applied sciences

MDPI

Article

A Novel Multi-Factor Authentication Algorithm Based on Image Recognition and User Established Relations

Diego Carrillo-Torres, Jesús Arturo Pérez-Díaz *, Jose Antonio Cantoral-Ceballos * and Cesar Vargas-Rosales

School of Engineering and Sciences, Tecnologico de Monterrey, Monterrey 64849, NL, Mexico
* Correspondence: jesus.arturo.perez@tec.mx (J.A.P.-D.); joseantonio.cantoral@tec.mx (J.A.C.-C.)

Abstract: Conventional authentication methods, like simple text-based passwords, have shown vulnerabilities to different types of security attacks. Indeed, 61% of all breaches involve credentials, whether stolen via social engineering or hacked using brute force. Therefore, a robust user authentication mechanism is crucial to have secure systems. Combining textual passwords with graphical passwords in a multi-factor approach can be an effective strategy. Advanced authentication systems, such as biometrics, are secure, but require additional infrastructure for efficient implementation. This paper proposes a Multi-Factor Authentication (MFA) based on a non-biometric mechanism that does not require additional hardware. The novelty of the proposed mechanism lies in a two-factor authentication algorithm which requires a user to identify specific images out of a set of randomly selected images, then the user is required to establish a self-pre-configured relation between two given images to complete authentication. A functional prototype of the proposed system was developed and deployed. The proposed system was tested by users of different backgrounds achieving 100% accuracy in identifying and authenticating users, if authentication elements and credentials were not forgotten. It was also found to be accepted by the users as being easy to use and preferable over common MFA mechanisms.

Keywords: multi-factor authentication; data breaches; graphical passwords

check for updates

Citation: Carrillo-Torres, D.; Pérez-Díaz, J.A.; Cantoral-Ceballos, J.A.; Vargas-Rosales, C. A Novel Multi-Factor Authentication Algorithm Based on Image Recognition and User Established Relations. *Appl. Sci.* **2023**, *13*, 1374. https://doi.org/10.3390/app13031374

Academic Editors: George Drosatos, Konstantinos Rantos and Konstantinos Demertzis

Received: 15 December 2022
Revised: 12 January 2023
Accepted: 13 January 2023
Published: 20 January 2023

1. Introduction

Day by day, the power of attacks to guess or harvest passwords to gain illicit access to a system or data are becoming greater as the sophistication of password cracking techniques increases and high-power computing becomes more affordable. In the last three years, the number of phishing attacks for the purpose of account or identity theft has more than tripled [1]. During the third quarter of 2022 alone, there were 15 million data breaches, due to internet users around the world having their accounts compromised by attackers [2]. Nowadays, we are so susceptible to account theft attacks that, statistically, at least one of our online accounts (email, social networks, banks) will be hacked or subjected to an attempted hack in in the next 12 months [3]. Hence, there is an important need to have more robust and secure access mechanisms to protect data and systems.

The most popular, yet the most basic, mechanism for user authentication is the use of passwords [4], mainly because the concept of using passwords is an efficient and cost-effective solution for user authentication. Passwords are an example of Single-Factor Authentication (SFA), which has been mostly adopted by the community due to its simplicity and user friendliness [5,6]. The fundamental requirement for any password is that it should be easy to remember and must be sufficiently secure. In other words, the authentication process must be efficient, and passwords must be tough to guess [7]. Nevertheless, this is the weakest level of authentication [8,9], and it has been realized that Single-Factor Authentication is not reliable to provide adequate protection, due to several security threats [10].

Multi- factor authentication was proposed to provide higher levels of safety [11] and to add strong protection against account theft by greatly increasing the difficulty for attackers to gain access to information systems and data, even if passwords or PINs are compromised by phishing attacks or other means. MFA manages to do this with a layered approach, that is, with MFA a system requires a user to present a combination of two or more credentials to verify identity so access can be granted [12]. MFA mechanisms are mostly based on biometrics, which is automated recognition of individuals, based on their behavioral [13,14], and biological characteristics [15]. However, the utilization of biological factors has its challenges, mainly related to ease of use [16], which largely impacts the usability of the MFA system. In addition, biometric mechanisms entail high implementation costs, and are still vulnerable to many different security attacks, such as presentation attacks, sensor output interception, denial of service attacks, and replay attacks [17], among others.

This paper proposes a novel multi-factor authentication mechanism that does not require additional hardware and is solely based on images and their user-established relations. The combination of text and graphics increases the password space, thereby making the authentication mechanism more robust and secure against various types of security threats. The contributions of this research work are the following:

- The design of a novel MFA algorithm, based on image selection and user-established relations.
- Functional prototype of the mechanism developed and deployed as a mobile application available for IOS and Android.
- An analysis of the accuracy, security, and usability results focusing on the benefits and areas of opportunity that working with an image selection and relations-based algorithm has in an MFA mechanism.

2. Literature Review

The number of scenarios in which authentication is needed is indeed large, thus MFA has a broad field of applications.

2.1. MFA Applied in Different Mechanisms

MFA has become critical in validation of user identity and electronic devices (or systems) [18,19], validation of infrastructure connection [20], and validation of interconnected IoT devices, such as a smartphone, tablet, wearable device, or any other digital token [21]. M. Bartłomiejczyk [22] proposed a distributed protocol that allows user authentication using three authentication factors, possession, knowledge, and inherence, with the possibility of carrying out the process in the mobile environment of the Android platform with guaranteed authentication support. It turned out to be a robust solution, since it combined three different factors, nevertheless it was limited to the Android platform and the protocol's own complexity increased the risk and vulnerability to common attacks. D. R. Ibrahim [23] proposed an MFA mechanism, based on facial recognition, that uses visual cryptography (VC) to secure biometric data, which, for the second factor of authentication uses the shared resources generated by the VC as authentication tokens and verifies them by the same algorithm of facial recognition used to recognize a live facial image of the user. D. Lu [24] proposed an MFA framework using both the motion signal of handwriting in the air and the geometry of the hand skeleton captured by a depth camera. The downside of the MFA approach presented in the two last mentioned papers is that they require hardware, and biometric techniques, which penalize usability and make the implementation complex and expensive and limits its application to the requirements of the hardware. S. Vaithyasubramanian [25] proposed a master PIN authentication scheme and multi-factor authentication to protect credit card transactions, using elements, such as location and preferred stores, to determine the authentication method; nevertheless, the use of PINs in both authentication methods made it vulnerable to common attacks, in addition to requiring constant user information. Lone, S.A. [26] proposed an authentication scheme, implemented as challenge-response authentication, where three factors (username, device number, and fingerprint) are used as a secret key between the client and the server. The method of encryption of the secret key is rather robust and interesting; however, the scheme requires biometric information and techniques which need specific hardware, whilst penalizing usability and authentication time.

