IDC School of Design अभिकल्प विद्यालय

IIT Bombay

Graphical Passwords for Emergent Users

A Comparative Study on PIN and Graphical passwords using faces that are Familiar and Unknown.

Guide: Prof. Anirudha Joshi

Zuha Asif P

216330014

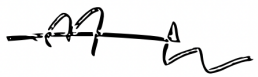
M.Des Interaction Design

Project Approval

The Project Titled “Graphical Passwords for Emergent Users: A comparative study between Pin and Graphical Passwords Known and Unknown Faces” by Zuha Asif P is approved for partial fulfillment of the requirement for the degree of ‘Master of Design’ in Interaction Design at Industrial Design Centre, Indian Institute of Technology, Bombay.

Guide:
Anirudha Joshi

Chairperson:
Bharat Parmar



Internal Examiner:
Venkatesh Rajamanickam

External Examiner:
Abhishek Shrivastava

Declaration

I declare that this written document represents my ideas in my own words and where others' ideas or phrases have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea, data, fact, or source in my submission. I understand that any violation of the above will be cause for disciplinary action by the institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Zuha Asif P

216330014

Interaction Design

IDC School of Design, IIT Bombay.

Acknowledgment

I would like to extend my heartfelt gratitude and appreciation to Professor Anirudha Joshi for his invaluable guidance, support, and mentorship during the course of my research project. His expertise, insightful feedback, and unwavering encouragement have played a pivotal role in shaping the direction and enhancing the quality of this study. I am immensely grateful for his dedication and commitment to my academic and personal growth.

I would also like to express my sincere thanks to all the faculty members in the Interaction Design department and my classmates for their valuable input and constructive discussions throughout the design process. Their perspectives and contributions have been invaluable in refining and strengthening the outcomes of this research.

I am also indebted to Ujjual Mahajan for her assistance with data collection. Her support and collaboration have been indispensable in conducting the study and collecting the necessary data. Lastly, I would like to express my deepest appreciation to my family and friends for their unwavering support and encouragement.

Zuha Asif P

Abstract

Numerical passwords (or PINs) are a commonly used "what you know" password mechanism. However, numbers could be difficult to remember, and particularly for emergent users. Graphical passwords, and especially Passfaces (passwords based on human faces) could be an alternative, as we humans remember and recognise other human faces easily. Further, we posit that if these human faces happen to be of well-known personalities (such as celebrities), these should be even easier to remember. In this paper, we present a within-subjects, counterbalanced, longitudinal study with 30 emergent users that systematically compares the performance of PINs with Passfaces of two types, one composed of unknown people (Passfaces for short) and Passfaces based on celebrities (Celebrities for short). Passfaces and Celebrities had a larger password space by design (and hence, arguably, were more secure) than PINs. Users were asked to memorise each password, and recall the same aftersubsequent intervals. The analysis of the results showed that PINs and Graphical passwords were not significantly different in terms of memorabiity.

Although graphical passwords have been explored a lot before, the motive of the study is to find their significance in this particular user group. The limitations of this study are also described in this paper along with a revised protocol for the next study based on the analysis of the current results and field experience.

Table of Contents

1. Introduction

In the last few years, researchers have referred to user groups from developing countries as emergent users. Such user groups are either less educated, economically disadvantaged, geographically dispersed, or have a culturally heterogeneous background. Millions of people in the developing world own mobile phones and large proportions of users have access to smartphones, owing to the availability of low-cost smartphones. It has been argued that emergent users, especially illiterate users, find it difficult to use text-based features on phones. Nonetheless, ensuring privacy and security remains a critical concern that must be upheld under any circumstance.

Creating and recalling a robust alphanumeric password can be an arduous task, even for younger individuals. This challenge is even more pronounced for emergent users, for whom text entry can be difficult. Unfortunately, the current system does not account for the unique challenges faced by this user group in India, where there is a broad diversity of languages and cultures. Though numerous studies have compared graphical passwords to PINS and alphanumeric passwords, these studies have not been conducted in the Indian context for this particular user group.

The focus user group of emergent users is prone to delegation of password setting and login tasks and to sharing of devices making them vulnerable to digital theft. To strengthen usability, Graphical-based password mechanisms have been widely explored.

According to A systematic literature review of graphical passwords, the different types of graphical passwords are:

- Recognition Based: Cognometrics/ Search Metrics
  In this, the user selects a no. of images and during authentication, they should identify them from a set of other images
- Recall Based:
  Draws or Selects a drawing and reproduces same on a grid
- Cue Recall Based: Locimetric Schemes
  Chooses password click points by selecting any specific region in the image. The user should click in the correct order
- Hybrid: Combination of one or more GPS

(Brostoff & Sasse, 2000) Proposed the Recognition-based method, which is used by the Passfaces scheme. This method is based on the observation that humans tend to remember faces with ease. In Passfaces, users select pre-selected faces from a grid to authenticate themselves, and multiple authentication rounds are used. However, Passfaces has some drawbacks, including biases towards certain faces and vulnerability to shoulder surfing attacks.

The difficulty of writing down or verbally disclosing graphical passwords is one of the major advantages of graphical passwords in terms of security.

However, like any password scheme, graphical passwords are vulnerable to various types of attacks such as shoulder surfing, brute force, social engineering, and dictionary attacks. Shoulder surfing, which involves observing someone entering their password, is particularly common in recognition-based graphical password schemes. Meanwhile, brute force attacks rely on a trial-and-error approach, while social engineering attacks manipulate people's behavior to gain access to their passwords. Finally, dictionary attacks involve systematically trying possible words or points to break into a system.

A systematic literature review of graphical passwords found that shoulder surfing attacks are more likely to succeed with pass faces if the location of the corpus of photos is not shuffled. However, brute force, social engineering, and dictionary attacks are less effective against graphical passwords compared to other forms of authentication.

2. Literature review

2.1 Password security

The types of passwords that are most easily cracked are the account holder's name, words from the dictionary, numbers related to personal information and permuted words, and a combination of all of these. (M. Bishop and D. V. Klein, 1995) These passwords can be written down and stored as well. A third person first tries to logically associate the date of birth and other numbers related to personal information as their first guess.

In addition to logical guessing, there are other types of attacks that can compromise password security, such as shoulder surfing. This type of attack involves a malicious user skillfully observing another user as they enter their password. To mitigate this risk, the layout of the password entry interface can be randomized to make it more difficult for attackers to predict the user's inputs.

In a study conducted by Kirkwood et al. (2022), the usability and security implications of randomizing the layout of a PIN entry keypad were evaluated. The results indicated that randomizing the numbers on the keypad significantly reduces the risk of shoulder surfing and thermal attacks, with no substantial impact on usability. While the randomized layout had a minor effect on entry accuracy, it was found to increase entry time compared to the standard keypad layout.

Markert et al. (2021) conducted a comprehensive analysis of the security of smartphone unlock PINs. The study was based on the analysis of over 80,000 smartphone PINs collected from participants through a user study. The study analyzed the distribution and strength of PINs, the impact of different factors such as demographics and device type on PIN selection, and the effectiveness of different PIN guessing attacks. The results of the study show that a significant number of users select weak and predictable PINs and that factors such as age, gender, and device type have a significant impact on PIN selection. The study also found that PIN guessing attacks can be highly effective, with over 40% success rate in some cases. The study concludes with recommendations for improving PIN security, including the use of longer and more complex PINs, and the implementation of mechanisms to prevent brute-force attacks. The study shows that using six-digit PINs instead of four-digit PINs provides little to no increase in security and surprisingly may even decrease security.

2.2 Related Works

According to a study by Coventry, et al. (2014), the use of multiple image-based passwords has been shown to increase security against guessing attacks while maintaining good usability. In this study, participants were asked to create and recall multiple passwords based on sets of images. The results showed that users were able to successfully recall a high percentage of their passwords and preferred the image-based

system over traditional text-based passwords. The study suggests that using multiple image-based passwords could be a viable alternative to traditional password systems.

De Angeli et al. investigated the usability and security of pictorial passwords compared to PINs in their paper "Usability and User Authentication: Pictorial passwords vs. PIN." They found that humans struggle to remember meaningless strings, and after a week's interval, pictures were less error-prone than numbers without compromising the speed of the transaction. Participants reacted positively to the Visual Identification Protocol (VIP) concept, perceiving it as more secure and easier to remember than PINs. However, the study also revealed that VIP's usability can be easily disrupted by inappropriate solutions, and the results need to take into account the novelty factors of VIP.

The paper compares picture passwords such as flowers, food, etc. against pins. VIP was found to be easier to remember and preferred by users, but its usability can be easily disrupted by an inappropriate solution.

