Frontiers in Virtual Reality

TYPE Systematic Review
PUBLISHED 17 November 2022
DOI 10.3389/frvir.2022.974652

OPEN ACCESS

EDITED BY
Jean-Rémy Chardonnet,
ParisTech École Nationale Supérieure d'Arts et Métiers, France

REVIEWED BY
Hai-Ning Liang,
Xi'an Jiaotong-Liverpool University, China
Mikhail Langovoy,
Karlsruhe Institute of Technology (KIT), Germany

*CORRESPONDENCE
Jinghuai Lin,
jinghuai.lin@uni-wuerzburg.de

SPECIALTY SECTION
This article was submitted to Technologies for VR, a section of the journal Frontiers in Virtual Reality

RECEIVED 21 June 2022
ACCEPTED 25 October 2022
PUBLISHED 17 November 2022

CITATION
Lin J and Latoschik ME (2022), Digital body, identity and privacy in social virtual reality: A systematic review. *Front. Virtual Real.* 3:974652. doi: 10.3389/frvir.2022.974652

Digital body, identity and privacy in social virtual reality: A systematic review

Jinghuai Lin* and Marc Erich Latoschik

Human-Computer Interaction (HCI) Group, Informatik, University of Würzburg, Würzburg, Germany

Social Virtual Reality (social VR or SVR) provides digital spaces for diverse human activities, social interactions, and embodied face-to-face encounters. While our digital bodies in SVR can in general be of almost any conceivable appearance, individualized or even personalized avatars bearing users' likeness recently became an interesting research topic. Such digital bodies show a great potential to enhance the authenticity of social VR citizens and increase the trustworthiness of interpersonal interaction. However, using such digital bodies might expose users to privacy and identity issues such as identity theft: For instance, how do we know whether the avatars we encounter in the virtual world are who they claim to be? Safeguarding users' identities and privacy, and preventing harm from identity infringement, are crucial to the future of social VR. This article provides a systematic review on the protection of users' identity and privacy in social VR, with a specific focus on digital bodies. Based on 814 sources, we identified and analyzed 49 papers that either: 1) discuss or raise concerns about the addressed issues, 2) provide technologies and potential solutions for protecting digital bodies, or 3) examine the relationship between the digital bodies and users of social VR citizens. We notice a severe lack of research and attention on the addressed topic and identify several research gaps that need to be filled. While some legal and ethical concerns about the potential identity issues of the digital bodies have been raised, and despite some progress in specific areas such as user authentication has been made, little research has proposed practical solutions. Finally, we suggest potential future research directions for digital body protection and include relevant research that might provide insights. We hope this work could provide a good overview of the existing discussion, potential solutions, and future directions for researchers with similar concerns. We also wish to draw attention to identity and privacy issues in social VR and call for interdisciplinary collaboration.

KEYWORDS

virtual reality, avatar, social VR, identity theft, privacy, systemactic review

1 Introduction

The past 2 years have witnessed a remarkable trend towards the digitalization and online presence of human activities and social interactions: COVID-19 pandemic has imposed severe restrictions on people's travel and physical contact, forcing many social activities, such as education, work, and healthcare, to be conducted remotely online (Wong et al., 2021). The unprecedented growing usage of social media and video conferencing tools, such as *Facebook*, *WhatsApp*, *Zoom*, and *Microsoft Teams* (Bary, 2020; Schultz and Parikh, 2020), are incredibly expanding how and where people can socialize, breaking the physical and distance barriers of social interaction, and transforming the norm of communications. Meanwhile, with the massive investments in the "metaverse" by tech giants such as *Meta*, *Nvidia* and *Microsoft* (Kim, 2021), the corresponding advances of HCI (human-computer interaction) technologies, and the popularity of affordable VR devices, leads virtual reality to becoming increasingly accessible and affordable to the public. In line with this trend, there are good reasons to believe that social virtual reality has great potential to lead the next revolution in the digitalization of social activities.

Social virtual reality (social VR or SVR) is a kind of multiuser VR application or platform that allows users to interact and communicate with each other within a virtual environment (McVeigh-Schultz et al., 2018; McVeigh-Schultz et al., 2019). define social VR as "*a growing set of multiuser applications that enable people to interact with one another in virtual space through VR head-mounted displays*" The concept of social VR is a successor of collaborative virtual environments (CVE), a term used in the 1990s that is defined as:

> A broad class of desktop and immersive VR systems that support collaboration in a common virtual environment where each participant is represented by an avatar (Liu and Steed, 2021).