2.2. MFA Based on Graphical Passwords

It has been proven that humans can remember pictures better than text, and, consequently, graphical password schemes are a better alternative to text-based schemes [27]. Pankhuri [7] proposed a mechanism which presents images at a time interval in which the user must click on a predefined space within the image and type a password to complete the authentication; however, security can be compromised if the defined click area is too large. B. O. ALSaleem [28] proposed a mechanism that requires the user to choose three images and memorize them in an initial registration phase; then, in the authentication phase, the user must choose the correct images that he or she considered during the registration process in a specific order. The downside of the mechanism is that when long periods of time elapse between authentications, users tend to forget the selected images. A. P. Sabzevar [29] proposed a mechanism in which the user receives an image on his or her screen, and on a second device the user receives information on where to click, the number of clicks, and in what order. The user follows the instructions on the image to complete authentication. This mechanism requires a second device, which makes implementation expensive and compromises user experience and usability.

All three of the reviewed mechanisms, based on graphical passwords, present some strengths; the main strength being that they provide a much larger password space compared to simple text-based passwords. The mechanisms also overcome many different security threats, such as key-loggers, screen capture, shoulder-surfing, and weak passwords. Furthermore, except for the latter one, the mechanisms entail low implementation costs.

2.3. Graphical Methods

There have also been interesting non-MFA graphical methods. N. A. A. Othman [30] proposed a shoulder-surfing-proof graphical-based authentication, in which the user must click images based on their selected direction during the registration process. For example, if the user chose the up direction, the user should click on the image that is above their actual Pass image. This approach results in a secure authentication mechanism, considering that, along the directional graphing authentication, there is a hashing function that validates information. Nevertheless, the number of directions is limited, and perhaps that is where this mechanism could see some improvement. Chang [31] proposed a graphical-based password KDA (Keystroke Dynamic-based Authentication) system for touch screen handheld mobile devices that utilizes the force of each person clicking or touching the touch panel as a biometric feature for authentication. This is a very good mechanism, since it has very good performance, even on low-power mobile devices. The probability of breaking the authentication is low as well, and the biometric features do not cause an extra burden on the user. However, testing was done on a very limited number of devices, and perhaps more testing with more devices of different brands and specifications should be done to really test the consistency of the mechanism across all devices. Gyorffy [32] proposed a system that utilizes a personal image to construct an image hash, which is provided as input into a cryptosystem that returns a password which requires the user to select a small number of points on the image. The embedded device then stretches these points into a long alphanumeric password for authentication. This approach allows many passwords to be generated from one single graphical password, which largely increases the entropy of the system. Nevertheless, the user experience is penalized by the complexity of the mechanism.

3. MFA Algorithm Design

A functional prototype of the mechanism was developed in React Native and deployed as a mobile app, both for android and IOS, using the Expo Go client. The database used, both for storing users' authentication information and generic images, was hosted on Back4App. The generic image database consisted of 110 images from Google. These images were uploaded from the cell phone gallery of internet users. This was an important factor in selecting the images for the database because it was intended that these images would mix seamlessly with the user´s own at the time of authentication.

Both configuration and authentication processes of the mechanism are described in detail below. Figure 1 depicts the flow process of the mechanism.

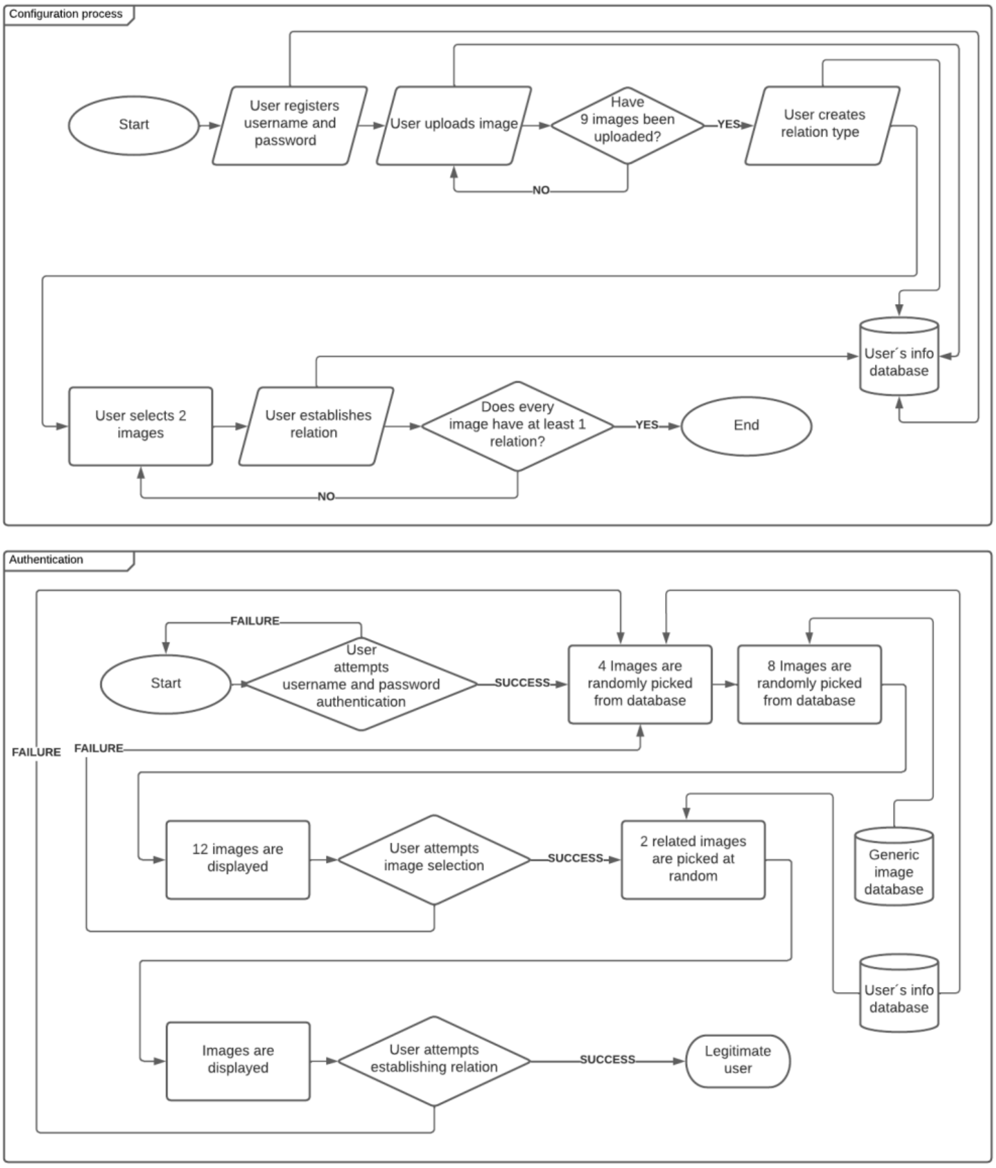
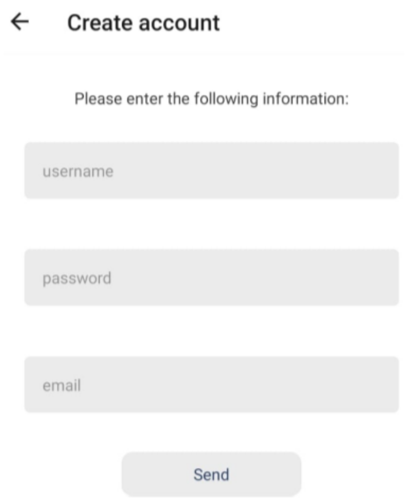