In a separate study, Brostoff (2003) compared Passfaces to traditional passwords in a field trial involving 34 student participants over three months. Passfaces had fewer login errors than passwords, even when the intervals between logins were long. However, the Passfaces scheme took a longer time to execute on the computer facilities regularly chosen by the participants.

In the paper "Graphical Password Authentication Using Cued Click Points: A Usability Analysis" by Biddle, Chiasson, and Van Oorschot (2012), the systems of the cued click points (CCP) graphical password scheme is evaluated. The usability analysis reveals several advantages of CCP compared to traditional alphanumeric passwords. CCP was found to be more memorable and efficient, offering an intuitive way for users to authenticate themselves. The graphical nature of CCP allows users to visually identify click points on a selected image, making it easier to remember and reproduce their password. This advantage contributes to improved user experience and potentially reduces the risk of forgotten passwords or the need to write them down.

In the paper "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System" by Wiedenbeck et al. (2005), the benefits of the PassPoints graphical password system are examined. The longitudinal evaluation demonstrates that PassPoints offers enhanced usability and security. Users were able to successfully authenticate using PassPoints over a password-based system. The system's usability benefits contribute to improved user satisfaction and potentially reduce the risk of password-related issues, such as forgotten or easily guessed passwords.

Thorpe and Van Oorschot (2015) investigate user choice in graphical passwords in their paper "An Empirical Investigation of User Choice in Graphical Passwords." The study highlights the advantages of user-centered design in graphical password systems. By analyzing data from a large-scale online survey, the authors identify the factors influencing users' choices of graphical passwords. The findings reveal that users prefer graphical passwords with certain characteristics, such as

familiarity, simplicity, and ease of memorization. Understanding these user preferences allows for the design of graphical password systems that align with users' mental models and increase their overall satisfaction and engagement with the authentication process.

In the paper "The Emperor's New Security Mechanism: A Graphical Password Generator" by Dunphy, Yan, and McBurney (2008), the advantages of a graphical password generator based on user-selected images are discussed. The proposed approach offers usability and security benefits. Users have the freedom to choose images that are meaningful to them, increasing the likelihood of password memorability. Additionally, the ability to create passwords by drawing shapes on selected images provides an intuitive and personalized method of authentication. The usability advantages of this approach contribute to improved user experiences and potentially reduce reliance on written passwords or the use of easily guessable alternatives.

The survey paper "Graphical Passwords" by Sobrado and Birget (2008) provides an overview of various graphical password schemes and their advantages. The authors summarize the benefits of graphical passwords, including increased memorability compared to alphanumeric passwords, resistance to shoulder surfing attacks, and improved user experience due to the visual nature of authentication. By highlighting the advantages of different graphical password techniques, the paper serves as a resource for researchers and practitioners interested in leveraging graphical passwords for enhanced security and usability.

Overall, these papers demonstrate the advantages of graphical passwords, such as improved memorability, enhanced user experience, resistance to certain types of attacks, and the potential for increased security compared to traditional alphanumeric passwords.

3. Study Details

3.1 Research Question

This experiment specifically targets to compare Passfaces with Pin. The research questions are:

1. Which password input method among Pin, Passfaces, and Passfaces with Celebrities is easier to recall over a given period of time?
2. Is there any significant difference between Passfaces with Celebrities and unknown faces?

In order to come up with a conclusion, the parameters that are measured are:

To determine if there is a significant difference between using Passfaces with celebrities and using a pin, appropriate statistical tests need to be conducted.

3.2 Hypothesis

Specific hypotheses with respect to multiple password input methods were as follows:

1. There is no significant difference between the recall of Pin and Graphical Passwords.
2. Graphical Passwords (Passfaces) are more secure than Pin passwords.
3. There is no significant difference between usability in terms of time taken for Pin and Graphical Passwords.

3.3 Variables

The scope of this study is to find out which among Pin, Passfaces unknown, and Passfaces with celebrities is easier to recall over a given period of time.

3.3.1 The variables used in this study

The different types of variables that should are accounted for, in the study are as below:

1. Independent Variables (Manipulated variable)
    a. Password type: Pin, Passfaces, Passfaces with celebrities

2. Dependent Variables (Response variable)
    a. Success of setting up password
    b. Time is taken by each participant for each attempt
    c. The number of errors in case of failure
3. Control Variables
    a. Grid size: 4*4
    b. Password length: 4
    c. Corpus of photos: Fixed
    d. The number of passwords at a time
    e. Feedback for incorrect selection of passwords
    f. Controlled use of photos
    g. The sequence of photos selection: Fixed

    h. Photo location: Fixed
4. Random Variables
    a. Phone: The study is carried out on the user's phone

4. Prototype

The prototypes were coded in Figma and hosted on Useberry. It allows users to record time, view the user's clicks, and also provide heatmaps of selection, providing metrics that indicate the completion of tasks. It also gives user flows which give a visualization of the path a user follows from one screen to the next. This helps in discovering how users behave and which screens they are on when they decide to leave. The prototype was modified twice based on the results from pre-pilot and pilot studies.

4.1 Pre-Pilot

A pre-pilot study was conducted before conducting the actual study. This was conducted on 7 users for graphical passwords with unknown faces to test if the users are able to follow through with the suggested prototype. For the mock-up prototype, 3*3 grids of foreign faces were used as shown in Fig. 3.

It was found that most of the participants tried to associate the faces with people they have seen before. Even though the faces were non-Indian, they tried to associate certain features to that of their family members, celebrities, etc. to remember. Thus, it was decided to use only Indian faces. So that the participants can relate more.

The grid size was changed to 5*5 for the pilot as the password space is very low when compared to that of Pin.

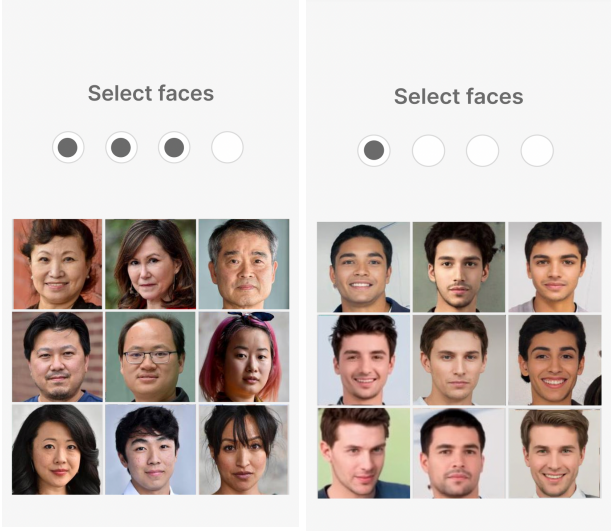


Fig.1 Mock-up prototype of pre-pilot for unknown faces

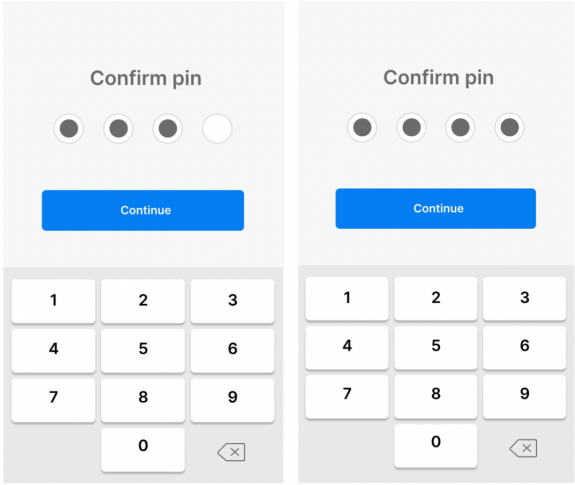


Fig.2 Mock-up prototype of pre-pilot for Pin

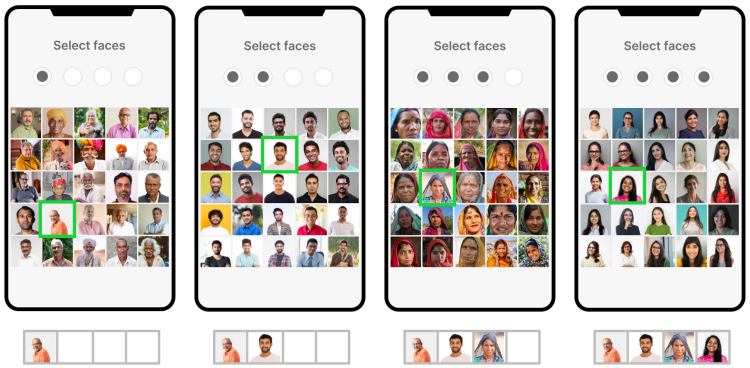


Fig.3 Prototype flow for Passfaces - unknown

Fig.4 Prototype flow for Passfaces - Celebrities

4.2 Pilot

According to the observations made from the pre-pilot study, the pilot prototype was changed into Indian faces, and the grid size was made 5*5.

