International Journal of Advanced Trends in Multidisciplinary Research
ISSN: 3139-0986, Volume 2 Issue 7
July 2026, PP 1-5

An Intelligent Image-Based Two-Factor Authentication System for Enhanced User Security

G.Chandram[1], Bhargavi Sammeta[2]
[1]Assistant Professor, Department of MCA, Megha Institute of Engineering and Technology for Women, Edulabad (Village), Ghatkesar (Mandal), Medchal District, Telangana, India.
[2]MCA Student, Department of MCA, Megha Institute of Engineering and Technology for Women, Edulabad (Village), Ghatkesar (Mandal), Medchal District, Telangana, India.

***Abstract* – The necessity for trustworthy and secure user authentication methods has grown dramatically due to the quick expansion of online services. Traditional password-based authentication techniques are susceptible to security risks such phishing, brute-force attacks, credential theft, and password reuse. This paper proposes a safe two-factor authentication (2FA) architecture that combines customized photo verification with conventional login credentials to solve these issues. Users provide basic login credentials and choose one or more personal photos, each linked to a distinct keyword, during user registration. One of the registered keywords is shown at random by the system once the username and password have been verified during the login procedure. The matching customized image must then be uploaded by the user as the second authentication factor. The Perceptual Hashing (pHash) technique, which effectively evaluates image similarity while retaining robustness against small image alterations, is used in image verification. The framework enhances system security by reducing the possibility of unauthorized access through password-guessing attacks by applying distinct authentication attempt limitations for recognized and unrecognized devices. Without the need for extra hardware or intricate verification processes, the suggested authentication paradigm improves account security. The framework is appropriate for contemporary web applications, cloud platforms, financial systems, educational portals, and enterprise authentication environments because it strikes a balance between security, usability, and computational efficiency by fusing personalized visual authentication with perceptual image hashing.**

***Keywords* – image-based authentication, cybersecurity, perceptual hashing (pHash), two-factor authentication (2FA), secure login, password protection, access management, and customized image verification..**

I. INTRODUCTION

The need for secure user authentication methods has grown dramatically due to the growing use of digital technology and internet-based services. Authentication systems are used by companies in a variety of industries, such as banking, healthcare, education, e-commerce, and cloud computing, to safeguard user privacy and stop illegal access. However, traditional text-based password authentication techniques are inadequate for protecting contemporary digital environments because of their growing susceptibility to cyberthreats such dictionary attacks, phishing, brute-force attacks, credential theft, and password reuse [7], [12]. As a result, researchers have concentrated on creating sophisticated authentication methods that improve security without sacrificing usability.

Two-Factor Authentication (2FA) has become one of the most widely adopted approaches for strengthening access control by requiring users to verify their identity using two independent authentication factors. As a result, financial institutions, cloud service providers, government organizations, and enterprise applications have increasingly incorporated two-factor authentication into their security infrastructures [20].

Although existing 2FA solutions provide enhanced security, many authentication systems depend on one-time passwords (OTPs), SMS verification, authentication applications, or biometric devices. These methods often require additional hardware, stable network connectivity, or specialized devices, which may reduce usability and increase deployment costs. Furthermore, OTP-based authentication remains susceptible to phishing attacks, SIM-swapping, and social engineering techniques, motivating researchers to investigate alternative authentication approaches that provide stronger security with improved user experience [10], [17].

Graphical and image-based authentication methods have emerged as promising alternatives to traditional password-based authentication. Unlike textual passwords, personalized images are generally easier for users to recognize and remember because human memory naturally retains visual information more effectively than random character combinations. Several recent studies have demonstrated that graphical password systems improve authentication usability while offering increased resistance against shoulder-surfing attacks, password guessing, and credential theft [3], [4], [13], [14]. Hybrid authentication models combining graphical passwords with conventional credentials further enhance overall system security by introducing multiple verification layers [6].

A fundamental challenge in image-based authentication systems is accurately verifying whether the uploaded image corresponds to the image originally registered by the user. Perceptual image hashing has become an effective solution for addressing this challenge because it generates compact digital signatures based on the visual characteristics of images rather than their exact pixel values. Unlike conventional cryptographic hash functions, perceptual

hashing algorithms produce similar hash values for visually similar images, even after common image manipulations such as resizing, compression, brightness adjustment, or minor rotations [1], [2], [4]. Consequently, perceptual hashing provides reliable and computationally efficient image comparison for authentication applications.

