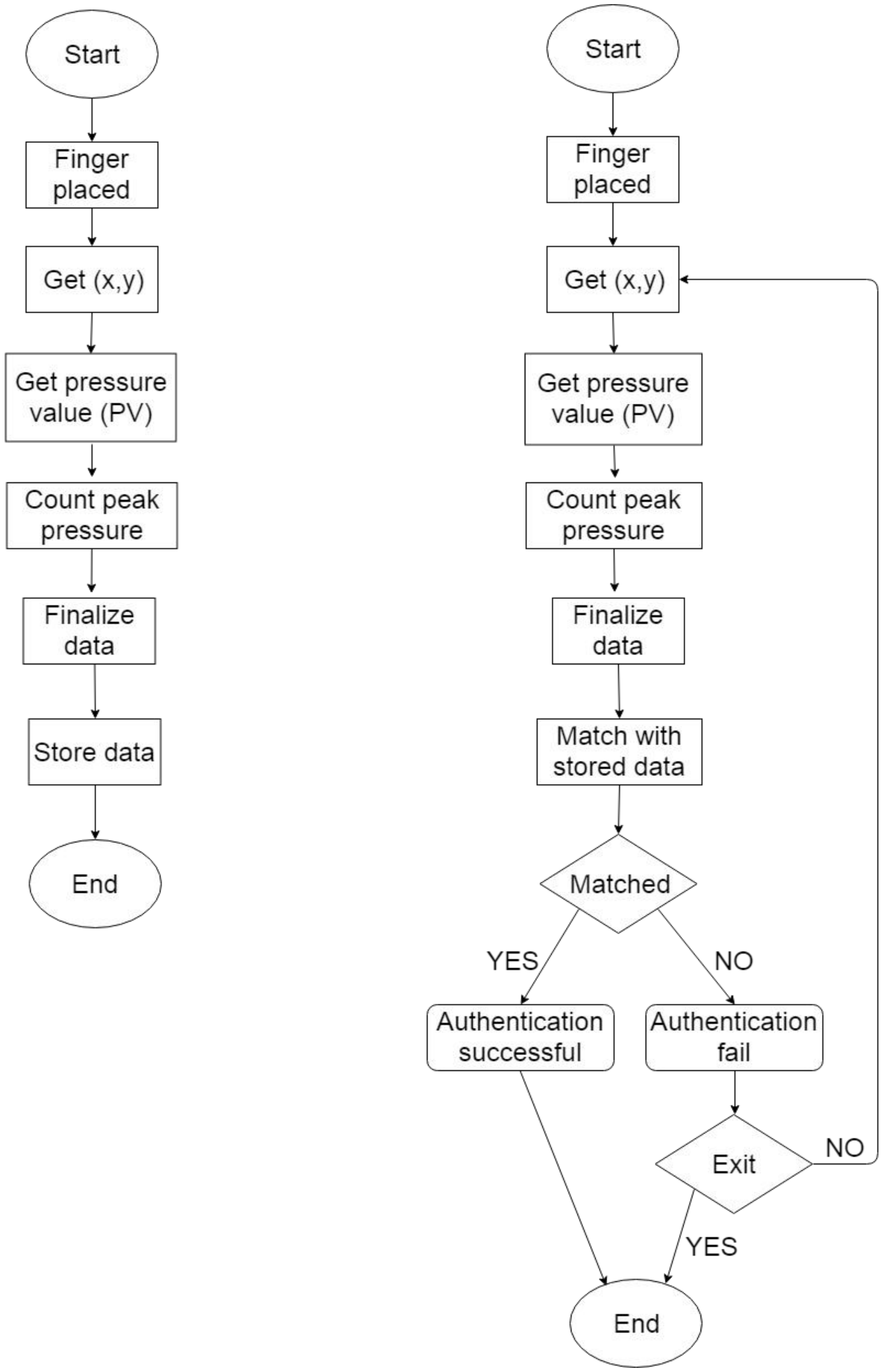


Figure 3.5 : System flowchart

3.2.4 Testing Method : Ad-Hoc Testing

The test is going to conduct informal and randomly without any written test cases which it is an unscripted software testing method. It is a method of software testing without any planning or documentation. Thus, this type of testing method is free to use any input in order to test the functionality of this research project. Ad-Hoc testing is conducted only once if there is no defect found. This testing method gives us quick result which will save the time. Most of the focus will be on testing the system rather than do the documentation.

In this research, once the development of the Android application which is this authentication scheme is done, we will test the scheme by installing the scheme in the Huawei P9 Lite and run the application and check whether it is functioning as what are we expecting and the password is successfully authenticated.

3.3 Software

This section discuss on the softwares that are necessary in order to develop the hybrid authentication scheme.

3.3.1 Android Studio

The Android Studio will be used to design and develop the Android application which will authenticate the user using the newly proposed authentication scheme.

3.4 Hardware

This section will discuss the hardwares that we are going to use in order to develop the hybrid authentication scheme.

3.4.1 Huawei P9 Plus

The Huawei P9 Plus will be used to test the effectiveness of this proposed authentication scheme application.

3.4.2 Lenovo A889

Lenovo A889 will be used to prove that this scheme is dependent on the screen resolution size.

3.5 Gantt Chart

Refer Appendix A, Figure 3.6

3.6 Implementation

In order to realize this research, the following steps and process will be involved while conducting this research and all the steps should work together :

a. Create an Android application which will be the interface for user to enter the password on the authentication scheme .
b. Create the authentication scheme which has the background of Malaysia map and dependent to screen resolution size.
c. Create the grid which based on the screen resolution to get the (x,y) coordinate when user pointing to the authentication scheme.
d. Combine the Press Touch Code to the authentication scheme to form a secure authentication scheme.