4.2.1 Passfaces with Unknown Faces

This prototype contains Indian faces classified into different categories as shown in Fig. 3. For example, for the first password entry, the section is elder men - which has a set of 25 pictures of elder Indian faces, which look more or less similar in terms of attire, age, region, etc. The second section includes young men and the third includes elderly women and the last section includes young Indian working women.

The prototype was classified into different sections in order to reduce biases towards any particular gender, section, or type. For example, one may choose only younger ladies or a particular age group in all the sections based on their interests. Which in turn might help a third person to guess them easily.

4.1.2 Passfaces with celebrity faces

The corpus for Passfaces with celebrities was made by a random selection of celebrities from the Film Industry all over India, Cricketers and other famous sports personalities, Politicians, artists from local shows, etc.

The familiarity matrix of these celebrities is already taken from a previous study conducted by a former student in IDC.

4.1.3 Pin

The interface for setting up the pin was the same as that of the pre-pilot test where the user can enter a 4-digit pin in the number pad and continue.

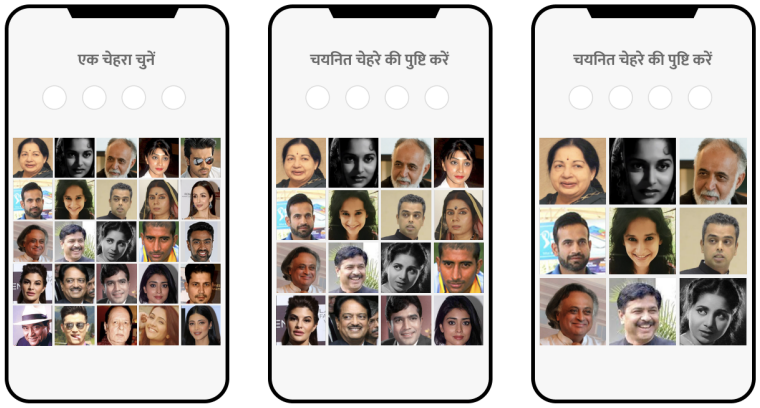


Fig.6 Different types of grid sizes that are compatible with mobile devices

4.2 Modifications in Prototype based on the findings

The Pilot study was conducted on a 5*5 grid with password length 4 which has a password space of 3,90,625 (25^4) against a 4-digit pin which has a password space of 10,000 (10^4).

It was found that some of the users found it difficult to see 25 images on one screen distinctly. Considering the visibility issues, the revised prototype is a 4*4 grid with a password length of 4 which has a password space of 65,536(16^4) against a 4-digit pin.

The different grid sizes that are possible for emergent users to see distinctly are shown in Fig. above.

Expert Jury also suggested that the touch targets for both Pin and graphical passwords should be more or less equal.

4.3 Revised Prototype

4.3.1 Grid size

The grid size was changed from 5*5 to 4*4 from the insights gathered from the pilot test. The password space of a (4*4) grid structure with a password length of 4 is 65,536. Which accounts for a guessability of 1/65,536. This is compared against a 4-digit Pin of password space 10,000.

4.3.2 Touch Targets

In order to make the touch targets of both Pin and Graphical passwords, only the center portion of the square grid was made interactive. The size of the interactive portion was made equal to that of the Pin as shown in Fig. 7.

Fig.7 Touch targets for Graphical Passwords and Pin

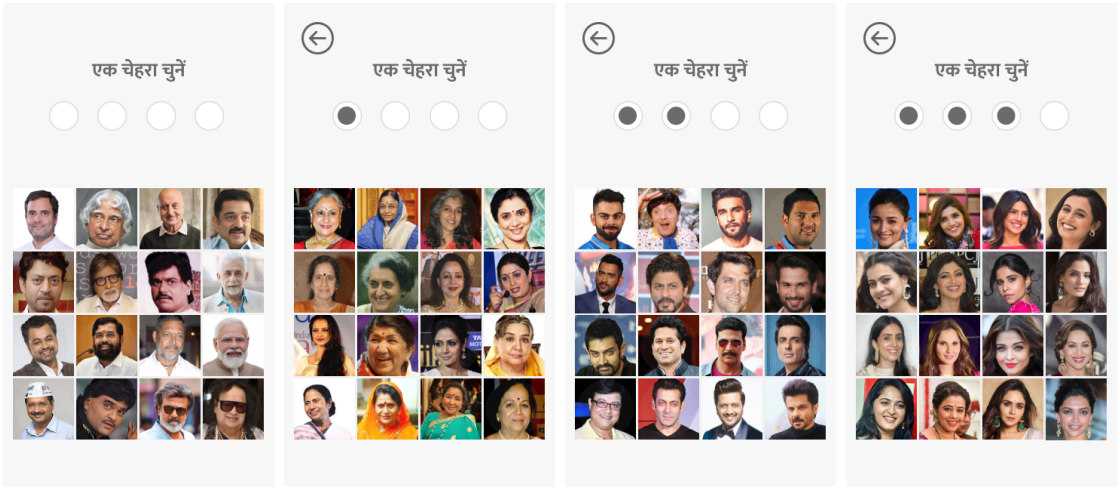


Fig.7 Prototype for Passfaces with Celebrities

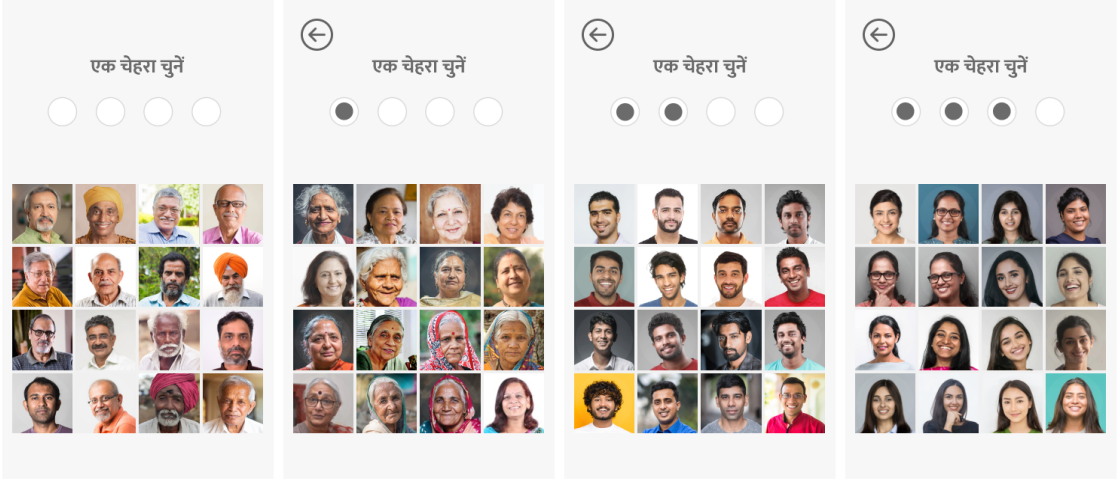


Fig.8 Prototype for Passfaces with Unknown Faces

4.3.3 Passfaces with Unknown Faces

Based on the Pilot results, certain faces were replaced which had very distinct features depending on the frequency of selection. The grid size was also changed to 4*4 and the different sections are slightly modified to Elder Men, Young Men, Elder Ladies, and young ladies. The updated prototype is shown in Fig. 7.

4.3.4 Passfaces with Celebrities

During the pilot study, a corpus of celebrity faces was utilized without any specific classification based on sections. The selection of celebrity images was random and included a mix of highly popular and less popular celebrities. However, this random distribution led to a bias in participant choices, with individuals tending to select celebrities from specific categories such as politicians or Bollywood actors across all four sections. To address this issue, a classification system was implemented to categorize celebrities based on factors like age and gender.

Additionally, the pilot study revealed that only a small number of celebrities were universally recognized by participants, while the majority of the celebrities were not familiar to them. This finding mirrored the results observed for unknown faces. The lack of recognition was attributed to the diverse regional backgrounds of the celebrities in the corpus, which did not align well with the participants who were primarily from Maharashtra. To improve the familiarity and identification of celebrities, future iterations of the study incorporated local Marathi celebrities to ensure a more relevant and recognizable set of faces for the participants.

The final prototype for Passfaces with Celebrities is shown in Fig. 8.