Configuration process
Start
User registers username and password
User uploads image
Have 9 images been uploaded?
YES
NO
User creates relation type
User´s info database
User selects 2 images
User establishes relation
Does every image have at least 1 relation?
YES
NO
End
Authentication
FAILURE
Start
User attempts username and password authentication
SUCCESS
4 Images are randomly picked from database
8 Images are randomly picked from database
FAILURE
FAILURE
12 images are displayed
User attempts image selection
SUCCESS
2 related images are picked at random
Generic image database
User´s info database
Images are displayed
User attempts establishing relation
SUCCESS
Legitimate user

Figure 1. Flow chart for proposed mechanism.

3.1. Configuration Process

The proposed mechanism requires that the user completes a configuration process prior to authentication.

Step 1: User creates an account by entering a unique username, password, and an email address. Figure 2 shows the screen where the user fills out the form to provide such information. These credentials are stored in a database so they can be used by the user to continue with the set-up.

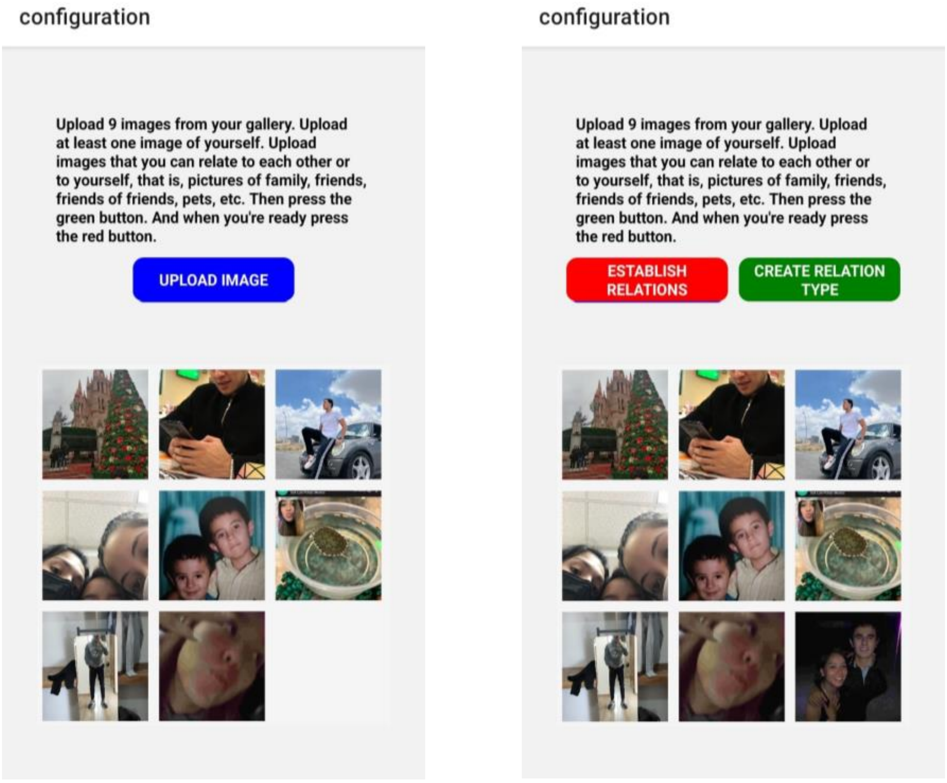


Create account

Please enter the following information:

Figure 2. Create-account screen.

Step 2: The user is required to upload at least 9 images from the cell phone gallery, and it is recommended that in these images there is at least one image of the user himself/herself, and no image is to be uploaded more than once. All the images have a meaning or represent something to the user so that, in some way, each of the images can be related to the other images. Figure 3a, b shows the image-upload screen.



configuration

Upload 9 images from your gallery. Upload at least one image of yourself. Upload images that you can relate to each other or to yourself, that is, pictures of family, friends, friends of friends, pets, etc. Then press the green button. And when you're ready press the red button.

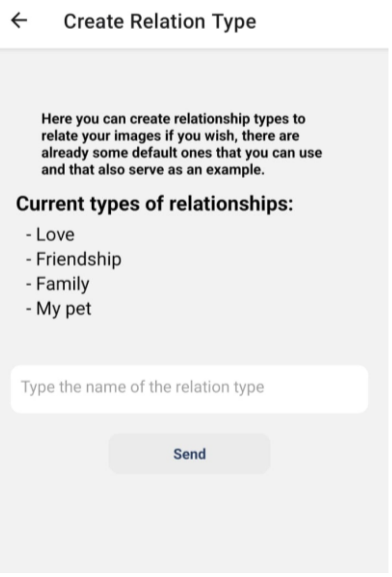
configuration

Upload 9 images from your gallery. Upload at least one image of yourself. Upload images that you can relate to each other or to yourself, that is, pictures of family, friends, friends of friends, pets, etc. Then press the green button. And when you're ready press the red button.

(**a**) (**b**)

Figure 3. (**a**) Image-upload screen; (**b**) Image-upload screen once user has uploaded 9 images.