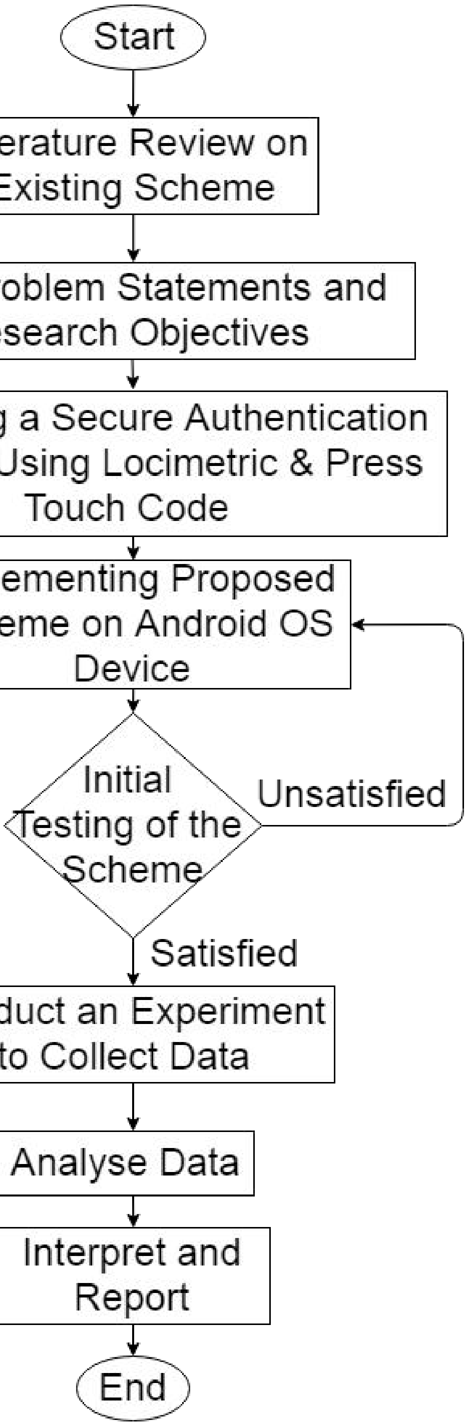

Start
Literature Review on Existing Scheme
Find Problem Statements and Research Objectives
Proposing a Secure Authentication Scheme Using Locimetric & Press Touch Code
Implementing Proposed Scheme on Android OS Device
Initial Testing of the Scheme
Unsatisfied
Satisfied
Conduct an Experiment to Collect Data
Analyse Data
Interpret and Report
End

Figure 3.7 : The flow of this research

3.7 Summary

This hybrid graphical password that combining Locimetric and Press Touch Code allowing more secure passwords to be produced and reducing the temptation for users to create unsafe passwords. If we work on this, the authentication scheme will be more secure and will have lower potential for the unauthorized access.

CHAPTER 4

IMPLEMENTATION, TESTING AND RESULT DISCUSSION

4.1 Introduction

This chapter discuss on the implementation of Locimetric and Press Touch Code techniques based on the design of algorithm. The main target of this chapter is to achieve the objective of this research. During the implementation, the data obtained is filtered using the Press Touch Finding Algorithm (PTFA) to find the number of press provide by the user on a x and y coordinate. After the implementation is done, this scheme is tested on Pressure Sensitive Technique enabled Android devices which are the Huawei P9 Plus to validate and verify the output of the combination techniques.

4.2 Implementation

Below is the methodology for the implementation of this proposed scheme

i. Dependent screen resolution size coordinates grid-based.

ii. Locimetric graphical based password

iii. Pressure peak finding of the Press Touch Code

iv. Combination of Locimetric and Press Touch Code

4.2.1 Dependent screen resolution size coordinate grid-based

The coordinate grid is set to follow the resolution of the phone screen, thus the size of this proposed authentication scheme is depends on the size of the screen resolution. The width and height pixels on the Android screen is firstly obtain programmatically. Next, we will get the x and y coordinates in integer values. For example, if the width is

1080, thus the maximum x-coordinate will be 11, same goes to the height, if the height is 1794, the maximum y-coordinate will be 18.

4.2.2 Locimetric graphical based password

The Malaysia map is utilized as the background of this proposed authentication scheme which help in enhancing the user memorability. The Malaysia map is set to follow the screen size of the Android phone, although nowadays there are various sizes of the smartphone screen.

4.2.3 Pressure peak finding of the Press Touch Code

The Press Touch Finding Algorithm is utilized in this Press Touch Code. The pressure intensity has between 0 and 1 based on the pressure exerted on the screen, which is the stabilize pressure and the press pressure. Any pressure detected on the screen will be collected and filter using the Press Touch Finding Algorithm.

```
Down = 0
Taken = 1
for   i = 0 to Pressure.size - 1 do
    if Pressure (i) > Pressure (i+1) do
        Down = 1
    Else
        Down = 0
        Taken = 1
        if i = Pressure.size - 2
        Down = 1
    end if

    if Down && Taken do
        Total + 1
        Taken = 0
    end if
end for
return Total
```

Figure 4.1 : Press Touch Finding Algorithm

4.2.4 Combination of Locimetric and Press Touch Code

These two techniques are implemented in this new proposed authentication scheme. This requires the user to tap on a point multiple time, and during this time, the x and y coordinate, and the pressure exerts at the coordinate will be captured. Then the pressure will be filtered using the Press Touch Finding Algorithm to calculate the total peak. Next, the x and y coordinates, and the total peak will be stored in the internal storage using the shared preferences.

4.3 Testing and Verification

In order to determine the accuracy and the effectiveness of this new proposed concept, the testing and the verification need to be done in order to validate the model by developing the Android application of this authentication scheme as the proof of the concept to ensure that the problem statement for this research can be solved by this authentication scheme. After developing the authentication scheme, we test the effectiveness and collect the required data that need to be analyse.

4.3.1 Prevent shoulder surfing attack and smudge attack

To ensure the effectiveness of this newly proposed authentication scheme against shoulder surfing attack, an experiment is conducted. In our experiment, we recorded some videos of several authentication sessions using a camera by varying the direction. Firstly, we recorded the videos from the back, front, and right of the person who is doing the authentication process as show in Figure 4.3, Figure 4.4 and Figure 4.5. After recording the videos of all sessions, we played the recorded videos to the participants and asked them to obtain the signature with three times to attempt. Their feedback on this newly proposed authentication scheme is gather based on their answer on the survey. In figure 4.2, the pie chart below shows the percentage of participants that not managed to obtain the signature for three times of the attempt.