Among various perceptual hashing techniques, the Perceptual Hash (pHash) algorithm has demonstrated excellent robustness, accuracy, and computational efficiency for image authentication. Recent advances in feature extraction, deep learning, and transformer-based perceptual hashing methods have further improved authentication accuracy while maintaining resilience against image modifications [1], [2], [5]. These characteristics make pHash highly suitable for secure image-based authentication systems where users submit visually identical images that may differ slightly because of compression or format conversion.

In this research, a secure two-factor authentication framework is proposed by integrating conventional username-password verification with personalized image-based authentication. During the registration process, users create their login credentials and select one or more personalized images, each associated with a unique keyword. During authentication, after successful password verification, the system randomly displays one of the registered keywords and requests the corresponding personalized image. The uploaded image is then verified using the Perceptual Hashing (pHash) algorithm by comparing its generated hash signature with the stored reference hash. Since only image hash values are stored instead of the original images, the proposed framework improves storage efficiency while enhancing data privacy and security [7], [15].

To further improve authentication reliability, the proposed framework incorporates adaptive login attempt restrictions based on device recognition. Trusted devices are permitted more authentication attempts than unrecognized devices, thereby reducing the effectiveness of brute-force attacks and unauthorized login attempts while maintaining usability for legitimate users [8], [9]. By combining personalized image verification, perceptual hashing, and adaptive authentication policies, the proposed authentication framework provides multiple layers of security without requiring additional hardware or expensive biometric sensors..

II. LITERATURE SURVEY

1. Y. Fang, C. Qin, G. Gao, and Y. Zhou [2025]
In order to enhance picture authenticity, Y. Zhou et al. suggested a perceptual image hashing architecture that combines window self-attention and feature fusion algorithms. The technique creates strong hash values that resist picture alterations like scaling, compression, and noise addition by extracting discriminative visual cues. When compared to traditional hashing algorithms, their experimental results show increased authentication accuracy and robustness.

2. Y. Zhou, S. Yao, C. Qin, F. Cao, and H. Yao [2024]
A perceptual authentication hashing method based on multi-domain feature extraction was created by F. Cao et al. Their method creates trustworthy image signatures that can differentiate between real and fake images by combining spatial and frequency-domain data. The suggested approach maintains effective authentication performance while demonstrating strong resistance against a variety of image processing techniques.

3. X. Qin, P. Rosenberg, and W. Li [2025]
X presented an image-based graphical authentication solution for Internet of Things (IoT) applications. Qin and colleagues. To increase login security and lessen the likelihood of shoulder-surfing assaults, their authentication method uses rounded picture selection. The solution strengthens protection against unwanted access while offering a simple authentication technique.

4. X. Xing, T. Xiang, H. Liu, C. Hu, F. Yang, and H. Xia [2024]
Two perceptual picture hashing techniques utilizing the Discrete Wavelet Transform (DWT) were proposed by C. Hu et al. Despite changes like scaling, filtering, or compression, their methods provide consistent hash values that may identify visually comparable photos. The study found that wavelet-based hashing enhances image integrity verification and authentication reliability.

5. M. Ben Yakhlef, S. El Hazzat, and M. Ben Aissi [2024]
Common perceptual hashing techniques, such as pHash, aHash, and dHash, were compared by M. Ben Aissi et al. Under various picture change scenarios, their investigation assessed robustness, computing efficiency, and authentication correctness. Because of its exceptional matching precision and resistance to picture alterations, pHash has been shown to be the most dependable method for secure image authentication.

6. G. Van Wallendael, J. De Geest, P. De Smet, H. Mareen, L. Bonetto, and P. Lambert [2024]
An image hashing method that extracts deep visual information using pretrained Vision Transformer models was introduced by J. De Geest et al. Highly discriminative perceptual hashes are produced by the suggested methods, which can increase authentication accuracy and resilience to visual distortions. Their approach shows how transformer-based feature extraction works well for contemporary picture authentication systems.

7. M. S. Kumaresan, R. S. Rajakumari, and N. I. Dias [2023]
To strengthen defense against shoulder-surfing attacks, N. I. Dias et al. suggested a graphical password authentication system based on deep learning. Their method increases authentication accuracy while preserving an easy-to-use login experience by combining graphical password selection with picture recognition techniques. Compared to

traditional graphical authentication techniques, the suggested alternative provides higher security.

8. P. Andriotis, A. Takasu, and M. Kirby [2023]
The Bu-Dash graphical password method was created by P. Andriotis et al. Its dynamic user interface modifies the graphical elements' arrangement continually during authentication. This dynamic nature enhances overall authentication security while making password monitoring considerably more challenging for attackers.

