Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 4 Issue 3 (2024)

Enhancing two-factor authentication: Integrating face recognition with a dynamically generated token mechanism for secure transactions.

[1]D. Saravanan
[2]Dr. Anusha Sreeram
[12]Faculty of Operations & IT ICFAI Business School (IBS), Hyderabad,
The ICFAI Foundation for Higher Education (IFHE),
(Deemed to be university u/s 3 of the UGC Act 1956), Hyderabad-India

Abstract:
Today, image processing plays a vital role in authentication and other security purposes. Most smartphone users now rely on face recognition as one of the key mechanisms for mobile security. Additionally, many organizations use face recognition systems for authentication and attendance purposes. In such systems, users are required to use a specific security mechanism for approval and related activities. In the proposed paper, instead of relying solely on physical presence, static image data is captured and supplemented by a one-time generated token to enhance the authentication process. This method allows users to present a static digital image in front of the authorization system, after which they enter the one-time generated token as an additional layer of security. The proposed system eliminates the need for constant physical presence while improving two-factor authentication—combining face recognition with a dynamically generated token. As a result, the user's presence is verified, and the overall efficiency of the process is enhanced. The proposed procedure demonstrates that this technique yields more effective results compared to existing one-time authentication methods.

1. Introduction

In today's technological world, authentication is one of the major concerns for the user community. Various mechanisms have been implemented to ensure security, often requiring physical presence, such as face or thumb-based authentication, or the use of a one-time password generated by the system. In both cases, the user's physical presence and network strength play vital roles in the operation. These mechanisms also require additional components, such as terminals, security systems, network connectivity, and a secure environment, to function effectively. Authentication mechanisms are used for various purposes, including protecting user documents, images, or personal information, preventing theft, securing data, and restricting unauthorized access to workplaces or systems. However, these mechanisms depend on several factors, including hardware, software, networking components, and maintenance, which can make implementation costly and complex for certain communities.

Organizations need to carefully plan and allocate budgets for security operations, considering the environmental and operational requirements. The increasing complexity of networks, machinery, and supporting functions has made it burdensome for many users and organizations to perform these operations effectively. To address these challenges, the proposed work introduces a system that eliminates the need for the user's physical presence while improving security through a two-factor authentication mechanism. Most existing techniques rely on users remembering secret keys, patterns, or specific terms. However, this can create a burden for users who must recall multiple authentication pins for various devices, such as terminals, mobile phones, security systems, and network equipment. The difficulty in remembering these keys often leads users to reuse the same pin across systems or write them down, which increases the risk of exposure to eavesdropping or unauthorized access.

To overcome these challenges, modern technology offers graphical-based authentication methods where users select specific parts of an image or design instead of entering content-based passwords. While this approach is easier for users, it still has vulnerabilities. This method allows users to present a static digital image in front of the authorization system, after which they enter the one-time generated token as an additional layer of security. The proposed system eliminates the need for constant physical presence while improving two-factor authentication—combining face recognition with a dynamically generated token. As a result, the user's presence is verified, and the overall efficiency of the process is enhanced. The proposed procedure demonstrates that this technique yields more effective results compared to existing one-time authentication methods.

If an eavesdropper identifies a user's preferences or interests, they might guess the chosen image, reducing security. The proposed technique addresses this issue by allowing users to use their own pictures for authentication. In this method, users can use personal photographs, which may appear to others as regular profile pictures. This adds an additional layer of security, as eavesdroppers are less likely to associate the image with authentication purposes. By leveraging personal images, the system helps to performs more protected tasks like, substitute to outdated content-based or graphical authentication methods, enhancing the overall security process without adding unnecessary complexity. This proposed system addresses the limitations of existing systems by allowing users to utilize their own images instead of system-recommended images or patterns. System-recommended options often add unnecessary burden to users and may inadvertently provide clues to hackers based on users' preferences or areas of interest. Similarly, content-based authentication methods require users to maintain different input keys for various operations. This creates an additional burden, as users must remember multiple keys for different functionalities, increasing complexity. To overcome these challenges, the planned scheme allows operators to use their individual pictures for authentication. This approach eliminates the reliance on predefined images or patterns, reduces user effort, and enhances security by minimizing predictable elements. By empowering users to select personal images, the system not only simplifies the process but also offers robust protection against unauthorized access. The proposed system enhances process efficiency while reducing the burden on users, making operations more user-friendly and cost-effective. It is designed for easy implementation in any environment without requiring additional resources, specialized input systems, or supporting terminals. The results demonstrate that the proposed system consistently delivers a user-friendly experience and is simple to use, making it an ideal solution for diverse applications without imposing extra financial or technical burdens.