5. Pilot

5.1 Participant Recruitment

A pilot was conducted with 10 users. The user groups are workers of the IIT Bombay campus and ladies from an NGO who are illiterate and starting to use phones and learning how to read, write and type in Marathi. Some of them own a smartphone whereas the others own a feature phone. Out of the 10 users, 4 are male and 6 are female.

5.2 Study

They were first briefed about what a password is and its importance. They were also asked to set up a password which they have to remember after a certain period of time.
The users were asked to set up a 4-digit pin and confirm it. Since some of the users already use a phone or a Bank account where pins could be used, they were asked to set up a pin that they have not used before. After this, they were asked to set up a graphical password with unknown faces in a 5 by 5 grid. The same process was repeated for celebrity-involved faces.

5.1 Pilot Results

5.1.1 Success Rates

1 out of the 10 users found it difficult to set up a pin, as numbers did not make much sense to her. Almost everyone was able to select a face as a password which, they thought they could remember. The setup was completely successful in terms of graphical passwords except, for one user who found it difficult to see clearly the images in a 5*5 grid. It was also found that as the time of recall increases the success rate decreased for all three cases.

Fig.9 Pilot study with students of Asha NGO

	PIN			Passfaces Unknown			Passfaces Celebrities		
Users	Success of setting up	Recall 1: 2 days	Recall 2: 1 week	Success of setting up	Recall 1: 2 days	Recall 2: 1 week	Success of setting up	Recall 1: 2 days	Recall 2: 1 week
User 1	Success	Success	Success	Success	Failure	Failure	Success	Success	Success
User 2	Success	Success	Success	Success	Failure	Success	Success	Success	Success
User 3	Success	Success	Success	Success	Success	Success	Success	Success	Failure
User 4	Success	Success	Success	Success	Failure	Failure	Success	Success	Failure
User 5	Success	Success	Failure	Success	Success	Failure	Success	Success	Success
User 6	Success	Failure	Failure	Success	Failure	Failure	Success	Failure	Success
User 7	Success	Success	Failure	Success	Success	Success	Failure	Failure	Failure
User 8	Failure	Failure	Failure	Success	Failure	Failure	Success	Failure	Failure
User 9	Success	Success	Success	Success	Success	Success	Success	Success	Success
User 10	Success	Success	Success	Success	Success	Success	Success	Success	Success
Total	**90%**	**80.00%**	**60%**	**100%**	**50%**	**50%**	**90%**	**70%**	**60%**

Fig.10 Success Rates of 3 cases in pilot study

5.1.2 Average Time

The average time that is taken to set up a pin and confirm it was 67.16 seconds with a 90% success rate. The average time to set up passfaces was 93.1s with a 100% success rate. Whereas the average time taken for celebrity faces was 85.77s with a 90% success rate.

Passfaces was 93.1s with a 100% success rate. Whereas the average time taken for celebrity faces was 85.77s with a 90% success rate.

It is noted from the above observations that the average time taken to set up and confirm celebrity Passfaces is lesser than unknown faces. This can be due to familiarity with faces rather than looking for distinct features to identify or differentiate. Some users found it difficult to see the images properly due to the size of a 5*5 grid.

Users	Time Taken to set up and confirm pin		
	PIN	Passfaces Unknown	Passfaces Celebrities
User 1	23	85.9	89.5
User 2	17	63.3	45.1
User 3	57.7	73.8	123.3
User 4	21.5	74.7	78.1
User 5	87.1	82.2	70.8
User 6	114.4	88.4	86.8
User 7	150.4	125.5	-
User 8	-	155.5	131.5
User 9	98.3	146.6	95
User 10	35.1	35.4	51.9
Average	**67.16666667**	**93.13**	**85.77777778**

Fig.11 Time taken to set up and confirm in pilot study

However, conclusions cannot be drawn based on a sample of only 10 users, thus it is necessary to expand the study to include at least 30 users in order to obtain more accurate results.

5.2 Initial Findings

- Some of the users had difficulty selecting an image from a corpus of 25 images, as the images were too small for them to select from easily.
- Users who are literate and already use PINs tend to create a password associated with important dates or events in their lives, making it easier for them to remember.
- The prototype used in the study did not specifically feature Marathi local actors, which was a shortcoming given that the study participants were from Maharashtra.

The corpus included celebrities from all over India, which led to some users being unable to identify familiar faces.

- For the unknown faces, 20% of users chose images based on location rather than attempting to find distinct users, leading to setup failure if the location of photos were shuffled. However, for the celebrity faces, none of the users chose based on location.
- One user in the study used photos to save all their important contacts on their phone, allowing them to identify contacts by image rather than having to read their names. This concept is similar to using graphical passwords for unlocking

6. Final Study

6.1 Participant Recruitment

For the study, a total of 39 participants were recruited. The participants belonged to the age group of 30 to 50 years and were selected based on having proper eyesight and being in good health. The recruitment pool included workers from the IIT Bombay campus, students from Asha NGO, and members of Youth Empowerment societies. All participants owned either a feature phone or a smartphone; however, none of them used passwords to unlock their phones prior to the study. It is worth noting that the participants had low levels of literacy with a maximum literacy level of 7th standard.

6.2 Method

We conducted a within-subject study to compare password input methods Pin, Passfaces with Unknown faces, and Passfaces with Celebrity faces.
The participants were asked to perform three tasks - To set up and recall Pin(task 1), set up and recall Passfaces with Unknown faces(task 2) and to set up and recall Passfaces with Celebrity faces(task 3). The study compared across two recalls - the first recall is after a one-day gap from set up and the second recall is after a week's gap from set up. Thus we had 3 setups and (2) x 3 recalls per user, resulting in 9 tasks per user.

The order in which these tasks were given was counterbalanced among the users. Thus the complete experiment flow for a user is as follows:

Create 1 → Confirm 1 → Create 2 → Confirm 2 → Create 3 → Confirm 3 → Gap 1 → Recall 1.1 → Recall 2.1 → Recall 3.1 → Gap 2 → Recall 1.2 → Recall 2.2 → Recall 3.2

The detailed model is as shown in Fig.
All participants were given a demo on how to set the password before the study. All the doubts were cleared before starting the study. When the participant was ready, they were given the phone to set up the password for task 1. After one round of setting up the password, they are asked to re-enter the same. The participant was asked if they are sure about the confirmation, if yes they were asked to tap the confirm button. The user was not informed if they had confirmed it correctly while setting up. After the confirmation of task 1, they were given task 2. That is to set up the second type of password and confirm. The user was not informed if they had confirmed it correctly. They were asked to proceed if they are sure about it. Similarly, task 3 was also done immediately after task 2.

After completing the three tasks on the first day, the participant is given a gap of one day and instructed to meet for the next recall.

