Poster: Hand-covered PIN Authentication for Virtual Reality

Kyle McCraine[1]
Louisiana State University
kmccr14@lsu.edu

Zeyu Deng
Louisiana State University
zdeng6@lsu.edu

Chen Wang[2]
Louisiana State University
chenwang1@lsu.edu

***Abstract*—In both real life and virtual reality (VR), privacy is of utmost importance. To ensure security in the virtual environment, users should be authenticated before accessing it. This paper proposes a hand-covered PIN authentication system for VR users. The system draws a virtual keypad on the user's non-dominant palm based on individually unique hand joint positions, which effectively conceals the user's PIN entry from the view of others in the physical world. By utilizing the visual hand-tracking data of the VR headset, the system verifies both the PIN code and the behavioral biometric to confirm the user's identity. We implement a system prototype on the Oculus Quest 2. Preliminary results demonstrate the potential of providing enhanced security to VR devices with hand-covered PINs.**

I. Introduction

Virtual Reality (VR) is growing at an unprecedented rate, and with it comes the need for increased security measures to protect users' privacy. Although some VR applications require users to set up authentication, not all apps require identity verification. This lack of efficient authentication in VR applications leaves users vulnerable to threats that exploit this gap and access their personal data. To address this issue, we propose designing an authentication application for VR devices that will enhance user security in the virtual world.

Current authentication methods for VR devices require a controller to input a password on a virtual keyboard or keypad [1]. However, when a user operates the controller in the virtual space to complete authentication, the password entry could be leaked to a nearby adversary in the physical world. To improve security, active work has been about extracting behavioral biometrics from the VR user's hand, head, or body motions for authentication [2], [3]. But these methods are not easy to use due to high behavioral inconsistency or additional hardware. In contrast, this work proposes an easy-to-use and security-enhanced PIN authentication system for current VR headsets (e.g., Oculus Quest 2 [4]). The system leverages the VR headset's built-in inside-out camera for hand tracking [5] and provides two-factor authentication, eliminating the need for external hardware.

The VR user can leverage their non-dominant hand as a number pad and use it to cover the PIN entry process and block the potential threats in the physical world from viewing the PIN. The illustration of our design is shown in Figure 1. In particular, the system dynamically generates a virtual number pad based on the joint positions of the user's non-dominant palm. The motions of the user's input hand on the virtual number pad are then captured by the system for authentication. Both the PIN entry and the behavioral biometric features associated with the key clicks are examined, achieving enhanced security.

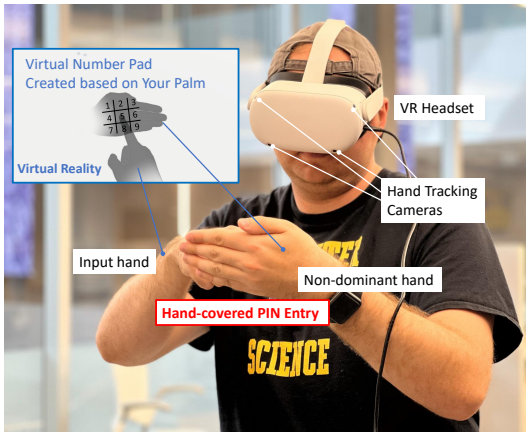


Fig. 1: Illustration of hand-covered PIN entry in VR.

II. System Design

Current VR devices have been equipped with visual sensors (e.g., 4 cameras on Oculus Quest 2) enabling device-free hand tracking so that the user does not need to hold handheld controllers to interact with the device. Our system leverages the visual hand-tracking interface to monitor hand motions and create hand avatars in the virtual space to enable hand-covered PIN entry. In particular, we focus on the accuracy of clicks while others have concentrated on the ability to register a click [6]. Specifically, we use the Oculus coding library OVR to track the user's hand movements. Each hand joint's position and rotation relative to the camera's location are sampled. The 3D coordinates of 24 hand joints (i.e., the 3D skeletal structure of the hand) are obtained at each time stamp. We then use the OVRCamera, which is integrated with Unity, to display the 3D models of both hands in VR and provide live hand motion feedback to the user.

The system further attaches a number pad to the user's non-dominant hand palm (left hand) and allows the user to input a PIN with the index finger of the input hand (right hand). When

[1]Kyle McCraine was an undergraduate researcher at LSU.
[2]Chen Wang is the corresponding author.