2. Existing Method

In the present scheme, authentication is typically based on content-based information, which poses several challenges for users. Users are required to remember complex combinations of input keys, often consisting of at smallest eight atmospheres, including capital words and samller letters, special characters, and numbers. This adds significant difficulty, especially as users are often required to set different passwords for various functions, preventing the reuse of the same input key across multiple operations. This complexity increases the cognitive load on users, making it hard to remember multiple unique passwords. Additionally, during the process of entering passwords, there is a higher risk of overhearing**,** where onlookers might guess or observe the input information. Content-based authentication, therefore, not only creates inconvenience for users but also exposes them to potential security vulnerabilities, highlighting the need for a more efficient and secure system.

2.3. Disadvantages of Existing System

- Authentication is typically based on content-based information.

- Users are often required to set different passwords for various functions, preventing the reuse of the same input key across multiple operations.
- The difficulty in remembering these keys often leads users to reuse the same pin across systems or write them down, which increases the risk of exposure to eavesdropping or unauthorized access.
- This complexity increases the cognitive load on users, making it hard to remember multiple unique passwords.
- User presence is highly required to enter the secreate key on the systems.
- Brings the high expanses, users has to spend more money on the various inputs systems such as terminals, security systems and network. It will gives the additional burden to the users.

2.4. Proposed System

The proposed technique addresses this issue by allowing users to use their own pictures for authentication. In this method, users can use personal photographs, which may appear to others as regular profile pictures. This adds an additional layer of security, as eavesdroppers are less likely to associate the image with authentication purposes. By leveraging personal images, the system offers a more protected, outdated content-based or graphical authentication methods, enhancing the overall security process without adding unnecessary complexity. The proposed system eliminates the need for constant physical presence while improving two-factor authentication—combining face recognition with a dynamically generated token. As a result, the user's presence is verified, and the overall efficiency of the process is enhanced. The proposed procedure demonstrates that this technique yields more effective results compared to existing one-time authentication methods.

Content-based input authentication often creates challenges for users. Nowadays, users are required to create passwords that comply with complex rules, including a minimum of eight characters, at least one uppercase letter, one special character, and one numerical digit. While these requirements aim to enhance security, they can be burdensome, especially for less tech-savvy or non-educated individuals. Even for educated users, managing multiple passwords for various applications can be daunting, as reusing the same password across platforms weakens security. Another significant drawback of content-based authentication is the periodic requirement to modification keywords, often each ninety days for safety causes. This adds further complexity, leading many users to adopt insecure practices such as writing down passwords or using easily guessable patterns. Recognizing these limitations, some systems have introduced graphical input-based authentication. However, these systems typically require users to select images predefined by the system, limiting user choice. Additionally, these image-based inputs can be easily observed and guessed by nearby individuals who recognize the user’s preferences or selections.

