ISSN 2278-2540 | DOI: 10.51583EMAS | Volume XV, Issue X, October2026

Potentiometer-Based Rotational Pattern Authentication System

Jibish Mathew [1*] and Abdul Rasheed [2]

[1]Department of Electronics, Prajyoti Niketan College, Pudukkad, Thrissur, Kerala India.

[2]Department of Electronics, WMO College, Wayanad, Kerala, India.

[*] Corresponding author

DOI: https://doi.org/10.51583/IJLTEMAS.2026.151000047

Received: 15 October 2026; Accepted: 20 October 2026; Published: 04 November 2026

ABSTRACT

Conventional authentication systems, including numerical passwords, graphical patterns, facial recognition, and fingerprint identification have certain limitations related to observation attacks and biometric spoofing. This research proposes a potentiometer-based rotational pattern authentication system. It uses a user-defined sequence of rotational movements as a personalized passkey for device access. In the proposed method, a potentiometer serves as the primary input device, converting rotational movements into corresponding electrical signals. During the registration phase, the user creates and stores a unique rotational pattern consisting of a sequence of selected angular positions and rotational directions. During authentication, the system captures the input rotational sequence and compares it with the stored pattern. Access is granted only when the entered sequence matches the registered pattern, otherwise, access is denied. The proposed approach provides an alternative to conventional password-based and biometric authentication methods.

Keywords: Potentiometer Rotational Pattern Authentication, Passkey, User Authentication, Microcontroller, Electronic Lock, Access Control, Embedded Security.

INTRODUCTION

Authentication is an essential component of electronic security systems, ensuring that access to devices, applications, and protected resources is restricted to authorized users. Conventional authentication methods i are numerical passwords, personal identification numbers, graphical patterns, and biometric techniques. But they have limitations related to security, implementation cost, and resistance to unauthorized access.

Authentication systems play an important role in protecting electronic devices from unauthorized access. Conventional password and Personal Identification Number (PIN)-based systems verify a user's identity by comparing the entered credentials with previously stored information. However, these systems may be vulnerable to attacks. Binbeshr et al. [1] presented a review of PIN-entry methods designed to resist shoulder-surfing attacks. They examined the security of different PIN-entry techniques. This research demonstrates that an authentication system depends not only on the password but also on the method used to enter it.

Graphical-password systems provide an alternative to alphanumeric passwords by allowing users to authenticate. Por et al. [2] presented–a systematic literature review of security attacks associated with graphical-password systems. These findings shows the importance of developing authentication systems that reduce the possibility of unauthorized access.

Biometric authentication is another method by identifying users through their physical characteristics. Kortli et al. [3] reviewed face-recognition techniques and discussed their advantages and limitations. Similarly, Maiti et al. [4] reviewed fingerprint-based authentication, examining recognition methods. Their study

ISSN 2278-2540 | DOI: 10.51583EMAS | Volume XV, Issue X, October2026

highlighted the significance of fingerprint identification while identifying challenges associated with security.

This research proposes a potentiometer-based rotational pattern authentication system in which the direction and sequence of rotational movements constitute a user-defined passkey. Unlike conventional systems that rely on numerical characters, graphical patterns, or biometric characteristics, the proposed technique authenticates users through a sequence of mechanical rotational inputs. During the registration phase, the user establishes a rotational pattern consisting of clockwise and anticlockwise rotation. The potentiometer converts rotation into electrical signals. These signals are sampled and processed by a microcontroller to identify the sequence. The resulting pattern is stored as authentication key. During access attempts, the system takes the input movements and compares with the registered sequence. Access is granted only when the entered pattern satisfies the authentication key; an incorrect sequence results in access denial.

RESEARCH METHODOLOGY

The proposed system shown in figure is a rotational pattern-based authentication. The system consists of four components: a potentiometer, a microcontroller board, a control unit, and a display unit. The potentiometer serves as the user input device for generating the authentication pattern, while the microcontroller board processes the input, stores the registered pass pattern, and performs pattern verification. The control unit operates the associated locking mechanism, and the display unit provides information about the authentication status. The system is designed to allow the control unit in according to the type of locking mechanism. Depending on the application, the control unit may include relays, electromagnetic locks, solenoid-operated locks, or other suitable control interfaces.

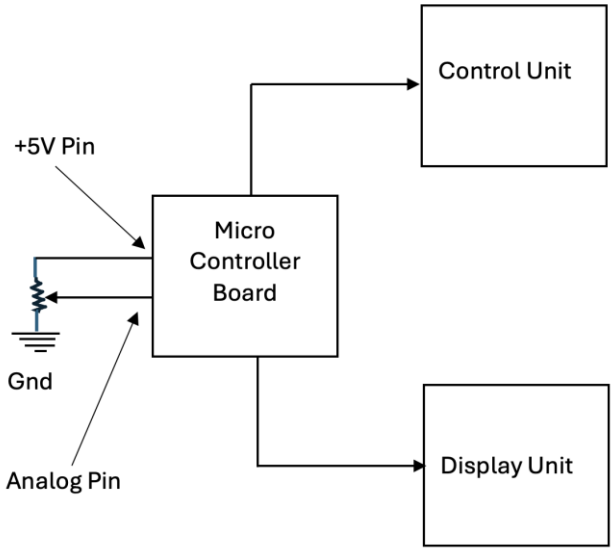


Figure. Block diagram of potentiometer-based rotational pattern authentication system

When a user attempts to access the system, the potentiometer is operated to reproduce the previously registered rotational pattern. The microcontroller continuously monitors the potentiometer output and identifies the sequence of movements using successive signal readings. The microcontroller then compares the entered pattern with the stored pass pattern. The comparison considers the direction and angle of the rotational movements. If the two patterns match, the authentication process is successful. Otherwise, the authentication attempt is rejected.