While the definitions above might have covered most of the multiuser VR applications, social VR also emphasizes cultivating social relationships, experiencing different virtual activities, and exploring self-representation (Maloney et al., 2021). Social VR has enormous potential for diverse applications, including but not limited to communication (Roth et al., 2017), gaming and entertainment (Roth et al., 2018; Wang, 2020), education (Le et al., 2015; Ripka et al., 2020; Foerster et al., 2021), collaborative work (Lohle and Terrell, 2014; Heath, 2021), and healthcare (Li et al., 2020; Shao and Lee, 2020). However, there are still many open questions including potential impacts of technological determinants on the experiences (Latoschik et al., 2019) or the overall design goals of such SVRs (Roth et al., 2015).

Meanwhile, social VR has been shifting from single-purpose virtual experiences to an alternative realm for human socio-cultural interaction (Dionisio et al., 2013). O'Brolcháin et al. (2016) have defined VRSN (Virtual Reality Social Network) as "*the convergence of virtual realities and social networks*" and hypothesized a scenario in which a significant portion of the world's population are members of a social network, which either are immersive or at least offer immersive experiences. They also emphasized that in such a scenario, "*users enter VRSN as themselves, rather than playing a character as in a game.*"

The graphical representation of a user in the virtual world is known as an avatar, which is usually required for users to be engaged in social activities, driven by the user's movements (Bailenson et al., 2004) and creating virtual embodiment (Roth and Latoschik, 2020) for the user. In general, there are three types of self-representation alternatives in social VR (Figure 1). The first type of self-representation allows users to select from a very diverse set (Liu and Steed, 2021) or upload avatars created by users themselves. Social VR application *VRChat*[1] is a typical example, where users can not only use cartoonish or anime characters but also appearances of elves, monsters, and robots as their avatars. The second type of self-representation is a customizable avatar that allows users to determine the color, shape, and style of different parts of the body (e.g., face, hair, eye, skin) and create their unique representations, which indicate their gender, race, aesthetics, hobbies, and so on. Customizable avatars are widely adopted by social VR applications, such as *RecRoom*[2] and *AltspaceVR*[3].

Recently, there has been a shift in users' self-representations toward personalized (photo)realistic avatars that accurately capture the likeness of the them (O'Brolcháin et al., 2016). That is the third type of self-representation. For instance, in *Spatial. io*[4]—a virtual workspace focusing on meetings and media sharing, users can upload a photo of themselves to create realistic avatars that capture their appearance. To a large extent, such an avatar works as an identifier of the user, and this identity is consistent with who they are in real life. This type of avatars are usually referred to as personalized avatars (Chen et al., 2014; Ichim et al., 2015; Waltemate et al., 2018) or personalized realistic avatars (Fribourg et al., 2020). A personalized avatar reproduces the user's appearance as realistic and recognizable as possible, serves as the proxy of their physical body in the virtual world, and uniquely determines the user (even though a user can have multiple such avatars). Thus, it can be considered a user's digital body (Slater, 2008; Neustaedter and Fedorovskaya, 2009; Triberti et al., 2017; Ferrari, 2021). Studies suggest that using a personalized avatar can support creative idea generation (Marinussen and de Rooij, 2019), enhance users' engagement,

[1] https://hello.vrchat.com/.

[2] https://recroom.com/.

[3] https://altvr.com/.

[4] https://spatial.io/.

