Secure Morph: A Secure Login System Using Visual Puzzle Authentication

Somireddi Sai Kiran
Reg. No. 24Q71F0062
saikiransomireddi@gmail.com
Department of Master of Computer Applications
Avanthi Institute of Engineering and Technology (Autonomous)
Vizianagaram, Andhra Pradesh, India
Under the guidance of Mr. S. Keseva Rao, Ph.D., Associate Professor
kesav546@gmail.com

***Abstract*—Secure Morph is an innovative approach to enhance user authentication by replacing traditional text-based passwords with a visual puzzle-based mechanism. Conventional login systems are highly vulnerable to security threats such as shoulder surfing, phishing, brute-force attacks, and keylogging. To address these issues, Secure Morph introduces an interactive authentication method in which users solve or recognise a predefined visual puzzle or image pattern to gain access. During registration, users select a sequence of images or configure a puzzle pattern that serves as their authentication key; during login, the system presents a randomized arrangement of images or puzzle elements, and the user must correctly identify or arrange them. Because visual patterns are difficult to guess, replicate, or capture compared with traditional passwords, this method significantly reduces the risk of unauthorized access, and dynamic puzzle generation introduces randomness that lowers predictability. The system improves both security and usability by providing an easy-to-remember yet highly secure authentication mechanism that leverages human visual memory, and it stores the configured pattern in encrypted form. The prototype is implemented with a Python (Flask/Django) backend, an HTML/CSS/JavaScript frontend, and a relational database, and was validated through nine functional test cases that all passed. Secure Morph can be effectively applied in domains such as banking, social media, and other secure applications where data protection is critical.*

***Keywords*—Graphical Authentication; Visual Puzzle; Secure Login; Shoulder-Surfing Resistance; Dynamic Puzzle Generation; Usable Security; Human Visual Memory; Access Control.**

I. INTRODUCTION

In the modern digital era, authentication systems play a crucial role in protecting sensitive information and ensuring secure access to systems and applications. With the rapid growth of internet-based services such as online banking, social media, e-commerce, and cloud platforms, the need for robust and reliable authentication mechanisms has become more important than ever. Traditional authentication methods, primarily based on text passwords, have been widely used due to their simplicity and ease of implementation, but they are increasingly vulnerable to various security threats.

Text-based passwords suffer from several weaknesses. Users often create simple, easily guessable passwords due to memory constraints, making them susceptible to brute-force and dictionary attacks, and password reuse across multiple platforms further increases risk. Attackers exploit these vulnerabilities

through phishing, keylogging, and credential stuffing, and passwords can be observed through shoulder surfing in public environments. To address these limitations, researchers have explored alternatives including biometric systems, multi-factor authentication, and graphical password schemes; among these, graphical authentication has gained attention because humans are generally better at recognising images and patterns than recalling complex alphanumeric passwords.

The proposed system, Secure Morph, introduces a novel approach to authentication using visual puzzle-based techniques. Users authenticate by solving a visual puzzle or selecting specific image patterns instead of entering a traditional password; the system generates dynamic puzzles that are difficult for attackers to predict or replicate, reducing the risk of shoulder surfing and phishing. Secure Morph aims to strike a balance between security and usability, leveraging human visual cognition while remaining intuitive and accessible, and is designed to be adaptable and scalable across different applications and platforms. The objectives are listed below:

- Analyse the limitations and vulnerabilities of existing text-based authentication.
- Design a secure, user-friendly visual puzzle-based authentication system.
- Use dynamic puzzle generation to add randomness and reduce predictability.
- Reduce susceptibility to brute force, phishing, shoulder surfing, and password theft.
- Store authentication patterns securely in encrypted form.
- Provide a scalable, adaptable solution deployable across platforms.

