

Conjugation of Graphical Password by Image Segmentation

Sudeshna Chakraborty, Manish Kumar Srivastav, Sourabh Sinha, Saurabh Kumar, Tanish Tyagi

School of Computer Applications and Technology

Galgotias University, Noida, Uttar Pradesh, India

ABSTRACT- A New Approach to Graphical Password Authentication by Image Segmentation. With the inherent problems in traditional text-based password, researchers have been searching for alternative authentication mechanisms. Graphical Passwords to The Rescue: One of the promising alternatives of passwords is graphical password because we remember images and shapes naturally, even when our textual memory diminishes away. By designing a system that breaks an image into segments which are possible components of one password. Once a user selects particular arrangement of these segments, and just like that have in simple words created what we now know as passwords. It makes dictionary and brute force attacks challenging by increasing the password space. The paper describes the authentications of segmentation algorithm, user interface design and evaluation system's security & usability through user.

Keywords: *Authentication, Encryption, Graphical, Password, Image, Login, Segmentation*

I. Introduction

In today's digital age, password-based authentication is still one of the most regularly utilized ways for safeguarding networks. However, text-based passwords typically have flaws, making them vulnerable to things like brute-force assaults, phishing, and even somebody looking over your shoulder. Graphical passwords, which employ graphics instead of text, have become an enticing way to handle these challenges. In this study, we offer a new way to graphical passwords utilizing picture [1] segmentation. In this method, users generate a password by selecting specified portions of an image in a particular order. This strategy uses our natural capacity to remember visual

information, delivering a more secure and user-friendly solution to preserve critical data.

Keywords: *Brute-force attacks, Phishing, Shoulder surfing, Visual memory, Digital security*

1. Background

Password-based authentication is a key aspect of keeping our digital lives secure, but standard text-based passwords come with their share of challenges. They can be subject to assaults like brute-force attempts, phishing scams, or keylogging. Plus, many users choose to create weak passwords or reuse the same ones across many sites, which increases the danger even more. To combat these challenges, graphical passwords have been introduced as an alternative, seeking to increase both security and convenience of use by tapping into our brain's strength in remembering visuals rather than text. Graphical passwords function in different ways. For example, in recognition-based systems like the Passfaces approach, users are prompted to identify recognizable faces from a grid of photographs. In another alternative, termed the create-A-Secret (DAS) method, users create a unique form on a grid that works as their password. While these systems have their merits, they also face challenges like being simple to forget, complicated to use, or subject to specific sorts of assaults (e.g., patterns being guessed or repeated). A potential way to increase security and usability is to develop graphical passwords utilizing advanced techniques like picture segmentation. Image segmentation is a tool from computer vision where an image is divided down into multiple sections depending on attributes like color or texture. In the context of graphical passwords, this technique can be

used to enable users chose certain sections of a picture as their password. This strategy adds complexity, making the system tougher to crack, while still making use of the human brain's natural ability to detect and memorize visual patterns.

