IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125168

3D AUTHENTICATION SYSTEM USING RUBIK'S CUBE

Mr. Narendra Kumar S[1], Anirudh G E[2], Basavesh S P[3], Divish Raj O[4], Kunal S Jain[5]

Assistant Professor, Department of Computer Science & Engineering, JNNCE, Shivamogga, India[1]

Students, Department of Computer Science & Engineering, JNNCE, Shivamogga, India[2-5]

Abstract: Authentication is an important security aspect in modern digital systems, and traditional methods such as passwords and PINs are vulnerable to security threats. Therefore, there is a need for innovative and efficient authentication solutions that can overcome these challenges. A possible authentication solution is to use Rubik's Cube, which is highly secure, unique, and difficult to guess or crack. This approach uses one side of the Rubik's Cube as a unique password, and playing the same side again results in successful authentication.

The faces of the Rubik's Cube can be read by the camera and the code can be written in Python using the cv2 module. The purpose of this study is to evaluate the feasibility, effectiveness, and usability of Rubik's Cube authentication approaches in various areas such as access control, security, and authentication. The study also examines the security implications and potential vulnerabilities of the approach, and suggests mitigation strategies to strengthen security. Using the Rubik's Cube as a potential solution for authentication provides insights for designing more secure and efficient authentication systems. This research contributes to research into innovative and efficient authentication solutions, which can be used as an alternative or supplementary authentication method to existing methods such as biometrics and multi-factor authentication.

Keywords: Authentication, Security, Python cv2

I. INTRODUCTION

Authentication is an important aspect of security in modern digital systems as it verifies the identity of a user or device before allowing access to a system or service. The authentication problem stems from the fact that traditional authentication methods such as passwords and PINs are vulnerable to various security threats such as brute force attacks, phishing, and social engineering. These attacks can lead to unauthorized access to sensitive information, financial loss, reputational damage, and other adverse consequences. To address these security challenges, researchers and practitioners have developed various authentication methods that are more secure and efficient than traditional methods. These methods include biometrics, two- factor authentication, multi-factor authentication, and behavioral authentication. However, despite the availability of these advanced authentication methods, they face several challenges related to cost, complexity, privacy concerns, and usability.

Therefore, there is a need to develop innovative and efficient authentication solutions that can overcome these challenges. One possible authentication solution is to use the popular 3D puzzle game Rubik's Cube as a password. This approach uses one side of the Rubik's Cube as a unique password, and playing the same side again results in successful authentication. The faces of the Rubik's Cube can be read by the camera and the code can be written in Python using the cv2 module. Using the Rubik's Cube as a potential solution for authentication has several advantages: B. Be highly secure, unique, and difficult to guess or crack. Moreover, it is cheap, easy to implement, and requires no additional hardware or software. Additionally, it can be used as an alternative or supplemental authentication method to existing methods such as biometrics and multi-factor authentication.

The purpose of studies using Rubik's Cubes for authentication is to evaluate the feasibility, effectiveness, and usability of approaches in various areas such as access control, security, and authentication. In addition, this study aims to explore the security implications and potential vulnerabilities of the approach and propose mitigation strategies to improve its security. This study provides insight into the potential of using Rubik's Cube as an innovative and efficient authentication solution and can contribute to the development of more secure and efficient authentication systems.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125168

II. LITERATURE SURVEY

Sl. No	Techniques	Benefits	Draw Backs	References
1	1. Capturing image of a Rubik's cube. 2. Image processing 3. Array development	1. String generation. 2. Provides better result.	1. Expensive. 2. Usage of more electronics.	[1]
2	1. Usage of Kociemba algorithm. 2. Advanced sensors. 3. Stepper motors using Arduino due.	1. Better colour recognition. 2. User Friendly.	1. ARCAS system is complicated. 2. Excess of hardware.	[2]
3	1. Building a database of gathered images 2. Classification of features.	1. Versatile. 2. Easy implementation.	1. Finger print may not work always.	[3]
4	1. Colour detection and 3D representation. 2. Usage of CFOP algorithm.	1. Easy to use.	1. Algorithm may not work always.	[4]
5	1. 3D air Signature 2. Usage of EEG.	1. Contactless authentication.	1. Prone to shoulder surfing attacks.	[5]

III. METHODOLOGY

The primary objective of this research project is to provide better authentication methods.

