ISSN No:-2456-2165

Assessment of the Usability and Acceptability of Passface Authentication Mechanism on Android Phones

Nasiru Muhammad Dakingari[1], Anas Shehu[2*], Shamsu Sani[2], Zauwali Sabitu Paki[3]
[1]Kebbi State Polytechnic Dakingari, Department of Social Science, Kebbi, Nigeria
[2]Kebbi State Polytechnic Dakingari, Department of Computer Science, Kebbi, Nigeria
[3] Yusuf Maitama Sule University, Department of Computer Science, Kano, Nigeria

Abstract:- The research aims at assessing usability and acceptability of Passfaces authentication scheme. Passfaces is an authentication scheme that allows users to select facial images of their choice as pass code to gain access to their phones, computers, or other computing resources. We have developed a special android app that simulated the Passfaces technology. We run experiments with 232 volunteers recruited via our social media contacts. The users were asked to create Passfaces passwords of size 4, 5, 6, and 8. The results reveal that Passfaces of size 4 is more usable with least average authentication time and minimal errors. Overall, 80% of the volunteers could authenticate in the first attempt, about 10% and 3% authenticated in the second and third attempts, respectively; and only 7% f
ailed to authenticate completely.

Keywords:- *Authentication, Configuration Setup, Smart-Phone, Usability, Two-Factor Authentication, Graphical Password.*

I. INTRODUCTION

The focus of this work is on the usability of Passfaces authentication scheme on Android devices. Authentication strategy aims at providing access to the content of smartphone to the authorised user. It ensures that only the right user accesses the device. That is security. Normally, security specialists measure the quality of a given security scheme by how difficult it is for an attacker to break it without any prior knowledge of the scheme.

However, usability entails the ease or difficulty with which user uses the authentication (in our case). It includes all aspects of a product like software, such as the menus, the dialogs, the displays, etc.

To achieve that, we will develop an Android app that simulates this authentication mechanism. we will fine-tune some parameters related to this authentication mechanism so as to determine the best thread-off [1]. The app will be used to experiment with real smart phone users to get real authentication data. The authentication data that the app will collect will facilitate and help in determining the ease or otherwise of the scheme and consequential acceptability.

There are other most common authentication mechanisms besides passfaces that are used to secure the content of smart phones. Examples are the fingerprint biometrics, facial recognition, and passwords. Implicit authentication (IA) [2] that uses behavioral biometric to authenticate user of a smartphone is receiving attention amongst the research community in recent time. This mechanism allows the user to be authenticated by using his behaviour such as how the user picks his phone. This can be used to create a two-factor authentication for better security.

Passfaces is an authentication mechanism that allows the user of a smartphone to set some images as his/her password. The major reason is to address the problems of the widely used authentication methods such as a password. Many people have poor memorability and hence resort to using weak credentials for authentication. The scheme uses the fact that the human brain can recognize the face of a known person within just 20 million seconds irrespective of age, gender, or language [3]. Therefore, with this scheme, user is not required to remember anything; just recognize the faces.

The user of Passfaces first selects the set of images as the Passfaces code, normally four like PIN code. During authentication, the user is presented with a grid of 3x3 tiles consisting of images of faces. The authentication is carried out in steps. The number of steps corresponds to the size of the Passfaces code. For example, if the number of images making up the user's Passfaces code is 3, the authentication will be in 3 steps. In each step, the user is presented with a 3x3 grid of faces out of which only 1 is genuine and the remaining 8 faces are decoys [4]. The user gain access to the phone if the face selected in each of the steps is genuine and denied access otherwise. To increase the security of the scheme, the type of images shown to the user in each step are very similar to the ones set. If for example, the user selects the face of a black person in the first step, faces of black people will be displayed in the first step during authentication. Figure 1 shows an example of 3x3 grid of Passfeces images.

ISSN No:-2456-2165

Fig 1:- Passfaces grid of 3x3 tiles for user to select one. Source: [4]

However, besides the faces of people we know, some people tend to remember things that they like most like their favourite food, fruits, natural sites, pets, and so on. It will help to investigate the possibility of using the images of these things as a variant of Passfaces and assess their usability and security. Users could set or select their favourite images as Passfaces code to secure their smart-phones.