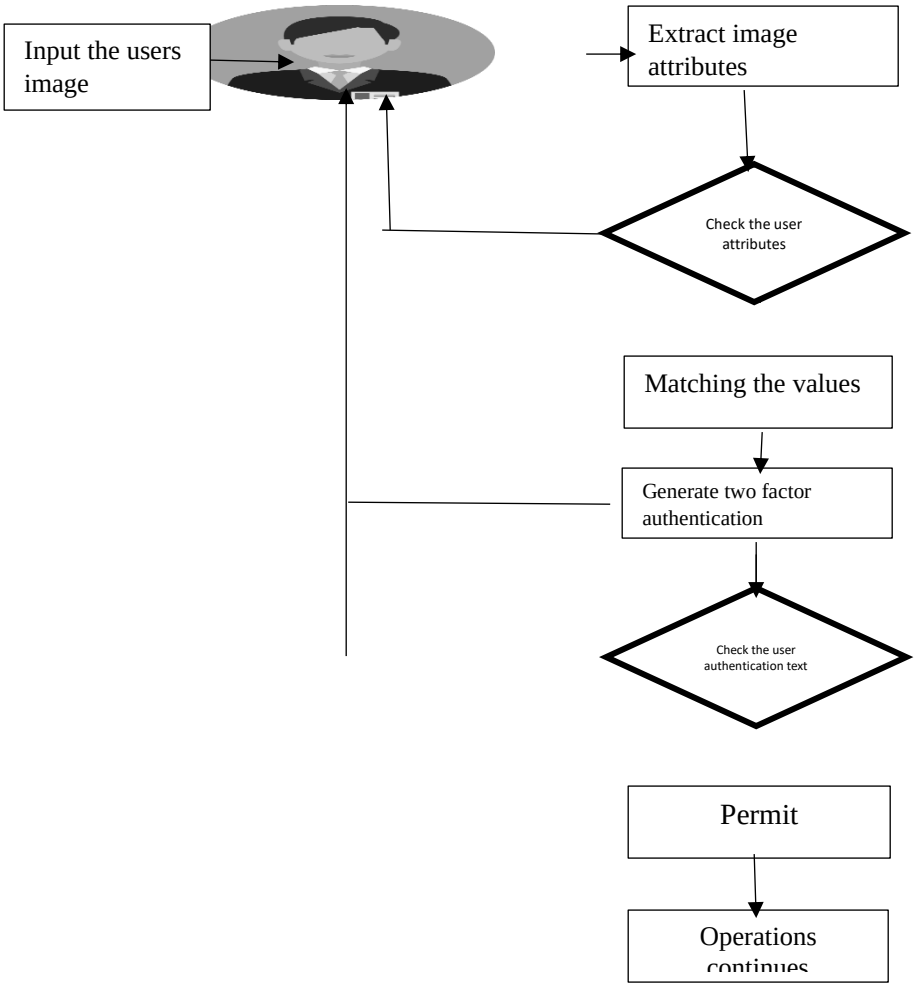

Fig 1. Proposed select by own picture and one time secrete key authentication architecture.

To address these shortcomings, the proposed model introduces a user-centric solution. Instead of relying on system-generated text or graphical inputs, users can select their own images as input data. They can then designate specific parts of their chosen image as authentication keys. This personalized approach enhances security and eliminates the need for users to memorize arbitrary passwords or follow restrictive rules. An added feature of this system is its dual authentication mechanism. Once a user provides their image-based input, the system generates a one-time authentication key that is sent to the user's mobile device. The user must enter this one time input within a stipulated time to complete the authentication process. This combination of personalized image input and time-sensitive ensures a robust, secure, and efficient authentication system.

Moreover, the proposed system eliminates the need for costly infrastructure such as terminals, additional security mechanisms, or complex network setups required by traditional systems. Users can authenticate themselves using existing devices, such as mobile phones, making the process more cost-effective and accessible.

Advantages of the Proposed System:

1. User-friendly: By allowing users to use their own images, there is no need to remember complicated passwords or system-defined inputs.

2. Enhanced Security: The dual authentication process (image input and OTP) significantly reduces the risk of unauthorized access.
3. Cost Efficiency: The system does not require specialized hardware or network configurations, reducing implementation costs.
4. Improved Performance: Time-bound authentication and streamlined processes enhance the overall efficiency and reliability of the system.

In conclusion, the proposed system offers a secure, cost-effective, and the substitute to outdated content-based and graphical authentication methods, addressing the limitations of existing systems while improving performance and usability.

3. Experimental arrangement:

The experimental setup of the proposed system differs significantly from the traditional system. In traditional systems, the user's physical presence is often mandatory for providing any input, making it a requirement for the process. However, our proposed system eliminates this dependency and introduces a two-factor authentication mechanism, unlike the single authentication used in existing systems. Considering these factors, the proposed technique is designed with the following modules.

- User profile creation.
- Input the users picture
- Agree or terminate
- Usability evaluation
- Draw line authentication
- Sudden disturbance effect

3.1 User profile creation:

By allowing users to use their own pictures for authentication. In this method, users can use personal photographs, which may appear to others as regular profile pictures. This adds an additional layer of security, as eavesdroppers are less likely to associate the image with authentication purposes. By leveraging personal images, the system provides a more secure, substitute to outdated content-based or graphical authentication methods, enhancing the overall security process without adding unnecessary complexity. This proposed system addresses the limitations of existing systems by allowing users to utilize their own images instead of system-recommended images or patterns. System-recommended options often add unnecessary burden to users and may inadvertently provide clues to hackers based on users' preferences or areas of interest. By leveraging personal images, the system provides a more safe, another to outdated content-based or graphical authentication methods, enhancing the overall security process without adding unnecessary complexity. The proposed system eliminates the need for constant physical presence while improving two-factor authentication—combining face recognition with a dynamically generated token. As a result, the user's presence is verified, and the overall efficiency of the process is enhanced.

3.2 Input the user image:

Instead of relying on system-generated text or graphical inputs, users can select their own images as input data. They can then designate specific parts of their chosen image as authentication keys. This personalized approach enhances security and eliminates the need for users to memorize arbitrary passwords or follow restrictive rules.