9. Q. Hu, M. R. Asghar, and G. C. Yang [2022]
The TIM authentication system for cellphones was proposed by G. C. Yang et al. and needs users to locate and recognize specific photos in order to log in. The method offers greater security than conventional password-only authentication while still being practical for mobile users by combining graphical verification with enhanced usability.
10. N. Kausar, B. S. Kim, M. A. Khan, I. U. Din, and A. Almogren [2022]

GRA-PIN is a hybrid authentication architecture that combines dynamic PIN generation with graphical passwords, according to N. Kausar et al. To improve security against replay attacks, password guessing, and unauthorized access while preserving usability, the system generates a distinct authentication sequence for each login session..

III. RESEARCH METHODOLOGY

The proposed authentication framework adopts a layered security approach to strengthen user verification by integrating traditional password authentication with personalized image-based validation. The methodology is divided into two major phases: user enrollment and secure authentication. During the enrollment phase, users register by creating a unique username, providing a valid email address, and defining a strong password that serves as the primary authentication credential. In addition to these credentials, users select one or more personal images that are meaningful and easy for them to recognize. Each selected image is linked with a unique descriptive keyword that functions as an identifier during future login sessions. To improve security and minimize storage overhead, the system does not retain the original image files. Instead, each registered image is processed using the Perceptual Hash (pHash) algorithm to generate a compact hash signature, which is securely stored in the authentication database.

During the authentication phase, the system initially validates the user's username and password. After successful verification of these credentials, the framework randomly chooses one of the previously assigned keywords and displays it to the user. Based on the displayed keyword, the user uploads the corresponding registered image. The uploaded image undergoes preprocessing, including resizing and grayscale conversion, before the pHash algorithm generates its perceptual hash value. The newly generated hash is then compared with the stored reference hash to determine whether both images represent the same visual content. Authentication is considered successful only when both the password verification and image matching processes are completed successfully.

To provide additional protection against unauthorized access, the proposed framework incorporates an adaptive login management strategy. The system distinguishes between trusted and unrecognized devices and applies different authentication attempt limits accordingly. Users accessing the system from previously verified devices are allowed a greater number of login attempts, whereas unknown devices are subjected to stricter restrictions. This adaptive mechanism effectively reduces the possibility of brute-force attacks, password guessing, and repeated unauthorized login attempts while maintaining convenience for legitimate users.

IV. EXISTING SYSTEM

Traditional user authentication systems primarily rely on username and password combinationsdigital services. Although password-based authentication is simple to implement and widely adopted across websites, mobile applications, banking systems, and enterprise platforms, it suffers from several security vulnerabilities. Users often create weak or easily predictable passwords, reuse the same credentials across multiple accounts, or become victims of phishing attacks, credential theft, brute-force attacks, dictionary attacks, and password leaks. To overcome these challenges, many organizations have implemented Two-Factor Authentication (2FA) using One-Time Passwords (OTPs), SMS verification, email-based verification, hardware security tokens, or biometric authentication. While these approaches improve overall security, they also introduce challenges such as dependence on external devices, network availability, additional infrastructure costs, and increased authentication time. Furthermore, graphical password and image-based authentication systems proposed in recent years have attempted to enhance security by using visual recognition techniques. However, many of these methods require complex image processing algorithms, dynamic user interfaces, deep learning models, or specialized hardware, which increase computational overhead and implementation complexity.

V. PROPOSED SYSTEM

The proposed framework that enhances traditional login security by combining password authentication with personalized image verification. Unlike conventional authentication methods that rely solely on textual passwords or external verification devices, the proposed framework incorporates a visual authentication mechanism that uses user-selected images as a second layer of security. During the registration process, users create their account by providing basic login credentials, including a username, email address, and password. They are then required to select one or more personalized images from their device and assign a unique keyword to each image. These

keywords serve as memory cues during authentication, making the verification process intuitive and convenient. To protect user privacy and minimize storage requirements, the system processes each selected image using the Perceptual Hash (pHash) algorithm and stores only the generated hash signatures instead of the original image files.

Do determine image similarity. Access is granted only when both the password verification and image matching processes are successfully completed. This dual-verification mechanism significantly improves authentication security by ensuring that an attacker must possess both the correct login credentials and the appropriate personalized image.