II. OTHER AUTHENTICATION SCHEMES

A. Face recognition

Face recognition is a technology that allows the recognition of a person via a facial image. The technology starts by detecting the face [5] and then extracting the salient facial features that serve as the basis for user authentication. Human face has several features that make up the facial characteristics [6]. This technology has recently been added to the smart-phones such that user could, instead of, for instance entering a PIN code or drawing a pattern, authenticate by just looking directly at the phone screen. This has the convenience that user does not need to remember, enter, or draw anything on the phone screen. This type of authentication is helpful to people with memorability problem. The initial intent of the technology was to combat crimes. Some facial recognition cameras were installed by some security agencies in United States especially to detect criminals that are on the watch list [6].

B. Fingerprint

A fingerprint system looks at the patterns found on a fingertip [7] to identify an individual. A fingerprint recognition system obtains user's finger impression via sensing device and keeps the data in the app database. During authentication, user's finger impression is also captured using the sensing device and the features extracted. The system compares the extracted features with those previously stored in the app database to authenticate the user [8]. Fingerprint biometrics in scenarios other than smart-phone can operate in two modes: verification and identification [9]. In the verification mode, the user first claims an identity which implicitly means telling the system I am who I claim I am. The system uses the claimed identity to retrieve the reference biometric template corresponding to the claimed identity and compares with the query template (fingerprint data extracted at the time of the authentication). The system confirms the identity if there is a match and rejects it otherwise [8]. This is 1:1 comparison. In the identification mode on the other hand, user does not claim any identity. The system only uses the fingerprint features extracted at the time of the authentication and performs an exhaustive search in the system database to find a match. This is a 1:N comparison and takes longer time than the verification.

Fingerprint biometrics is seen as one of the most successful and dominant [10-12] biometrics and has for long been used as reliable means of identification [13] because of its wide acceptability, low cost of sensing device, and robustness.

Fingerprint authentication mechanism was added to smartphones as an alternative to PIN code or pattern. With fingerprint biometrics, the problem of memorability does not even arise as the biological features that serve as the basis of the authentication are inseparable from the user. So, user does bother about remembering anything. Nowadays, most smartphones have this technology as an alternative authentication strategy.

C. PIN code

PIN is currently one of the most widely authentication mechanisms in smartphones [14]. It is an authentication mechanism that allows user to enter a 4-digit pin to gain access to the content of a smartphone. The use of PIN is not limited to smartphones alone. Other services such ATM, POS, NFC payment, and SIM card locking also use PIN. In the event of input error, a user is permitted to retry 2 more times before being blocked.

PIN code, being the most used authentication mechanism on smartphones, it is important to study its features more closely. Alphanumeric passwords have similar characteristics but are less used in smartphones, although theoretically more secure.

The Android Lock Pattern is also a popular mechanism for smartphone authentication. Moreover, some studies already exist for the classical implementation. It will be interesting to compare our analysis by varying certain parameters with these studies.