3.3 Agree or terminate:

In this module, the system verifies the credentials of the selected secure image using image coordinates. Each time a new image is provided as input, the corresponding image coordinates are generated and stored for future operations. These coordinate values play a critical role in the authentication process. During each authentication attempt, the system compares the input image's coordinates with the stored values. If both match, the user is directed to the second authentication technique. It is essential to capture and securely store these coordinates for subsequent operations. This module maintains a repository of coordinate values for all input images, enabling it to function as a key component in the authentication or validation process. By comparing the user's input against the stored values, the module enhances the overall efficiency and reliability of the system.

3.4 Usability evaluation:

- In this module system uses both public and private images for authentication.
- Here is the comparison take place between public and private images.
- This module is divides in to two modules. They are
- Public images
- Private Images
- Public images
- In Public images module have The system provide two or three images default to the system.
- User can select any of the images from the system and can select any point from the selected image and set as password to the system In.
- The point we marked in public images are hard to remember because the image published in public images are new to users.
- Private images:-
- In this module users can set their own image as password. System will not provide any images for setting the password.
- User can borrow their images from gallery and select any point from the image for setting password.
- Private image Authentications are more efficient than public image authentication. Because In this Authentication User will select their own images from gallery. It will easy to remember.

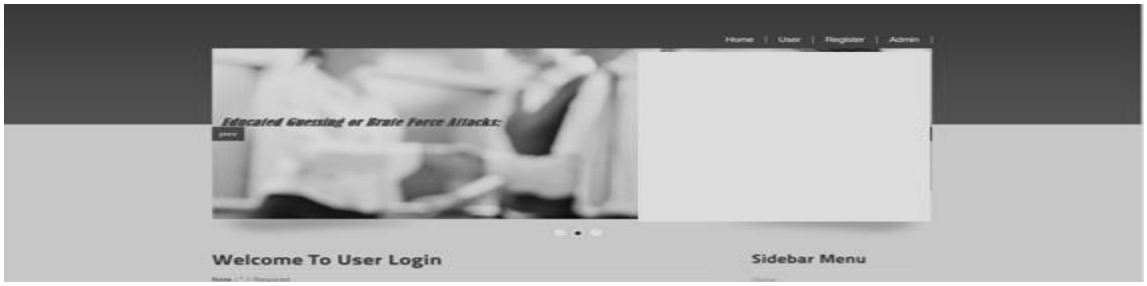

Figure 2. User registration process.

Figure 3. Collection of users particulars.

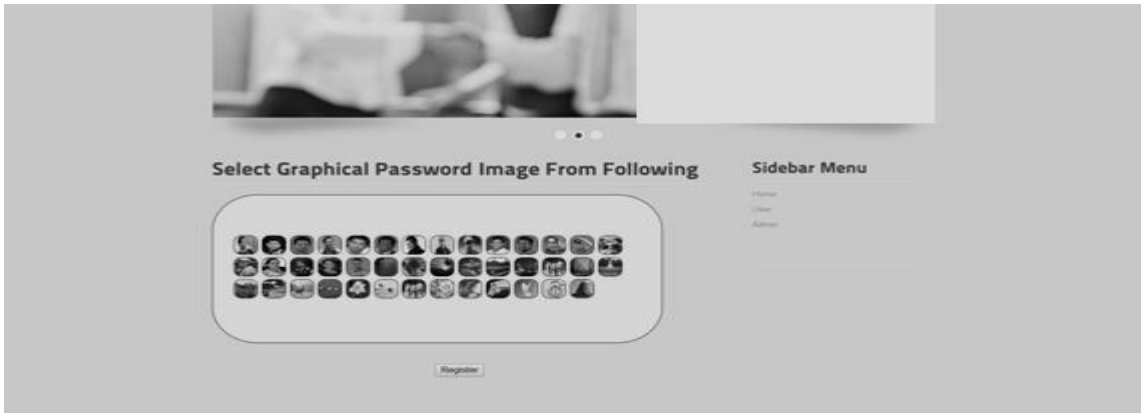

Figure 4. Operator image storage.

Figure 5 Operator accept/reject form.