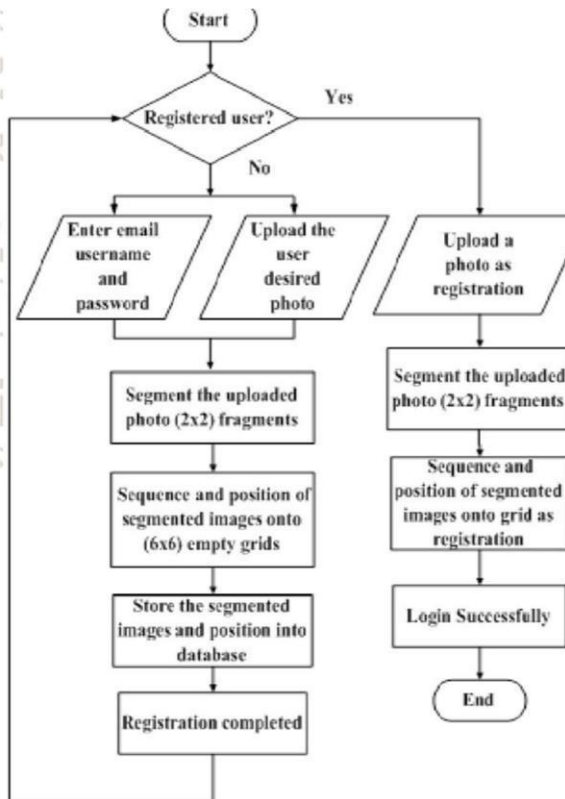


Fig1: working of Graphical password

1.2 Related Work

- I. Numerous graphical password systems have been created over the years, each possessing distinct advantages and disadvantages. This overview examines fundamental principles that have influenced the discipline, highlighting the role of picture segmentation in enhancing system security and user-friendliness. Passfaces, developed by Real user Corporation, is one of the earliest and most recognized graphical password systems. Passfaces operates on a straightforward concept: users are presented with a grid of human faces and must select the ones they previously designated as their password. It