ISSN No:-2456-2165

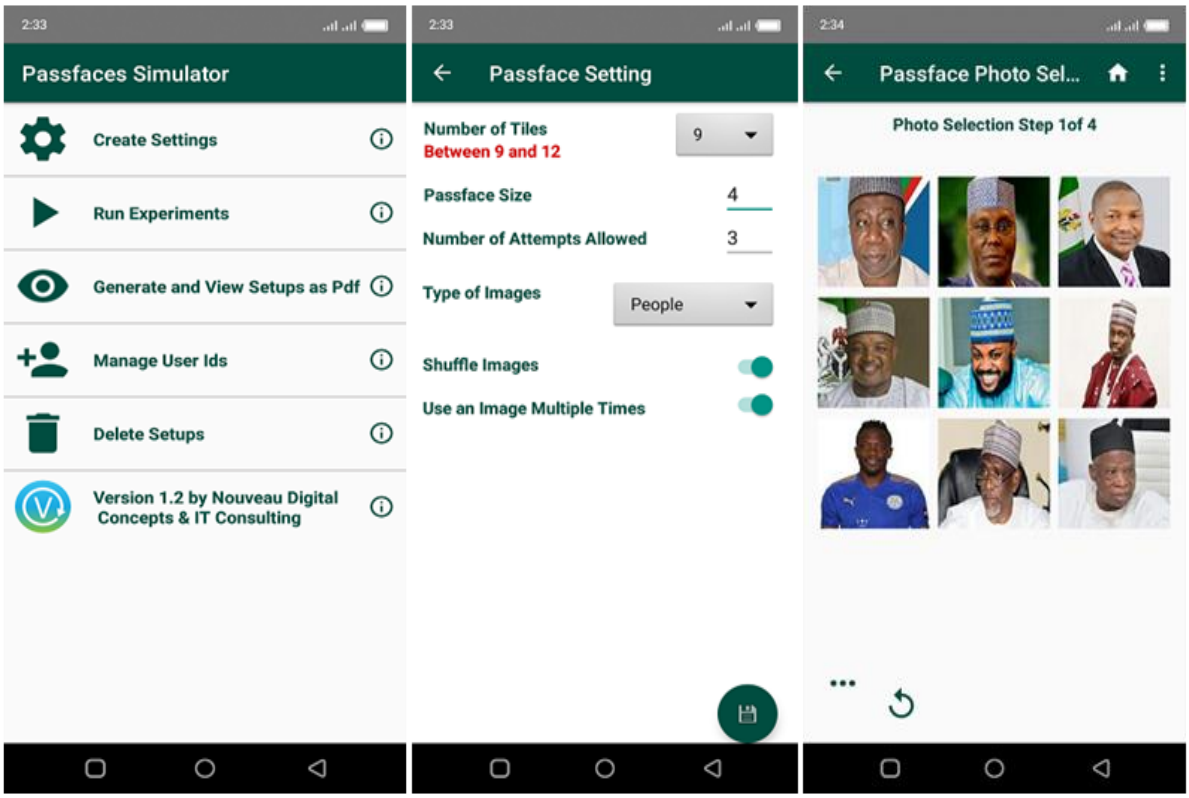
Concerning the Passfaces, it is interesting to analyze a mechanism on which few studies have been carried out. In addition, it will help to find out if Passfaces could replace the legacy authentication mechanisms like PIN code and password, the possible attacks on it, and how to improve its security while maintaining an acceptable level of usability. It will be good to see if it is possible to use images other than faces. Images of pets, natural sites, and favorite fruits could have similar remembrance as human faces. We will use the app to find out.

It should be noted that new authentication mechanisms are emerging such as authentication via voice (voice biometrics). Another form of authentication is the implicit authentication that can be used to create two factor authentication scheme [3, 15]. It is a kind of behavioural biometrics that allows for securing a smart-phone by how the user picks his/her phone, for example.