The proposed methodology for Rubik's Cube authentication involves using the Python cv2 module to capture and process images of a Rubik's Cube. Initially, a scrambled state of the cube is set as the password, which is stored as an array representation. During authentication, the user must present the Rubik's Cube in the same scrambled state to the camera. The cv2 module is then utilized to capture an image of the cube and process it to extract the color information. The color information is converted into an array representing the Rubik's Cube state. The stored password array and the user's array are compared, and if they are equal, the user is authenticated. Otherwise, a password mismatch occurs. To enhance accuracy, image processing techniques such as color thresholding, edge detection, and contour detection can be employed. Considerations should be made for cube orientation tolerance, noise and lighting conditions, error handling, and user experience. Additionally, security measures like combining it with other authentication factors or implementing encryption for password storage should be evaluated. Thorough testing and iteration are crucial to ensure reliability and accuracy of the authentication system before deployment. The proposed methodology for Rubik's Cube authentication using the Python cv2 module appears to be a feasible approach. By capturing and processing images of the Rubik's Cube, it allows for the comparison of the cube's state with a stored password to authenticate the user.

The initial step of setting a scrambled state of the cube as the password and storing it as an array representation is a reasonable approach. During authentication, the user is required to present the Rubik's Cube in the same scrambled state to the camera, and an image is captured using the cv2 module. This image is then processed to extract the color information, which is converted into an array representing the Rubik's Cube state.

To improve the accuracy of the authentication system, various image processing techniques can be employed. Color thresholding can help in extracting the cube's colors accurately, while edge detection and contour detection can assist in identifying the cube's individual cubies and their positions. These techniques can be customized and tuned to handle different lighting conditions and noise levels.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125168

a) **Rubik's Cube:** A Rubik's Cube can be utilized for authentication due to its vast number of possible scrambled states. With 43 quintillion possible configurations, each representing a unique password, the Rubik's Cube offers an immense password space. This makes it highly unlikely for two cubes to have the same scrambled state by chance, enhancing the security of the authentication system. By requiring users to present the cube in a specific scrambled state, the Rubik's Cube provides a challenging and diverse authentication factor that can be difficult for unauthorized individuals to replicate.

Fig 1. A Rubik's cube

b) **Python cv2 module:** The Python cv2 module is used for capturing video, also used for computer vision and image processing. It also provides a wide range of functions and algorithms to analyze and manipulate images or videos.