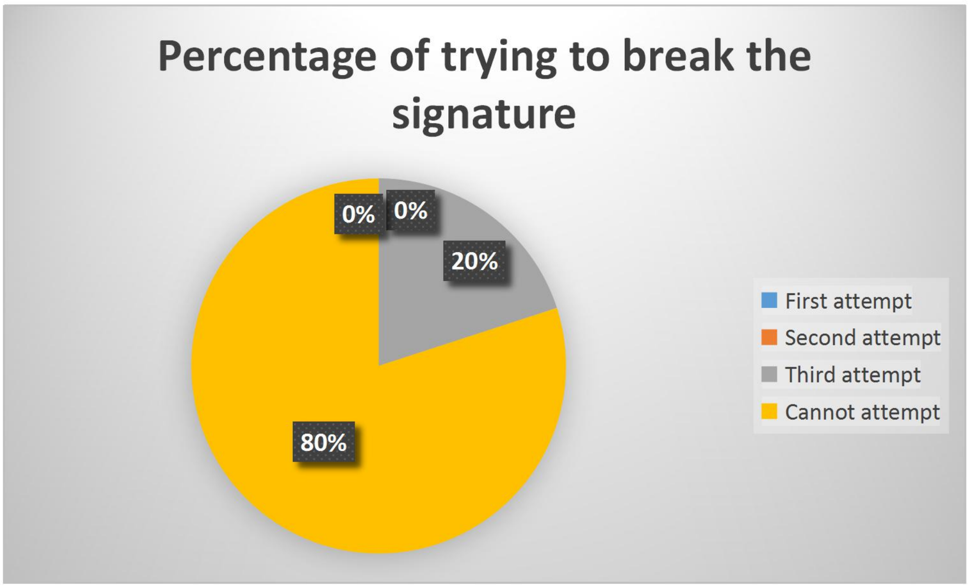


Figure 4.2 : Pie chart of percentage of participants that managed to attempt

Based on the analysis of the survey, 80% were unable to guess or attempt the signature in this authentication scheme while only 20% manage to break the signature with three times attempt. This show that, this newly proposed authentication scheme is resistant to shoulder surfing attack and smudge attack and partially prevent the brute force and guessing attack.

4.3.2 Increase memorability

Since this proposed authentication scheme is utilizing the Locimetric graphical password which is the Malaysia map, in order to test the participants memorability of this authentication scheme, the participants firstly need to register their own signature and then authenticate themselves during the authentication phase. In figure 4.6, the pie chart below shows the percentage of participants that is enabled to authenticate. 100% of the participant were successful and managed to authenticated, with 80% in first time attempt and only 20% attempt twice to authenticate. Thus, this newly authentication scheme helps the users to memorize their signature without the need to jot down the password.

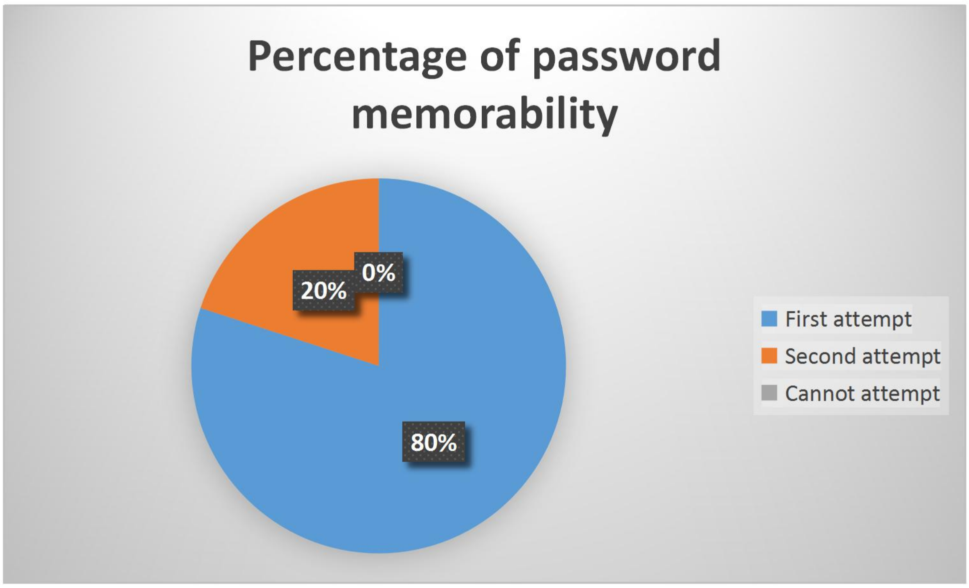
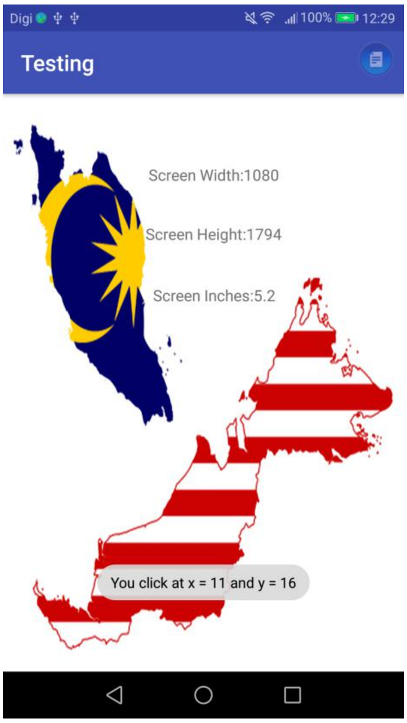


Figure 4.6 : Pie chart of percentage of participants that remember the signature during the authentication phase

4.3.3 Dependent screen resolution size

This newly proposed authentication scheme is a screen resolution size dependent. The maximum x-coordinate and y-coordinate will be depends on the screen resolution size.



Testing

Screen Width:1080

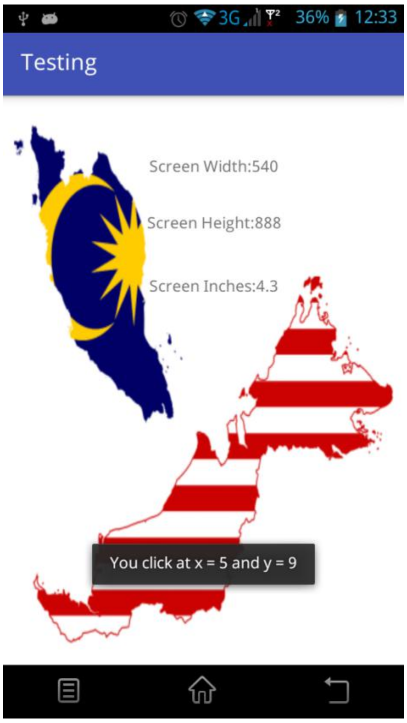
Screen Height:1794

Screen Inches:5.2

You click at x = 11 and y = 16

Figure 4.7 : Test with Huawei P9 Plus

Figure 4.7 above shows that the maximum x-coordinate is 11 and maximum y-coordinate is 16 because of the screen width is 1080 pixels while the screen height is 1794. While Figure 4.8 below, which is tested with Lenovo A889 shows that the screen width is 540 pixels, while the screen height is 888 pixels, thus the maximum x-coordinate is 5 and maximum y-coordinate is 9.



