

Graphical Password Vault - Final Project Report

1. Introduction

Graphical Password Vault is a browser-based secure storage system that authenticates users through a graphical pattern of images rather than traditional text-based passwords. This approach enhances user experience, improves memorability, and provides an alternative method of authentication based on visual recognition.

Users unlock their vault by selecting a predefined sequence of images from a 3x3 grid. The application also features pattern recovery through security questions, email, and SMS options making it resilient to forgotten credentials.

2. System Overview

The Graphical Password Vault includes:

- Graphical login using image pattern
- Pattern update and recovery functionality
- Security question-based fallback
- Access to a secure vault storing sensitive data
- Local storage of encrypted data for offline functionality

Objectives:

- Provide a visual password authentication experience
- Allow secure storage of sensitive data (e.g., credentials, crypto wallets)
- Enable password recovery via security questions or email/SMS
- Offer a smooth, mobile-responsive UI using HTML/CSS/JS

3. Technical Architecture

Technologies Used:

Graphical Password Vault - Final Project Report

- HTML5, CSS3 Web structure and styling
- JavaScript (Vanilla) UI interaction and logic
- LocalStorage API Client-side storage of pattern and vault data
- FontAwesome Iconography and visual design

Modules:

- auth.js: Handles graphical login logic, attempt limits, and vault access
- vault.js: Displays stored vault data and handles lock/change actions
- change-password.js: Updates the graphical pattern and security question
- forgot-password.js: Enables pattern recovery through user challenge
- style.css: Fully themed UI with dark mode and responsive layout

4. User Interface & Experience

Pages:

- index.html: Login interface with graphical grid
- vault.html: Display of secured items (passwords, documents, notes)
- change-password.html: Change pattern and update security question
- forgot-password.html: Recovery via question/email/SMS

Design Features:

- Glassmorphism and blurred cards
- Image-based 3×3 grid pattern input
- Smooth animations and feedback messages
- Dark-themed interface for better visual comfort

5. Working Process (Behind the Scenes)

Graphical Password Vault - Final Project Report

1. User selects 4-image pattern from the grid
2. Pattern stored securely in localStorage
3. On login, pattern is compared to stored version
4. Vault access granted if pattern matches
5. Users can change pattern or recover using a security question
6. Vault content shown on successful authentication

6. Key Strengths

- Unique and memorable graphical login
- Secure local pattern storage (client-only)
- Intuitive and responsive UI
- Multiple recovery options (question, email, SMS)
- Easy to use even for non-technical users

7. Limitations & Future Recommendations

Current Limitations:

- Data is not encrypted (stored as plain JSON)
- Recovery via email/SMS is mocked, not functional
- Entire system is client-side (no server or real backend)

Future Enhancements:

- Encrypt data using crypto-js or Web Crypto API
- Add backend for actual email/SMS recovery
- Turn project into a Progressive Web App (PWA)
- Session-based authentication for multi-user support
- Allow user-uploaded images for pattern personalization

Graphical Password Vault - Final Project Report

8. Sample Outputs

Correct Pattern:

Selected: Mountain, Ocean, Tree, Sun

Authentication successful! Redirecting to vault...

Incorrect Pattern:

Authentication failed. Pattern does not match.

Attempts remaining: 2

Vault Locked:

Vault locked! Too many failed attempts. Please try again later.

Recovery Example:

Security Question: What city were you born in?

User enters correct answer

Pattern recovery authorized

9. Pattern Grid Visualization

- 3x3 grid using nature-themed images (mountain, ocean, etc.)
- Click-based selection and real-time visual feedback
- Grid highlights selected sequence with glowing border
- Pattern shown in human-readable form (e.g., Ocean Tree Star)

10. Conclusion

The Graphical Password Vault is a secure and user-friendly alternative to traditional password systems. With its intuitive visual authentication and local-first approach, it is ideal for privacy-conscious users. Future enhancements like encryption, real recovery mechanisms, and backend integration could turn it into a robust and production-ready application.