Step 3: Users are given the option to create their own type of relationship so that establishing relationships between the images can be easier and more personalized, and this also makes authentication more secure. If the user chooses to create a type of relationship, the user must enter the name of it. Figure 4 shows the screen in which the user can create a relation type, the screen contains a text field, in which the user types the name of the relation. The user can also see the types that already exist. In Figure 4 we can see that the user has Love, Friendship, Family, and My Pet as already available types of relations.



Create Relation Type

Here you can create relationship types to relate your images if you wish, there are already some default ones that you can use and that also serve as an example.

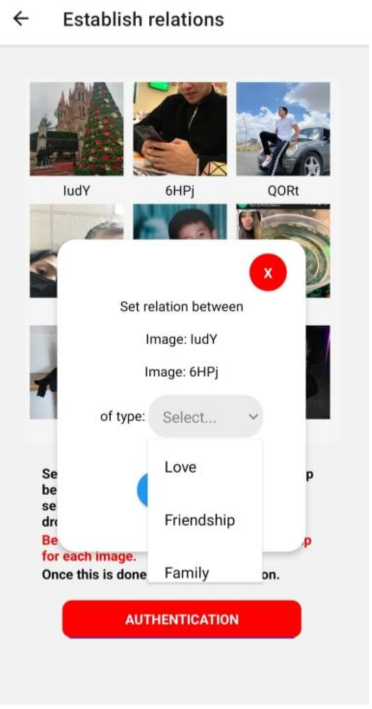
Current types of relationships:

- Love
- Friendship
- Family
- My pet

Type the name of the relation type

Figure 4. Create-Relation-Type screen.

Step 4: Uploaded images are displayed on the screen, and the user must select two images out of the group. Once this is done, a react native modal appears on the screen, as shown in Figure 5, wherefrom the user must select the type of relation that best suits both images; in other words, the type of relation that best represents what the images have in common, or that describes how the images relate to each other. This process must be repeated as many times as necessary so that every image of the group is related to at least one other image. No image can be related to itself. No image can have zero relations to other images.



Establish relations

Set relation between

Image: IudY

Image: 6HPj

of type: Select...

Se p
be
se
dr
Be p
for each image.
Once this is done on.

Figure 5. Establish-relations screen.

This concludes the set-up process the user must follow. All images uploaded, types of relationships created, and established relations are saved in the database as exclusive information for the user and available only for the users in their own authentication process.

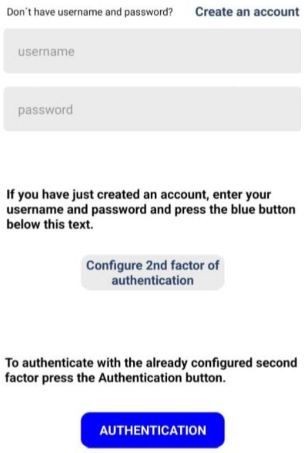
Once the set-up process is completed, the user can now go through with the authentication.

3.2. Authentication Process

The novelty of the proposed MFA mechanism lies in an algorithm which is based on image selection and user-established relations.

The complete authentication process is described thoroughly below, beginning with Step 1.

Step 1: User enters username and password in the screen, shown in Figure 6, for the first authentication factor.


Don´t have username and password?
Create an account
username
password

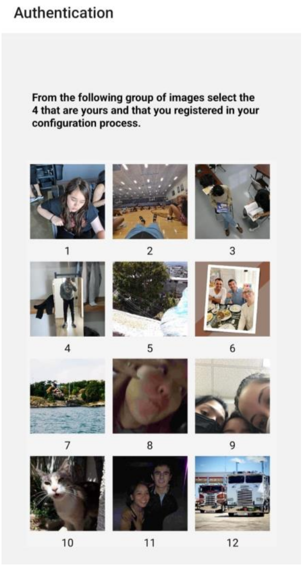
If you have just created an account, enter your username and password and press the blue button below this text.

Configure 2nd factor of authentication

To authenticate with the already configured second factor press the Authentication button.

Figure 6. Login screen.

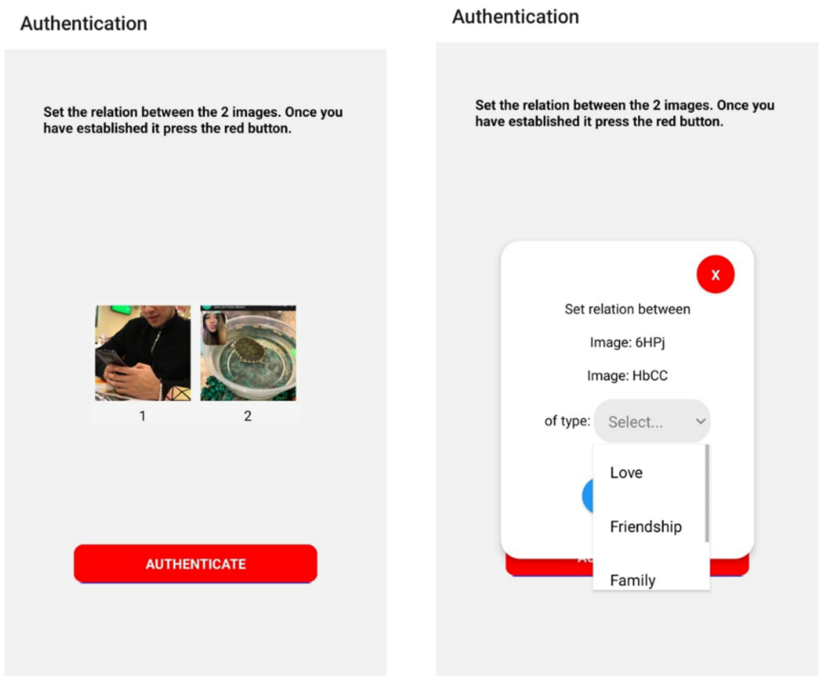
Step 2: If the user enters the correct credentials, twelve images are picked at random and are displayed on the screen, as shown in Figure 7; four of these images are picked from the group of images that the user uploaded in the set-up process and the rest of them are picked from a generic image database unaffiliated with the user´s images. This is done to create confusion and test the user to increase the entropy of the mechanism. The user must select all 4 images which belong to him/her correctly. No image can be selected twice. If the user fails to select the correct images, authentication fails.



From the following group of images select the 4 that are yours and that you registered in your configuration process.

Figure 7. Image-Selection screen.

