Introduction to the Special Issue on Security and Privacy of Avatar in Metaverse

Yushu Zhang, William Puech, Anderson Rocha, Rongxing Lu, Stefano Cresci, Roberto Di Pietro

Introduction to the Special Issue on Security and Privacy of Avatar in Metaverse

The Metaverse is a 3D interactive virtual community that has gained significant attention in academia, business, and industry as a potential future internet paradigm. In this space, avatars serve as key elements, acting as the primary means of human interaction. Avatars are expected to be created using real data, tailored to users' preferences, and controlled in real-time through signals from wearable devices.

Avatars allow users to feel as though they are extensions of their own bodies, creating an immersive experience that blurs the line between virtual and real compared to other virtual communities. On the other hand, the avatar faces serious security and privacy problems, especially when people and the law/regulation are increasingly less tolerant of security and privacy, such as copyright, false identity detection, dataset security, authentication, and content tampering. This special issue collects 15 papers reporting the recent developments of security and privacy of avatar in metaverse.

For the Avatar Copyright Protection.

"A Self-Defense Copyright Protection Scheme for NFT Image Art Based on Information Embedding" addresses copyright issues related to avatars produced in the Metaverse and proposes a copyright protection scheme that not only enables tracking and verification of avatar content transactions but also validates the legality of the source and ownership of the avatar content.

"Invisible Adversarial Watermarking: A Novel Security Mechanism for Enhancing Copyright Protection" addresses the potential for unauthorized access and use of image datasets used to generate avatars and proposes an image protection method that combines adversarial perturbations with invisible watermarks. This approach not only prevents illegal use of the image datasets but also enables effective tracking of data copyright.

In "FaceDefend: Copyright Protection to Prevent Face Embezzle," the authors propose a solution to the misuse problem arising from the theft of real facial image data used in avatar generation, based on defensive strategies. This approach effectively ensures copyright protection for real facial data.

For the False Identity Detection for Avatars.

The authors of "Audio-Visual Contrastive Pre-train for Face Forgery Detection" address the issue of potential facial privacy breaches due to the realism of avatars in virtual worlds, which can lead

ACM Reference format:
Yushu Zhang, William Puech, Anderson Rocha, Rongxing Lu, Stefano Cresci, and Roberto Di Pietro. 2024. Introduction to the Special Issue on Security and Privacy of Avatar in Metaverse. *ACM Trans. Multimedia Comput. Commun. Appl.* 21, 2, Article 41 (December 2024), 3 pages.
https://doi.org/10.1145/3702485

ACM 1551-6865/2024/12-ART41
https://doi.org/10.1145/3702485

to the creation of deepfake videos with false identities. They propose a video deepfake detection scheme based on temporal transformers using transfer learning techniques.

In "Feature Extraction Matters More: An Effective and Efficient Universal Deepfake Disruptor," the authors focus on the issue of malicious alterations to the facial attributes of avatars by designing a universal facial anti-manipulation perturbator that prevents successful modification of these attributes.

"Domain-invariant and Patch-discriminative Feature Learning for General Deepfake Detection" proposes a detection method for deepfake avatar videos to prevent malicious activities in the Metaverse, where individuals might use deepfake facial videos to frame others.

"Spatiotemporal Inconsistency Learning and Interactive Fusion for Deepfake Video Detection" explores the use of spatiotemporal inconsistencies to detect deepfake videos, proposing an interactive spatiotemporal inconsistency learning and fusion detection method composed of phase-aware sequential flows. This aims to address the significant security risks of falsifying user avatar identities in the Metaverse.

In "Deepfake Video Detection Using Facial Feature Points and Ch-Transformer," the authors design a deepfake facial detection scheme based on clues from the distribution of facial feature points and the differing displacement distances of real and fake facial feature points between frames. This aims to ensure the authenticity of avatar identities in the Metaverse.

For Dataset Security.

In "A Quality-Aware and Obfuscation-Based Data Collection Scheme for Cyber-Physical Metaverse Systems," the authors address the issue of personnel collecting real data potentially leaking task privacy. They propose a data collection method that does not expose the purpose of the tasks, achieving high-quality data collection for the Metaverse while ensuring the hiding of data tasks.

In "Exploiting Backdoors of Face Synthesis Detection with Natural Triggers," the authors consider the risk of backdoors in datasets used to train avatar models and propose a novel synthetic analysis backdoor attack targeting facial synthesis detection models. This approach demonstrates superior robustness compared to existing backdoor defense methods.

For Authentication Security.

In "A New Tensor Summary Statistic for Real-Time Detection of Stealthy Anomaly in Avatar Interaction," the authors investigate the security risks faced by avatars during interactions in the Metaverse and propose a tensor-based anomaly interaction detection and alerting method.

"VRVul-Discovery: BiLSTM-based Vulnerability Discovery for Virtual Reality Devices in Metaverse" discuss privacy issues in user authentication arising from vulnerabilities and security risks associated with Metaverse devices. They analyze the root causes of security risks in user authentication and scene interactions, and implement a prototype for vulnerability discovery and validation, successfully identifying seven vulnerabilities based on this prototype.

The authors of "Pivot: Panoramic-image-based VR User Authentication against Side-Channel Attacks" address the security issues of identity authentication in the Metaverse and propose a panoramic image-based authentication mechanism to mitigate the security risks associated with traditional password-based authentication. They validate the security of this mechanism from both theoretical and practical perspectives.

For Content Tampering.

"Cross-attention based two-branch networks for document image forgery localization in the Metaverse" discuss the serious consequences that may arise from the spread of tampered content in the Metaverse and propose a new dual-branch network to detect and locate forged regions in document images. This approach extracts manipulation traces from spatial information while also identifying anomalies from the noise domain.

In "Cascaded Adaptive Graph Representation Learning for Image Copy-Move Forgery Detection," the authors address the issue of content copy tampering and propose an innovative copy-move forensics framework based on graph representation learning. This framework effectively captures the homology between copy-move pairs and identifies inconsistencies between the target region and the background.

The guest editors would like to thank all the authors who submitted their articles and anonymous reviewers who carefully reviewed and evaluated them. They extend their sincere thanks to the Editor-in-Chief of the *ACM Transactions on Multimedia Computing, Communications, and Applications*, Prof. Abdulmotaleb El Saddik, for providing the opportunity and guidance to edit this Special Issue and the editorial staff for their continuous support in organizing the Special Section.

Yushu Zhang
Nanjing University of Aeronautics and Astronautics, Nanjing, China

William Puech
Université de Montpellier, Montpellier, France

Anderson Rocha
University of Campinas (Unicamp), Campinas, Brazil

Rongxing Lu
University of New Brunswick, Fredericton, Canada

Stefano Cresci
IIT-CNR, Monterotondo, Italy

Roberto Di Pietro
Hamad Bin Khalifa University, Doha, Qatar

Guest Editors