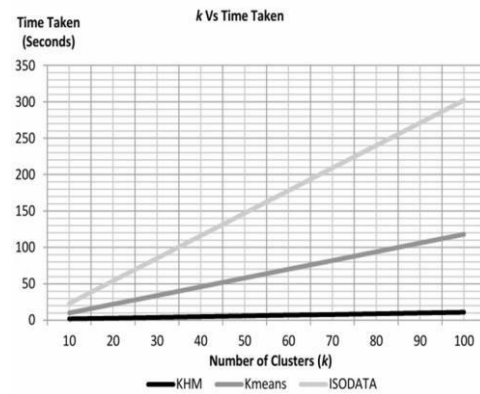


Figure 2: K-means

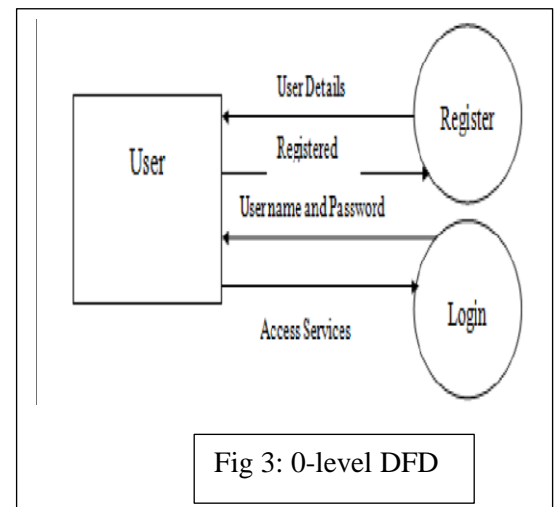


Fig 3: 0-level DFD

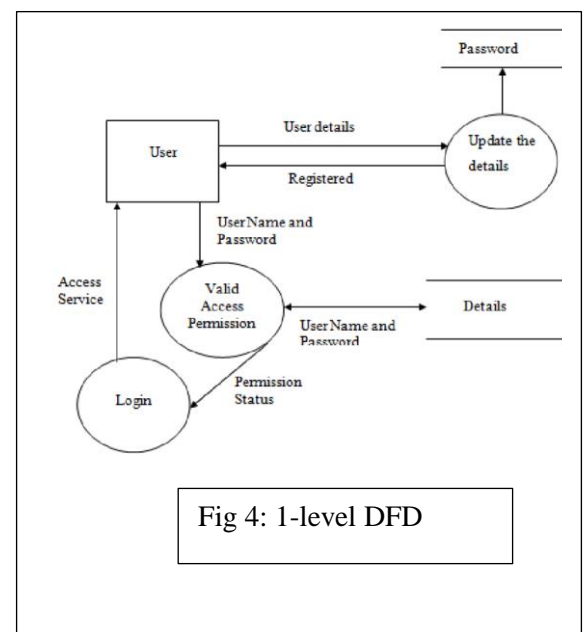


Fig 4: 1-level DFD

- II. capitalizes on our superior ability to recall faces compared to arbitrary sequences of text. Although useful in certain instances, Passfaces possesses limits. For instance, if a somebody observes you inputting your password, a practice referred to as "shoulder surfing," they could readily discern the characters you select. It necessitates an extensive database of photos to ensure the system's security against guessing attempts.
- III. Then there's [3] Draw-A-Secret (DAS), a method created in 1999 by Jermyn and colleagues. In DAS, users sketch a shape on a grid, and the system encodes the password based on where the lines connect. The benefit of drawing simplicity is countered by a significant drawback: individuals often produce analogous, predictable designs, facilitating password guessing by attackers. Plus, remembering complex forms might be tough for users, leading to dissatisfaction.

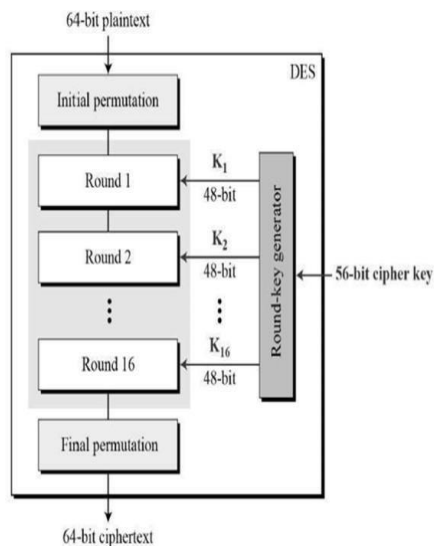


Fig 5: DAS Working

- IV. To make graphical passwords more secure and user-friendly, several researchers went to more complex approaches like picture segmentation. This strategy involves splitting an image into smaller, significant parts—based on

color, texture, or other features—that user can select as their password. For example, in one study, researchers studied how segmentation could make password creation both easy for users and tougher for attackers to guess. By selecting a specific section of a picture, users may build more unique passwords that are tough to hack but also easy to remember.

- V. Edge detection and region-based segmentation are two common approaches used in image processing that have also found its way into graphical password systems. Edge detection helps identify the boundaries inside an image, while region-based segmentation combines comparable pixels together. These strategies make it easier for users to pick specific areas of an image as their password, minimizing errors and boosting security by making the selection process more accurate.

1.3 Image Segmentation: A New Way to Create Graphical Passwords

Traditional passwords have been around forever, but let's face it—they have some serious issues. They're easy to forget, and they can be vulnerable to various attacks. That's why graphical passwords, where users pick or interact with images rather than typing a word, have gained attention. Building on this idea, a new approach that uses image segmentation could make these systems even more secure and user-friendly. Image segmentation is a fancy term from computer vision that means breaking an image into smaller, meaningful parts based on features like color, texture, or edges. Think of it like drawing invisible lines around different objects or areas in a picture, like separating the sky from the buildings in a cityscape.

This concept can be used in graphical passwords by having users pick specific parts of an image—those segments—as their password.

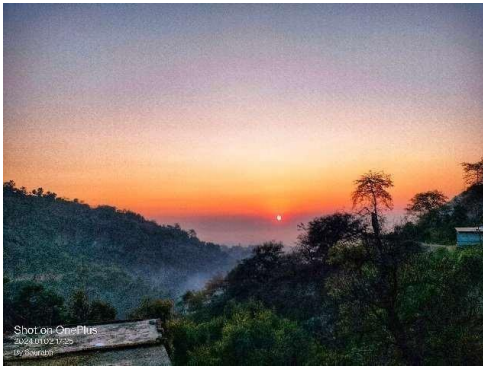


Fig6: Original Image



Fig7: Segmented Image with sequence clue

1.3.1 Working of Password-System:

In an image segmentation-based password system, you would be shown a segmented image—maybe a landscape or an abstract pattern. Instead of remembering a tricky sequence of text or clicking random points on an image, you'd pick certain segments of that image, like a tree in the background or a specific area of color. The mixture of these chosen segments would form your password

