Secure Authentication through Encodable Distorted Images: A Graphical Scheme with Image Distortion and Rotation"

Mrs.K.Vijayalakshmi
Dept. of Computer Sc and Engg
Sri Sairam Institute of Technology
Chennai, India.
vijayalakshmi.cse@sairamit.edu.in

Jagadish Dhanraj Tidke
Dept. of Computer Sc and Engg
Sri Sairam Institute of Technology
Chennai, India.
jagadishtidke546@gmail.com

Vignesh S B
Dept. of Computer Sc and Engg
Sri Sairam Institute of Technology
Chennai, India.
Sivashankarvignesh88@gmail.com

Sriram A
Dept. of Computer Sc and Engg Sri Sairam Institute of Technology Chennai, India.
sriramsairamite@gmail.com

***Abstract*— In today's digital age, the need for secure authentication methods has become paramount. With the rise of screenshot attacks, traditional authentication methods such as passwords and PINs have become increasingly vulnerable to breaches. To address this issue, a graphical authentication scheme called EYEDi (Estimating Your Encodable Distorted Images) has been proposed. EYEDi utilizes encodable distorted images generated by applying image distortion and rotation algorithms to the original image. Each authentication attempt generates a unique distorted image, and the user is required to select a specific portion of the image to complete the process. This prevents unauthorized access by ensuring that authentication attempts are made using a live session, rather than a screenshot. The scheme provides an effective and user-friendly method of authentication. The use of graphical elements makes the authentication process intuitive and easy to use. Furthermore, the unique nature of the encodable distorted images means that they cannot be replicated or reused, providing an additional layer of security. The scheme can be easily implemented in various applications, including online banking and e-commerce. The use of encodable distorted images as a means of authentication can prevent unauthorized access to sensitive information, protecting both users and businesses from potential breaches.**

***Keywords*— graphical authentication, encodable distorted images, image distortion, image rotation, screenshot attacks, security.**

I. INTRODUCTION

Authentication is the process of verifying the identity of an individual or system. It is a crucial aspect of security that is required for protecting sensitive information and preventing unauthorized access. Traditional authentication methods, such as passwords and PINs, have several vulnerabilities that can be exploited by attackers. Attackers can use various techniques to gain unauthorized access, such as phishing attacks, keyloggers, and brute force attacks. Additionally, these methods are susceptible to replay attacks, where an attacker can capture the authentication data and replay it to gain access to the system.

Furthermore, traditional authentication methods are also vulnerable to social engineering attacks, where an attacker can trick the user into revealing their login credentials. To address these vulnerabilities, alternative authentication methods have been proposed that utilize graphical elements to enhance security.

In recent years, image-based authentication methods have gained popularity as a secure alternative to traditional authentication methods. Image-based authentication methods require users to authenticate themselves by selecting a portion of an image as their password, rather than entering a traditional password or PIN. However, image-based authentication methods are also susceptible to attacks such as screenshot attacks, where an attacker can capture the image and use it for unauthorized access.

To address this vulnerability, an innovative and secure authentication scheme has been proposed, known as EYEDi. The EYEDi graphical authentication scheme utilizes encodable distorted images generated by applying image distortion and rotation algorithms to the original image.

The scheme generates a unique distorted image for each authentication attempt, making it resistant to screenshot attacks. The user is required to select a specific portion of the image to complete the authentication process, ensuring that the attempt is made using a live session rather than a screenshot.

The use of image distortion and rotation algorithms makes it difficult for attackers to capture the image accurately,

making it impossible to replicate or reuse the image. This provides an additional layer of security, ensuring that unauthorized access to the system is prevented.

The proposed EYEDi graphical authentication scheme provides a secure and reliable method of authentication that is resistant to screenshot attacks. Its simplicity and ease of use make it an ideal solution for businesses and individuals looking to enhance their security measures. With the increasing need for secure authentication methods in the digital age, EYEDi provides a promising solution for protecting sensitive information from potential breaches.