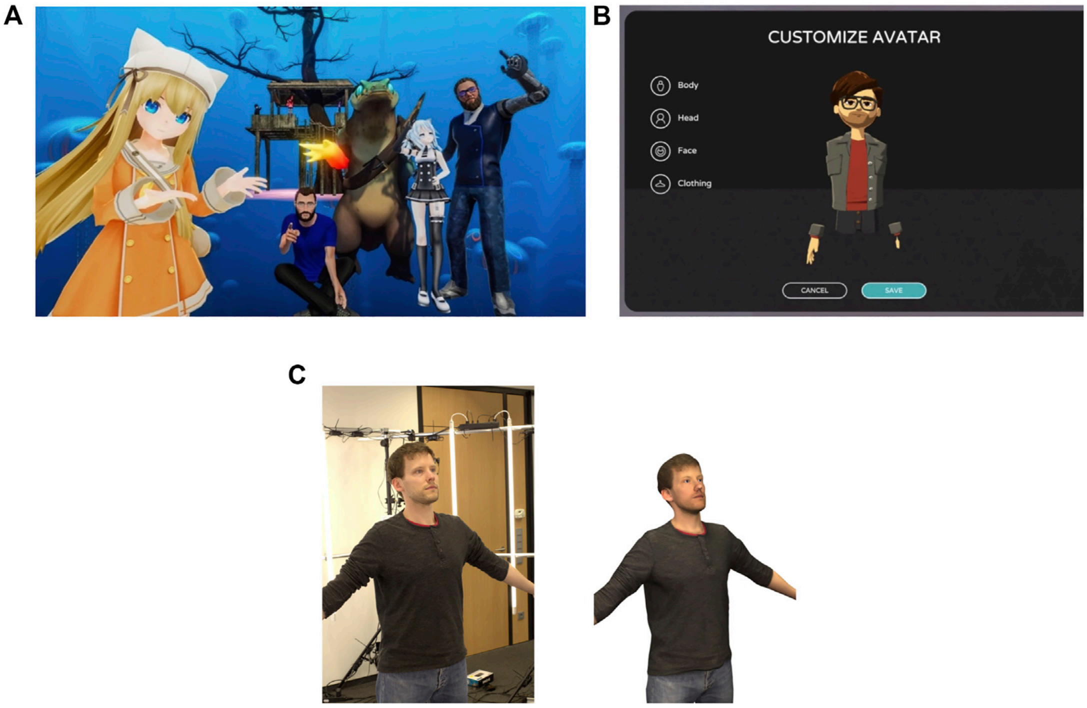

FIGURE 1
Examples of three types of self-representations in social VR. **(A)** Self-uploaded avatar. Example: various of self-presentations uploaded by users in *VRChat*[5]. **(B)** Customizable avatar. Example: the avatar customization interface in *AltSpaceVR*[6]. **(C)** Personalized (photo)realistic avatar. Example: generating a photorealistic avatar from a body-scanner. Panel reproduced from (Achenbach et al., 2017).

and make them feel more connected (Lucas et al., 2016). Social interactions with high-fidelity digital bodies in virtual reality will create a more substantial acceptance of virtual body ownership (VBO) (Latoschik et al., 2017). Waltemate et al. (2018) also point out that personalized photo-realistic avatars resembling the users will significantly increase presence [the sensation of being in the virtual world (Schuemie et al., 2001)] and dominance [the perceived state of own social dominance or submission (Waltemate et al., 2018)].

However, unlike physical bodies, the digital bodies can be altered or changed at the users' will, which allow them to disguise their identity; identity theft will easily occur as cybercriminals "steal" or generate avatars of others and pretend to be them (Lake, 2020). In other words, the "authenticity" (whether one's identity online or in the virtual world is who one claims to be and can be identified with a unique identity in reality) of a social VR citizen cannot be guaranteed. Social VR applications where users enter as themselves and use their personalized avatars (e.g., *Spatial. io*) are not without limitations. For example, identity verification is still lacking (in *Spatial. io,* so long as a photo is provided, users can generate and use a personalized avatar from that photo regardless of whom it belongs to), therefore the authenticity of the identity still cannot be guaranteed. It has been widely reported that identity thefts and phishing attacks exist in video conferencing using "deepfake" and similar technologies (Cole, 2020; McElroy, 2021). It will not be surprising that similar cybercrimes targeting avatars will occur in social VR.[5,6]

With the aforementioned future trend of social VR, there will be significant challenges and necessities in protecting users' digital bodies, building the authenticity of social VR citizens, and protecting them from identity misappropriation. Such efforts are essential in enhancing the trust among social VR citizens and increasing people's acceptance of social VR, as the trustworthiness of avatars has a significant and favorable influence on net-based social activities and collaboration (Bente et al., 2014; Chae et al., 2016; Pan and Steed, 2016; Pan and Steed, 2017). In addition, providing a trustworthy, intelligent, and comfortable virtual environment is the prerequisite for building human-centered social VR that everyone can trust and enjoy.

The presented systematic review addresses potential threats to users' identity and privacy in social VR, with a specific focus on the protection of their digital bodies. While this is a relatively new field that receives insufficient scholarly

[5] Image source: https://hello.vrchat.com/.

[6] Image source: https://docs.microsoft.com/en-us/windows/mixed-reality/altspace-vr/explore/beginners-guide.