III. MATERIALS AND METHOD

➢ *Passfaces android app*

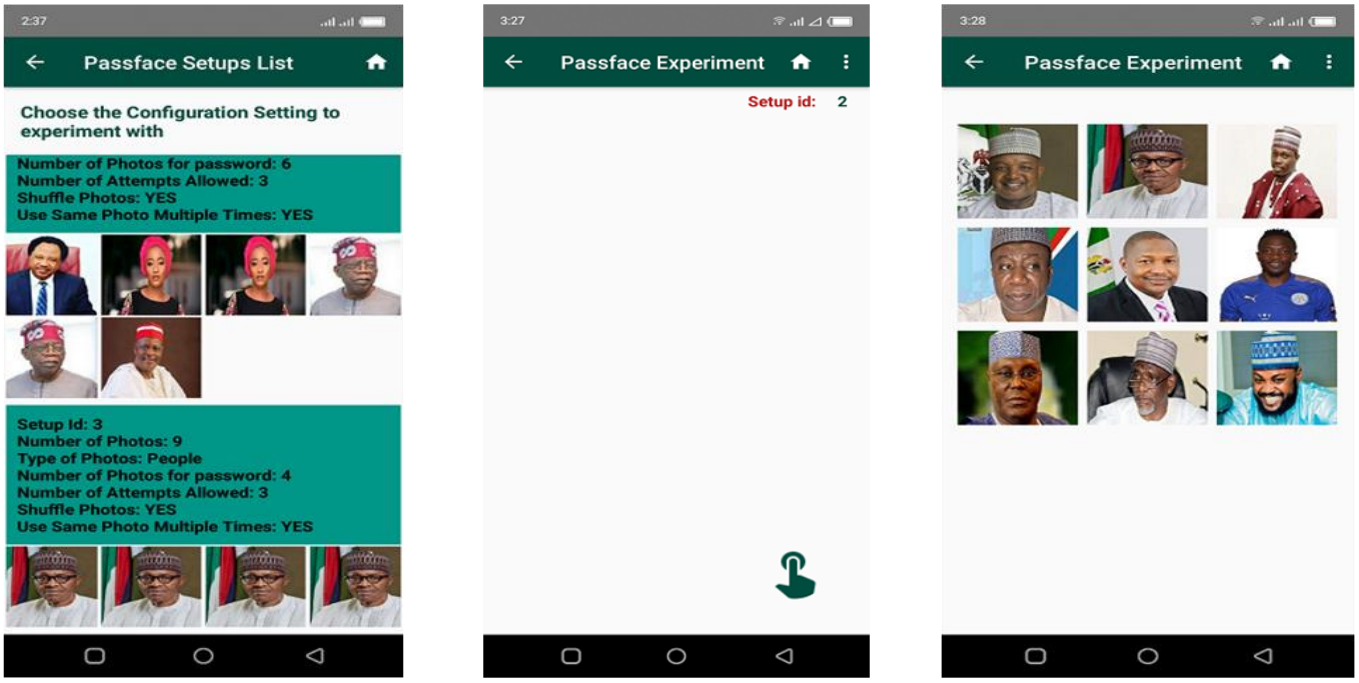
For the purpose of experimenting with the new technology, we have developed a special android app that mimics the Passfaces technology. The app allows the experimenter to create setups with varying parameters and run experiments with the setups created. Refer to Figures 2 and 3 for the various screens of the app.



(a) (b) (c)

Fig 2:- (a) The main screen of the app with tabs to perform different task, (b) this is the experiment configuration creation screen. It allows for specifying the various parameters for a particular setup configuration. (c) Picture selection screen for a given setup configuration.

ISSN No:-2456-2165



(a) (b) (c)

Fig 3:- (a) List of experiment setups that the user has created, (b) Start Passfaces experiment screen with the selected setup (c) List of Passfaces pictures displayed for the user to select while experimenting.

The app records the user activities during an experiment saves them on the phones memory as a comma separated values (CSV) file. The information it records comprises the duration for an experiment, success status, number of retries (if any), and the kinds of pictures the user selected. After the completion of the experiments, we retrieved the CSV file for analysis.

➢ *Creating setups for experiments*

The app we have created allows an experimenter to create as many setups as needed. We intended to vary the different parameters so the app is developed in a way it allows that (see Figure 2 (b)). The parameters are number of tiles, size of the Passfaces, number of attempts allowed, and whether a user can use the same picture more once. The number of tiles determines how many pictures are displayed. The only options are 9 and 12 tiles. 9 tiles means the app displays 9 pictures on a 3 x 3 grid. 12 tiles give 4 x 4 grid of 12 pictures. The size of Passfaces gives the number of pictures that make up a Passfaces password. Number of attempts gives how many retries are allowed before app blocks a user in the event of wrong pictures selection by the user during experiment. The minimum is 3 retries. The shuffle images option, if enabled, rearranges images on the grid. This can improve the security of the Passfaces scheme. This option is enabled by default but can be disabled if needed. The option, use the same image/picture multiple times, is enabled by default but can be disabled. It lets us compose Passfaces password with one picture. This has effect on the security and usability of the Passfaces scheme. Initially, Passfaces technology permits the use of facial images as password. We indented to extend the type of pictures so that we use non-facial images to verify its usability.