II. LITERATURE SURVEY

Authentication systems have evolved significantly, moving from simple password-based methods to more advanced and secure techniques. Traditional text-based authentication is widely used due to its simplicity but suffers from brute-force attacks, dictionary attacks, phishing, and shoulder surfing, and users often create weak passwords or reuse them across platforms. As a result, researchers have developed alternative mechanisms that improve both security and usability.

Graphical authentication systems have emerged as a promising solution by leveraging human visual memory. Work by Dhamija and Perrig introduced graphical password schemes in which users identify images instead of typing passwords, and later techniques such as PassPoints and image-based click systems allowed users to select specific points on an image; these methods are easier to remember and more resistant to certain attacks, although some still face shoulder-surfing vulnerability and increased authentication time. Recent research focuses on hybrid methods that combine graphical techniques with dynamic and interactive elements—visual puzzle-based authentication is one such approach, where users solve puzzles or recognise patterns to gain access, enhancing security by introducing randomness and reducing predictability. Despite improvements, challenges such as system complexity, usability for diverse users, and computational overhead remain areas for further research.

TABLE I. SUMMARY OF REPRESENTATIVE PRIOR WORK

S.No	Author(s) / Year	Methodology	Contribution	Limitation
1	Dhamija & Perrig, 2000	Graphical password (Déjà Vu)	Image-based authentication	Large image database
2	Suo et al., 2005	Graphical passwords survey	Categorised schemes	Survey only
3	Dunphy & Yan, 2007	Draw-a-Secret variants	Background-image study	Shoulder-surfing risk
4	Gao et al., 2013	Analysis & evaluation	Security/usability analysis	Trade-offs
5	Ur et al., 2015	Usability study	Improved usability	Security trade-offs
6	Kaur & Singh, 2017	Visual cryptography	Secure authentication	Computational overhead

III. EXISTING SYSTEM AND PROPOSED SYSTEM

A. Existing System

Existing authentication systems primarily rely on text-based passwords and, in some cases, PINs or OTPs for user verification. Users create a username and password combination to access their accounts, and some applications add an OTP layer. While simple and easy to implement, these systems suffer from several limitations.

Limitations of the existing system:

- Weak passwords: users choose simple or easily guessable passwords.
- Password reuse across multiple platforms.
- Vulnerable to brute force, phishing, dictionary attacks, and keylogging.
- Susceptible to shoulder surfing in public environments.
- Static credentials provide limited resistance to modern attacks.

B. Proposed System

The proposed system, Secure Morph, introduces a visual puzzle-based authentication mechanism to overcome these limitations. Instead of entering a text password, users authenticate by solving a visual puzzle or identifying specific graphical patterns. The system uses graphical authentication with dynamic puzzle generation, presenting a different puzzle on each login attempt to increase security and resistance to shoulder surfing, phishing, and brute-force attacks, while remaining intuitive for users.

Key features and advantages:

- Graphical authentication using images and puzzles instead of text passwords.
- Dynamic puzzle generation: a different puzzle each login attempt.
- Enhanced resistance to shoulder surfing, phishing, and brute force.

- Leverages human visual memory for easy recall.
- Encrypted storage of the configured puzzle pattern.
- Scalable and adaptable across applications and platforms.