Testing

Screen Width:540

Screen Height:888

Screen Inches:4.3

You click at x = 5 and y = 9

Figure 4.8 : Test with Lenovo A889

The password complexity formula for this newly proposed authentication scheme is summarized as below :

$$\text{Password complexity} = (m \times n) \times p$$

where m is the maximum x-coordinate

n is the maximum y-coordinate

p is the total number of press

For example, for the Huawei P9 Plus, the maximum x-coordinate is 11 while the maximum y-coordinate is 16. If the user provide 20 presses, the password complexity will be 3520.

4.4 Result Discussion

As for the result, the intensity of pressure will determine the total number of press and the (x,y) coordinate will determine the position of the press. The pressure data is collected through the authentication scheme that we have developed. The subsection below shows how is the pressure data is collected and convert the pressure data in the form of a line graph to show the total number of peak pressure.

4.4.1 Test the pressure data to find the total number of peak pressure

The newly proposed authentication scheme was tested for three times with different number of press; one press, three presses and six presses. The total number of the peak pressure shown in the line graph is same as the total number of the peak pressure that calculated using the Press Touch Finding Algorithm (PTFA). The raw data in Figure 4.9, Figure 4.11 and Figure 4.13 was collected before convert the data into a line graph.

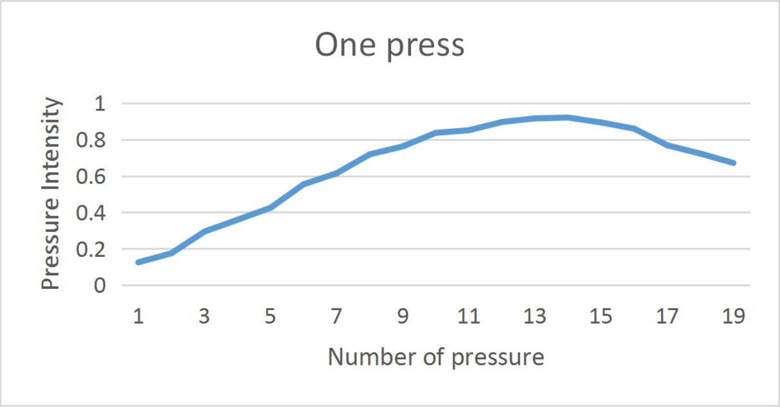


Figure 4.10 : Graph of one total peak

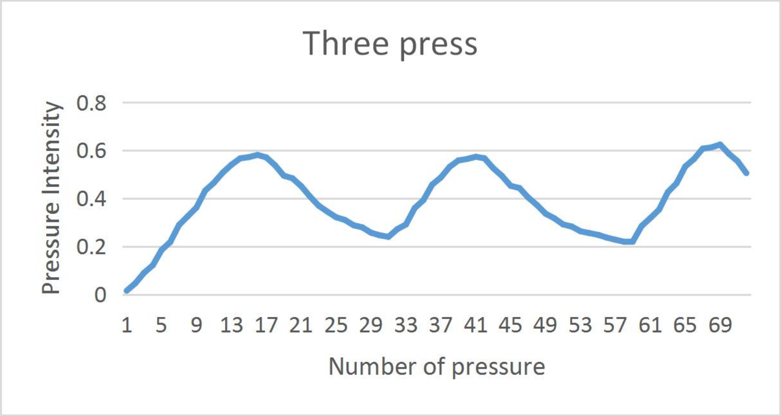


Figure 4.12 : Graph of three total peak

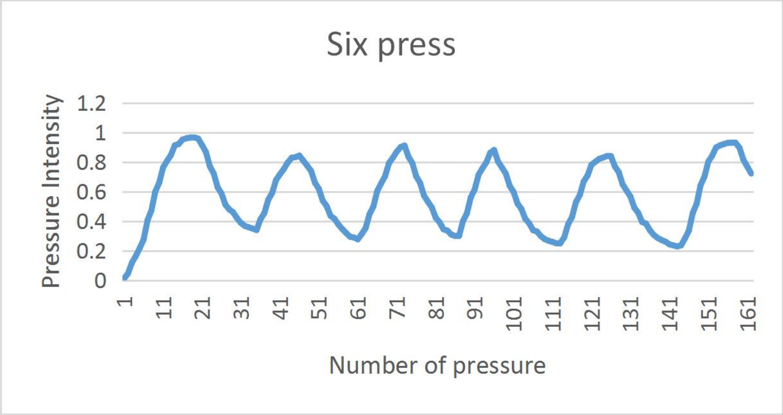
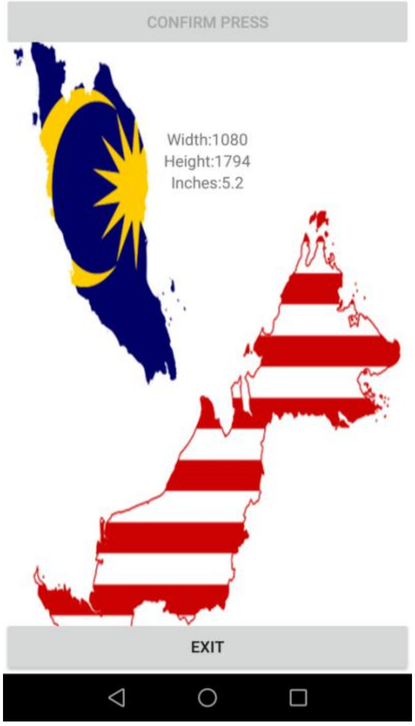


Figure 4.14 : Graph of six total peak

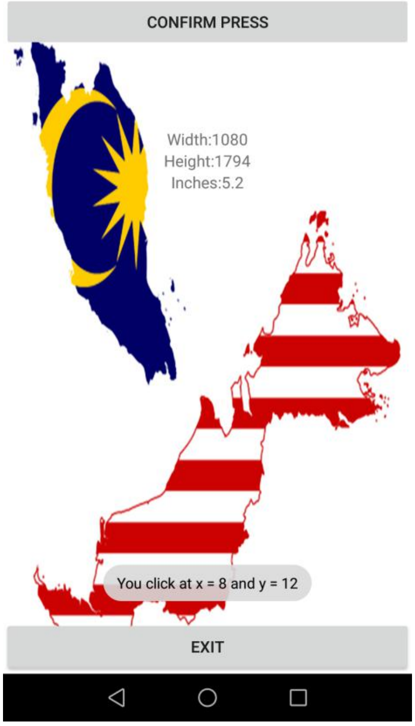
4.4.2 Final product

Figure 4.15 to Figure 4.20 below show the flow of the authentication scheme. This final product is developed as Android application that act as the proof of the concept of the combination between these two techniques, Locimetric and Press Touch Code. This newly proposed authentication scheme can also be utilized in any similar devices of different operating systems with some modifications so that this scheme is able to work with different operating systems.