We can create several configuration setups. In this work, we have created 234 configuration setups.

The app was developed with preloaded pictures. They comprise facial images of prominent personalities such as politicians, leaders, and footballers.

➢ *User recruitment*

The users' recruitment process was done via our contact list on social media such Facebook, WhatsApp, and Instagram. The users were put to groups of 20 people. We select a group and run the experiment with the members in the group before going to the next group. We created the configuration setups and asked the volunteers to select the pictures of their choice to make up the Passfaces password and requested them to try and remember those pictures they have chosen. 3 days after the creation of configuration setups for a group, we run the experiment for a particular group. Before starting an experiment, we displayed on the phone the set of pictures the user had selected for his/her Passfaces password as a brief reminder and then begin the experiment instantly.

The size of Passfaces graphical passwords, in this experiment, can be 4, 5, 6, or 8. Table 1 gives the number of volunteered users per Passfaces size. We have a total of 232 volunteers.

ISSN No:-2456-2165

Passfaces size	#Users
4	80
5	35
6	74
8	43
Total	**232**

Table 1:- Number of Volunteered Users

As can be seen on Table 1, configuration setup with 4 pictures is the highest with 80 users. The least is the setups with size 5.

IV. RESULTS

It took us 3 months (between 5th July and 10th October 2022) to finish the experiment with the volunteers. The ease with which users authenticate with the Passfaces authentication mechanism is manifested in the time taken to authenticate and the number of retries (attempts) a user had to make before succeeding. Table 2 gives average time taken authenticate a user.

Passfaces size	Average Time (s)
4	15.69
5	20.49
6	17.86
8	46.74

Table 2:- Average authentication time

On the possible error rates during authentication, we the app has captured this information so that it facilitates analysis. Table 3 and Figure 4 summarize the error rates for all the 4 Passfaces sizes.

Attempt	4 Pictures	5 Pictures	6 Pictures	8 Pictures	Percentage
First	71	27	60	28	80.17
Second	3	3	9	6	9.05
Third	3	0	1	1	2.16
unsuccessful	3	5	4	8	8.62
Total	80	35	74	43	100.00

Table 3:- Users' successes per authentication attempt

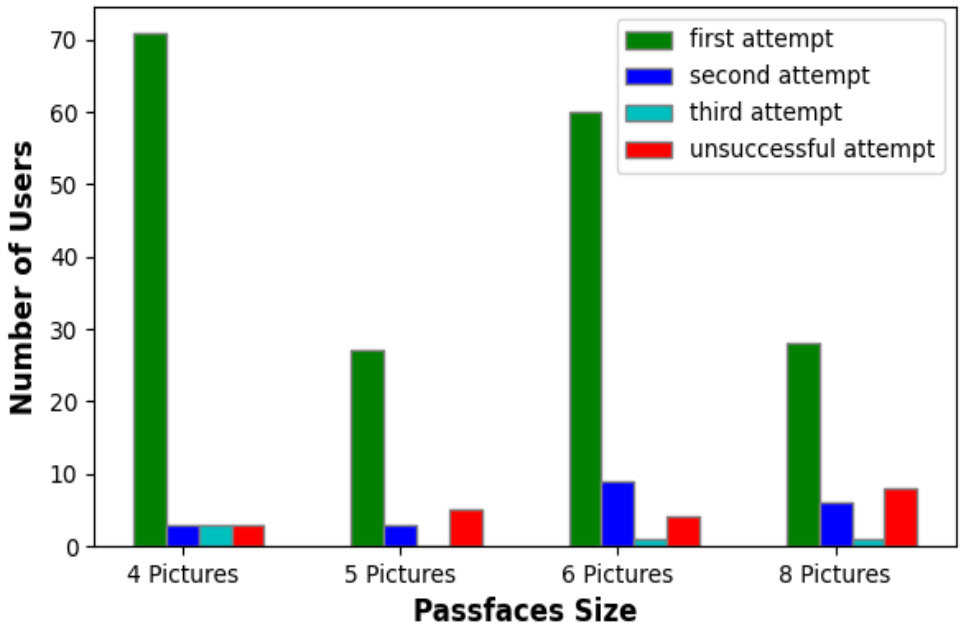


Fig 4:- Distribution of users with regards to the number of pictures that make up Passfaces password and the status of authentication attempts (success in first attempt, second attempt, third attempt, or unsuccessful)