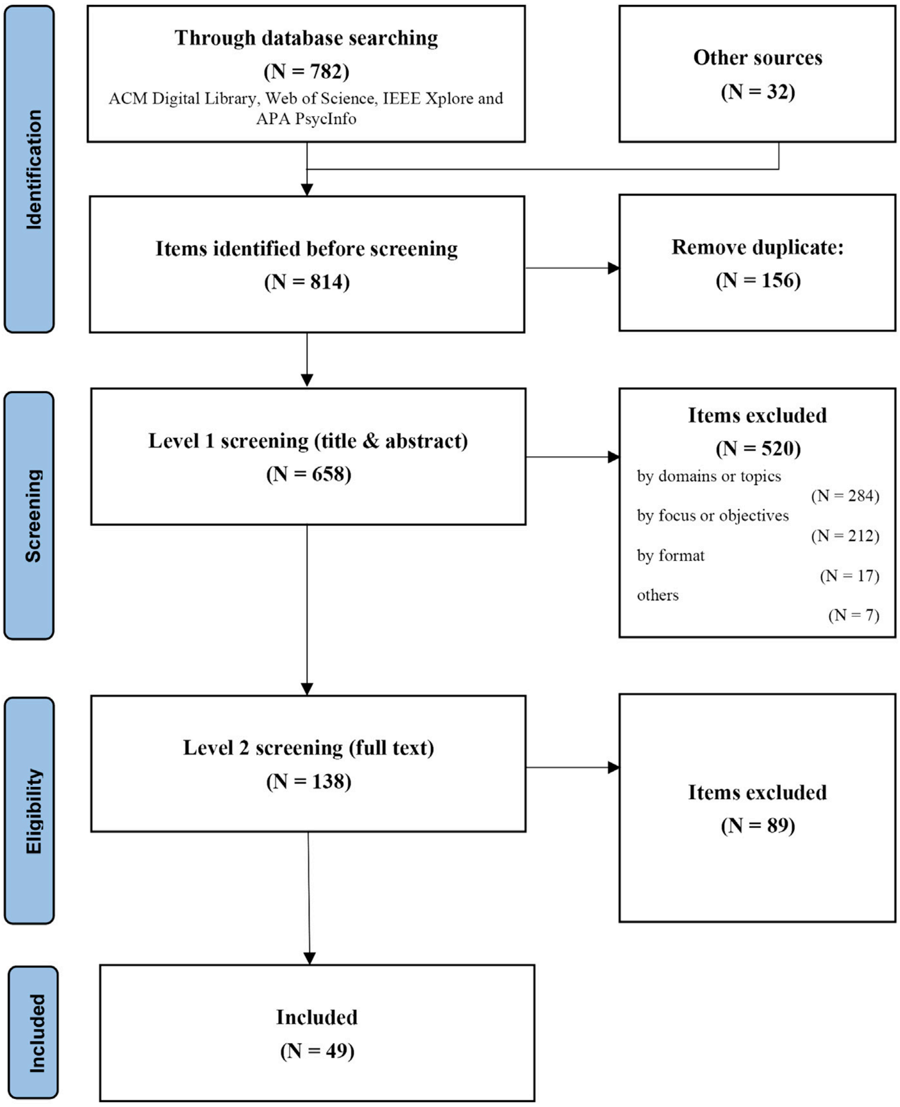
Identification
Through database searching
(N = 782)
ACM Digital Library, Web of Science, IEEE Xplore and APA PsycInfo
Other sources
(N = 32)
Items identified before screening
(N = 814)
Remove duplicate:
(N = 156)
Screening
Level 1 screening (title & abstract)
(N = 658)
Items excluded
(N = 520)
by domains or topics (N = 284)
by focus or objectives (N = 212)
by format (N = 17)
others (N = 7)
Eligibility
Level 2 screening (full text)
(N = 138)
Items excluded
(N = 89)
Included
Included
(N = 49)

FIGURE 2
Flow diagram of the selection process, numbers of included and excluded items in each step.

attention, we aim to collect relevant research, identify research gaps, and call for attention and interdisciplinary collaboration from privacy-preserving computing technologies, artificial intelligence (AI), law, ethics, psychology, and human-computer interaction (HCI). As an outcome of this study, we aim to answer the following research questions or give insight towards potential answers backed-up by the current related work:

(RQ1) What are the existing and potential threats to privacy and identity when using digital bodies in social VR?
(RQ2) How can we protect digital bodies and users from those threats?
(RQ3) What is the current stage of digital bodies usage in social VR, in terms of usability and user acceptance?
(RQ4) How to indicate the authenticity of social VR citizens' identity?
(RQ5) How do we evaluate the trust among social VR citizens?