Step 3: Once the user successfully selects the four images, the screen displays only two out of the four images, as seen on Figure 8a. Now, the user must select both images, and, once this is done, a modal appears on the screen, as seen on Figure 8b. The user must select the type of relation that exists between both images. The user must press the "AUTHENTICATE" button to validate the relation. If said relation is not correct the authentication attempt fails, otherwise, the user is authenticated successfully.



Authentication

Set the relation between the 2 images. Once you have established it press the red button.

(**a**)

Authentication

Set the relation between the 2 images. Once you have established it press the red button.

Set relation between

Image: 6HPj

Image: HbCC

of type: Select...

(**b**)

Figure 8. (**a**) Authentication screen; (**b**) Authentication screen with react native modal displayed.

4. Discussion and Result Analysis

To test the MFA algorithm, a functional prototype of the algorithm was deployed using the expo go platform, making it available for users as a mobile app for both android and IOS.

The algorithm was tested on users from different backgrounds, including young technology savvy users, and older users with little familiarity to new technologies. Table 1 depicts the demographics of the users that tested the mechanism.

Table 1. User demographic information.

Users	% of Male Users	% of Female Users	% of Users between 18 and 30 Years Old	% of Users Older than 40	% of Users Accustomed to Technology
52	72%	28%	70%	30%	73%

The experimentation and testing of the app was carried out following a specific procedure. All 52 users tested the application twice. On the first encounter, each user followed the setup process to configure their authentication profile, and then each user went on to attempt authentication as many times as they needed so they could get a feel of the algorithm and get accustomed to it.

One week later, all 52 users tested the application for a second time. This time, they were only required to attempt authentication. This was done to gather information regarding the difficulties that the user could encounter when attempting to authenticate after an extended period. After each user finished testing for the second time, a survey was conducted to gather information about the qualitative aspects of the algorithm, such as user experience, difficulty in remembering the authentication elements (images, relations), user approval, etc.

Once the testing was done, information was collected regarding the authentication process of the algorithm. The proposed MFA mechanism achieved 100% accuracy in identifying and authenticating users if they did not forget their authentication elements and credentials. Table 2 shows that the 52 users made a total of 425 authentication attempts, out of which 70.35% were successful; the failed attempts were due to users forgetting their authentication elements, which is discussed later.

Table 2. Authentication process information.

Total Authentications	% of Successful Authentications	% of Failed Authentications	Average Authentication Time
425	70.35%	29.64%	19.75 s

The average authentication time recorded for the successful attempts was 19.75 s, which was a satisfactory result, considering that the standard MFA takes an average of 15 s to complete [33]. On top of that it was an early experimentation stage, as well as the users' very first authentication attempts.

There were authentication times as long as 75 s, and as low as 6 s. Nonetheless, it was observed that the authentication time was directly related to the ability of the user to remember the authentication elements (images, relations), as well as their focus on the authentication process. Note that these results were from the very first authentication attempts from users with no previous experience or knowledge of the mechanism, and so would certainly change as the users became accustomed to the mechanisms. In the following attempts, the percentage of successful authentications would be higher.

Table 2 shows that 29.64% of all authentication attempts failed. Considering there were two steps to the authentication process, the first requiring users to select four out of 12 images that belonged to them, and the second step requiring users to establish a relation between two of the images that were selected, it was necessary to know where the users were failing.

As shown in Figure 9, most failed authentications happened when the user had to establish relations between the images. Via user input, it was determined that the cause of these failed authentication attempts was due to the users having forgotten the relations established between the given images.

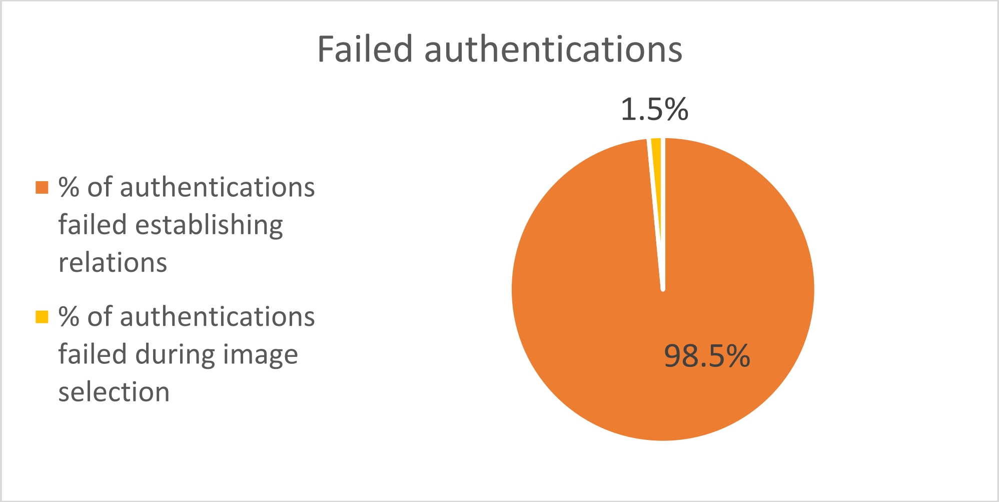


Figure 9. Failed authentication attempts information.

Figure 10 shows that out of the 585 total relations that were established by all 52 users (in average, each user established 11 relations), 81% of them were established using the predefined types of relations, and only 19% using user-set types of relations. Taking this into account, we could determine that there was no problem in letting the user set their own type of relations, as long as users had a good set of predefined types that could actually be used when relating the images. This is also supported by the fact that only 35% of all users created and used their own relation types, the majority of them using the predefined types.

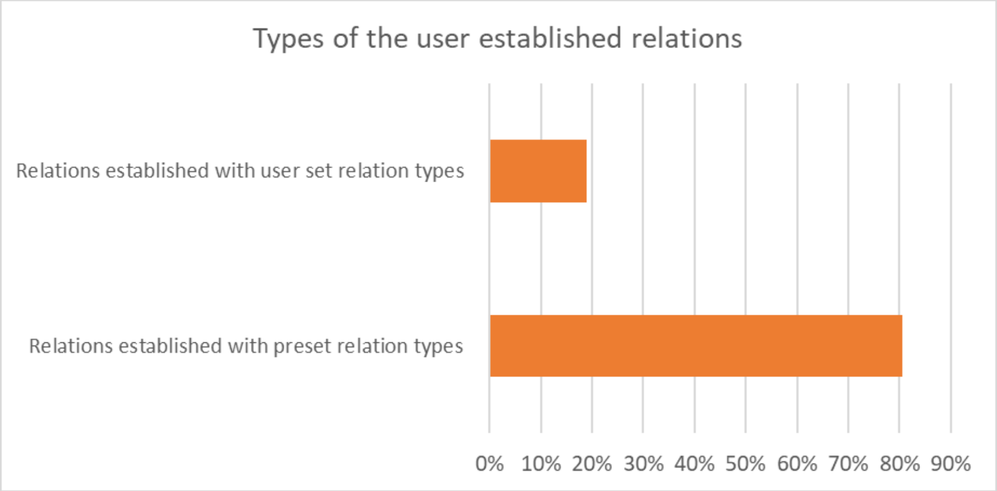


Figure 10. Information about the user established relations.