ISSN No:-2456-2165

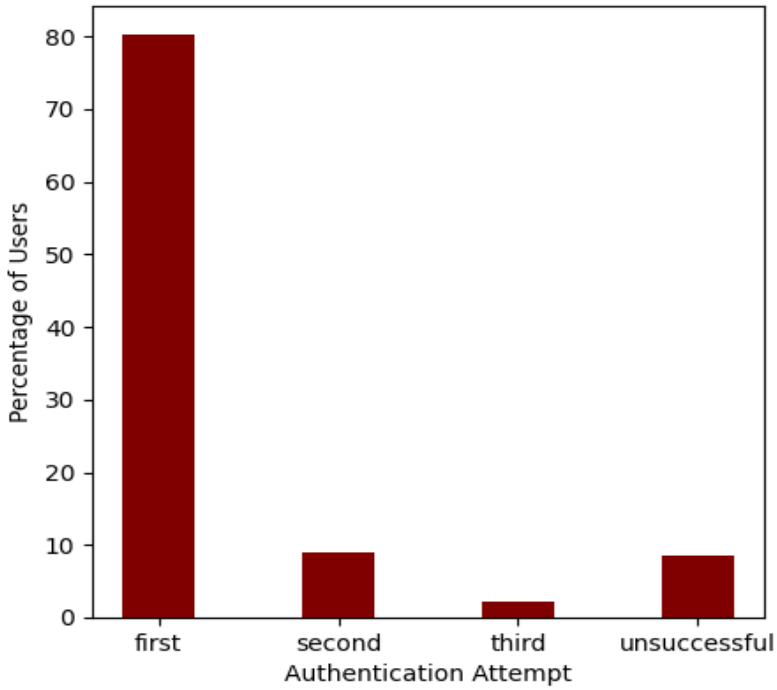


Fig 5:- Three retries were allowed for each user during authentication process. 4 types of authentication statuses; first, second, and third represent the percentages of users that were able to authenticate within first attempt, second attempt, and third attempt respectively. The unsuccessful category indicates those that could not authenticate in the third attempt.

V. DISCUSSION

We have run 232 experiments with the volunteer users. We can see that the average time to unlock a phone varies with the size of the graphical password as shown in Table 2. The time tends to increase with the increase in the size of Passfaces password. The users' recognition speed may be affected with an increase in the number of pictures to be selected. But this may not be totally true because, from Table 2, the average unlock time for Passfaces password of size 5 and 6 were 20.49s and 17.89s respectively. This may be due to difference in the individual recognition speed; some people can recognize quickly the pictures they have chosen while others take a little bit of time.

On the issue of errors during authentication experiments, we can see from Table 3 and Figure 4 that the number of retries increases with the size of Passfaces password. This is normal because as the size of the password increases, people tend to make mistakes selecting the right pictures. However, majority of them succeed in the second or third retries. Only few of them could not succeed even in the third retry.

More so, we notice from Figure 5 about 80% of the entire users were able to authenticate within the first attempt. Only about 10% and 3% could authenticate in the second and third attempts, respectively. Also just about 8% could not authenticate completely.

Though the average authentication time for different Passfaces sizes was a bit high, the percentage of successful authentication attempts can be an indication of the user-friendliness of the scheme.