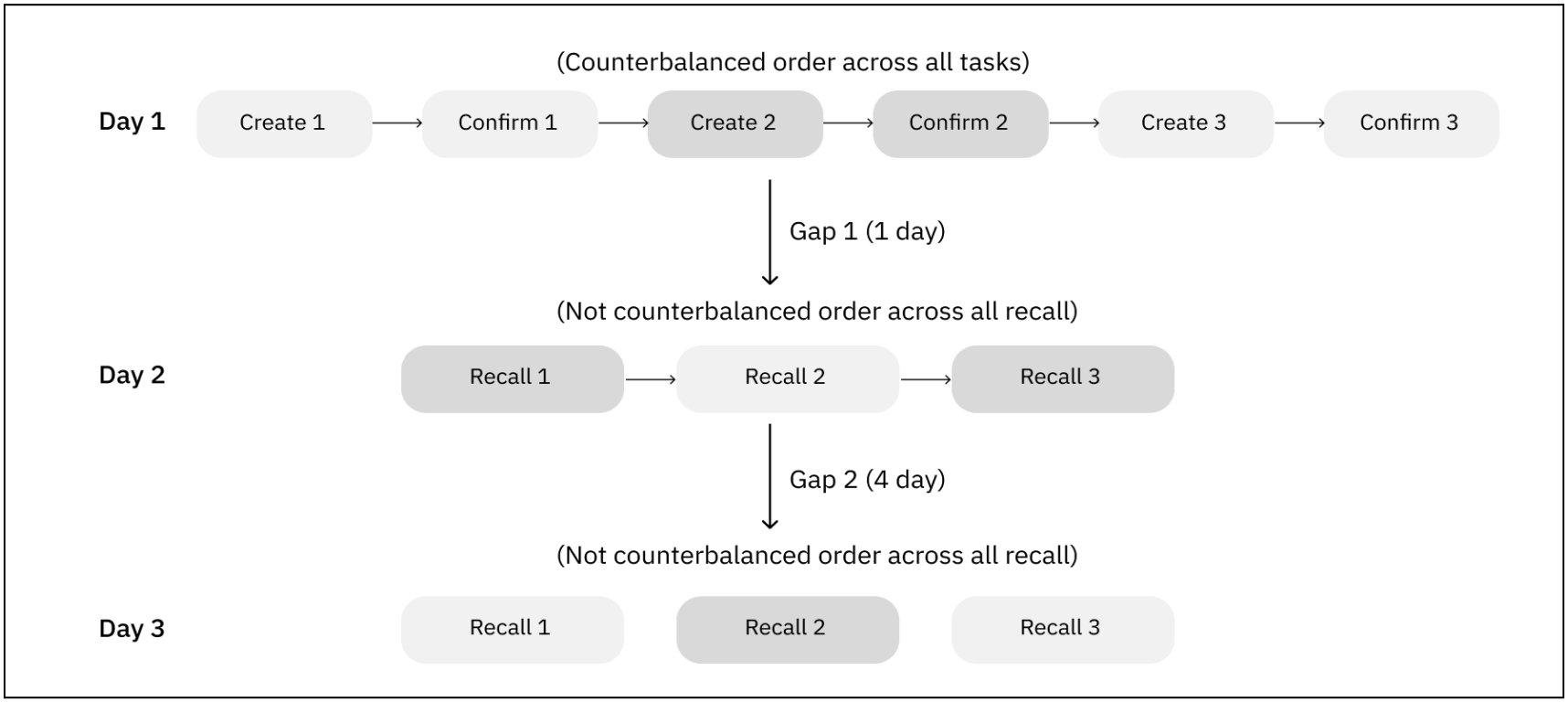


Fig.12 Experiment Flow Model

After gap 1, the participant is asked to do the first recall of task 1. They are not given any feedback in case of a wrong entry. Reattempts were given only to the users who have doubts about what they have entered/ requested for a reattempt. After the user is done with the recall of task 1, they are asked to do the recall of task 2. Which is followed by task 3 recall. The order in which these tasks were given was not counterbalanced for the recall session. After all the sets of recalls were completed, the participant is given a gap of 4 days and instructed to meet after the gap.

After gap 2, the participant is asked to do the second recall. The process for the second recall is the same first one.

6.3 Data Collection

The data collection process for the study lasted for a period of 14 days. This phase of the study was considered challenging. To facilitate easier tracking and follow-up, the data collection was divided into different sets, each with different starting dates. All three types of passwords (PIN, Passfaces, and Celebrity-involved Passfaces) were set up by the participants simultaneously on the same day. Similarly, the recall of passwords was also conducted in a similar fashion. However, it is important to note that the order of the recall was not counterbalanced, as it was assumed that there would be no learning effect associated with the order of recall. The data collection model is illustrated in the provided figure.

Fig.13 Snapshot from the field

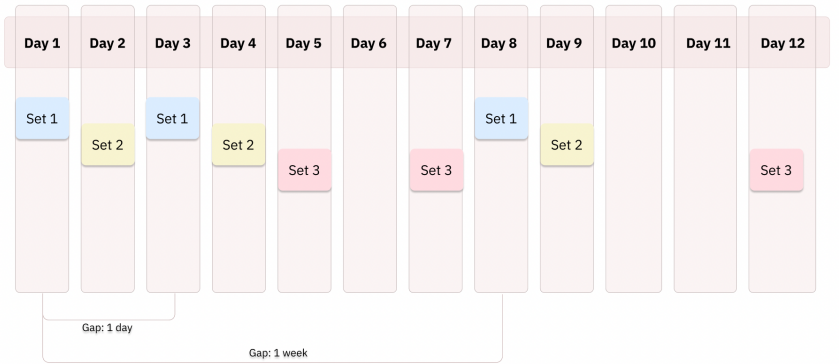


Fig.14 Data Collection Model for the Study

Users	Gender	Age Group	Succes of setting up pin	Succes of setting up passfaces	Succes of setting up celebrities	Gap 1	Success of Pin Recall after 2 days	Success of passfaces Recall after 2 days	Success of Celebrity Recall after 2 days	Gap 2	Success of Pin Recall after a week	Success of passfaces Recall after a week	Success of Celebrity Recall after a week
Shobha	Female	20 - 30…	Success	Success	Success		Success	Success	Success		Success	Success	Success
Nilam Garat	Female	30 - 40…	Success	Success	Success		Success	Success	Success		Success	Success	Success
Sunita Kakre	Female	40 - 50…	Success	Success	Success		Success	Success	Success		Success	Success	Success
Mamta solanki	Female	30 - 40…	Success	Success	Success		Success	Success	Success		Success	Failure	Success
Ranjana	Female	30 - 40…	Success	Success	Failure		Success	Failure	Failure		Success	Failure	Failure
Sushila	Female	30 - 40…	Success	Failure	Failure		Failure	Failure	Failure		Failure	Failure	Failure
Shashikala	Female	20 - 30…	Success	Success	Success		Failure	Success	Success		Failure	Failure	Success
Santosh Gawar VMCC	Male	20 - 30…	Success	Success	Success		Success	Success	Success		Success	Success	Success
Rashmi Rahul	Female	30 - 40…	Success	Success	Success		Failure	Success	Success		Failure	Success	Success
Smitha AW	Female	30 - 40…	Success	Failure	Success		Success	Failure	Success		Success	Failure	Success
Archana AW	Female	30 - 40…	Success	Success	Success		Success	Success	Success		Success	Success	Success
Vanita AW	Female	50 +	Failure	Success	Success		Failure	Failure	Failure		Failure	Failure	Failure
Lakshmi VMCC	Female	40 - 50…	Success	Success	Success		Success	Success	Success		Success	Success	Failure
Aasma AW	Female	30 - 40…	Success	Success	Success		Success	Success	Success		Success	Success	Success
Sunil Ingale VMCC	Male	40 - 50…	Success	Success	Success		Failure	Success	Failure		Failure	Success	Failure
Roh. Khaire VMCC	Male	30 - 40…	Success	Success	Success		Success	Success	Failure		Success	Success	Success
Vinod Gulmohar	Male	30 - 40…	Success	Success	Success		Success	Success	Failure		Success	Success	Failure
Shailesh Gulmohar	Male	30 - 40…	Success	Success	Success		Success	Failure	Success		Success	Failure	Success
Ramesh Gumohar	Male	20 - 30…	Success	Success	Success		Success	Failure	Success		Success	Failure	Success
Chetan Gulmohar	Male	30 - 40…	Success	Success	Success		Failure	Success	Success		Failure	Success	Success
Babita More H10	Female	50 +	Failure	Failure	Success		Failure	Failure	Success		Failure	Failure	Failure
Anita Londhe	Female	40 - 50…	Success	Success	Success		Success	Success	Success		Success	Success	Success
Chaya Shejval	Female	40 - 50…	Success	Failure	Success		Success	Failure	Failure		Success	Failure	Success
Kalubhai	Female	30 - 40…	Success	Success	Success		Success	Success	Success		Success	Success	Success
Sheela	Female	40 - 50…	Success	Success	Success		Success	Success	Success		Success	Success	Success
Kunda Salve	Female	40 - 50…	Success	Success	Success		Success	Success	Failure		Success	Failure	Failure
Manda Bhole	Female	40 - 50…	Success	Failure	Success		Success	Failure	Failure		Failure	Failure	Failure
Chaya Chawhan	Female	30 - 40…	Success	Success	Success		Success	Success	Success		Success	Success	Success
Alka Dongre	Female	30 - 40…	Success	Success	Success		Success	Failure	Failure		Success	Failure	Failure
Megha Shejwal	Female	30 - 40…	Success	Success	Success		Success	Success	Success		Success	Success	Success
Total	**7 / 23**		**93.33**	**83.33**	**93.33**		**76.67**	**66.67**	**66.67**		**73.33**	**56.67**	**66.67**

Fig.15 Success rates of final study

7. Results

The data collected from the user study was analyzed using standard statistical methods to determine whether the observed differences between the conditions were statistically significant. Three different statistical tests were performed to evaluate the degree of difference between the groups being studied with respect to the factor under consideration. The goal of these tests was to determine whether the observed differences were due to chance or whether they reflected genuine differences between the groups.

ANOVA was used to figure out if there is any significant difference between the time taken for each password type. The Pairwise KS test was used to test ordered categorical data with a number of errors. Chi-square ($\chi 2$) tests to compare non-ordered categorical or nominal data (e.g., comparing login success/fail ratios). In all cases, we regard a value of $p < .05$ as indicating that the groups being tested are different from each other with at least 95% probability, making the result statistically significant. In the tables, “not significant” indicates that the test revealed no statistically significant differences between the two conditions (i.e., $p > .05$).