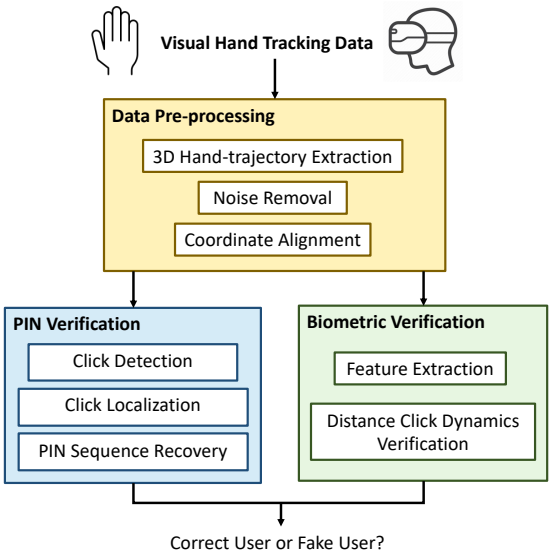


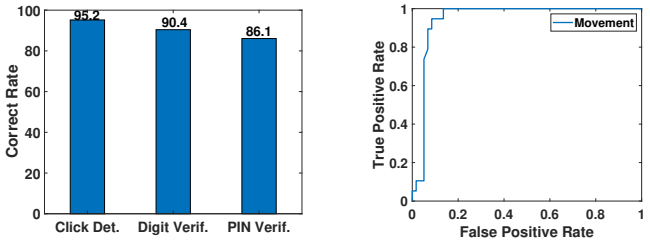
Fig. 2: Overview of hand-covered PIN authentication system.

users enter their PIN codes, our system records their left-hand gestures and right-hand movements, in addition to calculating the dynamic number pad position, for authentication. The data is exported from Unity as a CSV file and analyzed offline.

Figure 2 shows an overview of the hand-covered PIN authentication algorithm. The Data Pre-processing component extracts the 3D hand trajectory from the VR device's visual sensors and prepares the data for further analysis. High-frequency noises and visual sensing errors due to the self-occlusion of the hands are reduced. Because the movement trajectory of the input hand is obtained in the VR device's coordinate system, we translate it to that in the number pad's coordinate via coordinate alignment. The pre-processed data is input into PIN verification and biometric verification algorithms for two-factor authentication.

The PIN verification algorithm matches the number pad and hand position data to determine the clicked numbers and verify the PIN sequence. It first detects the click events based on the Z-axis motions on the number pad and separates the data sample points of the index finger into clicking and moving groups. Then the algorithm predicts the clicked numbers using the dynamic number pad position by calculating Euclidean distances and recovers the PIN sequence. The hash value of the recovered PIN is compared with that stored in the authentication system to determine whether the PIN is correct.

The biometric verification algorithm first derives the behavioral biometric features of the PIN entry-associated hand movements. We derive the hand motion features, including the movement speeds between clicks (e.g., three separate movements for a 4-digit PIN code). The movement speed is unique to each user, and our algorithm calculates the Euclidean distances of these dynamic series to the user's biometric template for biometric authentication. The system grants access when the PIN sequence and biometric features are successfully verified.



(a) PIN Verification (b) Biometric Verification

Fig. 3: VR User Authentication Performance.

III. Preliminary Result

Preliminary evaluation includes click detection, digit/PIN verification, and biometric verification. The results of our PIN verification detection method are shown in Figure 3a. The most common reason for failed PIN verification is the sensing error when detecting a user's movement to another number, which can result in two clicks being combined. Additionally, difficulty in identifying the correct click may arise if the user clicks between two numbers on the number pad.

To train our data, we select a percentage of user data to determine the average distance between points during the movement stage of entering a PIN code. The remaining user and non-user data are then used to generate true positive and false positive rates, which are applied to a receiver operating characteristic (ROC) curve. Figure 3b displays the ROC curve generated by testing multiple tolerance levels and calculating their associated true positive and false positive rates.

While the preliminary results show the potential of hand-covered PIN authentication, we will continue to improve the system. We will add more biometric features to capture hand biometrics. For instance, we can utilize the shape of the user's hands or the way they move when clicking on a particular number. Besides, we will develop more advanced PIN authentication and biometric learning algorithms. Additionally, we will design better algorithms to address the sensing errors.

Acknowledgments. This work was supported in part by LABoR LEQSF(2020-23)-RD-A-11 and NSF CNS-2155131.

References

[1] J. Liebers, S. Brockel, U. Gruenefeld, and S. Schneegass, "Identifying users by their hand tracking data in augmented and virtual reality," *International Journal of Human–Computer Interaction*, pp. 1–16, 2022.

[2] M. Sivasamy, V. Sastry, and N. Gopalan, "Vrcauth: continuous authentication of users in virtual reality environment using head-movement," in *2020 5th International Conference on Communication and Electronics Systems (ICCES)*. IEEE, 2020, pp. 518–523.

[3] X. Wang and Y. Zhang, "Nod to auth: Fluent ar/vr authentication with user head-neck modeling," in *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–7.

[4] Meta. (2023) Quest 2 by oculus. [Online]. Available: https://www.meta.com/quest/products/quest-2/

[5] E. Guerra-Segura, A. Ortega-Pérez, and C. M. Travieso, "In-air signature verification system using leap motion," *Expert Systems with Applications*, vol. 165, p. 113797, 2021.

[6] C. Harrison, H. Benko, and A. D. Wilson, "Omnitouch: wearable multitouch interaction everywhere," in *Proceedings of the 24th annual ACM symposium on User interface software and technology*, 2011, pp. 441–450.