1. Flow Chart

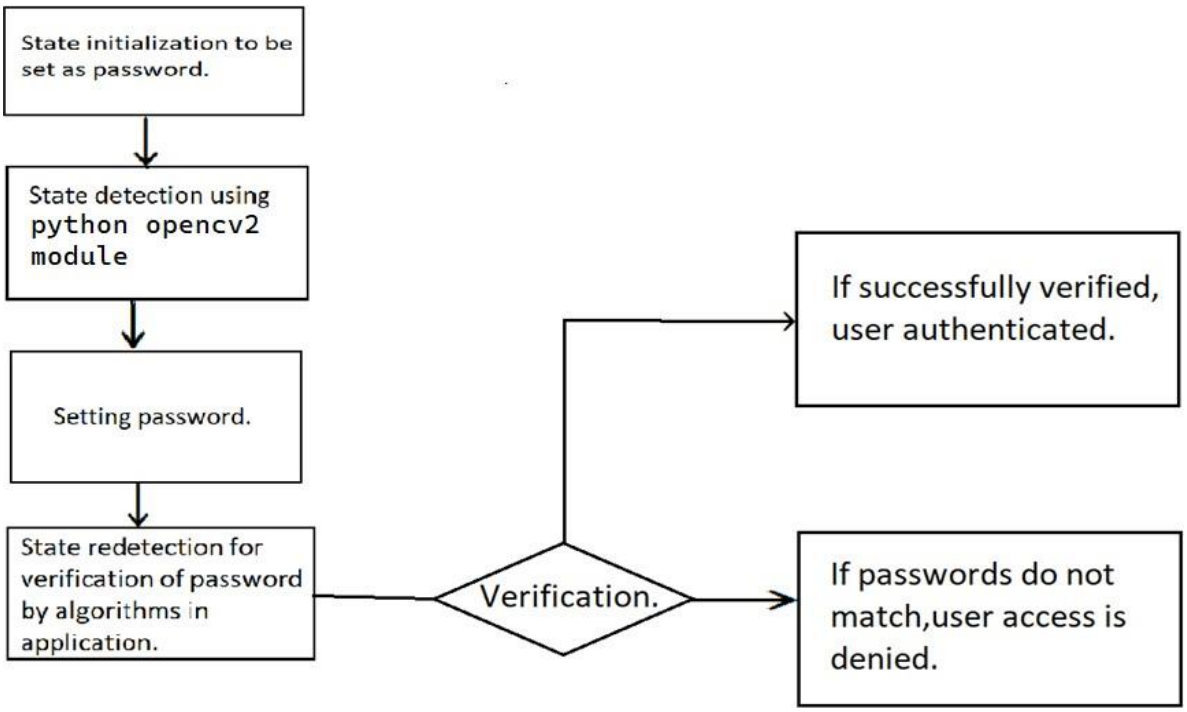

Fig 2. Flow chart of the system

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125168

IV. RESULTS AND DISCUSSION

The results of a 3D authentication system project includes a comparison of the extracted features from the 3D object captured by the camera to the pre-stored set of features for authentication. The accuracy and efficiency of the authentication process could be evaluated by testing the system on different 3D objects with varying features. The system's performance in terms of processing speed and the number of objects that can be authenticated simultaneously could also be measured.

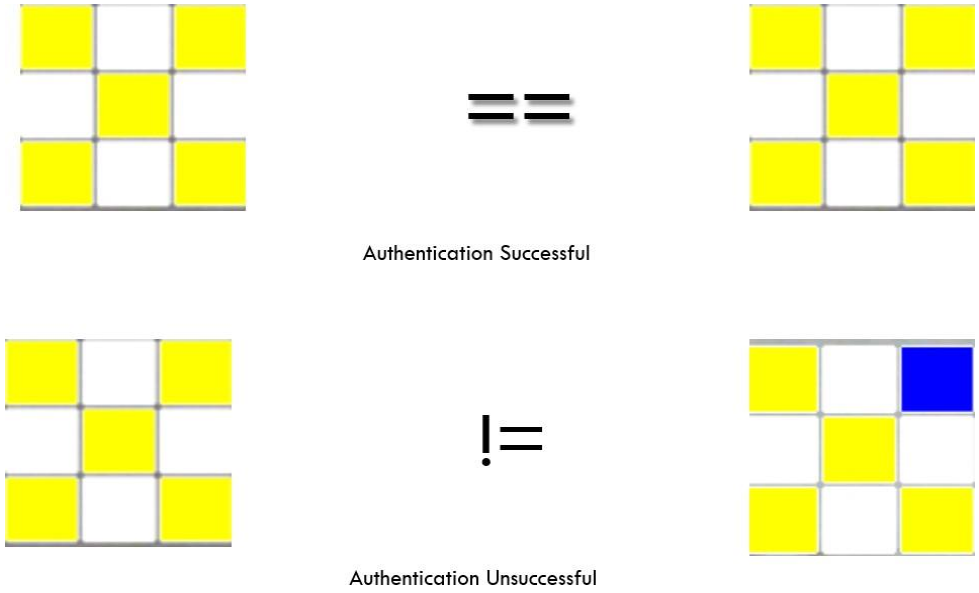

Fig 3. Password comparison.

```
========== RESTART: C:\Users\ANIRUDH G E\Desktop\dummyidi.py ==========
[31m
[32m
[32m
[32m
[32m
[32m
[31m
[31m
[32m
[32m
[32m
[32m
[31m

[35mPlease refer preview window for which side you have scanned and which color should be in centre on each side.
[31m
[32m
[32m
[32m
[32m
[32m
[31m
[31m
[32m
[32m
[32m
[32m
[31m

[35mPl ease refer preview window for which side you have scanned and which color should be in centre on each side.
Authentication successful
['yellow', 'white', 'yellow', 'white', 'yellow', 'white', 'yellow', 'white', 'yellow']
['yellow', 'white', 'yellow', 'white', 'yellow', 'white', 'yellow', 'white', 'yellow']
```

Fig.4. Output showing authentication is successful

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125168

```
========== RESTART: C:\Users\ANIRUDH G E\Desktop\dummyIdf.py ==========
[31m
[32m
[32m
[32m
[32m
[32m
[31m
[31m
[32m
[32m
[32m
[32m
[31m

[35mPlease refer preview window for which side you have scanned and which color should be in centre on each side.
[31m
[32m
[32m
[32m
[32m
[32m
[31m
[31m
[32m
[32m
[32m
[32m
[31m

[35mPlease refer preview window for which side you have scanned and which color should be in centre on each side.
Incorrect password
['white', 'white', 'white', 'white', 'yellow', 'white', 'red', 'yellow']
['white', 'white', 'white', 'yellow', 'white', 'yellow', 'red', 'white', 'yellow']
```