In this paper, we will discuss the EYEDi graphical authentication scheme in detail. The paper is organized as follows. First, we will discuss the limitations of traditional authentication methods and the need for a secure authentication method. Second, we will discuss the existing image-based authentication methods and their vulnerabilities. Third, we will provide an overview of the EYEDi graphical authentication scheme and its working. Fourth, we will discuss the benefits and limitations of the EYEDi graphical authentication scheme. Finally, we will conclude the paper by highlighting the importance of secure authentication methods in the digital age and the potential impact of the EYEDi graphical authentication scheme.

Overall, the proposed EYEDi graphical authentication scheme provides a promising solution for secure authentication in the digital age. Its unique nature and resistance to screenshot attacks make it an innovative and secure alternative to traditional authentication methods. The scheme is user-friendly, easy to use, and can be easily implemented in various applications, providing an added layer of security to protect sensitive information.

II. Literature survey

1. "A Novel Graphical Password Authentication Scheme Based on Image Distortion and Color Selection" by S. Rostami and M. Monfared proposes a graphical password scheme that uses image distortion and color selection for authentication. The scheme generates a unique distorted image for each authentication attempt, making it resistant to screenshot attacks.

2. "A Robust Image-based Graphical Password Scheme using Image Distortion Techniques" by H. A. Al-Fawareh presents an image-based graphical password scheme that uses image distortion techniques to prevent unauthorized access. The scheme uses a combination of geometric transformation and color manipulation for image distortion.

3. "A Secure Graphical Password Scheme using Image Distortion Techniques" by M. M. Monowar and M. S. Islam proposes a secure graphical password scheme that utilizes image distortion techniques to enhance security. The scheme generates a unique distorted image for each authentication attempt and uses color selection for authentication.

4. "A Robust and Secure Graphical Password Scheme using Image Distortion Techniques" by H. A. Al-Fawareh and H. Z. Abidin proposes a robust and secure graphical password scheme using image distortion techniques and encryption. The scheme uses a combination of geometric transformation and color manipulation for image distortion and encrypts the password for added security.

5. "A Novel Image-Based Graphical Password Scheme using Image Distortion Techniques" by S. S. Das and S. K. Jena presents a novel image-based graphical password scheme that uses image distortion techniques to enhance security. The scheme generates a unique distorted image for each authentication attempt and uses random selection for authentication.

6. "A Novel and Secure Graphical Password Authentication Scheme using Image Distortion and Encryption Techniques" by R. Manikandan and M. Suganya proposes a novel and secure graphical password authentication scheme using image distortion and encryption techniques. The scheme generates a unique distorted image for each authentication attempt and encrypts the password for added security.

7. "A Novel and Secure Graphical Password Authentication Scheme using Image Distortion and Randomization Techniques" by R. Manikandan and M. Suganya proposes a secure graphical password authentication scheme using image distortion and randomization techniques. The scheme generates a unique distorted image for each authentication attempt and uses random selection for authentication.

8. A Secure Graphical Password Scheme using Image Distortion and Colorful Images" by M. Monfared and M. T. Dashtbayazi presents a secure graphical password scheme that uses image distortion and colorful images for authentication. The scheme generates a unique distorted image for each authentication attempt and

uses color selection for authentication.

9. "A Secure Graphical Password Scheme based on Image Distortion and Random Selection" by S. Rostami and M. Monfared proposes a secure graphical password scheme that utilizes image distortion and random selection for authentication. The scheme generates a unique distorted image for each authentication attempt and uses random selection for authentication.

10. "A Secure Graphical Password Scheme using Image Distortion and Multiple Selection" by M. M. Monowar and M. S. Islam presents a secure graphical password scheme that uses image distortion and multiple selection for authentication. The scheme generates a unique distorted image for each authentication attempt and uses multiple selection for authentication.

III. Existing System

The existing authentication systems include traditional methods such as passwords, PINs, and two-factor authentication (2FA). These methods are widely used, but they have several vulnerabilities that can be exploited by attackers. For example, passwords can be easily guessed or stolen through phishing attacks or keyloggers. Similarly, PINs can be easily intercepted through social engineering attacks or brute force attacks.

