Put your glasses on: A voxel-based 3D authentication system in VR using eye-gaze

Rumeysa Turkmen*
Kadir Has University
Dalhousie University

Chukwuemeka Nwagu†
Dalhousie University

Prashant Rawat‡
Dalhousie University

Poppy Riddle§
Dalhousie University

Kissinger Sunday¶
Dalhousie University

Mayra Barrera Machuca‖
Dalhousie University

ABSTRACT

Due to the current push of social Virtual Reality (VR) apps and mobile VR headsets, users are surrounded by people in real life and virtually. Users need a private method to authenticate payments or login into apps. In this paper, we propose VoxAuth, a novel voxel-based 3D authentication system, allowing users to input their password in a private way. By using eye-gaze as a secure, input method, people outside VR are prevented from observing the password. Sunglasses on the avatar appear during the authentication process both as a gaze observation prevention and as a signal that the user is still connected.

Index Terms: H.5.m [Multimedia Information Systems]: User Interfaces —;

1 INTRODUCTION

Virtual reality (VR) is becoming a tool for social connection between users, as shown by VR applications like AltSpace, VRChat or Horizon Worlds. Thanks to the advent of mobile VR headsets, e.g., Meta Quest 2, people use VR in libraries, coffee shops or classrooms where they are surrounded by others. While using these applications in social spaces (Fig. 1), users need to authenticate their identity, such as to make a payment or add friends. However, due to the nature of VR, users currently use physical movements that their avatar mimics to add this information, which may provide clues as to their actions to observers. This presents a security risk both in the virtual and physical space. Minimizing the observation threat is a high priority for secure authentication, which needs to be fast, secure, memorable, and easy to repeat.

In this paper, we present VoxAuth, a novel, voxel-based 3D authentication system, that addresses these needs. We designed VoxAuth to solve two problems with authentication in VR: 1) observation threat when entering the password, and 2) difficult and complex passwords. Next we describe how we achieved these goals:

1. *Observation Threat*: We use an eye-gaze input method as users outside the virtual environment (VE) cannot see the eye movement due to the VR head mounted display (HMD). Users inside the VE can see the eye movement, especially with the current generation of avatars. To prevent them from seeing eye movement, the user's avatar is wearing sunglasses to cover the eyes, thus hiding gaze-based movements as a security concern [6]. Using the sunglasses is also a signal to the other users, that the user is still connected with the VE even if no movement is happening.

2. *Secure and Memorable Password*: We build on the cube space idea [9], memorability of graphical passwords, and use of color as an additional level of password complexity. In our system, every user uploads a unique image, which is automatically converted to a 3D voxel. Then, the user pre-selects different voxels in places that are memorable. We enable a 3DOF manipulation of the 3D voxel matrix for additional complexity of the password.

*e-mail: rumeysa.turkmen@stu.khas.edu.tr
†e-mail:cnwagu@dal.ca
‡email:prashant.rawat@dal.ca
§email:poppy.riddle@dal.ca
¶email:kissinger.sunday@dal.ca
‖e-mail:mbarrera@dal.ca

Figure 1: VR users in a social, physical environment, as well as a social, immersive environment.

VoxAuth builds on previous work that investigates authentication within VE using graphical passwords. For example, Abdelrahman et al. [1] explored cue-based authentication benefits and Düzgün et al. [3] investigated the advantages of graphical-based passwords for use with HMDs. Mathis et al. [9] used eye-gaze to select color digit combinations on a cube as a graphical password. Our proposal is unique as we use 3D voxels created from user-selected images to improve memorability.

2 VOXAUTH DEMO

We developed the VoxAuth demo using Unity 2021.3 version and the Meta Quest Pro, which has integrated eye-tracking capabilities. Our demo consists of two tasks: 1) setting the password and 2) entering the password when surrounded by other users. Next, we describe each task separately.

2.1 Setting the password

The first task requires the user to set their voxel-based authentication targets. Prior to entering the VE, the user chooses an image as their security image during account set-up. The image would be pixelated upon upload – this provides benefits as it makes salient targets explicit and divides the image into discrete blocks of color to be turned into voxels. While image complexity increases security [10], we have used a low-resolution image to provide a basis for

979-8-3503-4839-2/23/$31.00 ©2023 IEEE
DOI 10.1109/VRW58643.2023.00316

understanding how gaze-based passwords [6] are chosen. For our test, we are using a proxy image (Fig. 2) [1].

Once an image is uploaded, the system creates a 3D shape by constructing a voxel from each color square. The depth of the matrix is determined by color with the spectrum mapped onto scalar values that determines depth within the cube space. In this way, every image has a different 3D shape, providing more complex password choices. Once the 3D matrix is automatically created, the user selects 4 voxels to create their password using eye-gaze and the controller. To select a voxel, the user points using their eye gaze and selects with the controller trigger. To add a complexity layer to the password, the cube may be rotated in 3DOF using the controller so that not all selected voxels are on the same face of the cube space. Selected voxels are captured as a library to verify in task 2.

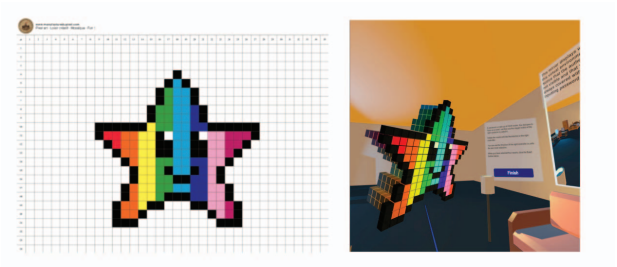

Figure 2: Left: the pixelated image [8]. Right: the voxelated image in the immersive environment.