Width:1080
Height:1794
Inches:5.2

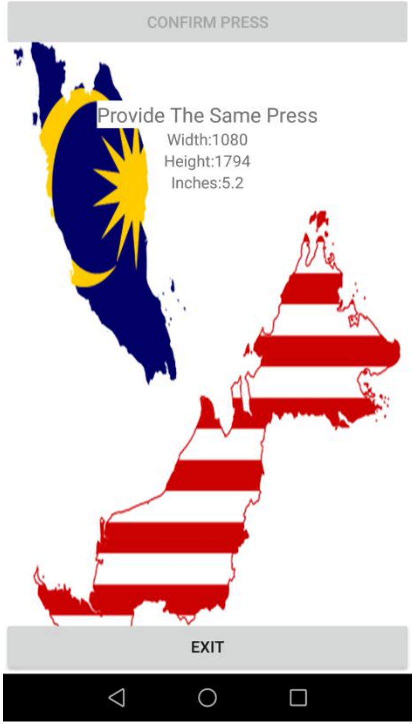
Figure 4.15 : Registration phase



Width:1080
Height:1794
Inches:5.2

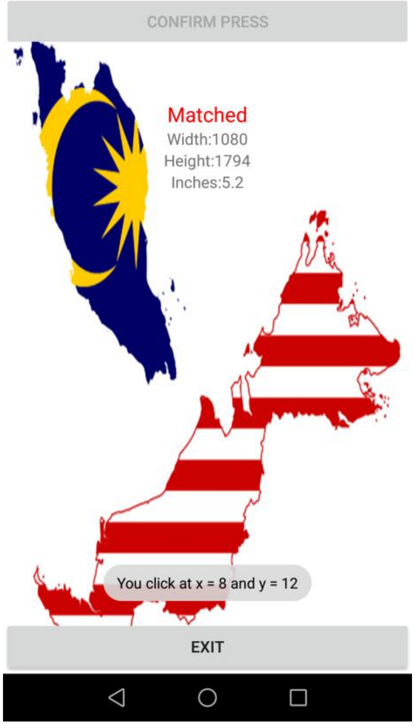
You click at x = 8 and y = 12

Figure 4.16 : Tap on a point and click ‘CONFIRM PRESS’ for registration



Provide The Same Press
Width:1080
Height:1794
Inches:5.2

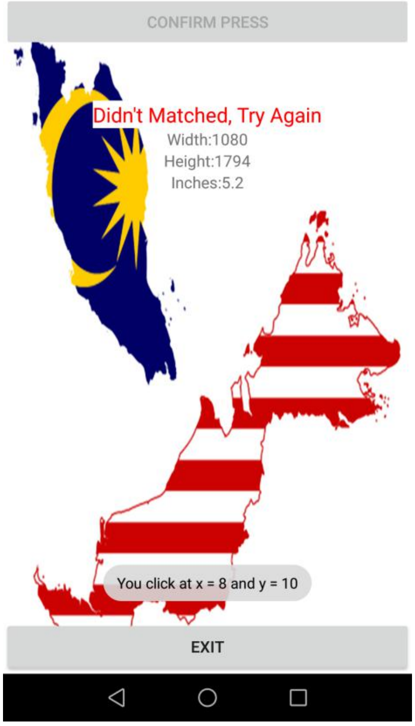
Figure 4.17 : Authentication Phase



Matched
Width:1080
Height:1794
Inches:5.2

You click at x = 8 and y = 12

Figure 4.18 : 'Matched' message will pop up if successfully authenticated

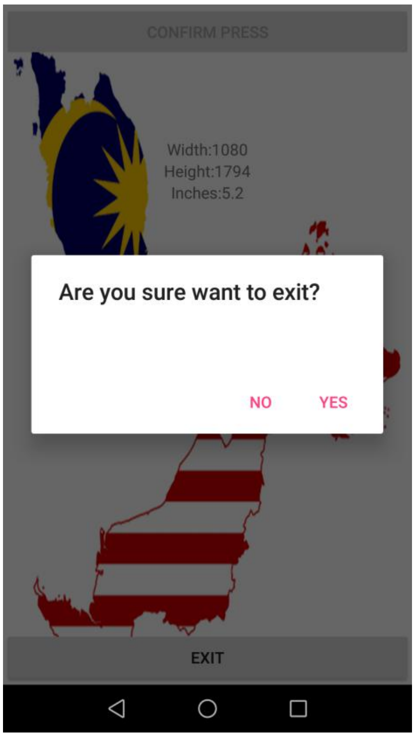


Didn't Matched, Try Again

Width:1080
Height:1794
Inches:5.2

You click at x = 8 and y = 10

Figure 4.19 : ‘Didn’t Matched, Try Again’ message will pop up if failed to authenticate



Width:1080
Height:1794
Inches:5.2

Are you sure want to exit?

Figure 4.20 : Option to exit the application

CHAPTER 5

CONCLUSION

5.1 Introduction

The purpose of this chapter is to summarize all the content of this research together with the constraint and future work.

The authentication scheme adds a big measure of security and convenience to the users. With the rapid development of wireless technology, passwords are a vital component of system security, which usually controlled by the small size pocket computer for example the smartphone. However, the existing passwords have some limitations such as in terms of memorability because most of the users preferred to choose weak texts as passwords to make it easy for themselves to remember which giving lower or no security since the password are easy to guess and break.

There are many techniques that have been proposed to overcome those limitations. For this research, we combine the Locimetric and Press Touch Code techniques to make the newly proposed authentication scheme is more secure. The purpose of this research is to design a secure hybrid authentication scheme using the two techniques mentioned above which is dependent to screen resolution size and test the effectiveness of the proposed authentication scheme on Android based operating system.

From the literature review, it has discuss more details on the authentication scheme and the concept of Locimetric and Press Touch Code. Some part of the Passpoint Locimetric method together with the Press Touch Code and grid concept has been utilized in this research.

In this research, the implementation start by designing the authentication scheme. The coordinate grid-based is utilized and the coordinate is based on the screen resolution size. Next, we put the Malaysia map as the background layout. We capture the pressure intensity data and convert the data to line graph to find the number of pressure peak. The number of pressure peak finding found in the graph is validated with the Press Touch Finding Algorithm (PTFA). The experiment conducted with the participants shows that this newly proposed authentication scheme is able to solve the problem such as shoulder surfing attack, low memorability, and fat finger error.