Fig.5 Output showing authentication unsuccessful

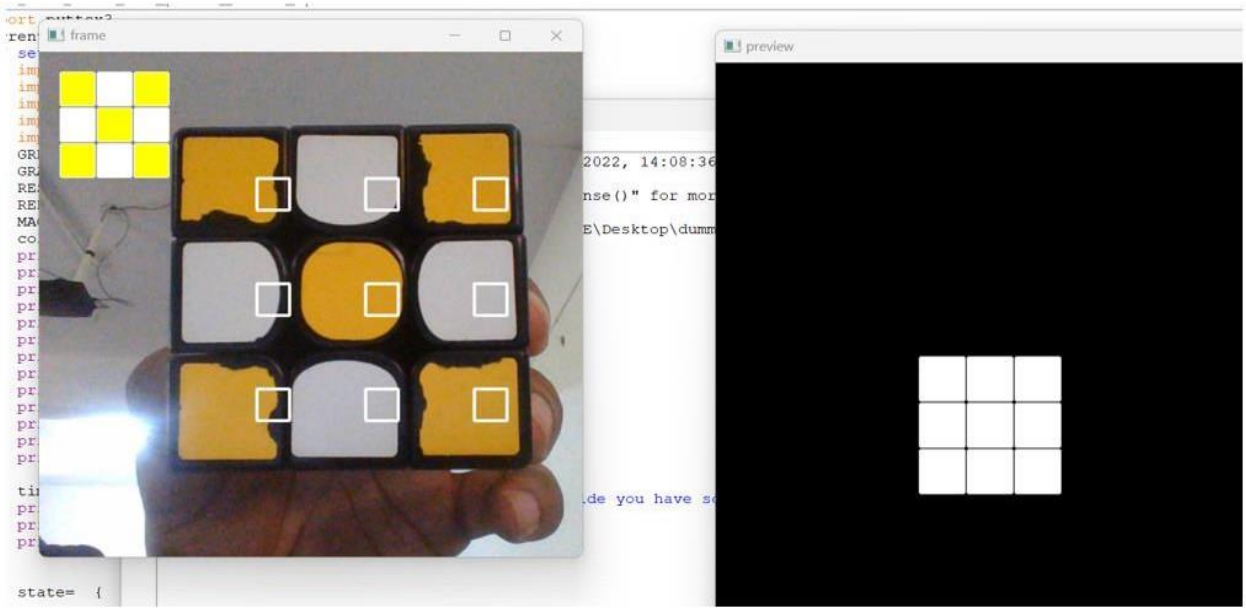

Fig.6 State detection using cv2 module.

V. CONCLUSION

The results of the 3D authentication system project would provide insights into the system's ability to accurately and efficiently authenticate using 3D objects, as well as its robustness against potential attacks.

These results could inform future developments and improvements of the system for various practical applications in domains such as access control, security, and authentication.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.125168

REFERENCES

[1] Ms. Ekta S. Toshniwal Mr. Yogesh Golhar, "Rubik's Cube Solver: A Review" , 2019 9th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing (ICETET-SIP-19)
[2] Vasile Dan, Gabriel Harja, Ioan Naşcu, "Advanced Rubik's Cube Algorithmic Solver" 2021 International Conference on Automation, Robotics and Applications, DOI: 10.1109/ICARA51699.2021.9376564
[3] Hemalatha S, "A systematic review on Fingerprint based Biometric Authentication System", 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), EEE 10.1109/ic-ETITE47903.2020.342
[4] Ayushi Desai, Aniket Brahmecha, Riya Bhagat, Aparna Halbe, "A Novel Approach to Solve Rubik's Cube Using Advanced Fridrich CFOP Algorithm", Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS 2020) IEEE Xplore Part Number: CFP20K74-ART; ISBN: 978-1-7281-4876-2
[5] Santosh K. Behera , Pradeep Kumar, Debi P. Dogra "A Robust Biometric Authentication System for Handheld Electronic Devices by Intelligently Combining 3D Finger Motions and Cerebral Responses, IEEE Transactions on consumer electronics, vol. 67, no. 1, February 2021