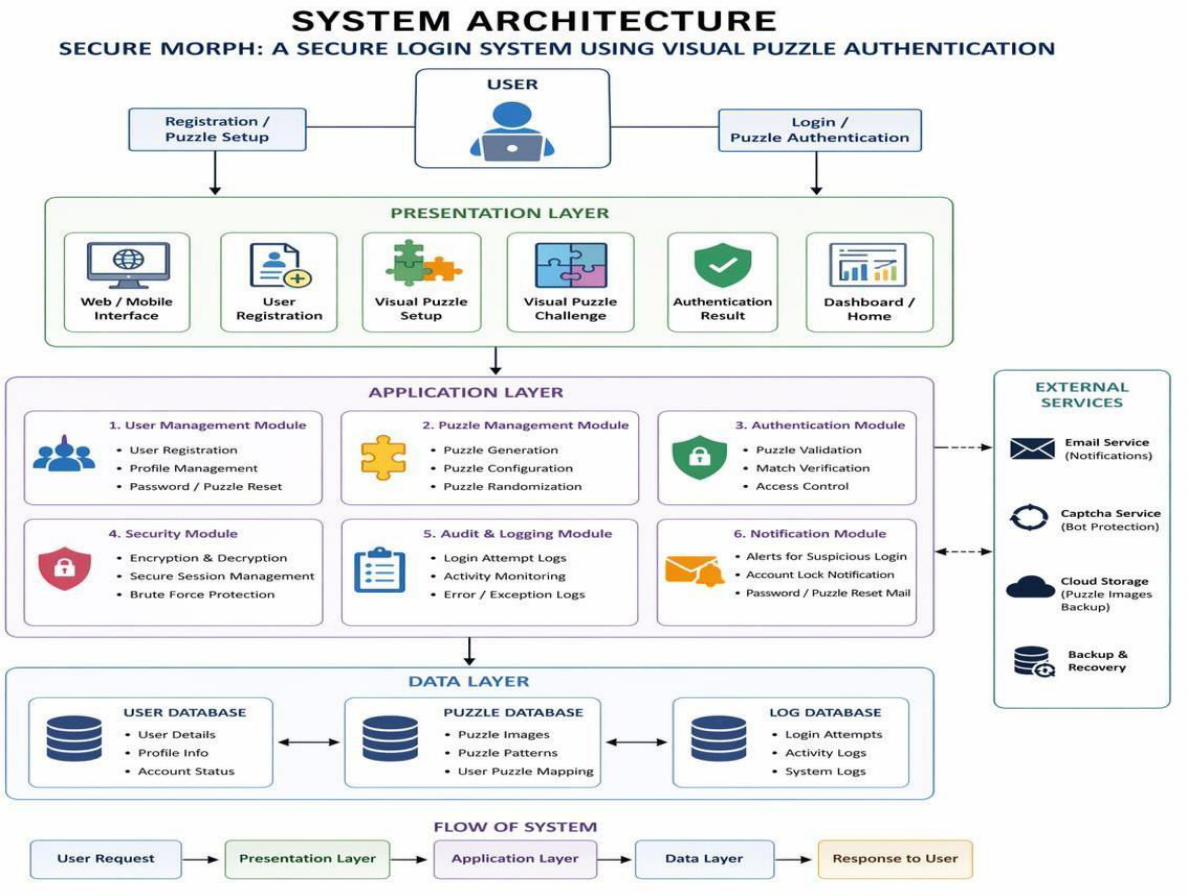
IV. SYSTEM ANALYSIS AND DESIGN

A. Requirements

Functionally, the system must support user registration with a configured puzzle pattern, secure encrypted storage of that pattern, dynamic puzzle generation at login, verification of the user's puzzle solution, denial of access on incorrect solutions, protection against repeated failed attempts (temporary lockout or CAPTCHA), and puzzle/password reset for valid user requests. Non-functional requirements include security (encryption, resistance to common attacks), usability (intuitive interaction and easy recall), performance (responsive handling of multiple users), and scalability.

B. System Architecture

Secure Morph follows a modular architecture with frontend, backend, and database components. The frontend (HTML, CSS, JavaScript) presents the registration and login interfaces and the interactive puzzle. The backend (Python with Flask or Django) manages user accounts, dynamic puzzle generation, verification logic, lockout/CAPTCHA control, and reset handling. The database stores user records and the configured puzzle pattern in encrypted form. This separation supports maintainability and integration into different platforms.