As a conclusion, this research has achieved the entire objective of this research in order to solve the problem.

5.2 Research Constraint

The constraint while conducting this research are :

i. Problem in installing the Android Studio, SDK not found.
ii. Limited time
iii. Lack of internet resources to refer
iv. Internet connection problem

5.3 Future Work

In future work, the design of this authentication scheme in terms of the (x,y) coordinate can be more than one coordinate as this can fully prevent the brute force attack and guessing attack. Thus, this authentication scheme can be enhanced by making the scheme to be able to tap on multiple coordinate.

REFERENCES

Adebola, O., Ithnin, N., Jali, M.Z., Akosu, N.: Graphical password Schemes design: enhancing memorability features using Autobiographical Memories. J. Theor. Appl. Inf. Technol. 53(1), 10 July 2013.

Aviv AJ, Gibson K, Mossop E, Blaze M, Smith JM. Smudge attacks on smartphone touch screens. Proceedings of the USENIX 4th Workshop on Offensive Technologies. 2010.

Biddle R, Chiasson S, Oorschot PCV. Graphical Passwords: Learning from the First Twelve Years.ACM Computing Surveys. 2012; 44(4). https://doi.org/10.1145/2333112.2333114

Chakraborty N, Randhawa GS, Das K, Mondal S. MobSecure: A Shoulder Surfing Safe Login Approach Implemented on Mobile Device. Procedia Computer Science. 2016; 93:854±61. https://doi.org/10.1016/j.procs.2016.07.256

Chiasson, S., Forget, A., Biddle, R., & van Oorschot, P. C. (2008, September). Influencing users towards better passwords: persuasive cued click-points.In Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction-Volume 1 (pp. 121-130). British Computer Society.

Debnath A, Singaravelu PK, Verma S. Privacy in wireless sensor networks using ring signature. Journal of King Saud UniversityÐComputer and Information Sciences. 2014; 26(2):228±36. https://doi.org/10.1016/j.jksuci.2013.12.006

Dhapade, M. S. L. (2013, June). Implementation of Persuasive Cued Click-Points Techniques for Folder Security using Secure Hash Algorithm.InInternational Journal of Engineering Research and Technology (Vol. 2, No. 6 (June-2013)).ESRSA Publications.

G. E. Blonder. (1996). Graphical passwords. United States Patent 5559961.

I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter and A. D. Rubin, “The Design and Analysis of Graphical Passwords,” in Proceedings of the 8th USENIX Security Symposium, (1999), pp. 1–14.

M. R. (2015, February). What is authentication? - Definition from WhatIs.com. Retrieved from https://searchsecurity.techtarget.com/definition/authentication

Perkins, D. N., Higbee, K. L., & Baddelev, A. D. (1979). Your Memory: How It Works and How to Improve It. Leonardo, 12(1), 72. doi:10.2307/1574098

Ranak, M. S., Azad, S., Nur Nadiah Hanim Binti Mohd Nor, & Zamli, K. Z. (2017). Press Touch Code: A finger press based screen size independent authentication scheme for smart devices. Plos One, 12(10). doi:10.1371/journal.pone.0186940

Sahu, S. B., & Singh, A. (2014). Secure User Authentication & Graphical Password using Cued Click-Points. International Journal of Computer Trends and Technology, 18(4), 156-160. doi:10.14445/22312803/ijctt-v18p137

SFR Software. visKey for Pocket PC. Retrieved from http: //www.sfr-software.de/cms/EN/pocketpc/viskey/

Shepard, R. N. (1967). Recognition memory for words, sentences, and pictures. Journal of Verbal Learning and Verbal Behavior, 6(1), 156-163. doi:10.1016/s0022-5371(67)80067-7

S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon. (2005). Authentication using graphical passwords: Basic results. In Human-Computer Interaction International (HCII 2005), Las Vegas, NV.

S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon. (2005). Authentication using graphical passwords: Effects of tolerance and image choice. In Symposium on Usable Privacy and Security (SOUPS), Carnegie Mellon University, Pittsburgh.

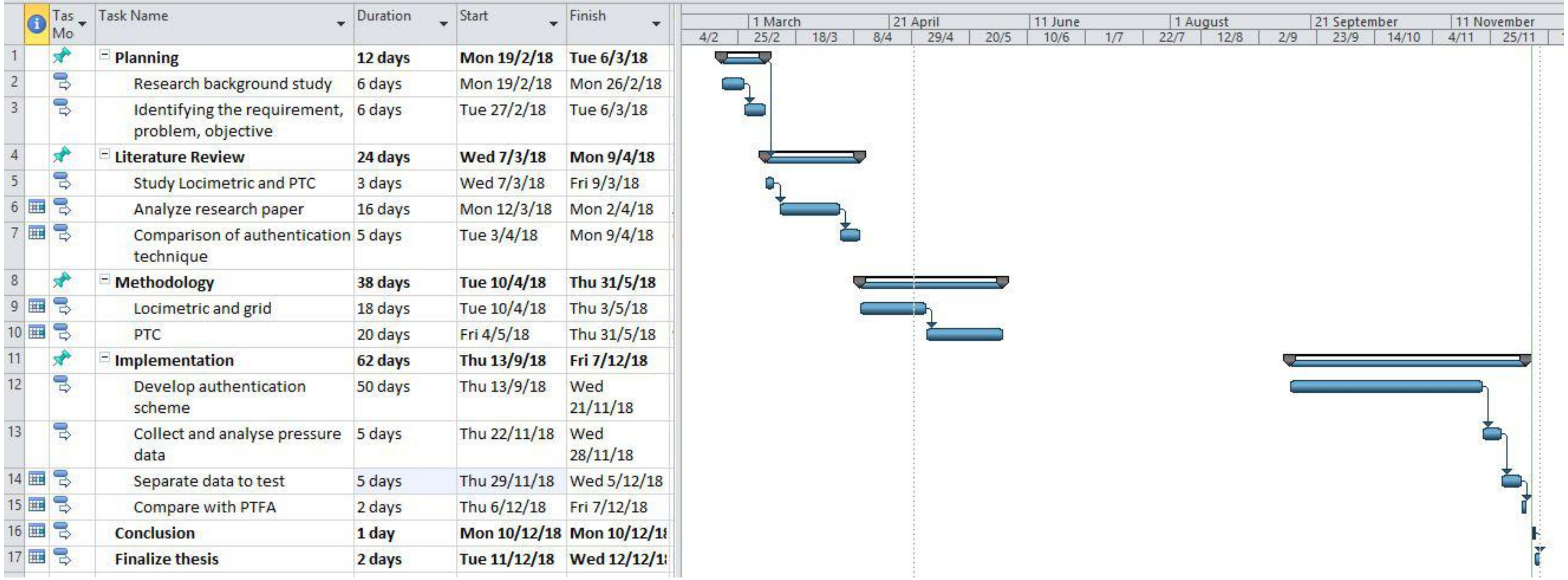
S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon. (2005). Passpoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human Computer Studies, 63.