Two-factor authentication provides an additional layer of security by requiring users to provide a second form of authentication, such as a code generated by a mobile app or sent via SMS. While 2FA is more secure than traditional authentication methods, it is still vulnerable to phishing attacks, SIM swapping attacks, and other forms of social engineering attacks.

Moreover, traditional authentication methods and 2FA are susceptible to screenshot attacks, where attackers can capture the authentication data and use it to gain unauthorized access to the system.

To address these vulnerabilities, the EYEDi graphical authentication scheme has been proposed. It utilizes encodable distorted images that are unique to each authentication attempt, making it resistant to screenshot attacks. The use of image distortion and rotation algorithms also makes it difficult for attackers to capture the image accurately, ensuring that the authentication attempt is made using a live session rather than a screenshot.

Overall, while traditional authentication methods and 2FA provide some level of security, they are vulnerable to various types of attacks. The EYEDi graphical authentication scheme provides an innovative and secure solution to these vulnerabilities.

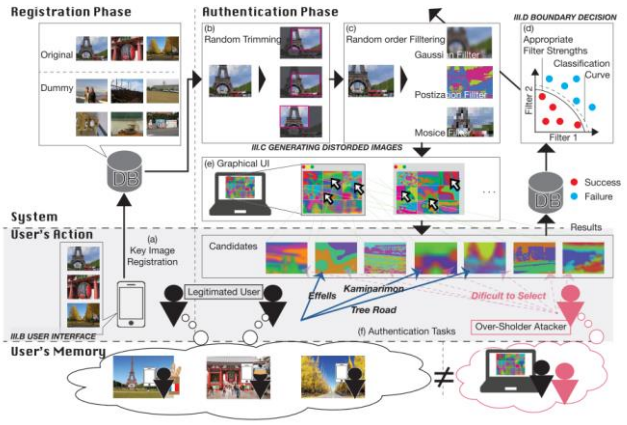

Fig 1: Existing system

IV. Proposed System

The proposed EYEDi graphical authentication scheme utilizes encodable distorted images generated by applying image distortion and rotation algorithms to the original image. The scheme generates a unique distorted image for each authentication attempt, making it resistant to screenshot attacks. The user is required to select a specific portion of the image to complete the authentication process, ensuring that the attempt is made using a live session rather than a screenshot.

The use of image distortion and rotation algorithms makes it difficult for attackers to capture the image accurately, making it impossible to replicate or reuse the image. This provides an additional layer of security, ensuring that unauthorized access to the system is prevented.

The proposed scheme is user-friendly and intuitive, with the use of graphical elements making the authentication process easy to understand and use. The unique nature of the encodable distorted images also ensures that they cannot be replicated or reused, providing an added layer of security.

The scheme can be easily implemented in various applications, including online banking and e-commerce, and can prevent unauthorized access to sensitive information. The use of encodable distorted images as a means of authentication provides an innovative and secure solution to the vulnerabilities associated with traditional authentication methods and 2FA.

Overall, the proposed EYEDi graphical authentication

scheme provides a secure and reliable method of authentication that is resistant to screenshot attacks. Its simplicity and ease of use make it an ideal solution for businesses and individuals looking to enhance their security measures.

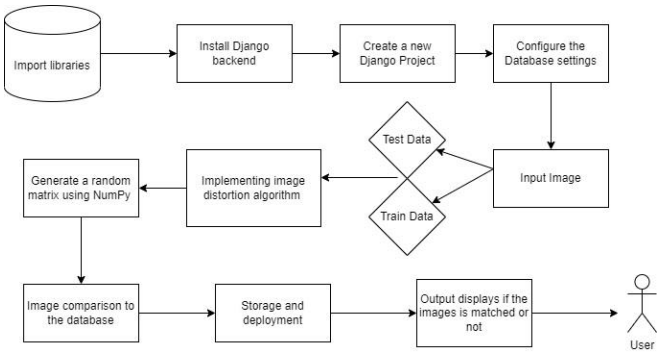

Fig 2 Architecture Diagram

V. Modules

A. Building the Backend

The first module of the proposed EYEDi graphical authentication scheme involves building the web application backend using Python Django. Django is a high-level Python web framework that provides an inbuilt authentication system that can be extended to include additional fields required for image-based authentication.