C. Authentication Workflow

During registration, the user provides valid details and configures a puzzle pattern (for example, selecting a sequence of images); the pattern is encrypted and stored securely. During login, the system presents a randomized arrangement of puzzle elements; the user must correctly solve or arrange them. A correct solution authenticates the user, while an incorrect solution denies access. Repeated failed attempts trigger a temporary lockout or CAPTCHA, and a valid reset request allows the puzzle to be reconfigured. Because the puzzle is randomized each time, observing one successful login does not reveal a reusable static credential.

V. SYSTEM IMPLEMENTATION

A. Technology Stack

TABLE II. TECHNOLOGY STACK

Component	Technology / Tool
Programming Language	Python
Backend Framework	Flask / Django
Frontend Technologies	HTML, CSS, JavaScript

Component	Technology / Tool
Database	MySQL / MongoDB
Security	Encrypted storage of puzzle pattern
Authentication Mechanism	Dynamic visual puzzle generation and verification
Architecture	Modular frontend–backend–database design

B. Implementation Details

The implementation focuses on developing a secure and user-friendly authentication mechanism using visual puzzles, built with modern web technologies and a modular architecture. The frontend renders the registration flow, where the user configures a puzzle pattern, and the login flow, where a randomized puzzle is presented. The backend generates the dynamic puzzle, validates the user's response, enforces lockout/CAPTCHA after repeated failures, and handles reset requests. The selected puzzle pattern is securely stored in the database in encrypted form so that even if the data store is accessed, the pattern is not directly readable.

C. Security Considerations

Security is strengthened through dynamic puzzle generation (randomising the challenge each time so observation does not yield a reusable secret), encrypted storage of the authentication pattern, and protection against automated guessing via temporary lockout or CAPTCHA after multiple failed attempts. Together these measures address the brute-force, phishing, shoulder-surfing, and keylogging weaknesses of static text passwords while keeping the experience intuitive.

VI. SYSTEM TESTING AND RESULTS

The system was validated through nine functional test cases covering registration with valid and invalid details, puzzle setup, login with correct and incorrect puzzle solutions, dynamic puzzle generation, handling of multiple failed login attempts, puzzle reset, and data-security verification. All test cases passed and behaved as expected.

TABLE III. REPRESENTATIVE TEST CASES

ID	Scenario	Input	Expected Output	Status
TC01	Registration (valid)	Valid details + puzzle setup	User registered successfully	**Pass**
TC03	Puzzle setup	Select images/pattern	Pattern saved securely	**Pass**
TC04	Login (correct puzzle)	Correct puzzle input	User authenticated	**Pass**
TC05	Login (incorrect puzzle)	Wrong puzzle input	Access denied	**Pass**
TC06	Dynamic puzzle generation	Login attempt	Puzzle randomised each time	**Pass**

ID	Scenario	Input	Expected Output	Status
TC07	Multiple failed attempts	Repeated wrong puzzle	Lockout / CAPTCHA triggered	**Pass**
TC09	Data security check	Stored user data	Data encrypted and secure	**Pass**

A. Observed Results

The implementation demonstrates that visual puzzle-based authentication can replace or complement text passwords while improving resistance to common attacks. Dynamic puzzle generation prevents a single observation from yielding a reusable credential, encrypted storage protects the configured pattern, and lockout/CAPTCHA limits automated guessing, all while keeping the interaction intuitive through human visual memory. The source reports these outcomes qualitatively; no specific numeric metrics are claimed here, and usability for diverse users and computational overhead remain considerations.

Representative screenshots from the prototype implementation:

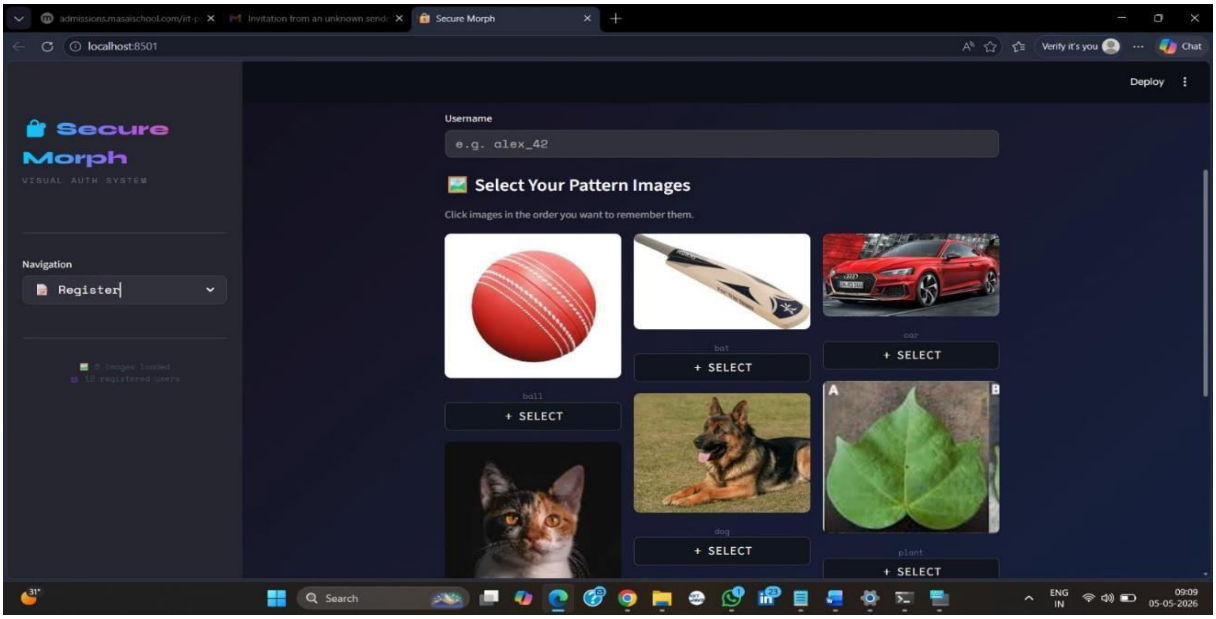


Fig. 1. Registration with puzzle-pattern setup.