2.2 Enter the password

For the second task, the user is still within the VE which includes dummy avatars representing other users and is prompted to authenticate to access a group. The user selects the 'enter password' icon and sees their voxelated authentication image. The voxel-image can be rotated using the controller to choose targets using eye gaze pointing. The controller trigger is used to select the target voxel that has been indicated by the eye gaze-directed pointer. If correctly chosen, the user is notified of successful completion of the task and the user returns to the VE.

If a non-matching sequence is performed, the user is notified and permitted to repeat the process until a correct sequence is entered. If successful, the voxel-image disappears and a success notification is displayed.

3 Limitations/Challenges

Many challenges remain including understanding how users choose graphical passwords, perceptions of strength, prediction due to visual salience [6], or effects of password reuse [2]. Additionally, it is unknown how gaze pointing for authentication may need accommodation for neurodiverse users, though advantages for those with upper extremity impairment have been recognized [7]. There are also information management issues not clearly understood at this time including access to iris image data [5], or how unconscious movements may complement other data that can be identifying [4].

4 Conclusion

In this proposal we have created VoxAuth, a novel graphical authentication method for users surrounded by people in both real and VE for the purpose of minimizing observation threat. Using an explicit, multimodal gaze-based pointing and controller selection, users select target voxels that are mapped within 3D space based upon a user-chosen image. Instead of disabling the avatar's eye gaze, the user's avatar wears a pair of sunglasses during the authentication process, both as a functional obscuring of the avatar's eye gaze movements as well as a signal to others that the user is busy and has not been disconnected.

Future research should evaluate the usability of this approach, especially for its learnability and memorability of the pattern of target voxels. While a multimodal approach of pointing and selection has been used in this test, unimodal methods of pointing and selection using eye gaze should be explored. More work is also needed to understand what constitutes a strong level of security for spatial-based targets, how prediction of visually salient targets may affect their strength, and perceptions of strength and memorability based on the image selection.

[1] https://manufacturedupixel.com/pixel-creator

References

[1] Y. Abdelrahman, F. Mathis, P. Knierim, A. Kettler, F. Alt, and M. Khamis. CueVR: Studying the Usability of Cue-Based Authentication for Virtual Reality. In *Proceedings of the 2022 International Conference on Advanced Visual Interfaces*, AVI 2022. Association for Computing Machinery, New York, NY, USA, 2022. Frascati, Rome, Italy. doi: 10.1145/3531073.3531092

[2] Y. Abdrabou, J. Schütte, A. Shams, K. Pfeuffer, D. Buschek, M. Khamis, and F. Alt. "Your Eyes Tell You Have Used This Password Before": Identifying Password Reuse from Gaze and Keystroke Dynamics. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22. Association for Computing Machinery, New York, NY, USA, 2022. New Orleans, LA, USA. doi: 10.1145/3491102.3517531

[3] R. Düzgün, P. Mayer, and M. Volkamer. Shoulder-Surfing Resistant Authentication for Augmented Reality. In *Nordic Human-Computer Interaction Conference*, NordiCHI '22. Association for Computing Machinery, New York, NY, USA, 2022. Aarhus, Denmark. doi: 10.1145/3546155.3546663

[4] K. J. Emery, M. Zannoli, L. Xiao, J. Warren, and S. S. Talathi. Estimating Gaze From Head and Hand Pose and Scene Images for Open-Ended Exploration in VR Environments. In *2021 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pp. 554–555. IEEE, Lisbon, Portugal, Mar. 2021. doi: 10.1109/VRW52623.2021.00159

[5] B. John, S. Jorg, S. Koppal, and E. Jain. The Security-Utility Trade-off for Iris Authentication and Eye Animation for Social Virtual Avatars. *IEEE Transactions on Visualization and Computer Graphics*, 26(5):1880–1890, May 2020. doi: 10.1109/TVCG.2020.2973052

[6] C. Katsini, Y. Abdrabou, G. E. Raptis, M. Khamis, and F. Alt. The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, pp. 1–21. Association for Computing Machinery, New York, NY, USA, 2020. Honolulu, HI, USA. doi: 10.1145/3313831.3376840

[7] B. Lewis and K. Venkatasubramanian. "I...Got My Nose-Print. But It Wasn't Accurate": How People with Upper Extremity Impairment Authenticate on Their Personal Computing Devices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21. Association for Computing Machinery, New York, NY, USA, 2021. Yokohama, Japan. doi: 10.1145/3411764.3445070

[8] manufacturedupixel. Étoile Arc-en-Ciel, June 2019.

[9] F. Mathis, K. Vaniea, and M. Khamis. RepliCueAuth: Validating the Use of a Lab-Based Virtual Reality Setup for Evaluating Authentication Systems. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, pp. 1–18. Association for Computing Machinery, New York, NY, USA, May 2021. doi: 10.1145/3411764.3445478

[10] G. E. Raptis, C. Katsini, A. J.-l. Cen, N. A. G. Arachchilage, and L. E. Nacke. Better, Funner, Stronger: A Gameful Approach to Nudge People into Making Less Predictable Graphical Password Choices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21. Association for Computing Machinery, New York, NY, USA, 2021. Yokohama, Japan. doi: 10.1145/3411764.3445658