Boosting Remote Multi-user AR Privacy through a Magic Rope

Feng Qian
University of Minnesota
Minneapolis, MN,USA
fengqian@umn.edu

Bin Li
Pennsylvania State University
State College, PA, USA
binli@psu.edu

ABSTRACT

In remote Multi-user AR (MuAR), a user shares with remote users his/her physical environment, which is enhanced by computer-generated perceptual information. Despite its important role in Metaverse, a user may have serious privacy concerns for MuAR: the user may want to share only a portion, or may want to block certain areas in their environment. Today's object detection and AR tracking techniques fall short of reliably, efficiently, and accurately supporting this use case, in particular on an (already overloaded) headset without offloading to an edge/cloud server for privacy preservation purposes.

In this poster, we propose a novel primitive called Magic Rope to boost remote MuAR privacy. A user employs a flexible rope to circle enclosed areas as whitelisted (expose externally) or blacklisted (exclude/blur from sharing). The rope has specially designed markers allowing an AR headset to accurately and efficiently detect its enclosed area, as well as to drastically reduce the tracking overhead. We are working on addressing several research questions such as the marker design, efficient detection of chained markers on a rope, occlusion handling, multi-rope connection, and human-computer interaction design. We also plan to develop a full-fledged prototype of Magic Rope and integrate it with real remote MuAR applications. We will conduct extensive evaluations (including an IRB-approved user study) on real AR headsets.

CCS CONCEPTS

• **Human-centered computing** → **Ubiquitous and mobile computing**; **Mixed / augmented reality**; • **Security and privacy** → **Privacy protections**.

KEYWORDS

Mobile Augmented Reality, Privacy Preservation, Magic Rope

ACM Reference Format:
Feng Qian and Bin Li. 2022. Boosting Remote Multi-user AR Privacy through a Magic Rope. In *The 20th Annual International Conference on Mobile Systems, Applications and Services (MobiSys '22), June 25-July 1, 2022, Portland, OR, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3498361.3538795

1 BACKGROUND AND PROBLEM

In Multi-user AR (MuAR), several users collaboratively or interactively accomplish a task in a real-world environment enhanced by computer-generated perceptual information [5]. While the participants can be physically co-located, a more exciting scenario is what we call *remote MuAR* where users are geographically distributed. In remote MuAR, user(s) in one location share their physical environment with user(s) in other locations. For example, through remote MuAR, the author living in Minnesota can invite his friends in Shanghai to build LEGO bricks virtually in his house; the friends wearing AR headsets can see the author's house with the LEGO model rendered on the study table (Figure 1).

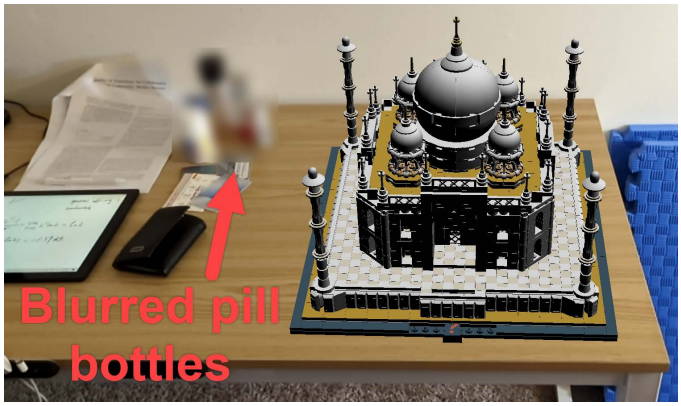

Figure 1: AR-based multi-user LEGO from the co-author's prior work [7]. Some objects are blurred to demonstrate an AR system assisted by Magic Rope.

Remote MuAR constitutes an exciting use case of Metaverse. However, it poses an interesting research problem of privacy preservation. In the above scenario, the author may want to share only part of the table with his friends (*e.g.,* excluding papers, medicine pill bottles, and a tablet in Figure 1), or he may want to digitally hide/blur certain objects in his room. A similar scenario appears in video conferencing, where a participant's background can be blurred or replaced. However, in remote MuAR, the problem is much more challenging: instead of being binary (foreground human body/face vs. background), the recognition is fine-grained for arbitrary pre-defined objects; users may exhibit excessive movement compared to video conferencing, making recognition even more difficult. Furthermore, to minimize the privacy concern, we prefer all recognition tasks and object blocking be performed locally on an (already overloaded) headset without offloading to an edge/cloud server.

The above problem of removing/blurring objects in AR is known as "diminished reality" (DR) in the VR/AR literature [2]. Despite existing work on DR (see [3] for a survey), its core technical components, namely user tracking and object detection, remain challenging tasks. For privacy preservation, the requirement for recognition accuracy is particularly high – a single missed object detection (false

MobiSys '22, June 25-July 1, 2022, Portland, OR, USA

ACM ISBN 978-1-4503-9185-6/22/06.
https://doi.org/10.1145/3498361.3538795

negative) will cause information leaks [6], whereas a false detection (false positive) will incur undesired object blocking, hurting user experience and even causing motion sickness. The state-of-the-art tracking and detection techniques fall far short of real-time DR for privacy preservation, in particular given the absence of edge/cloud support.