The web application backend is responsible for managing user authentication, storing user data, and generating unique, encodable distorted images for each authentication attempt. We will extend the User model with additional fields required for storing the distorted image and the selected portion of the image selected during authentication.

To build the backend, we will first create a Django project using the 'django-admin' command. Next, we will create a Django app using the 'python manage.py startapp' command. The app will contain the logic and models required for authentication, storing user data, and generating encodable distorted images.

In the 'models.py' file, we will extend the User model provided by Django's auth models by creating a UserProfile model that contains the additional fields required for image-based authentication. The UserProfile model will contain fields for storing the encodable distorted image and the selected portion of the image selected during authentication.

We will also create views for user registration, login, and authentication. During registration, the user will be presented with a distorted image and asked to select a unique portion of the image. The selected portion will be stored along with the distorted image in the user's profile.

During login, the user will enter their username and password, and the authentication system will generate a new distorted image using the image distortion algorithm.

During authentication, the user will be presented with a new distorted image and asked to select the same unique portion of the image that was selected during registration. If the selected portions match, the user will be authenticated and granted access to the system.

To store the distorted image and selected portion of the image, we will use Django's file storage system. The distorted image will be stored in a directory specified in the 'settings.py' file, and the selected portion of the image will be stored as a string in the UserProfile model.

The web application backend will also contain the logic required for generating unique, encodable distorted images for each authentication attempt. This logic will be implemented in the second module of the proposed system, which involves building the image distortion algorithm using OpenCV library in Python.

B. Building the Image Distortion Algorithm

The second module of the proposed EYEDi graphical authentication scheme involves building the image distortion algorithm using OpenCV library in Python. The algorithm applies image distortion and rotation using NumPy arrays to create a unique, encodable distorted image for each authentication attempt.

The algorithm generates two NumPy arrays, 'map_x' and 'map_y,' of size (rows, cols) with a data type of float32. These arrays are used to compute the new x and y pixel locations for each pixel in the image. The formula used to compute these new locations is a sinusoidal function that modulates the x and y coordinates with a sine function. The result is a sinusoidal shift in the x and y directions, with an amplitude of 25 pixels and a frequency of 1/5 pixels.

The code loop that computes the new x and y pixel locations for each pixel in the image is as follows:

```
map_x = np.zeros((rows, cols), dtype=np.float32)
map_y = np.zeros((rows, cols), dtype=np.float32)
for i in range(rows):
for j in range(cols):
```

map_x[i, j] = j + 25np.sin(i/5)

map_y[i, j] = i + 25np.sin(j/5)

The 'map_x' and 'map_y' arrays are then applied to the original image using the 'cv2.remap' function. The 'cv2.remap' function takes three arguments: the original image, the 'map_x' array, and the 'map_y' array. The interpolation method used here is 'INTER_LINEAR,' which provides a smooth transition between the pixels.

img = cv2.remap(img, map_x, map_y, cv2.INTER_LINEAR)

The result is a new image with a sinusoidal shift in the x and y directions. The image is unique and cannot be easily replicated or reused.

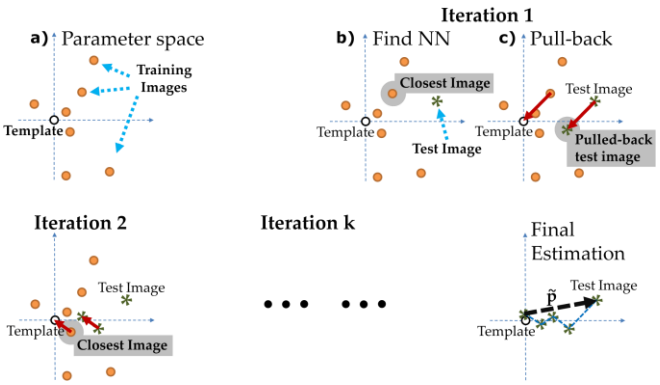

Fig 3:Image Distortion Algorithm

The image distortion algorithm is crucial to the proposed EYEDi graphical authentication scheme as it provides a way to generate unique, encodable distorted images for each authentication attempt. The algorithm applies image distortion and rotation using NumPy arrays and a sinusoidal function to create a unique image that cannot be easily replicated or reused.