Teng, J., Snoussi, H., & Richard, C. (2009). Decentralized variational filtering for simultaneous sensor localization and target tracking in binary sensor networks. 2009 IEEE International Conference on Acoustics, Speech and Signal Processing. doi:10.1109/icassp.2009.4960063

Thorpe, J., Macrae, B., & Salehi-Abari, A. (2013). Usability and security evaluation of GeoPass. Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS 13. doi:10.1145/2501604.2501618

Zakaria, O., Zangooei, T., & Shukran, M. A. (2012). Enhancing Mixing Recognition-Based and Recall-Based Approach in Graphical Password Scheme. International Journal of Advancements in Computing Technology, 4(15), 189-197. doi:10.4156/ijact.vol4.issue15.22

APPENDIX A



	i	Tas Mo	Task Name	Duration	Start	Finish
1		📌	⊟ **Planning**	**12 days**	**Mon 19/2/18**	**Tue 6/3/18**
2		⇨	Research background study	6 days	Mon 19/2/18	Mon 26/2/18
3		⇨	Identifying the requirement, problem, objective	6 days	Tue 27/2/18	Tue 6/3/18
4		📌	⊟ **Literature Review**	**24 days**	**Wed 7/3/18**	**Mon 9/4/18**
5		⇨	Study Locimetric and PTC	3 days	Wed 7/3/18	Fri 9/3/18
6	▦	⇨	Analyze research paper	16 days	Mon 12/3/18	Mon 2/4/18
7	▦	⇨	Comparison of authentication technique	5 days	Tue 3/4/18	Mon 9/4/18
8		📌	⊟ **Methodology**	**38 days**	**Tue 10/4/18**	**Thu 31/5/18**
9	▦	⇨	Locimetric and grid	18 days	Tue 10/4/18	Thu 3/5/18
10	▦	⇨	PTC	20 days	Fri 4/5/18	Thu 31/5/18
11		📌	⊟ **Implementation**	**62 days**	**Thu 13/9/18**	**Fri 7/12/18**
12		⇨	Develop authentication scheme	50 days	Thu 13/9/18	Wed 21/11/18
13		⇨	Collect and analyse pressure data	5 days	Thu 22/11/18	Wed 28/11/18
14	▦	⇨	Separate data to test	5 days	Thu 29/11/18	Wed 5/12/18
15	▦	⇨	Compare with PTFA	2 days	Thu 6/12/18	Fri 7/12/18
16	▦	⇨	**Conclusion**	**1 day**	**Mon 10/12/18**	**Mon 10/12/1**
17	▦	⇨	**Finalize thesis**	**2 days**	**Tue 11/12/18**	**Wed 12/12/1**

Figure 3.6 : Gantt chart

APPENDIX B

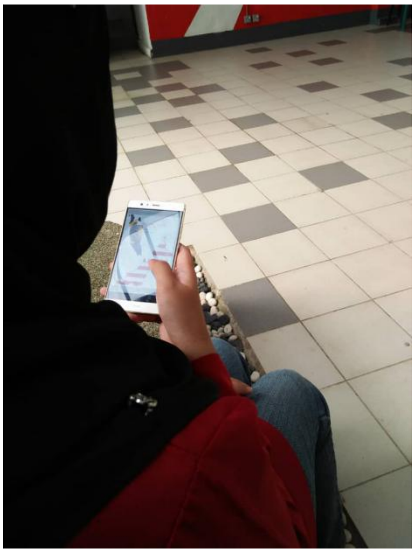


Figure 4.3 : Shoulder surfing from the back

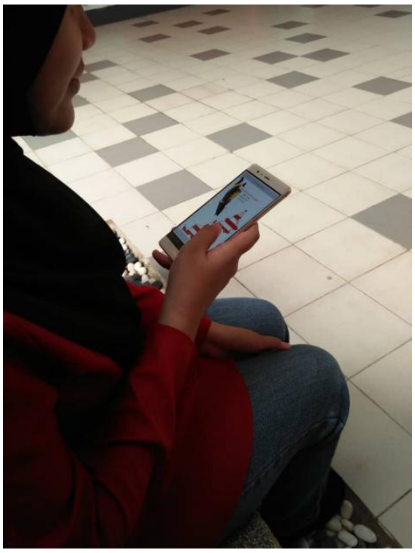


Figure 4.4 : Shoulder surfing from the right

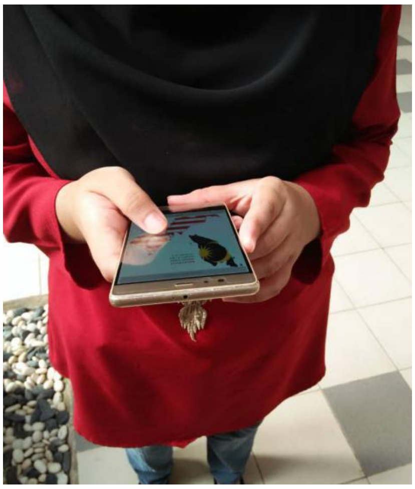


Figure 4.5 : Shoulder surfing from the front

APPENDIX C

```
8,12,0.12495613098144531|8,12,0.1750362366437912|8,12,0.2939497828483581
5|8,12,0.3590142726898l934|8,12,0.42475011944770813|8,12,0.5538872480392
456|8,12,0.6144502758979797|8,12,0.7181353569030762|8,12,0.7620050311088
562|8,12,0.8364690542221069|8,12,0.850629448890686|8,12,0.89585715532302
86|8,12,0.9156633615493774|8,12,0.9202258586883545|8,12,0.89323264360427
86|8,12,0.8593118190765381|8,12,0.7679255604743958|8,12,0.72231632471084
6|8,12,0.6708323955535889|
```