To further strengthen system security, the proposed framework incorporates an adaptive authentication policy based on device recognition. Devices that have been previously verified are classified as trusted and are allowed a higher number of login attempts, while unknown or unrecognized devices are subject to stricter authentication limits. This intelligent login management strategy effectively minimizes brute-force attacks, password guessing, and repeated unauthorized access attempts without affecting the experience of legitimate users. By integrating password authentication, personalized image verification, perceptual image hashing, and adaptive access control into a unified authentication framework, the proposed system provides a practical, scalable, and reliable security solution suitable for web applications, cloud platforms, banking services, healthcare systems, educational portals, and enterprise environments where strong user authentication is essential.

VI. SYSTEM ARCHITECTURE

with a centralized database responsible for securely storing user credentials and image hash information. This architecture ensures that users must successfully complete two independent verification steps before access

During the Registration Phase, a new user begins by creating an account using a unique username, are securely stored in the database after appropriate encryption. Following credential creation, the user selects one or more personalized images from their local device. Each selected image is associated with a unique keyword that helps the user identify the corresponding image during future login attempts. Instead of storing the original images directly, the system preprocesses every selected image by resizing This preprocessing step ensures uniformity and reduces computational complexity during image comparison. After preprocessing, the Perceptual Hash (pHash) algorithm generates a unique 64-bit hash signature representing the visual characteristics of each image. Only these hash values, along with their associated keywords, are stored in the database, thereby improving user privacy and minimizing storage requirements.

During the Login or Authentication Phase, the user first enters the registered username and password. The system verifies these credentials against the stored database records. If the primary credentials are incorrect, authentication is immediately terminated, and access is denied. The selected keyword is displayed on the screen, prompting the user to upload the corresponding personalized image. This random keyword selection ensures that attackers cannot predict which image will be requested during each login session, thereby increasing authentication security.

Once the user uploads the requested image, the system performs preprocessing operations identical to those used during registration, including image resizing and grayscale conversion. The uploaded image is then processed using the Perceptual Hash (pHash) algorithm to generate a new perceptual hash value. This newly generated hash is compared with the stored reference hash using Hamming distance similarity measurement. If the similarity exceeds the predefined threshold, the uploaded image is considered authentic, and the second authentication factor is successfully verified. Consequently, the user is granted access to the application dashboard. If the hash comparison fails, authentication is rejected, and access is denied.

To further strengthen security, the proposed architecture incorporates an Adaptive Login Policy based on device recognition. The system differentiates between trusted devices that have previously authenticated successfully and unrecognized devices attempting to access the system for the first time. Trusted devices are allowed a higher maximum number of authentication attempts, while unknown devices are restricted to fewer attempts. This adaptive strategy effectively minimizes brute-force attacks, password guessing, and unauthorized login attempts while preserving a smooth authentication experience for legitimate users.

VII. CONCLUSION

This research presented a secure and efficient two-factor authentication framework that enhances conventional password-based authentication by incorporating personalized image verification. The proposed system combines knowledge-based authentication with visual recognition, enabling users to authenticate using both their login credentials and a personalized image associated with a predefined keyword. The integration of the Perceptual Hash (pHash) algorithm enables reliable image verification by generating compact hash signatures that remain robust against minor image transformations, thereby ensuring accurate authentication without storing the original image files. This approach improves both data privacy and storage efficiency while maintaining a high level of authentication accuracy.

The proposed authentication framework also introduces an adaptive security mechanism by applying different authentication attempt limits for trusted and unrecognized

devices. This additional protection minimizes the risk of brute-force attacks, unauthorized login attempts, and password-guessing techniques without compromising user convenience. Compared with traditional single-factor authentication methods, the proposed solution provides multiple layers of security while remaining simple to implement and easy for users to operate. Furthermore, the use of personalized images makes the authentication process more intuitive and memorable, reducing the dependence on complex passwords alone.

Overall, the proposed framework successfully demonstrates that integrating personalized image verification with perceptual image hashing can significantly strengthen user authentication in modern digital environments.