2 Methods

We performed a structured systematic review following the guideline and procedures from the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) statement (Page et al., 2021). In the following sections, we describe our

TABLE 1 Search term queries used in all databases

Combination 1

1st keyword	And	2nd keyword	
avatar	OR	identity	OR
"digital body"		privacy	OR
		authentication	OR
		authenticity	OR
		protect*	

Combination 2

1st Keyword	AND	2nd Keyword
VR	OR	"identity theft"
"virtual reality"		

eligibility criteria, information sources, search strategy, data collection process, as well as the selection process. The exclusion criteria, the number of items after selection in each step of the selection process, and the number of items included in the review, are presented in a flowchart (Figure 2) adapted from (Page et al., 2021).

2.1 Eligibility criteria

We aimed to identify papers that either describe or raise concerns about the addressed threats to identity and privacy, provide technologies and potential solutions for protecting digital bodies in social VR, or analyze the relationship between the digital bodies and identities of social VR users.

Regarding privacy and identity issues in social VR, we only focus on those stemming from the use of digital bodies. Therefore, other privacy issues [many of which have been discussed by O'Brolcháin et al. (2016)] such as the misuse of data, and the prevalence of recording devices, will not be considered.

Regarding technologies and potential solutions for protecting digital bodies in social VR, we search for grounded evidence, technical solutions, or design guidelines in the area of virtual reality. While some articles provide mere ideas or inspiration for future research, we considered them not eligible and more suitable to be referred to in the discussion. Similarly, technologies in other areas that could be potentially applied to digital bodies and social VR are considered out of scope and only referred to in the discussion.

Due to the lack of research on the addressed topic and the desire for interdisciplinary knowledge, we did not limit our search to human-computer interaction, but have broadened it to include psychology, law, ethics and more. We also do not restrict the research methods and forms of study, so long as they are peer-reviewed academic journal articles, conference papers, book sections, reports, or doctoral theses strongly related to our research topic.

2.2 Information sources and search strategy

The databases that have been scanned are ACM Digital Library, Web of Science, IEEE Xplore and APA PsycInfo. For each source, we always used the search term queries shown in Table 1. The search keys must be included in the title, abstract or author keywords of the article (for Web of Science, we search with "topic," which includes the three previously mentioned and "keywords plus"). We searched articles published within the period from January 2000 to January 2022. Although concepts such as "virtual reality" and threats in the cyberspace have been around since long before 2000, we believe that the vision back then was out of touch with current development and lacked reference value. We constructed the search term queries in two sets of combinations: 1) in the first set of combinations, we used ("avatar" OR "digital body") as the first keyword AND ("identity" OR "privacy" OR "authentication" OR "authenticity" OR "protect") as the second keyword; 2) additionally, we use the second set of combinations ("VR" OR "virtual reality") as the first keyword AND "identity theft" as the second keyword. On databases that allow us to specify the language of paper while searching, we select "English." Addition articles identified *via* other sources and cited reference searching are also added to the collection.

2.3 Data collection

Data was collected and managed with *Zotero*[7] and *Zotero Connector* Chrome extension. Titles, authors, abstracts and sources of all items were collected on 13 January 2022, either by automatic grabbing with *Zotero* Connector or by importing RIS files generated from the databases. Full texts of items were either collected by automatic grabbing with *Zotero* Connector (last access 13 January 2022) or by manually downloading during the selection process. All data access was provided by the library of the authors' host institution.

2.4 Selection process

The selection process is illustrated by a flow diagram in Figure 2. Firstly, duplicated items were removed. Secondly, we performed level 1 screening, primarily by their title and abstract, and a few by browsing the full text. In this step, we excluded papers by domains or topics (studies that are not related to virtual

[7] https://www.zotero.org/.

TABLE 2 Overview of selected papers.