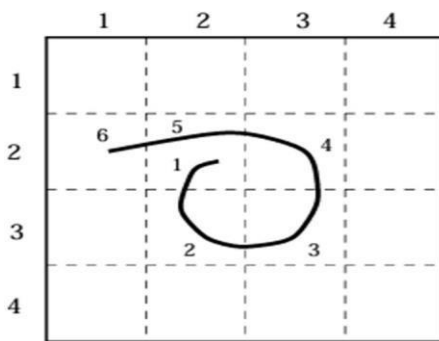


Fig8: working of password system

Here's what the process might look like:

- I. **Image Selection:** You're given an image that's been divided into different parts.
- II. **Choosing Segments:** You select specific segments, such as items or areas in the image (e.g., a car, a mountain, or a bright red section).
- III. **Password Creation:** The unique mix of segments becomes your

password . When you log in, you'd the process of selecting those segments in the right order,

II. Discussion

While the suggested approach boosts security and usability, it is not without limitations. For instance, the system's reliance on predetermined images may limit user personalization. Additionally, the intricacy of image segmentation could increase computational cost, impacting system performance. Despite these restrictions, the system delivers significant advantages in terms of memorability and resistance to typical attack vectors.

2.1 Strengths of the Proposed System:

- I. **[5]Enhanced Memorability:** One of the primary advantages of employing photos for password creation is the better memorability. Humans are often better at recalling visual information than to text-based material. In the picture segmentation system, users select distinct areas of an image, providing a unique password that is easier to memorize. This tackles one of the most common concerns with traditional passwords, where users typically forget their complex alphanumeric passwords, leading to undesirable practices like
 - II. password reuse or simplifying their passwords to make them more remember.
- III. **Resistance to Common Attacks:**

The system provides a substantial benefit in terms of security. Graphical passwords, especially when paired with picture segmentation, are resistant to many traditional assaults. Here are several examples:

- IV. **Brute-force Attacks:** With traditional passwords, attackers commonly utilize brute-force techniques to guess passwords through trial and error. However, with picture segmentation, the sheer number of conceivable combinations of image segments increases the difficulty of such attacks dramatically.
- V. **Phishing:** Since the password is not text-based, phishing attacks, where users are tricked into revealing their password, are less effective.
- VI. **Shoulder Surfing:** The segmented image makes it harder for an attacker to replicate the exact password just by watching someone log in, as the segments may appear visually similar to the observer but contain subtle differences.

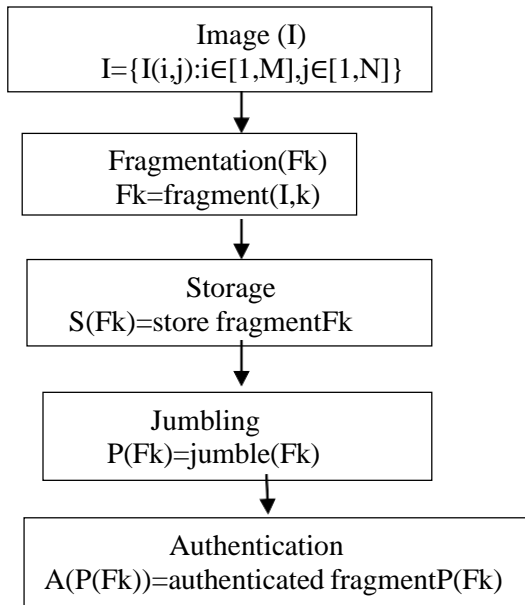
Flexibility in Design: The technique can be applied to numerous sorts of photographs, including landscapes, abstract art, or customized images made expressly for password generating. This adaptability enables for varied applications and perhaps boosts user engagement by allowing them to interact with a wide variety of visual content. Tougher for an attacker to duplicate the exact password only by watching someone log in, as the segments may appear visually similar to the observer but contain small changes.

2.1.2 Multifactor Compatibility: The graphical password system can be combined with other authentication methods such as biometrics or traditional passwords to create a [7] multifactor authentication (MFA) system. This offers an additional layer of security, especially in environments where high-level protection is necessary.