Figure 4.9 : Raw data of one press

```
4,4,0.01521324459463358|4,4,0.046616312116384506|4,4,0.09018082171678543
|4,4,0.12138552218675613|4,4,0.18474097549915314|4,4,0.21832609176635742
|4,4,0.2890669107437134|4,4,0.32538339495658875|4,4,0.3617914021015167|4
,4,0.4322270452976227|4,4,0.46495765447616577|4,4,0.5065690279006958|4,4,
0.5396963357925415|4,4,0.5663233399391174|4,4,0.5715876817703247|4,4,0.5
80743134021759|4,4,0.5702296495437622|4,4,0.5376821756362915|4,4,0.49430
07528781891|4,4,0.48339053988456726|4,4,0.45065996050834656|4,4,0.407782
10759162903|4,4,0.3692835867404938|4,4,0.34450292587280273|4,4,0.3211871
385574341|4,4,0.31006333231925964|4,4,0.2880140244960785|4,4,0.279133290
05241394|4,4,0.2567482888698578|4,4,0.24612802267074585|4,4,0.2396581918
001175|4,4,0.2715037763118744|4,4,0.29118791222572327|4,4,0.359502553939
81934|4,4,0.3925078213214874|4,4,0.4569008946418762|4,4,0.48694589734077
454|4,4,0.5309529304504395|4,4,0.5577782988548279|4,4,0.5638208389282227
|4,4,0.573006808757782|4,4,0.5666742920875549|4,4,0.5256428122520447|4,4,
0.4934004843235016|4,4,0.45189592242240906|4,4,0.4430457055568695|4,4,0.
40366217494010925|4,4,0.37248799204826355|4,4,0.3360952138900757|4,4,0.3
169298768043518|4,4,0.29144731163978577|4,4,0.2824750244617462|4,4,0.262
77562975883484|4,4,0.2553749978542328|4,4,0.24811169505119324|4,4,0.2366
521656513214|4,4,0.22755779325962067|4,4,0.21934844553470612|4,4,0.22099
64096546173|4,4,0.2847333550453186|4,4,0.3178454339504242|4,4,0.35281911
49234772|4,4,0.425711452960968|4,4,0.4624704420566559|4,4,0.532417774200
4395|4,4,0.5636682510375977|4,4,0.6070038676261902|4,4,0.612161457538604
7|4,4,0.6238040924072266|4,4,0.5855039358139038|4,4,0.5544670820236206|4
,4,0.504921019077301|
```

Figure 4.11 : Raw data of three presses

```
8,11,0.012252994813024998|8,11,0.046784162521362305|8,11,0.11906614899635315|8,
11,0.16446173191070557|8,11,0.21750210225582123|8,11,0.27594414353370667|8,11,0
.40538644790649414|8,11,0.4723735451698303|8,11,0.6005645990371704|8,11,0.65963
22655677795|8,11,0.7625696063041687|8,11,0.8067445158958435|8,11,0.84628063440
32288|8,11,0.9129472970962524|8,11,0.921736478805542|8,11,0.9519646167755127|8,
11,0.9604638814926147|8,11,0.9657739996910095|8,11,0.9662622809410095|8,11,0.95
84038853645325|8,11,0.9143663644790649|8,11,0.8677805662155151|8,11,0.77116042
37556458|8,11,0.7224841713905334|8,11,0.6294956803321838|8,11,0.58669412136077
88|8,11,0.5113908648490906|8,11,0.4790264666080475|8,11,0.4593118131160736|8,11
,0.41922637820243835|8,11,0.38759440183639526|8,11,0.3674219846725464|8,11,0.35
841917991638184|8,11,0.3496299684047699|8,11,0.33975738286972046|8,11,0.412726
0148525238|8,11,0.45442894101142883|8,11,0.5447928309440613|8,11,0.59069198369
97986|8,11,0.6778057813644409|8,11,0.7169909477233887|8,11,0.7527428269386292|
8,11,0.7963073253631592|8,11,0.8284885883331299|8,11,0.8329899907112122|8,11,0.8
42984676361084|8,11,0.809475839138031|8,11,0.7755245566368103|8,11,0.739589512
348175|8,11,0.659403383731842|8,11,0.618005633354187|8,11,0.538246750831604|8,1
1,0.5017776489257812|8,11,0.43579766154289246|8,11,0.4163118898868561|8,11,0.37
77370750904083|8,11,0.3467612862586975|8,11,0.3195239305496216|8,11,0.29462119
936943054|8,11,0.2892957925796509|8,11,0.27718013525009155|8,11,0.312535285949
70703|8,11,0.3527428209781647|8,11,0.4472877085208893|8,11,0.49900051951408386
|8,11,0.6046845316886902|8,11,0.6556649208068848|8,11,0.7044327259063721|8,11,0.
7924162745475769|8,11,0.8293430805206299|8,11,0.8702220320701599|8,11,0.901411
4737510681|8,11,0.9114976525306702|8,11,0.8355535268783569|8,11,0.792507827281
9519|8,11,0.7029068470001221|8,11,0.6581215858459473|8,11,0.572335422039032|8,1
1,0.531303882598877|8,11,0.4928511381149292|8,11,0.42325475811958313|8,11,0.392
2636806964874|8,11,0.3447928726673126|8,11,0.3359731435775757|8,11,0.308812081
81381226|8,11,0.2999466061592102|8,11,0.3003280758857727|8,11,0.40038147568702
7|8,11,0.45220112800598145|8,11,0.5606012344360352|8,11,0.6138704419136047|8,11
,0.7130998969078064|8,11,0.7579308748245239|8,11,0.7976043224334717|8,11,0.8626
382946968079|8,11,0.8813000917434692|8,11,0.8036011457443237|8,11,0.7633020281
791687|8,11,0.7216907143592834|8,11,0.6383611559867859|8,11,0.5974975228309631
|8,11,0.5192950367927551|8,11,0.48290225863456726|8,11,0.4159914553165436|8,11,
0.38579386472702026|8,11,0.33882656693458557|8,11,0.3299000561237335|8,11,0.298
3749210834503|8,11,0.27815669775009155|8,11,0.2671854794025421|8,11,0.25978484
749794006|8,11,0.24963760375976562|8,11,0.252323180437088|8,11,0.2903181612491
6077|8,11,0.3791866898536682|8,11,0.4278171956539154|8,11,0.5276874899864197|8,
11,0.5762722492218018|8,11,0.6681467890739441|8,11,0.7092851400375366|8,11,0.78
19180488586426|8,11,0.801708996295929|8,11,0.8216372728347778|8,11,0.830350220
2033997|8,11,0.8405889868736267|8,11,0.8389715552330017|8,11,0.770061790943145
8|8,11,0.731364905834198|8,11,0.6484016180038452|8,11,0.6070496439933777|8,11,0.
5667353272438049|8,11,0.4911268651485443|8,11,0.4565346837043762|8,11,0.394110
```

Figure 4.13 : Raw data of six presses