7.1 Success Rates

We first examine success rates as a measure of participants' performance. The success rate is the percentage of successful password entry attempts. Here success is measured only on the first attempts. The participants are not given reattempts. The total success rates are shown in the Table. 1.

Type	Set up	Recall 1	Recall 2
Pin	93.34	76.67	76.67
Passfaces - Unknown	83.34	63.34	56.67
Passfaces - Celebrities	93.3	66.67	66.67

Table: 1 Succes rates of setting up and recalling

7.1.1 Success rate of Initial Setup and confirmation

It was noted that the success rate of setting up a pin is 93.34% whereas unknown Passfaces and celebrity Passfaces are 83.34% and 93.34% respectively. It can be inferred that the initial usability and intuitiveness of Passfaces with celebrities and pins are almost the same and higher when compared to that of Passfaces with unknown faces.

In order to determine if this difference is significant, the chi-squared test is used.

The chi-square statistic is 2.2222. The p-value is .329193. The result is not significant at $p < .05$..

7.1.2 Success rate of Recall 1

The success rate of the pin in the first recall (after a day) is found to be 76.67%, whereas that of Passfaces with unknown faces and celebrities are both found to be 63.33 %. This leads to an interesting observation when it comes to the memorability of celebrities and unknown faces. Though the usability of Passfaces with celebrities was found to be more than that of Passfaces with unknown faces, the memorability is found to be equal. This has to be further studied based on the third recall.

The chi-square statistic is 0.9524. The p-value is .621145. The result is not significant at $p < .05$.

7.1.2 Success rate of Recall 2

The success rate of the pin in the first recall (after a week) is found to be 76.67%, whereas that of Passfaces with unknown faces and celebrities are both found to be 56.67% and 66.67% respectively

The chi-square statistic is 1.8699. The p-value is .392611. The result is not significant at $p < .05$.

7.2 Time taken

The average time taken for a pin is 43.41s whereas unknown Passfaces and celebrity Passfaces are 74.3s and 67.8s respectively. Which indicates celebrity faces have slightly higher usability than unknown faces.

	Setup	Recall 1	Recall 2
Pin	43.4	18.3	16.5
Passfaces Unknown	74.2	40.3	30.5
Passfaces Celebrities	67.7	34.3	25.4

Table 2: Average time in setting up and recall

The table shows the average time taken to complete the setup, recall 1 and recall 2. These times represent the total time spent during a given step. For example, the time to set up begins when the first screen to choose a password comes and continues until the user confirms the password. Comparing the three cases, the participants took more time in setting up and recalling graphical passwords over Pin. But it is also noted that there is a gradual decrease in the time taken for all three cases.

It can be noted that as the number of days and practice also increases, the time taken to recall/ login in all three cases has become closer and lesser than the initial phase. Therefore in practice, the usability of graphical passwords will be at the same level as that of the pin. People are used to seeing Pin everywhere

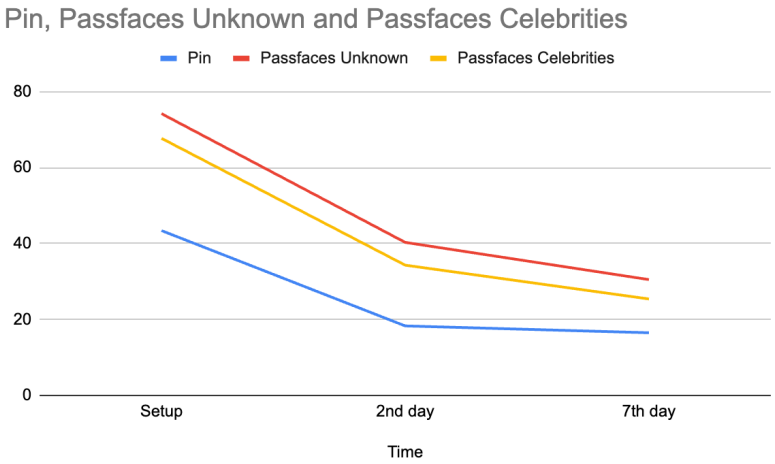


Fig.16 Prototype for Passfaces with Unknown Faces

and there is a reason for it to be biased due to the sense of familiarity to the users.

7.2.1 Recall 1

In the case of recall 1, where the means of Pin, Passfaces unknown, and Celebrities are 18.3, 40.3, and 34.3 respectively, ANOVA was done to calculate if these differences are statistically significant.

The results indicate that the f-ratio value is 8.66489. The p-value is .00037. The result is significant at $p < .05$.

It was found that there is a significant difference between the Pin and Passfaces unknown where Q = 5.70 (p = .00035). It shows

Pairwise Comparisons		$HSD_{.05}$ = 12.9795 $HSD_{.01}$ = 16.2842	$Q_{.05}$ = 3.3722 $Q_{.01}$ = 4.2308
T_1:T_2	M_1 = 18.34 M_2 = 40.26	21.92	Q = 5.70 (p = .00035)
T_1:T_3	M_1 = 18.34 M_3 = 34.27	15.93	Q = 4.14 (p = .01203)
T_2:T_3	M_2 = 40.26 M_3 = 34.27	5.99	Q = 1.56 (p = .51676)

Table 3 ANOVA results for recall 1

that Pin is quicker than unknown faces. From the test, it is also found that there is a significant difference between Pin and Passfaces with celebrities. Here Q = 4.14 (p = .01203). This also shows that Pin is significantly faster than Passfaces with Celebrities.

Whereas the difference between Passfaces unknown and celebrities is not statistically significant.

Pairwise Comparisons		$HSD_{.05}$ = 8.0530 $HSD_{.01}$ = 10.1033	$Q_{.05}$ = 3.3722 $Q_{.01}$ = 4.2308
T_1:T_2	M_1 = 16.51 M_2 = 30.54	14.03	Q = 5.87 (*p* = .00022)
T_1:T_3	M_1 = 16.51 M_3 = 25.36	8.85	Q = 3.71 (*p* = .02769)
T_2:T_3	M_2 = 30.54 M_3 = 25.36	5.18	Q = 2.17 (*p* = .28070)

Table 4: ANOVA results for recall 2

7.2.2 Recall 2

In the case of recall 2, the means of Pin, Passfaces unknown and Celebrities are 16.51, 30.54 and 25.36 respectively, ANOVA was done to calculate if these differences are statistically significant.

The results indicate that the f-ratio value is 8.8227. The p-value is .000325. The result is significant at $p < .05$.

It was found that there is a significant difference between the Pin and Passfaces unknown where Q = 5.87 (*p* = .00022). It shows that Pin is quicker than unknown faces. From the test it is also found that there is a significant difference between Pin and Passfaces with celebrities. Here Q = 3.71 (*p* = .0276). This also shows that Pin is significantly faster than Passfaces with Celebrities.

Whereas the difference between Passfaces unknown and celebrities is not statistically significant. This is similar to that of recall 1, but the difference between the values of Passfaces with celebrities and that of Pin has become slightly lesser than that of recall 1.

7.3 Password Types and Security

The types of passwords set by the user were classified into location-based (pattern) and non-location based.

7.3.1 Pins

The different types of Pins set by the user are classified into the following categories based on the results:

1. Consecutive number, which is considered a pattern in number. Eg: 1234, 4567, etc.
2. Numbers forming a pattern by location. Eg: 7890, 8989, etc.
3. Random numbers. These can be based on personal information/logic. Eg: Birth year, Important dates, etc

Cases one and two form a pattern as shown in Fig. 17. These are more susceptible to attacks. A blacklist category of susceptible pins is introduced by ios and some of the pins fall under it, which results in reduced security.

7.3.2 Graphical Passwords

In order to classify the types of the password set in the case of faces, The location of each tile was numbered in order from 1-16 as shown in Fig. 17. The location of each password was noted down and analyzed to see if there is any pattern/location-based selection.