2.2 Challenges and Limitations

- I. **Limited Personalization:** One of the key drawbacks of the system is in its dependence on predefined images. Users are frequently more comfortable with customization, and the inability to choose or upload personal photographs could detract from the overall user experience. This constraint may inhibit widespread adoption, as users can feel constricted by the limited variety of images, leading to disengagement or lower usability.
- II. **Usability Trade-offs:** While the method promotes security and memorability, it could create usability issues for certain users.
- III. **Cognitive Load:** For users who are not visually oriented or have trouble recognizing patterns, picking portions from complicated images could become a tedious operation. The segmentation must be straightforward enough to not overwhelm consumers with too many choices or confusing segment borders.
- IV. **Learning Curve:** Users inexperienced with graphical password systems may find it challenging to adopt. Training or user onboarding may be essential, which introduces friction during initial adoption. Additionally, if users must be taught how to engage with specific portions, this could present accessibility difficulties for individuals with cognitive or motor disabilities.

III. Proposed work:



1. Framework Plan and Engineering

The main period of the proposed work includes planning the engineering of the graphical secret word framework. This incorporates:

I. Frontend Advancement:

Making an instinctive and responsive UI (UI) that permits clients to interface with pictures for secret key creation and confirmation. Carrying out picture division, where pictures are separated into more modest fragments or interactive focuses. Clients can choose different portions in a particular grouping to frame their secret phrase.

II. Backend Improvement:

Creating secure capacity and handling of graphical passwords. Chosen picture sections or snap directions will be put away safely utilizing encryption and hashing calculations to safeguard against unapproved access. Planning a productive informationbase construction to deal with enormous volumes of graphical secret key information without compromising execution.

Picture Division and Determination

The center component of the framework is the division of pictures for secret word creation:

I. Picture Division:

The framework will isolate the chose picture into numerous interactive regions or sections. Each section will have explicit directions or limits that the framework will perceive during both secret word creation and confirmation.

The division should be adjusted to guarantee a suitable degree of intricacy: fragments ought to be neither too huge nor too little to even consider adjusting among convenience and security.

II. Secret phrase Creation:

Clients will make their passwords by clicking or choosing a predefined number of portions inside the picture in a specific request. This choice will act as the client's secret key, with the grouping and area of the snaps put away safely. A "tick resilience" element will be carried out to permit slight variety in the area of snaps during verification, guaranteeing convenience without forfeiting security.

2. Secret key Verification Cycle

The validation cycle will expect clients to rehash similar choices made during the secret word creation stage:

I. Signaled Review:

During validation, the framework will give clients a similar picture utilized for secret phrase creation. Clients should choose similar sections in the specific request for the framework to check their

character.

A signaled review system will assist clients with recalling their secret word by involving the visual picture as a brief, decreasing mental burden contrasted with text-based passwords.

II. Mistake Taking care of and Input:

The framework will furnish clients with input assuming they inaccurately select picture sections. In any case, criticism systems will be painstakingly intended to try not to offer a lot of data about the right secret phrase for the sake of security. A predetermined number of confirmation endeavors will be implemented to safeguard against savage power and speculating assaults.

2. Security Improvements

A few security components will be incorporated to address explicit weaknesses and guarantee powerful insurance:

I. Encryption and Secure Stockpiling:

Secret word information, including picture fragments and snap arranges, will be hashed and encoded areas of strength for utilizing techniques. This will guarantee that regardless of whether the framework is penetrated, the secret phrase information stays secured.

II. Animal Power Opposition:

To forestall animal power assaults, the framework will guarantee that the graphical secret phrase space is huge, with various conceivable fragment mixes and snap groupings.

The framework will carry out account lockout or Manual human test systems after a specific number of fizzled login endeavors to forestall robotized speculating.

III. Shoulder Surfing and Smirch Assault Moderation:

Since graphical passwords can be powerless against shoulder

surfing (where aggressors notice the login interaction) and smirch assaults (where aggressors investigate fingerprints or smears left on touchscreens), extra security elements, for example, randomizing the picture or utilizing dynamic picture overlays might be investigated.