Figure 6. Registered users creational

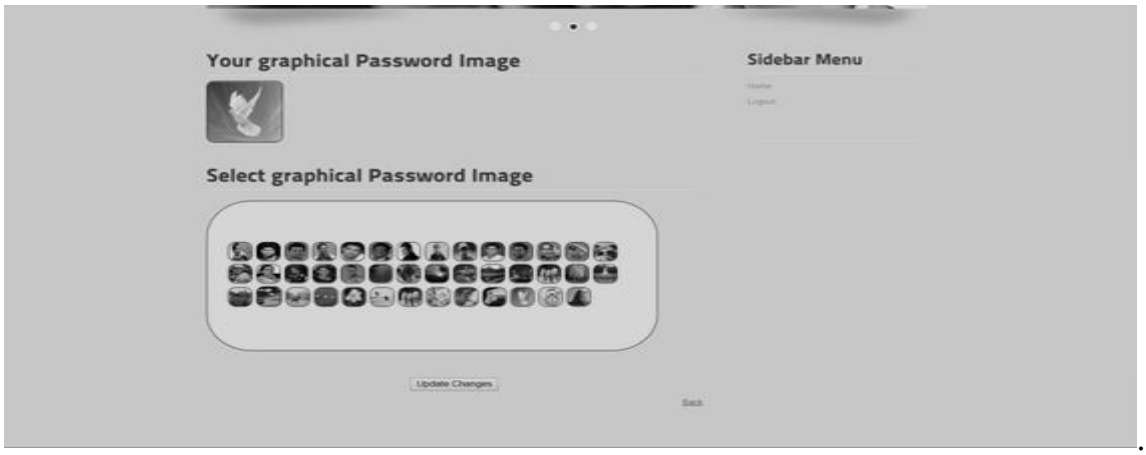

Figure 7. Input the Select image.

Figure 8. Input the one time secret key

Conclusion

In today's technological world, authentication is one of the major concerns for the user community. Various mechanisms have been implemented to ensure security, often requiring physical presence, such as face or thumb-based authentication, or the use of a one-time password generated by the system. In both cases, the user's physical presence and network strength play vital roles in the operation. . In this method, users can use personal photographs, which may appear to others as regular profile pictures. This adds an additional layer of security, as eavesdroppers are less likely to associate the image with authentication purposes. By leveraging personal images, the system provides a more secure, user-

friendly alternative to traditional content-based or graphical authentication methods, enhancing the overall security process without adding unnecessary complexity. Moreover, the proposed system eliminates the need for costly infrastructure such as terminals, additional security mechanisms, or complex network setups required by traditional systems. Users can authenticate themselves using existing devices, such as mobile phones, making the process more cost-effective and accessible

References:

[1]A. Adams and M. Sasse, "Users are not the enemy," Commun. ACM, vol. 42, pp. 40–46, 1999.
[2] M. Adham, A. Azodi, Y. Desmedt, and I. Karaolis, "How to attack twofactor authentication internet banking," in Proc. 17th Int. Conf. Financial Cryptography, 2013, pp. 322–328.
[3] D.Saravanan,Dr. Dennis Joseph," Image data extraction using image similarities", Lecture otes in Electrical engineering, Volume 521, Pages 409-420, ISBN:978-981-13-1905-1,Nov 2018.
[4] D.Saravanan," Effective Data Retrieval using image key frame selection", First International conference on computational intelligence and informatics(ICCII-2016),May 2016, Pages 1-6.
[5] F. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using mobile phones," Proc. Comput. Syst. Appl., 2009, pp. 641–644.
[6] R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Surveys vol. 44, no. 4, p. 19, 2012.
[7] D.Saravanan**,"**CURE Clustering Suitable for video data retrieval"**,** in the Proc. Of 2016 IEEE International Conference on Computational Intelligence and computing Research, Pages 306-309, Dec 2016.
[8] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in Proc. IEEE Symp. Security Privacy, 2012, pp. 553–567.
[9] S.Chiasson, R. Biddle, and P. van Oorschot, "Asecond look at the usability of click-based graphical passwords," in Proc. 3rd Symp. Usable Privacy Security, 2007, pp. 1–12.
[10] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in Proc. 12th Eur. Symp. Res. Comput. Security, 2007, pp. 359–374.
[11] D. Saravanan, "Secure Financial transactions by using the picture binding secret writing scheme", European Economic Letters, ISSN:2323-2533, Volume 14, Issues 1(2024) Pages 1766-1773.
[12] D. Saravanan, Dr. KVVSSN Murty, "Information flow identification using the Package marking systems" Journal of informatics educations and research, Vol 3 issues 2(2023), ISSN: 1526-4726,
[13] S. Chiasson, A. Forget, R. Biddle, and P. C. Oorschot, "User interface design affects security: Patterns in click-based graphical passwords, Int. J. Inf. Security, vol. 8, no. 6, pp. 387–398, 2009.