Prior to testing, it was believed that giving the user the freedom to establish relations, using their own types of relations (other than the predefined types that were given as an option) would cause a high number of failed attempts at authentication, due to the user forgetting not only the relation between images, but also the type of relation. Nevertheless, no evidence was found to support this.

Regarding the qualitative aspects of the mechanism, the data collected from the survey after the testing process showed that most users found both the set up and authentication process relatively easy, as depicted in Figure 11.

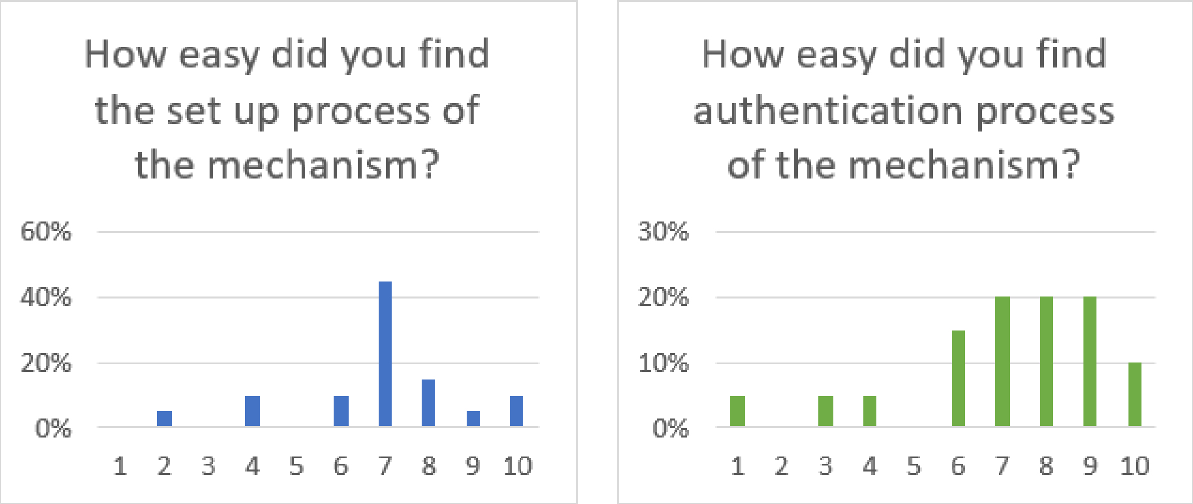


Figure 11. User experience results (1 being very hard, and 10 very easy).

In the same survey, users were also asked if they would use the proposed MFA mechanism instead of commonly used ones, such as OTP. Figure 12 shows that 55% of users said that they would use it, with most users approving the mechanism as something usable and applicable.

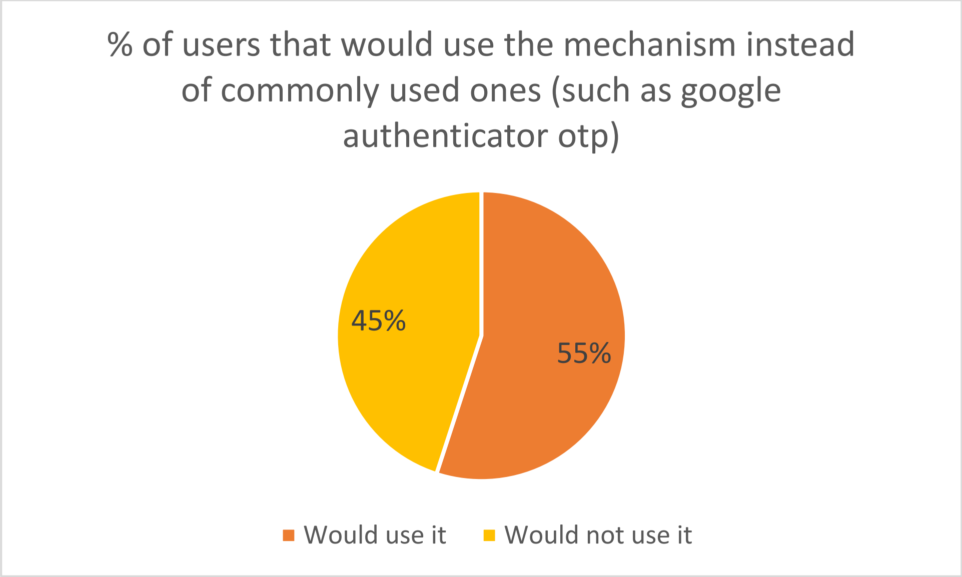


Figure 12. User acceptance results.

4.1. Security Analysis

Regarding the novel authentication factor developed in this paper, namely, the second factor of the proposed MFA mechanism, the password space would be given by calculating all the possible combinations out of the following:

- All the possible combinations of 4 images pulled from the user´s uploaded set of images.
- All the possible combinations of 8 images pulled from the generic image database.
- All the user´s registered types of relations.
- Al the predefined types of relations.

The password space could then be calculated using the following formula:

$$({}^{s1}C_4 \times {}^{s2}C_8) \times ({}^{4}C_2 \times R) \quad (1)$$

In this formula, s1 represents the number of images the user uploaded to the database and s2 represents the number of images stored in the generic image database. C stands for the binomial coefficient (also known as combination number or simply combinations) and is used to calculate how many ways one can choose k items from n items without repetition and without order. R stands for the number of available types of relations, including both the predefined types, and the ones registered by the user.

It is a fact that the more images and types of relations the user has available for his or her authentication, the bigger the password space would be and, therefore, the more secure it would be. Consequently, the mechanism was designed and developed to not only require a minimum of 9 images to be uploaded initially, but also to enforce the user keeping the uploading images after every authentication until a total of 20 images are stored in the database. The mechanism, once in production, is thought to have at least 10 predefined types of relations, and it encourages the user to register at least 5 of his or her own. Similarly, the generic image database is thought to have a minimum of 500 images once the mechanism is in a production stage.