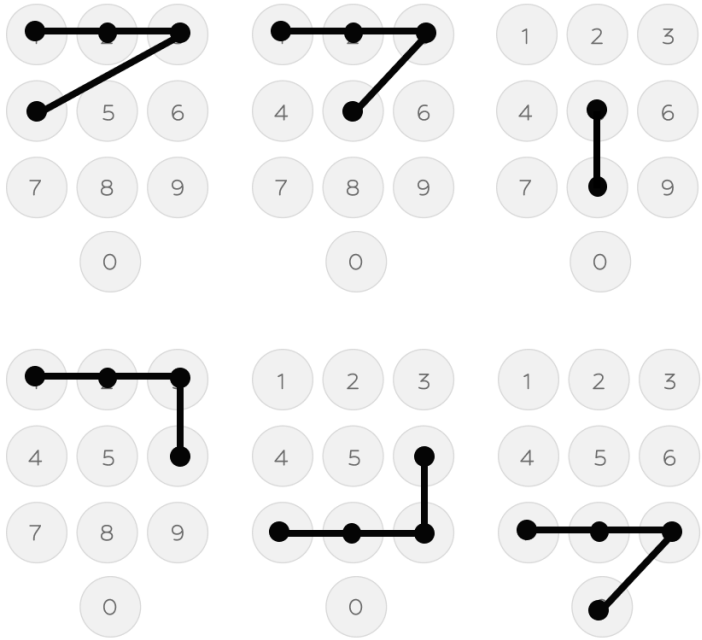


Fig. 17 Patterns set by users for PIN

It is found that 53.3% of Pins are location-based whereas in the case of graphical passwords, unknown faces have 20% location-based selection and Celebrity has only 10% location-based selection.

In the case of graphical passwords, location-based selections often involve clicking on the same point consistently. This observation suggests that graphical passwords tend to offer higher security compared to PINs. Although PINs may have

higher success rates, it is worth noting that over 50% of the pattern-based PINs used in the study were listed in the blacklist implemented by iOS for 4-digit PINs. Guessing graphical passwords proves to be comparatively more challenging than guessing PIN passwords. Another factor contributing to the higher success rates for PINs could be the users' familiarity with this authentication method.

Fig. 18 Location of each tile in numbers (graphical)

8. Limitations

The current study had several limitations related to the prototype used, which had a significant impact on the results. One major drawback was that the prototype was not coded, resulting in various issues. Firstly, while the order of tasks for setting up PIN, Passfaces, and Passfaces with Celebrities was counterbalanced, the order of recall for Recall 1 and 2 was fixed and not counterbalanced. This lack of counterbalancing could have introduced bias into the results.

Another limitation was that in the initial setup and recall phases, participants were not provided with feedback in case of wrong password confirmation. This limitation was due to the technical constraints of the prototype and it affected the external validity of the study. Participants who made mistakes were not alerted or given the opportunity to correct them, which could have influenced their performance and subsequent recall accuracy.

Additionally, reattempts to set up the password were only given to participants who were aware of their mistake and requested it. This approach may have introduced a bias, as participants who did not recognize their mistake or did not request a reattempt were not given the same opportunity to correct their passwords.

Furthermore, during the setup process, the selected password was not shown to participants, as it was hidden. This lack of visibility and feedback on the chosen password may have impacted participants' ability to accurately remember and recall their passwords during the study.

These limitations should be taken into consideration when interpreting the results and generalizing the findings of the study.

9. Revised Study

A new study is proposed to address the limitations of the previous study by introducing distraction tasks and modifying the password setup process. In this proposed study, participants will be subjected to distraction tasks after the password setup phase to simulate real-life scenarios where individuals may face cognitive distractions after setting their passwords. This will provide insights into the impact of distractions on password selection and memorization. Additionally, instead of setting all three passwords simultaneously, participants will be asked to set only one password at a time, allowing for a more focused and controlled approach. This modification will provide a clearer understanding of the factors influencing password creation and the memorability of individual passwords. By implementing these changes, the proposed study aims to enhance the ecological validity and reliability of the findings, contributing to a more comprehensive understanding of password behavior and user authentication.

9.1 Revised Model

This is a within-subject study to compare password input methods Pin, Passfaces with Unknown faces, and Passfaces with Celebrity faces. In this method, there are 4 sessions in total duration of the study per user is 15 - 28 days depending on the user The detailed method of the study is as follows:
The participants are asked to perform three tasks - To set up and recall Pin(task 1), set up and recall Passfaces with Unknown faces(task 2) and to set up and recall Passfaces with Celebrity faces(task 3). The Study is formulated in such a way that the participant has to set up and recall only one password at a time. Only after the final recall of the first password, the second password is set.
The study consists of two recalls - the first recall is after a distraction task from set up and the second recall is after a week's gap from set up. After which the user is made to set up the second type of password. The same process is repeated until the final recall of the third password. Thus there are (3) x { 1 setup, 1 confirm, distraction task, and 2 recalls} per user, resulting in 15 tasks per user.
The order in which these tasks were given was counterbalanced among the users. Thus the complete experiment flow for a user is as follows:

Create 1 → Confirm 1 → Distraction Task (5 mins) → Recall 1 → Gap 1(1 week)→ Recall 1.2 → Create 2 → Confirm 2 → Distraction Task (5 mins) → Recall 2.1 → Gap 2(1 week) → Recall 2.2 → Create 3 → Confirm 3 → Distraction Task (5 mins) → Recall 3.1 → Gap 3(1 week) → Recall 3.2

The detailed model is shown in Fig. 18. Before starting the study, all the participants are given a brief overview about the importance of setting up a password. They are also asked fr consent and informed about the monetary benefits of participating in the study.
All participants are taken through a training protocol before performing the tasks. The training protocol includes a demo on how to set up the three types of passwords. After the demo, each

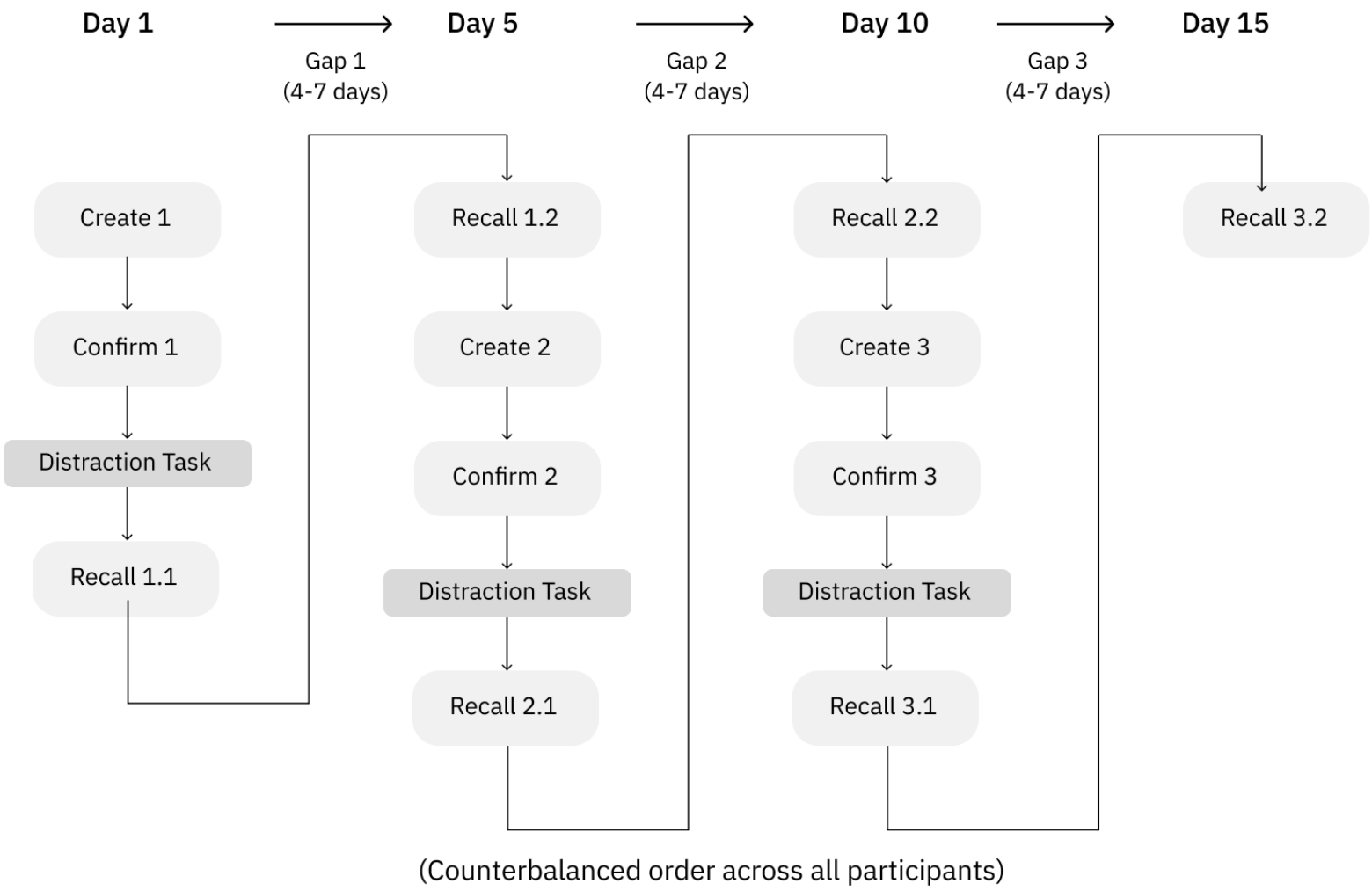


Fig. 18 Revised experiment flow model

participant is given a practice session to set up and confirm all three tasks.
In the practice session, the experimenter makes the participant set their own password and informs them that it is not important to remember this.