2 THE MAGIC ROPE

In this poster, we propose a novel primitive to preserve privacy for remote MuAR. The basic idea is as follows. Before sharing their environment, a user employs a specially designed physical rope (referred to as *Magic Rope*) to mark certain enclosed areas. The rope is flexible, lightweight, and cheap (production cost estimated to be less than $5). We envision two usage scenarios. (1) *Whitelist:* using a rope to circle areas to be exposed to the external world; the rest of the environment will be excluded or blurred. (2) *Blacklist:* use one or more ropes to circle area(s) to be excluded or blurred; only the rest of the environment will be shared externally.

Equally spaced *markers* are printed on the rope. Each marker is unique. It encodes its relative position, *i.e.,* the offset from the beginning of the rope, similar to a tick on a ruler. A marker may also include an indicator or arrow that helps distinguish the inside vs. outside of its surrounded region. Conceptually, the markers can be regarded as a chain of (customized) bar codes or QR codes that can be easily manipulated by users. They will drastically reduce the workload for object detection and tracking in two aspects. First, computer vision algorithms can easily detect markers to identify whitelisted or blacklisted regions. Specifically, after quickly localizing the markers' 3D positions, the headset will interpolate the markers into a closed loop, and extrude the loop (*i.e.,* hoist the Z-axis) to establish an enclosed wall. Objects falling inside the enclosed wall will be properly whitelisted or blacklisted. The second benefit of the chained markers along the rope is that they can assist the tracking algorithm in general, as QR codes have been commonly used to provide the tracking/localization ground truth. The tracking algorithm can, for example, simply use markers and IMU (inertial measurement unit) to track user's motion, instead of relying on more heavy-weight approaches such as SLAM (Simultaneous Localization and Mapping [4]).

While its high-level idea appears straightforward, Magic Rope brings unique inter-disciplinary research questions that we are currently working on, as elaborated next.

• *How to design the markers?* There are several key design decisions to make, including the thickness of the rope, the spacing between markers, and the style of markers (*e.g.,* bar code vs. block code, color vs. monochrome). In particular, the markers should be robust to curving and twisting the rope.

• *How to efficiently detect chained markers?* While there exist algorithms for detecting a single marker [1], identifying *a sequence of markers* in a robust and efficient manner is a new problem. For example, along the rope, we can add certain "guiding patterns" between markers, so that subsequent markers can be quickly identified after detecting the first marker. Also, it is not necessary to detect all the markers in all frames; if most markers are detected, then the shape of the closed loop can be reasonably reconstructed.

• *How to handle occlusions?* When part of the rope is occluded, identifying the enclosed loop can be challenging. A possible solution is to ask the user to scan the entire rope when the AR application starts. This short, one-time training phase will help the system learn the shape of the rope and each marker's position. Later, the remembered shape can be leveraged to reconstruct the occluded part.

• *How to use multiple ropes to enclose a large area?* We allow connecting several short rope segments to enclose a large area. The connection can be either physical or virtual – in the latter case, we will design an algorithm to identify rope segments in proximity and form them into a loop.

• *Understanding human factors.* We will conduct an IRB-approved user study to answer the following questions. How do people view privacy issues in remote MuAR? Is Magic Rope easy to use? How long does it take to set up the rope? How much training do users need? Do users prefer whitelist or blacklist? The results will help us understand and improve the human factors of Magic Rope.

We are currently working on the complete design and implementation of Magic Rope. We plan to integrate it with real remote MuAR applications (*e.g.,* multi-user LEGO) running on commodity AR headsets, and conduct extensive evaluations (including a user study).

REFERENCES

[1] L. Belussi and N. Hirata. Fast qr code detection in arbitrarily acquired images. In *2011 24th SIBGRAPI Conference on Graphics, Patterns and Images*, pages 281–288. IEEE, 2011.

[2] Y. F. Cheng, H. Yin, Y. Yan, J. Gugenheimer, and D. Lindlbauer. Towards understanding diminished reality. In *CHI Conference on Human Factors in Computing Systems*, pages 1–16, 2022.

[3] S. Mori, S. Ikeda, and H. Saito. A survey of diminished reality: Techniques for visually concealing, eliminating, and seeing through real objects. *IPSJ Transactions on Computer Vision and Applications*, 9(1):1–14, 2017.

[4] R. Mur-Artal, J. M. M. Montiel, and J. D. Tardos. Orb-slam: a versatile and accurate monocular slam system. *IEEE transactions on robotics*, 31(5):1147–1163, 2015.

[5] X. Ran, C. Slocum, Y.-Z. Tsai, K. Apicharttrisorn, M. Gorlatova, and J. Chen. Multi-user augmented reality with communication efficient and spatially consistent virtual objects. In *Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies*, pages 386–398, 2020.

[6] N. Raval, A. Srivastava, A. Razeen, K. Lebeck, A. Machanavajjhala, and L. P. Cox. What you mark is what apps see. In *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services*, pages 249–261, 2016.

[7] X. Yao, J. Chen, T. He, J. Yang, and B. Li. A scalable mixed reality platform for remote collaborative lego design. In *IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops*, pages 1–2. IEEE, 2022.