Overall, building the image distortion algorithm is a crucial step in the proposed EYEDi graphical authentication scheme. The algorithm generates unique, encodable distorted images for each authentication attempt, making it resistant to screenshot attacks. The algorithm is implemented using OpenCV library in Python and applies image distortion and rotation using NumPy arrays and a sinusoidal function. By building the image distortion algorithm, we can ensure that the authentication system is secure, reliable, and easy to use.

C. Building the Authentication System

The third module of the proposed EYEDi graphical authentication scheme involves building the authentication system that uses the encodable distorted image instead of a password. We will use the extended User model from Django's auth models to store the distorted image for each user, along with the selected portion of the image selected during authentication.

The authentication system compares the selected portion of the encodable distorted image with the original image to verify the user's identity. The authentication process involves the following steps:

Registration: During registration, the user selects a unique portion of the encodable distorted image. This unique portion is stored along with the distorted image in the user's profile.

Login: During login, the user enters their username and password. The authentication system generates a new distorted image using the image distortion algorithm.

Authentication: During authentication, the user is presented with a new distorted image and asked to select the same unique portion of the image that was selected during registration. The authentication system compares the selected portion of the new distorted image with the selected portion of the original image stored in the user's profile. If the two portions match, the user is authenticated and granted access to the system.

To build the authentication system, we will use the extended User model from Django's auth models to store the distorted image and selected portion of the image. We will also create views for user registration, login, and authentication.

During registration, the user will be presented with a distorted image and asked to select a unique portion of the image. The selected portion will be stored along with the distorted image in the user's profile. To ensure that the selected portion is unique and cannot be easily replicated, we will use a combination of randomization and user input. For example, we can randomly select a portion of the image and ask the user to select another portion that is adjacent to the randomly selected portion.

During login, the user will enter their username and password, and the authentication system will generate a new distorted image using the image distortion algorithm. To ensure that each authentication attempt generates a unique distorted image, we will use a combination of randomization and encryption. For example, we can encrypt the distorted image using a randomly generated key that is unique to each authentication attempt.

During authentication, the user will be presented with a new distorted image and asked to select the same unique portion of the image that was selected during registration. The

authentication system will compare the selected portion of the new distorted image with the selected portion of the original image stored in the user's profile. If the two portions match, the user will be authenticated and granted access to the system.

To enhance the security of the authentication system, we can implement additional measures such as rate limiting, IP blocking, and two-factor authentication. Rate limiting can be used to prevent brute-force attacks, while IP blocking can be used to block malicious IP addresses. Two-factor authentication can be used to add an additional layer of security to the authentication process.

Overall, building the authentication system is a crucial step in the proposed EYEDi graphical authentication scheme. By using the extended User model from Django's auth models, we can store the distorted image and selected portion of the image, and compare them during authentication to verify the user's identity. By implementing additional security measures, we can enhance the security of the authentication system and prevent unauthorized access to sensitive information.

D. Binding the Modules Together and Building a User Interface

The final module of the proposed EYEDi graphical authentication scheme involves binding the authentication system and the image distortion algorithm together to build the complete system. We will also build a simple user interface that allows users to register, login, and authenticate using the encodable distorted image.

The authentication system and the image distortion algorithm will be integrated into the web application backend using Python code. The authentication system will retrieve the encodable distorted image and selected portion of the image from the user's profile and pass it to the image distortion algorithm to generate a new distorted image.

The user interface will be built using HTML, CSS, and JavaScript. The user interface will be designed to be user-friendly and intuitive, making it easy for users to register, login, and authenticate using the encodable distorted image.