Having said that, password space would be given by the following equation:

$$({}^{20}C_4 \times {}^{500}C_8) \times ({}^{4}C_2 \times 15) \quad (2)$$

This would result in a password space of 39,933,078,553,126,253,137,500.

With this number, the mechanism achieves a much larger password search space compared to the commonly used 6-digit OTP (like Google Authenticator´s), which has a password search space of 1,000,000.

However, the security of this novel mechanism does not reside solely on password space, considering that the mechanism is based on the user recognizing elements that are only known to him/her out of a larger set of deceiving elements, meaning that the user is able to select images that they keep privately in their personal device, as well as relations that only they know, causing the entropy to be larger.

Taking this into account, as well as the fact that every time there is a wrong attempt the images displayed are refreshed and changed, common attacks like shoulder surfing, brute force, and key logging do not pose any threat. Remembering, or having knowledge of which images are selected by the user and the correct relation, is really of no use since every authentication attempt would be different. In Table 3 there is a comparison of the security of the proposed mechanism with other similar solutions. Unlike other graphical passwords, our proposed mechanism can bypass the mentioned attacks, thanks to the refresh feature of the mechanism, alongside the unique and personalized characteristics of the authentication elements.

Table 3. Common attacks which other graphical passwords are vulnerable to compared to the proposed method.

Vulnerability	Graphical Passwords	Proposed Method
Smudge attack	YES	NO
Dictionary attack	NO	NO
Spyware/Key loggers	YES	NO
Shoulder surfing	YES	NO
Guessing	YES	NO

4.2. Storage Requirements

Maintaining images in a database could demand large amounts of storage. The database used for testing stored the authentication elements of a total of 52 users with an average of 9 images per user. This database was hosted in Back4App and had a total of 246 MB in file storage.

The developed prototype, once deployed and downloaded as a mobile app, would require 75.6 MB of storage.

4.3. Attack Implementation Testing

The proposed mechanism was tested by implementing an attack on it. The attack worked as follows.

A user went through the required configuration process and then authenticated several times. The user put together a group of 6 people to attempt authentication on the user's own account. The user provided his own username and password to this group of people consisting of 2 close friends, 3 close family members (mother, father, and brother), and the user's girlfriend. This was done to focus the testing on the novel algorithm and to simulate that the login credentials of the mechanism's first authentication factor had been compromised.

Each person out of the group attempted authentication several times. In this initial round of attempts there were no successful authentications; in fact, no one was able to go through the image selection step. Only two of the "attackers" were able to correctly guess 2 images out of the 4 required. This was all the success achieved by the attackers in this initial test.

However, it was important to know how easy it was for attackers to guess the relations as well, so the following test was set up in a way that the "attackers" skipped straight on to the establishing relations step. In this test a total of 3 relations were guessed correctly out of around 10 attempts by each attacker. The common trait among the compromised relations is that they described the relation between the user and the said "attacker".

Nonetheless, the requested pictures were refreshed in every attempt, as well as the relationship needed for authentication, making it difficult for the attacker to guess correctly in every new attempt. Furthermore, most of the attackers would not be close people to the users and, considering that, in this test, the attackers had no success in authenticating the full process, account breaches seemed very unlikely.

5. Conclusions and Future Work

In this paper we presented the design of a novel MFA mechanism based on image recognition and user established relations. The results of the testing and experimentation, along with an analysis of said results focusing on the accuracy, security, and usability achieved, were also presented.

The mechanism achieved 100% accuracy in identifying and authenticating users if they did not forget their authentication elements and credentials, and 70.35% of total successful authentications in the very first attempts by users not accustomed to the mechanism.

The mechanism proved to be an effective, user friendly, and novel method of MFA. This was ascertained by the large success rate of authentications and the user feedback, where users described the method as interactive and easy to use. The mechanism has an edge over mechanisms like OTP or biometric MFA mechanisms since it does not require a second device nor extra special hardware to complete authentication. This was mentioned by users in the feedback as a positive characteristic.

Some of the limitations of the proposed MFA mechanism are that users found it difficult to memorize their authentication elements after an extended period, mainly the relations established between images. This caused failed authentications and push back from the users in the feedback, where they stated that this issue was an argument not to use this mechanism over more common alternatives.

Future work could be focused on finding relations more seamlessly and in a way that facilitates memorization of such relations, perhaps by tweaking the user interface. However, it is a fact that it would be less likely for users to forget the established relationships if they utilized the mechanism regularly. User testing and experimentation including this type of adjustment would continue to improve the proposed MFA system with the objective of achieving user friendliness and acceptance.

Author Contributions: D.C.-T.: Data Curation, Investigation, Software, Resources, Visualization and Writing—original draft; J.A.P.-D.: Design of the system, Supervision and Writing—review & editing; J.A.C.-C.: Writing—review and editing. C.V.-R.: Writing—review & editing. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the project "Digital Technologies to Create Adaptive Smart Cities" by Tecnologico de Monterrey Challenge-Based Research Funding Program. And partially supported by "Red temática Ciencia y Tecnología para el Desarrollo (CYTED) 519RT0580" by the Ibero-American Science and Technology Program for Development CYTED.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data available on request due to restrictions eg privacy or ethical. The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy concerns regarding images obtained from users' cell-phone gallery.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Cook, S. Identity Theft Facts & Statistics: 2019–2022. Comparitech. Available online: https://www.comparitech.com/identity-theft-protection/identity-theft-statistics/. (accessed on 1 August 2022).
2. Statista. Global Number of Breached Data Sets 2020–2022. Available online: https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/ (accessed on 11 November 2022).