When the participant is ready, they are asked to set up the password for task 1. After one round of setup, they are asked to re-enter the same for confirmation. If the participant is not able to confirm the password correctly, attempts are given. If the participant is unable to confirm even after reattempts, they are given one more chance to set up a new password.

After successful confirmation of task 1, the participant is given a distraction task for 5 mins. This is to distract their short-term memory. The distraction tasks include one or more tasks like solving a physical puzzle to identifying parameters from a given video.

The participant is asked to recall task 1 after the distraction task. They are given as many reattempts as they want until they give up. The attempt is recorded as a failure if they cannot log in even after the reattempts.
If the login is a success, the participant is asked to come for the next session which is after a 4-7 days gap.
The second recall for task one is done after the first gap. The participant is given reattempts in case of a failure until they give up. The number of reattempts is recorded by the experimenter if any. After the second recall, the participant is asked to set up the next password.(task 2)

The procedure for setting up is the same as task one. Another distractor task is provided after the setup and the first recall is done after the distractor task. This process is repeated until the final recall of task 3.

The participant is also informed about how much money they have earned after each session. There is a post-test survey after the final recall of task 3, to understand the user behavior about the criteria behind the selection of each type of password.

The dependent variables of the study are The success of setting up and recalling, the Number of attempts, the time taken for each attempt, and the total number of errors in case of failure. For example, if a login attempt is a failure, how many mistakes has the user made for failure? This is to understand in depth the memorability of the various password types that are being tested.

9.2 Participant Recruitment

To recruit participants for the study, an agent will be responsible for identifying individuals who meet the following criteria:

1. Proper eyesight and good health: Participants should have no vision impairments that would hinder their ability to view and interact with the study materials. They should also be in overall good health to ensure their participation does not pose any risks.

2. Age group: The preferred age range for participants is between 30 and 55 years. This age range is chosen to ensure a diverse representation of participants while targeting an age group that is likely to have experience with mobile devices and passwords.

3. Literacy level: Participants with a literacy level of 7th standard and below are preferred. This criterion is important to include individuals from varying literacy backgrounds and assess the usability and effectiveness of the password system among participants with different literacy levels.

4. Gender balance: An equal number of male and female participants are preferred to counterbalance gender differences and ensure a balanced representation in the study. This will help in analyzing any potential gender-related effects on password usage and performance.

5. Smartphone and feature phone users: It is preferable to have a mix of participants, with half of them using smartphones and the other half using feature phones. This variation allows for a comparison of password usability and performance across different device types, considering the potential differences in user experience and interface capabilities.

By considering these requirements and working with the agent, a total of 60 participants can be recruited for the study, ensuring a diverse and representative sample for the research.

9.3 Monetary Incentives

In the proposed study, participants will be provided with monetary incentives as a token of appreciation for their time and effort in participating in the research as explained in Table 5. The researchers understand the value of participants' contributions and the importance of their involvement in the study. As a result, participants will be reimbursed for transportation charges incurred for each visit, ensuring that their travel expenses are covered. Additionally, participants will receive a loyalty bonus for each visit, recognizing their commitment and dedication to the study. Moreover, participants will have the opportunity to earn extra money if they successfully recall the answers during the recall sessions. This incentivization approach aims to motivate participants, enhance their engagement, and acknowledge their valuable contributions to the research. By providing monetary incentives, the study seeks to create a mutually beneficial environment where participants feel valued and rewarded for their active participation.

According to the current model, each participant can earn up to Rs 1000, If they come for all 4 sessions and recall everything in the first attempt. Even if the participant forgets they will get a minimum of at least Rs 700.

Trips	Transportation	Loyalty Bonus	Recall Bonus
1	100	0	0
2	100	50	100 - 20
3	100	100	100 - 20
4	100	150	100 - 20
Total	**400**	**300**	**300**
Max			**1000**

Table 5: Chart showing monetary benefits in each level for participation

9. Discussions

The primary objective of this project was to examine the password input behavior of emergent users, specifically focusing on Passfaces. Although various other potential studies could have been conducted within the Passfaces framework, the current study did not include the randomization of the grid layout. Introducing randomization would have made it even more challenging to memorize Passfaces. However, one of the main reasons for not implementing randomization was that the layout of PINs is typically fixed and not randomized in existing applications.

It is worth noting that randomization could have provided additional security benefits by mitigating attacks such as shoulder surfing and location-based attacks. In this study, PINs were used as a benchmark for comparison, but it is important to acknowledge that other graphical passwords and alphanumeric passwords could also be valid points of comparison for future research.

The study utilized a fixed corpus of photos, which was selected based on several trials. However, if this design is implemented in practical applications, it would be crucial to regularly regenerate the corpus. Additionally, when using celebrity photos, regional considerations should be taken into account to ensure that the pictures are recognizable to the target user population. Due to the scope and time limitations of the current study, these variables were controlled to maintain feasibility and manageability.

10. Conclusions

The pilot study conducted with 10 users and the subsequent study involving 30 users have provided valuable insights and observations regarding the subject matter. However, it is important to acknowledge that the limited sample size restricts the ability to draw definitive conclusions from these studies alone. The findings have shed light on specific limitations and challenges that need to be addressed in future research endeavors.

Based on the identified limitations and the need for further exploration, a new study is proposed. This upcoming study aims to build upon the previous research by incorporating improvements and addressing the identified limitations. By doing so, the goal is to enhance the study's methodology, increase the sample size, and improve the reliability and validity of the findings.

Through iterative research efforts, it becomes possible to refine and expand upon existing knowledge. By undertaking a new study that accounts for the limitations identified in previous research, it is anticipated that more robust and reliable findings can be obtained. This will contribute to a deeper understanding of the subject matter, facilitate the development of informed conclusions, and potentially drive advancements in the field.

In conclusion, the proposed new study represents a vital step forward in the ongoing exploration of the subject matter. It demonstrates a commitment to continuous improvement, ensuring that future research efforts can overcome the limitations of the past and provide a more comprehensive understanding of the topic at hand.

11. References

1. Bishop, M., & Klein, D. V. (1995). Improving Passwords: From Fifty-Five Characters to Five. IEEE Security & Privacy Magazine, 13(1), 42-49.

2. Brostoff, S. (2003). Passfaces: User-friendly Login. BT Technology Journal, 21(3), 139-143.

3. Coventry, L., Briggs, P., Blythe, M., & Turland, J. (2014). Multiple Passwords, Multiple Personas: Why Users Adopt Different Passwords. Human-Computer Interaction, 29(6), 612-650.

4. De Angeli, A., Coventry, L., Johnson, G. I., Renaud, K., & Grace, P. (2005). Usability and User Authentication: Pictorial Passwords vs. PIN. In Proceedings of the 2005 Symposium on Usable Privacy and Security (SOUPS) (pp. 55-66). USENIX.

5. Kirkwood, C., Goh, H., Paterson, K. G., & Brostoff, S. (2022). Usability and Security of Randomly Reordering Numeric Keypads. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (pp. 1804-1819). ACM.

6. Markert, A., Volkamer, M., & Dechand, S. (2021). Who Chooses Weak PINs? An Analysis of PIN Selection in the Wild. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (pp. 1220-1237). ACM.

7. Markert, A., Volkamer, M., & Dechand, S. (2021). Who Chooses Weak PINs? An Analysis of PIN Selection in the Wild. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (pp. 1220-1237). ACM.

8. Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2012). Graphical Password Authentication Using Cued Click Points: A Usability Analysis.

9. Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005). PassPoints: Design and Longitudinal Evaluation of a Graphical Password System.

10. Thorpe, J., & Van Oorschot, P. C. (2015). An Empirical Investigation of User Choice in Graphical Passwords.

11. Dunphy, P., Yan, J., & McBurney, P. (2008). The Emperor's New Security Mechanism: A Graphical Password Generator.

12. Sobrado, L. A., & Birget, J. C. (2008). Graphical Passwords.