5. Ease of use and Client Experience Assessment

To guarantee that the framework is easy to understand and simple to take on, convenience testing will be a vital part of the proposed work:

I. Client Testing:

A progression of client tests will be led to assess how instinctive and paramount the graphical secret key framework is contrasted with conventional text-based passwords. Test members will make and confirm their passwords in different situations.

Convenience measurements, for example, task consummation time, achievement rate, and mistake rate will be dissected to distinguish likely regions for development.

II. Memorability Studies:

Studies will be directed to survey the memorability of graphical passwords after some time, deciding how effectively clients can review their graphical passwords after various time periods use.

IV. Conclusion:

Graphical passwords using image segmentation offer a fresh and promising alternative to traditional text-based passwords, leveraging the human brain's natural ability to remember and recognize images. By choosing segments of an image as a password, users can enjoy a more secure and memorable way to protect their accounts.

This approach greatly increases the complexity of guessing attacks, making it harder for hackers to crack passwords using brute force or common patterns.

The system is not only more secure but also user- friendly, as people usually find it easier to remember images than complex text or number combinations. However, difficulties remain. Striking the right balance between security and usability is crucial, as overly complicated segmentations may frustrate users, while overly simple ones might risk security. Future work should focus on making the system adaptive, allowing personalized images and [11] dynamic segmentation based on user tastes.

There are still worries about real-world attacks, such as shoulder surfing, where someone could observe the password entry. To counter this, future versions.

V. Future Work

The graphical password system employing picture segmentation offers great promise, but there are various ways it might be enhanced and expanded. In the future, there are a number of critical topics to examine to make the system even more secure, usable, and adaptable to regular users.

I. Personalized Images:

Currently, the system uses set images, but people might connect more with personal photos that mean something to them. Future versions could allow users to add their own pictures, [9] making the password creation process more personal and engaging. This would not only make the system feel more user-friendly but also build more unique and harder-to-guess passwords.

II. [10] Smarter Image Segmentation:

Not all photos work the same way when broken into segments. A family picture might need different processing compared to a landscape or abstract art. Future study could focus on smarter algorithms that automatically adjust to different

types of images, ensuring that the segments are meaningful and easy for users to remember.

III. User-Customized Segmentation:

People like to have power over their technology. Allowing users to decide how their images are segmented could improve their connection to the system and their knowledge of how it works. For example, they could highlight or select parts of the picture that they feel are most memorable or meaningful to them.

IV. Defending Against Real-World Attacks:

Even though graphical passwords are more secure than text-based ones, they are still vulnerable to attacks like shoulder surfing (where someone watches you enter your password). Future improvements could include features like randomized image segments that change positions between logins or adding small variations to make it harder for anyone watching to copy.

V. Combining with Other Authentication Methods:

Combining graphical passwords with other security methods, such as fingerprints or face recognition, could provide an extra layer of security. This would also give users more choices, allowing them to choose a combination of methods that they are most comfortable with could randomize segments or mix graphical passwords with other security methods like biometrics or multi-factor authentication for extra protection.

Title	Method	Description	Issues	Key Changes
Brostoff & Sasse (Are Passfaces More Usable Than Passwords? A Field Trial Investigation) (2000)	Passfaces	Users select specific faces from a grid that they previously designated as their password.	Vulnerable to "shoulder surfing" where observers can see selections.	Introduced face recognition as a password system, leveraging users' ability to remember human faces
Jermyn et al. (The Design and Analysis of Graphical Passwords) (1999)	Draw-A-Secret (DAS)	Users draw a pattern or shape on a grid, which is encoded as a password.	Users often create predictable designs that are easy to guess.	Simplified password input by allowing freeform drawing, although it can lead to common, guessable patterns.
Chiasson et al. (Influencing Users Towards Better Passwords: Persuasive Cued Click-Points) (2009)	Cued Click Points (CCP)	Users click on specific points of an image to form their password, using visual cues for memory retention.	Patterns can be easily observed and guessed if monitored.	Enhanced click-based systems with visual cues, making them more memorable and reducing reliance on text-based passwords.
Gao et al. (Design and Analysis of a Graphical Password Scheme) (2009)	Edge Detection	Uses algorithms to detect edges in images, providing a more accurate segmentation process.	Sensitive to noise, which can adversely affect segmentation quality.	Improved accuracy in identifying distinct regions, enhancing reliability in graphical password systems
[8] Hayashi & Hong (A Diary Study of Password Usage in Daily Life) (2011)	Region-based Segmentation	Segments images based on pixel similarity (color and intensity) to create more homogeneous regions.	High computational cost; potential issues with noise affecting accuracy.	Offers a more accurate segmentation method that enhances the effectiveness of graphical passwords based on visual similarity.