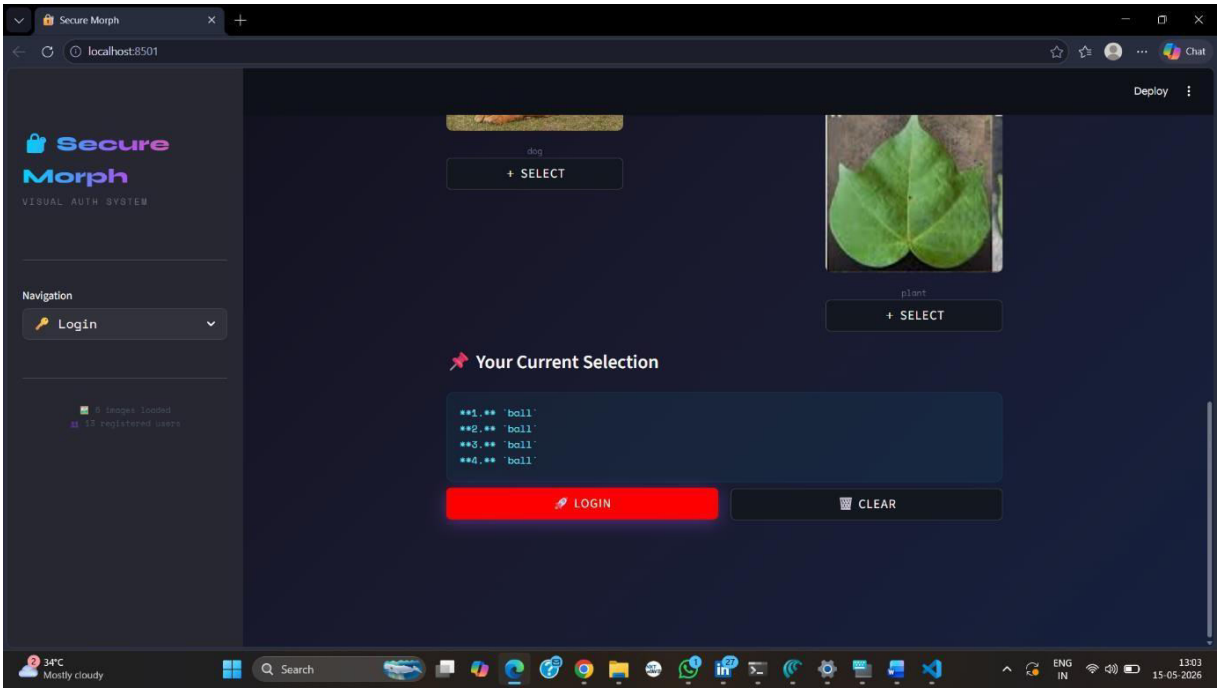


Fig. 2. Dynamic visual puzzle at login.

VII. CONCLUSION AND FUTURE SCOPE

Secure Morph presents an innovative and practical approach to user authentication by replacing vulnerable text-based passwords with a visual puzzle-based mechanism. By leveraging human visual memory and dynamic puzzle generation, the system significantly reduces the risk of shoulder surfing, phishing, brute-force attacks, and keylogging, while encrypted storage of the authentication pattern and lockout/CAPTCHA protection further strengthen security. The modular implementation with a Python backend, a web frontend, and a secure database keeps the system usable and adaptable, and functional testing confirmed correct behaviour across registration, dynamic puzzle generation, verification, failure handling, and data security. Secure Morph thus represents a meaningful step forward in usable, secure authentication suitable for banking, social media, and other security-critical applications.

The system can be further enhanced in several ways. Integrating multi-factor authentication would combine the visual puzzle with an additional factor for stronger protection. Adaptive difficulty and AI-assisted puzzle generation could tailor challenges to balance security and usability for diverse users. Mobile and cross-platform deployment would broaden applicability, and additional resistance to advanced shoulder-surfing (for example, gaze-based or one-time visual challenges) and rigorous security auditing would harden the system for large-scale, real-world use.

REFERENCES

[1] R. Dhamija and A. Perrig, “Déjà Vu: A User Study Using Images for Authentication,” in Proc. USENIX Security Symposium, 2000.

[2] X. Suo, Y. Zhu, and G. S. Owen, “Graphical Passwords: A Survey,” in Proc. Annual Computer Security Applications Conference (ACSAC), 2005.

[3] P. Dunphy and J. Yan, “Do Background Images Improve Draw-a-Secret?,” in Proc. ACM Conf. Computer and Communications Security, 2007.

[4] H. Gao, X. Liu, S. Wang, and R. Dai, “Analysis and Evaluation of Graphical Passwords,” IEEE Trans. Dependable and Secure Computing, vol. 10, no. 5, pp. 233–245, 2013.

[5] B. Ur et al., “The Design and Evaluation of Graphical Passwords,” in Proc. USENIX Security Symposium, 2015.

[6] M. Kumar, S. Garfinkel, D. Boneh, and T. Winograd, “Reducing Shoulder-Surfing by Using Gaze-Based Password Entry,” in Proc. Symposium on Usable Privacy and Security (SOUPS), 2007.

[7] W. Meng, D. S. Wong, S. Furnell, and J. Zhou, “Surveying the Development of Biometric User Authentication on Mobile Phones,” IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1268–1293, 2015.

[8] S. Kaur and M. Singh, “A Study of Visual Cryptography Techniques for Secure Authentication,” International Journal of Computer Applications, 2017.

[9] A. Ayesh et al., “Secure Authentication Using Image Processing,” International Journal of Computer Science and Information Security, 2013.

[10] OWASP, “Authentication Security Guidelines.” [Online]. Available: https://owasp.org/