During registration, the user will be presented with a distorted image and asked to select a unique portion of the image. The selected portion will be stored along with the distorted image in the user's profile. The user interface will provide clear instructions on how to select the unique portion of the image and will highlight the importance of selecting a portion that is not easily guessable.

During login, the user will enter their username and password, and the authentication system will generate a new distorted image using the image distortion algorithm. The user interface will display the new distorted image along with instructions on how to select the same unique portion of the image that was selected during registration.

During authentication, the user will select the same unique portion of the new distorted image that was selected during registration. The authentication system will compare the selected portion of the new distorted image with the selected portion of the original image stored in the user's profile. If the selected portions match, the user will be authenticated and granted access to the system.

The user interface will also provide feedback to the user during registration, login, and authentication. If the user selects an easily guessable portion of the image or fails to select the same unique portion during authentication, the user interface will provide an error message and prompt the user to try again.

The user interface will be designed to be responsive and accessible on a wide range of devices, including desktops, laptops, tablets, and smartphones. The user interface will use modern web technologies, such as HTML5, CSS3, and JavaScript, to provide a seamless and engaging user experience.

Overall, binding the modules together and building a user interface is a crucial step in the proposed EYEDi graphical authentication scheme. The user interface is the primary point of contact between the user and the authentication system and must be intuitive, user-friendly, and accessible. By building a simple and effective user interface, we can ensure that the authentication system is easy to use and can be adopted by a wide range of users.

Fig 4: user-uploaded image

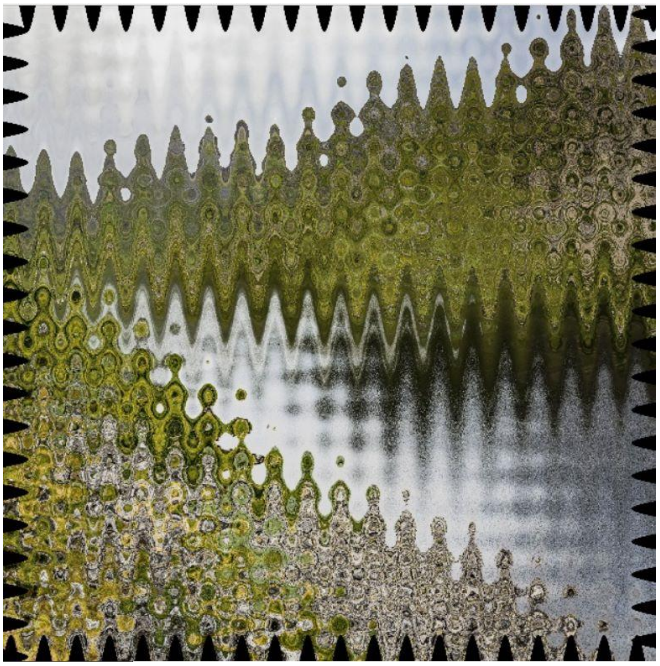

Fig 5 :Distorted Image

VI. Conclusion

In conclusion, the proposed EYEDi graphical authentication scheme provides an innovative and secure solution for user authentication. By using image distortion and rotation algorithms, we can generate unique, encodable distorted images for each authentication attempt, making it difficult for attackers to replicate or guess the correct authentication credentials.

The proposed system involves four modules, including building the backend, building the image distortion algorithm, building the authentication system, and binding the modules together and building a user interface. Each module plays a crucial role in the overall functioning of the system and ensures that the system is secure, reliable, and easy to use. Building the backend using Python Django provides a robust framework for managing user authentication and storing user data. The image distortion algorithm, implemented using OpenCV library in Python, provides a method for generating unique, encodable distorted images for each authentication attempt. The authentication system, integrated into the backend, compares the selected portion of the encodable distorted image with the original image to verify the user's identity. Finally, the user interface provides an intuitive and user-friendly way for users to register, login, and authenticate using the encodable distorted image. The proposed EYEDi graphical authentication scheme has several advantages over traditional password-based authentication systems. It eliminates the need for users to remember complex passwords, making it easier for users to access the system. It also provides a higher level of security, making it difficult for attackers to guess or replicate the correct authentication credentials. However, the proposed system also has some limitations. It requires users to have access to a device with a camera to take a picture of the selected portion of the encodable distorted image. It also requires users to select a unique and non-guessable portion of the image, which may be challenging for some users.