REFERENCES

1. Y. Zhou, G. Gao, Y. Fang, and C. Qin, "Perceptual Image Authentication Hashing Based on Window Self-Attention Feature Fusion," Journal of Computer Research and Development, vol. 62, no. 7, pp. 1786–1796, 2025.
2. "Perceptual Authentication Hashing for Digital Images Based on Multi-Domain Feature Fusion," Signal Processing, vol. 223, Art. no. 109576, 2024; F. Cao, S. Yao, Y. Zhou, H. Yao, and C. Qin.
3. X. Qin, W. Li, and P. Rosenberg, "RoundImage: Towards Secure Graphical Password Authentication via Rounded Image Selection in IoT," IEEE Internet of Things Journal, vol. 12, no. 12, pp. 20473–20483, 2025.
4. "Two Robust Perceptual Image Hashing Schemes Based on Discrete Wavelet Transform," IEEE Transactions on Consumer Electronics, vol. 70, no. 4, pp. 6533–6546, 2024; C. Hu, F. Yang, X. Xing, H. Liu, T. Xiang, and H. Xia.
5. "Evaluation of Perceptual Hashing Algorithms for Digital Image Authenticity," M. Ben Aissi, S. El Hazzat, and M. Ben Yakhlef, Proceedings of the Third International Conference on Embedded Systems and Artificial Intelligence (ESAI), IEEE, 2024.
6. "Perceptual Hashing Using Pretrained Vision Transformers," J. De Geest, P. De Smet, L. Bonetto, P. Lambert, G. Van Wallendael, and H. Mareen, Proceedings of the IEEE Games, Entertainment and Media Conference (GEM), 2024.
7. "SmartHash: Perceptual Hashing for Image Tampering Detection and Authentication," P. Samanta and S. Jain, Proceedings of the ACM International Conference on Knowledge and Information Management (CIKM), 2024.
8. "Deep Learning Based Graphical Password Authentication Approach Against Shoulder-Surfing Attacks," N. I. Dias, M. S. Kumaresan, and R. S. Rajakumari, Multiagent and Grid Systems, vol. 19, no. 1, pp. 99–115, 2023.
9. "Bu-Dash: A Universal and Dynamic Graphical Password Scheme," P. Andriotis, M. Kirby, and A. Takasu, International Journal of Information Security, vol. 22, no. 2, pp. 381–401, 2023.
10. "TIM: Secure and Usable Authentication for Smartphones," G. C. Yang, Q. Hu, and M. R. Asghar, Journal of Information Security and Applications, vol. 71, Art. no. 103374, 2022.
11. "GRA-PIN: A Graphical and PIN-Based Hybrid Authentication Approach for Smart Devices," N. Kausar, I. U. Din, M. A. Khan, A. Almogren, and B. S. Kim, Sensors, vol. 22, no. 4, Art. no. 1349, 2022.
12. A. S. Shaik, R. K. Karsh, M. Islam, and R. H. Laskar, "A Review of Hashing-Based Image Authentication Techniques," Multimedia Tools and Applications, vol. 81, no. 2, pp. 2489–2516, 2022.
13. T. Takada and M. Yoshida, "Pict-Place Authentication: Recognition-Based Graphical Password Using Image Layout for Better Balance of Security and Operation Time," Proceedings of the CHItaly Conference, 2021, pp. 1–7.
14. "Easy-Auth: Graphical Password Authentication Using a Randomization Method," Proceedings of the IEEE Latin-American Conference on Communications (LATINCOM), 2021, pp. 1–6, M. Harshini, P. L. Sai, S. Chennamma, A. G. Reddy, and H. S. Kim.
15. "Multi-Factor Authentication to Systems Login," B. O. Alsaleem and A. I. Alshoshan, Proceedings of the National Computing Colleges Conference (NCCC), IEEE, 2021, pp. 1-4.
16. F. Ghiyamipour, "Secure Graphical Password Based on Cued Click Points Using Fuzzy Logic," Security and Privacy, vol. 4, no. 2, p. e140, 2021.
17. "PassPage: Graphical Password Authentication Scheme Based on Web Browsing Records," X. Chu, H. Sun, and Z. Chen, Financial Cryptography and Data Security, LNCS, vol. 12063, Springer, 2020, pp. 166–176.
18. S. Dabeer, M. Ahmad, M. S. Umar, and M. H. Khan, "A Novel Hybrid User Authentication Scheme Using Cognitive Ambiguous Illusion Images," in Advances in Intelligent Systems and Computing, vol. 1049, Springer, 2020, pp. 107–118.
19. G. C. Yang, "Next-Generation Personal Authentication Scheme Based on EEG Signal and Deep Learning," Journal of Information Processing Systems, vol. 16, no. 5, pp. 1182–1196, 2020.
20. "Google Map-Based Password Authentication Systems Using Tolerant Distance and Homomorphic Encryption," IEEE Transactions on Dependable and Secure Computing, vol. 22, no. 5, pp. 4565–4579, 2025; Z. Zhou, S. Wang, G. Nan, S. Cimato, Y. Zheng, and Q. Wang.