The result of pattern verification determines the operation of the control unit. When the entered pattern matches the stored pattern, the microcontroller generates an authorization signal that activates the control unit. The control unit then operates the connected locking mechanism. If the entered pattern does not match the stored pattern, the locking mechanism remains in its locked state. The display unit indicates the authentication result, whether access has been granted or denied.

ISSN 2278-2540 | DOI: 10.51583EMAS | Volume XV, Issue X, October2026

Working Principle

The proposed system operates by comparing a user-entered rotational pattern with a previously registered pass pattern. The potentiometer functions as both the pattern-registration interface and the authentication input device. Its rotation produces electrical signals corresponding to angular position, which are processed by the microcontroller to identify the direction and sequence of movements.

The operation of the system consists of the following stages.

Registration of the Pass Pattern

Initially, the system is configured to register the pass pattern of an authorized user. The user rotates the potentiometer through a selected sequence of movements. The microcontroller takes the potentiometer output and identifies the rotational sequence from changes in readings. The detected sequence is encoded and stored in the microcontroller's memory as the reference pass pattern. The stored data are retained for comparison during subsequent authentication attempts.

Entry of the Authentication Pattern

When access is required, the user operates the same potentiometer to enter the registered pass pattern. The microcontroller monitors the potentiometer output and reconstructs the input sequence by identifying the direction and order of rotational movements. The input pattern is represented in the same format as the stored reference pattern. Consistent movement-detection thresholds and pattern-encoding rules are applied during registration and authentication to ensure that both patterns can be compared correctly.

Pattern Comparison

After the user completes the input sequence, the microcontroller compares the entered pattern with the stored reference pattern. The comparison verifies whether the sequence and direction of the rotational movements correspond to those of the registered pass pattern. If the entered pattern matches the stored pattern, the microcontroller recognizes the user input as valid and generates an authorization signal.

This signal is transmitted to the control unit, which activates the appropriate mechanism to unlock the protected device or enable the electronic system. The display unit indicates that authentication has been successful and access has been granted. If the entered pattern differs from the stored pattern, the microcontroller rejects the authentication attempt and does not issue the authorization signal. The control unit therefore remains in its locked or access-restricted state. The display unit indicates that authentication has failed and access has been denied.

Operation of the Control Unit

The control unit provides the interface between the authentication system and the protected equipment. Its configuration depends on the intended application. The microcontroller determines whether the control unit is authorized to operate. This arrangement separates the authentication process from the physical or electronic mechanism being controlled.

Display of Authentication Status

The dislay unit communicates the outcome of the authentication process. Following successful pattern verification, it displays a message such as "Access Granted" or "Unlocked".

When the entered pattern does not match the stored pattern, it displays "Access Denied" or "Incorrect Pattern". The display provides immediate feedback to the user and helps distinguish successful authentication from rejected attempts.

ISSN 2278-2540 | DOI: 10.51583EMAS | Volume XV, Issue X, October2026

RESULTS AND DISCUSSION

The proposed potentiometer-based rotational pattern authentication system is designed to provide controlled access through a user-defined sequence of rotational movements. Its operation is based on registering a reference pattern, capturing an input pattern, comparing the two sequences, and controlling the connected device according to the comparison result.

When the user enters the same rotational pattern that was registered previously, the microcontroller compares the input sequence with the stored reference pattern. If the direction and order of the movements satisfy the matching criteria, the system generates an authorization signal. The control unit responds to this signal by unlocking the associated locking mechanism or enabling the protected electronic system. The display unit indicates successful authentication.

When the user enters a pattern that differs from the registered pass pattern, the microcontroller identifies the mismatch and rejects the authentication attempt. No authorization signal is issued, and the control unit maintains the protected system in its locked or access-restricted state. The display unit indicates authentication failure.

This test evaluates whether the system can distinguish the registered pattern from incorrect rotational sequences and prevent unauthorized access under the tested conditions.

SUMMARY OF FINDINGS

The proposed design establishes a framework for rotational pattern authentication using a potentiometer, a microcontroller board, a control unit, and a display unit. The architecture supports user-defined pass patterns, sequence-based verification, conditional control of a connected device, and visual indication of authentication status.

The system's main potential advantages are its customizable input mechanism, relatively simple hardware requirements, and adaptability to different access-control applications. Its effectiveness as a security mechanism must ultimately be demonstrated through experimental measurements and comparative evaluation. The results of such testing will determine its suitability for practical deployment in electronic locks and other embedded access-control systems.

REFERENCES

1. F. Binbeshr, M. L. Mat Kiah, L. Y. Por, and A. A. Zaidan, “A systematic review of PIN-entry methods resistant to shoulder-surfing attacks,” Computers & Security, vol. 101, Art. no. 102116, Feb. 2021, doi: 10.1016/j.cose.2020.102116.
2. L. Y. Por, I. O. Ng, Y.-L. Chen, J. Yang, and C. S. Ku, “A systematic literature review on the security attacks and countermeasures used in graphical passwords,” IEEE Access, vol. 12, pp. 53408–53423, Mar. 2024, doi: 10.1109/ACCESS.2024.3373662.
3. Y. Kortli, M. Jridi, A. Al Falou, and M. Atri, “Face recognition systems: A survey,” Sensors, vol. 20, no. 2, Art. no. 342, Jan. 2020, doi: 10.3390/s20020342.
4. D. Maiti, M. Basak, and D. Das, “A review on fingerprint based authentication—Its challenges and applications,” Computer Science Review, vol. 57, Art. no. 100735, Aug. 2025, doi: 10.1016/j.cosrev.2025.100735.