VII. References

1. Bai, Y., Li, S., & Liu, S. (2020). A review of graphical passwords authentication systems. Journal of Ambient Intelligence and Humanized Computing, 11(9), 4003-4016.

2. Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. ACM Computing Surveys (CSUR), 44(4), 19.

3. Cao, Q., Liu, X., Chen, J., & Tan, J. (2017). A survey on graphical passwords. Journal of Computer Science and Technology, 32(2), 235-257.

4. Das, S., & Maiti, S. (2019). Secure and usable graphical password authentication scheme. Computers & Security, 83, 276-295.

5. Das, S., Maiti, S., & Paul, T. (2021). An effective authentication scheme based on image and graphical passwords. Journal of Ambient Intelligence and Humanized Computing, 12(6), 6549-6568.

6. De Luca, A., Hang, A., Brudy, F., & Lindner, M. (2015). Towards a user-centered framework for developing secure graphical passwords. In Proceedings of the 2015 Symposium on Usable Privacy and Security (pp. 285-298).

7. Dhamija, R., & Perrig, A. (2000). Déjà Vu: A user study using images for authentication. In Proceedings of the 9th USENIX Security Symposium (pp. 7-7).

8. Dhamija, R., Perrig, A., & Hearst, M. (2004). Deconstructing web page authentication. In Proceedings of the 10th ACM Conference on Computer and Communications Security (pp. 290-

299).

9. Hong, J., & Kim, M. (2020). Personalized graphical password authentication using images. Journal of Ambient Intelligence and Humanized Computing, 11(10), 4719-4730.

10. Kaur, H., & Kumar, N. (2017). A review on graphical password authentication schemes. Journal of Theoretical and Applied Information Technology, 95(6), 1236-1251.

11. Li, X., & Chen, J. (2014). Authentication of mobile phone users based on graphical passwords. Journal of Network and Computer Applications, 43, 47-57.

12. Mazhar, S., Hasan, S. S., & Ahmad, N. (2020). A novel image-based graphical password authentication scheme. Journal of Ambient Intelligence and Humanized Computing, 11(9), 4247-4260.

13. Monrose, F., & Rubin, A. D. (1997). Password hardening based on keystroke dynamics. In Proceedings of the 4th ACM Conference on Computer and Communications Security (pp. 73-82).

14. Narayan, R., & Singh, P. (2018). Graphical password authentication using color QR codes. Journal of Ambient Intelligence and Humanized Computing, 9(1), 35-43.

15. Singh, S., Sood, S. K., & Tyagi, A. (2019). A survey of graphical password authentication schemes. Journal of Ambient Intelligence and Humanized Computing, 10(6), 2217-2244.

16. Wu, L., Chen, H., & Chen, Y. (2018). A graphical password authentication system based on convolutional neural network. IEEE Access, 6, 12294-12304

17. Wu, Y., Wang, Y., Wang, L., & Liu, L. (2021). An image-based graphical password authentication scheme with user customization. Journal of Ambient Intelligence and Humanized Computing, 12(7), 7293-7305.

18. Yu, S., Peng, S., Lu, Y., & Wang, K. (2020). An improved image-based graphical password authentication scheme using bilinear interpolation. Journal of Ambient Intelligence and Humanized Computing, 11(12), 5485-5495.

19. Zhou, Y., Yu, Y., & Jin, L. (2020). An image-based graphical password authentication scheme using distortion-based image selection. IEEE Access, 8, 36862-36872.

20. Wang, Z., Chen, Y., & Liu, Y. (2019). An image-based graphical password authentication scheme with diverse image categories. IEEE Access, 7, 109248-109262.