3. Statista. Likelihood of Suffering a Hacker Attack 2021, by Country. Available online: https://www.statista.com/statistics/1228062/opinion-online-security-worldwide/ (accessed on 27 October 2022).
4. Abhishek, K.; Roshan, S.; Kumar, P.; Ranjan, R. A comprehensive study on multifactor authentication schemes. In *Advances in Computing and Information Technology*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 561–568.
5. Konoth, R.K.; van der Veen, V.; Bos, H. How anywhere computing just killed your phone-based two-factor authentication. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 22–26 February 2016; Springer: Berlin/Heidelberg, Germany, 2016; pp. 405–421.
6. Kim, J.J.; Hong, S.P. A method of risk assessment for multi-factor authentication. *J. Inf. Process. Syst.* **2011**, *7*, 187–198. [CrossRef]
7. Sinha, A.; Shrivastava, G.; Kumar, P. A Pattern-Based Multi-Factor Authentication System. *Scalable Comput. Pract. Exp.* **2019**, *20*, 101–112. [CrossRef]
8. Dasgupta, D.; Roy, A.; Nag, A. Toward the design of adaptive selection strategies for multi-factor authentication. *Comput. Secur.* **2016**, *63*, 85–116. [CrossRef]
9. Bonneau, J.; Herley, C.; Van Oorschot, P.C.; Stajano, F. Passwords and the evolution of imperfect authentication. *Commun. ACM* **2015**, *58*, 78–87. [CrossRef]
10. Gunson, N.; Marshall, D.; Morton, H.; Jack, M. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Comput. Secur.* **2011**, *30*, 208–220. [CrossRef]
11. Ometov, A.; Bezzateev, S.; Mäkitalo, N.; Andreev, S.; Mikkonen, T.; Koucheryavy, Y. Multi-Factor Authentication: A Survey. *Cryptography* **2018**, *2*, 1. [CrossRef]
12. Shacklett, M.E. What Is Multifactor Authentication and How Does It Work? *SearchSecurity*. Available online: https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA (accessed on 3 November 2021).
13. Frank, M.; Biedert, R.; Ma, E.; Martinovic, I.; Song, D. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 136–148. [CrossRef]
14. Jorgensen, Z.; Yu, T. On mouse dynamics as a behavioral biometric for authentication. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, China, 22–24 March 2011; ACM: New York, NY, USA, 2011; pp. 476–482.
15. National Research Council; Whither Biometrics Committee. *Biometric Recognition: Challenges and Opportunities*; National Academies Press: Washington, DC, USA, 2010.
16. Rane, S.; Wang, Y.; Draper, S.C.; Ishwar, P. Secure biometrics: Concepts, authentication architectures, and challenges. *IEEE Signal Process. Mag.* **2013**, *30*, 51–64. [CrossRef]
17. How Biometrics Are Attacked. Available online: https://www.ncsc.gov.uk/collection/biometrics/how-biometrics-are-attacked (accessed on 15 November 2022).
18. Han, K.; Potluri, S.D.; Shin, K.G. On authentication in a connected vehicle: Secure integration of mobile devices with vehicular networks. In Proceedings of the International Conference on Cyber-Physical Systems (ICCPS), Philadelphia, PA, USA, 8–11 April 2013; pp. 160–169.
19. Ishtiaq Roufa, R.M.; Mustafaa, H.; Travis Taylora, S.O.; Xua, W.; Gruteserb, M.; Trappeb, W.; Seskarb, I. Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. In Proceedings of the 19th USENIX Security Symposium, Washington, DC, USA, 11–13 August 2010; pp. 11–13.
20. Chaurasia, B.K.; Verma, S. Infrastructure based authentication in VANETs. *Int. J. Multimed. Ubiquitous Eng.* **2011**, *6*, 41–54.
21. Rossi, B. Connected Car Security: Why Identity Should Be in the Driving Seat. 2016. Available online: http://www.information-age.com/connected-car-security-why-identity-should-be-driving-seat123461078/ (accessed on 15 November 2022).
22. Bartłomiejczyk, M.; Imed, E.; Kurkowski, M. Multifactor Authentication Protocol in a Mobile Environment. *IEEE Access* **2019**, *7*, 157185–157199. Available online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8879478&isnumber=8600701 (accessed on 15 November 2022). [CrossRef]
23. Ibrahim, D.; The, J.; Abdullah, R. Multifactor authentication system based on color visual cryptography, facial recognition, and dragonfly optimization. *Inf. Secur. J. Glob. Perspect.* **2019**, *30*, 149–159. [CrossRef]
24. Lu, D.; Huang, D.; Deng, Y.; Alshamrani, A. Multifactor User Authentication with In-Air-Handwriting and Hand Geometry. In Proceedings of the 2018 International Conference on Biometrics (ICB), Gold Coast, QLD, Australia; 2018; pp. 255–262. Available online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8411230&isnumber=841184 (accessed on 17 November 2022).
25. Vaithyasubramanian, S. Authentication using Robust Primary PIN (Personal Identification Number), Multifactor Authentication for Credit Card Swipe and Online Transactions Security. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 541–546. [CrossRef]
26. Lone, S.A.; Mir, A.H. A novel OTP based tripartite authentication scheme. *Int. J. Pervasive Comput. Commun.* **2022**, *18*, 437–459. [CrossRef]
27. Amit, E.; Rim, S.; Halbeisen, G.; Priva, U.C.; Stephan, E.; Trope, Y. Distance-dependent memory for pictures and words. *J. Mem. Lang.* **2019**, *105*, 119–130. [CrossRef]
28. ALSaleem, B.O.; Alshoshan, A. Multi-Factor Authentication to Systems Login. In Proceedings of the 2021 National Computing Colleges Conference (NCCC), Taif, Saudi Arabia, 27–28 March 2021. Available online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9428806&isnumber=9428786 (accessed on 17 November 2022).

29. Sabzevar, A.; Stavrou, A. Universal Multi-Factor Authentication Using Graphical Passwords. In Proceedings of the 2008 IEEE International Conference on Signal Image Technology and Internet Based Systems, Bali, Indonesia, 30 November–3 December 2008; pp. 625–632. Available online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4725863&isnumber=4725761 (accessed on 17 November 2022).
30. Othman, N.; Rahman, M.; Sani, A.; Ali, F. Directional Based Graphical Authentication Method with Shoulder Surfing Resistant. In Proceedings of the 2018 IEEE Conference on Systems, Process and Control (ICSPC), Melaka, Malaysia, 14–15 December 2018; pp. 198–202. [CrossRef]
31. Chang, T.Y.; Tsai, C.; Lin, J. A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. *J. Syst. Softw.* **2012**, *85*, 1157–1165. [CrossRef]
32. Gyorffy, J.C.; Tappenden, A.F.; Miller, J. Token-based graphical password authentication. *Int. J. Inf. Secur.* **2011**, *10*, 321–336. [CrossRef]
33. Continuous Multi-Factor Authentication: The Future of MFA. Twosense. Available online: https://www.twosense.ai/blog/continuous-multi-factor-authentication-the-future-of-mfa#:~{}:text=The%20most%20commonly%20used%20MFA,identity%2020%2B%20times%20a%20day (accessed on 21 November 2022).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.