Table1: Table of Comparison

VI. References:

- [1] Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys*, 44(4), 1-41.
<https://doi.org/10.1145/2333112.2333114>
- [2] Brostoff, S., & Sasse, M. A. (2000). Are passfaces more usable than passwords? A field trial investigation.
In *Proceedings of the British HCI Group Annual Conference** (pp. 405-424).
Springer. https://doi.org/10.1007/978-1-4471-1186-5_27
- [3] Chiasson, S., Forget, A., Biddle, R., & Van Oorschot, P. C. (2009). Influencing users towards better passwords: Persuasive cued click-points. In *Proceedings of the British HCI Group Annual Conference** (pp. 121-130). ACM. <https://doi.org/10.1145/1572532.1572566>
- [4] Davis, D., Monrose, F., & Reiter, M. K. (2004). On user choice in graphical password schemes. In
13th USENIX Security Symposium (pp. 11-11). USENIX
Association. <https://doi.org/10.5555/1251375.1251376>
- [5] Dunphy, P., & Yan, J. (2007). Do background images improve "draw a secret" graphical passwords?
In *Proceedings of the 14th ACM Conference on Computer and Communications Security**
(pp. 36-47). ACM.
<https://doi.org/10.1109/ICICIC.2009.219>
- [6] Gao, H., Liu, X., Dai, R., Wang, S., & Liu, H. (2009). Design and analysis of a graphical password scheme. In **2009 Fourth International Conference on Innovative Computing, Information and Control** (pp. 675-678). IEEE.
<https://doi.org/10.1109/ICICIC.2009.219>

- [7] Goldberg, J., Hagman, J., & Sazawal, V. (2002). Doodling our way to better authentication: Exploring the effect of free-form doodles on authentication performance. In *Proceedings of the ACM Conference on Human Factors in Computing Systems* (pp. 279-280). ACM. <https://doi.org/10.1145/503376.503458>
- [8] Hayashi, E., & Hong, J. I. (2011). A diary study of password usage in daily life. In *Proceedings of the 2011 ACM Conference on Human Factors in Computing Systems* (pp. 2627-2630). ACM. <https://doi.org/10.1145/1978942.1979326>
- [9] Khot, R. A., & Bianchi, A. (2015). Exploring mobile authentication methods: What do users want? In Proceedings of the ACM Conference on Human Factors in Computing Systems* (pp. 2455-2464). ACM. <https://doi.org/10.1145/2702123.2702293>
- [10] Luo, Y., & Lin, X. (2016). Graphical passwords: A survey. *Journal of Network and Computer Applications, 42*, 55-69. <https://doi.org/10.1016/j.jnca.2016.04.006>
- [11] Man, S., Hong, D., & Memon, N. (2004). Password management for draw-a-secret (DAS) schemes. In Proceedings of the 2004 ACM Conference on Computer and Communications Security* (pp. 224-231). ACM. <https://doi.org/10.1145/1041335.1041363>
- [12] Nelson, D. L., Reed, U. S., & Walling, J. R. (1977). Pictorial superiority effect. *Journal of Experimental Psychology: Human Learning and Memory, 3*(5), 485-497. <https://doi.org/10.1037/0278-7393.3.5.485>