The different parameters that this scheme provides can provide resistance to some form of attacks. For example shuffling pictures during authentication will counter smudge attack in which the attacker tries to infer the password from the traces the user's finger left on the phone [16]. It can also counter shoulder surfing attack [17] in which the attacker peeps through the victim's shoulder in order to get the password. This is possible because, with the shuffling of the pictures, the display of the pictures is random each time the user authenticates; no definite order. Also, limiting the maximum number of attempts to 3 counters brute force attack.

VI. CONCLUSION

In this work, we have studied Passfaces technology that can serve as a two-factor authentication scheme on android devices. The results revealed that the scheme is highly usable. As future work, the security of the scheme needs to be thoroughly investigated.

REFERENCES

[1]. H. Khan, U. Hengartner, and D. Vogel, "Usability and Security Perceptions of Implicit Authentication: Convenient, Secure, Sometimes Annoying," presented at the Symposium on Usable Privacy and Security (SOUPS), Ottawa Canada, 2015.

[2]. W. H. Lee, X. Liu, Y. Shen, H. Jin, and R. B. Lee, "Secure Pick Up: Implicit Authentication When You Start Using the Smartphone," presented at the SACMAT'17, Indianapolis, IN, USA, 2017.

[3]. Kohlmayer, Prasser, and Kuhn, "The cost of quality : Implementing Generalization and Suppression for Anonymizing Biomedical Data With Minimal Information Loss," *Journal of Biomedical Informatics*, vol. 58, pp. 37-48, Sep. 2015.
[4]. Prasser, Kohlmayer, and Kuhn, "The Importance of Context: Risk-based De-identification of Biomedical Data," *Methods of Information in Medicine*, vol. 55, pp. 347-355, 2016.
[5]. E. Hjelmas and B. K. Low, "Face Detection: A Survey," *Computer Vision and Image Understanding*, pp. 236–274, 2001.
[6]. K. Bonsor and R. Johnson. (2022, 15/06/2022). *How Facial Recognition Systems Work*. Available: https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm
[7]. S. Liu and M. Silverman, "A Practical Guide to Biometric Security Technology," *IT Pro*, pp. 27-32, February 2001 2001.
[8]. X. Jiang, "Fingerprint Classification," in *Encyclopedia of Biometrics*, A. Maraikayar, Ed., ed: Springer-Verlag Berlin Heidelberg, 2009, pp. 439-446.
[9]. S. C. Dass and A. K. Jain, "Fingerprint-Based Recognition," *Technometrics*, vol. 49, pp. 262-276, 2007.
[10]. DigitalPersona. (2009, Best Practices for Implementing Fingerprint Biometrics in Applications. *Digitalpersona Camera Manual*.
[11]. Neurotechnology. (2022, 15/05/2022). *Neurotechnology Company Brochure*. Available: https://download.neurotechnology.com/Neurotechnology_Brochure_2022-02-17.pdf
[12]. V. A. Sujan and M. P. Mulqueen, "Fingerprint identification using space invariant transforms," *Pattern Recognition Letters* pp. 609 – 619, 2002.
[13]. C. H. Park and H. Park, "Fingerprint classification using fastFourier transform and nonlinear discriminant analysis," *Pattern Recognition*, pp. 495–503, 2005.
[14]. M. Harbach, A. D. Luca, and S. Egelman, "The Anatomy of Smartphone Unlocking A Field Study of Android Lock Screens," presented at the CHI 2016, San Jose, CA, USA, 2016.
[15]. H. Khan, U. Hengartner, and D. Vogel, "Usability and Security Perceptions of Implicit Authentication: Convenient, Secure, Sometimes Annoying," in *Symposium on Usable Privacy and Security (SOUPS)*, Ottawa, Canada., 2015.
[16]. J. Zheng and S. K. Chigurupati, "M-Pattern: A novel scheme for improving the security of Android Pattern unlock against smudge attacks," *ICT Express*, vol. 5, pp. 192-195, 2019.
[17]. F. Binbeshr, M. L. Mat, K. Lip, Y. Por, and A. A. Zaidan, "A systematic review of PIN-entry methods resistant to shoulder-surfing attacks," *Computers & Security*, vol. 101, p. 102116, 2020.