References	Short summary
Gorini et al. (2008)	Discuss the relevant and risks of using 3D virtual worlds for online health service
Deng and Ruan, (2009)	Discuss privacy issues from *Second Life* Library and provide potential suggestions
Gavrilova and Yampolskiy, (2010)	Provide a review on state of the art in avatar authentication
Graber and Graber, (2010)	Discuss whether avatars are protection by the rights similar to those of biological bodies
Boukhris et al. (2011)	present a biometric identification system for avatar faces
Mohamed and Yampolskiy, (2012)	present two algorithms for avatar face recognition
Segovia and Bailenson, (2012)	Describe a user study on users' response to ostracizers whose avatars do not look like them
Vanacker and Heider, (2012)	Discuss ethical-relevant avatar harms in virtual world
Yampolskiy et al. (2012)	Introduce a new subfield of security research: *Artimetrics*
Yampolskiy et al. (2012)	Present a set of algorithms for avatar face recognition
Bader and Ben Amara, (2014a)	Present a watermarking algorithm of avatar's face
Bader and Ben Amara, (2014b)	Present a 3D avatar dataset for research purpose
Feng et al. (2014)	Present methods to generate 3D characters and subjects' gestures; present a user study that show that 3D characters with gesture of original subjects are more recognizable
Kanamgotov et al. (2014)	Discuss different attributes of identity users use to build their avatar and how the level of avatar customization corresponds to the degree of user-avatar association
Carruth and Hill, (2015)	Examine and discuss the assumption that when people interact online *via* avatar, they encounter each other
Ichim et al. (2015)	Present a pipeline for creating fully rigged, personalized 3D facial avatars from hand-held video
Bader and Ben Amara, (2016)	Present an identity management approach for securing access to virtual worlds
Achenbach et al. (2017)	Present a pipeline for generating fully rigged, personalized 3D avatars
Bader and Ben Amara, (2017)	Present a virtual world platform for the implementation of a biometrical access control mechanisms
Conrad et al. (2017)	Discuss the how to use virtual worlds for situated learning and corresponding challenges
Feng et al. (2017)	Present a system for generating 3D personalized avatars
Hu et al. (2017)	Present an automatic framework for digitalizing 3D heads with hair from single image
Alldieck et al. (2018a)	Present a method for generating 3D human avatar from monocular video
Alldieck et al. (2018b)	Present a method for generating 3D human avatar from monocular video in which a person is moving
Falchuk et al. (2018)	Discuss technology that will help VR participants increase the degree of privacy while immersed in social VR.

(Continued in next column)

TABLE 2 (*Continued*) Overview of selected papers.

References	Short summary
Lemley and Volokh, (2018)	Discuss upcoming legal challenges in VR and AR.
Nagano et al. (2018)	Present a method for generating dynamic facial avatars from a single image
Alldieck et al. (2019a)	Present a learning-based model to infer the personalized 3D shape of people from a few frames of a monocular video in which the person is moving
Alldieck et al. (2019b)	Present a method to infer detailed full human body shape from only a single photograph
Lazova et al. (2019)	Present a method to generate 3D avatar of a person from a single image
Pfeuffer et al. (2019)	Investigate body motion as behavioral biometrics for virtual reality
Tummon et al. (2019)	Describe a user study with VR airport control to investigate face matching in complex environments
Zheng et al. (2019)	Present an image-guided CNN for 3D human reconstruction from a single image
Beacco et al. (2020)	Present an automatic animatable 3D character reconstruction method from frontal and lateral pictures
Huang et al. (2020)	Present an end-to-end framework for reconstruction of 3D clothed human from a monocular image
John et al. (2020)	Implement and evaluate a hardware-based eye tracking configuration to secure the iris biometric from unauthorized identification
Lake, (2020)	Discuss identity risks in VR and proposed legal solutions
Miller et al. (2020a)	Present method to identify users under typical VR viewing circumstances with no specially designed identifying task
Miller et al. (2020b)	Present analysis of behavioral-based authentication within and across multiple VR system
Tummon et al. (2020)	Describe a user study that investigate the influence of body language on facial identity matching with a virtual airport environment
Wenninger et al. (2020)	Present an automated 3D-reconstruction method for generating high-quality virtual humans from monocular video
Falk et al. (2021)	Present a novel de-anonymization attack that identifies users by their avatars
Freeman and Maloney, (2021)	Describe a qualitative user study to investigate how users construct and experience their self and interact with others in social VR
Fysh et al. (2021)	Present a photorealistic avatar generation method for the psychological research community and demonstrated a series of studies exploring the identification of the avatar faces
Jones et al. (2021)	Provide a literature review on virtual reality authentication
Liebers et al. (2021)	Investigate the identification of users in task-driven scenarios in VR.
Miller et al. (2021)	Present an approach on using behavioral biometrics to perform cross-system authentication of user in VR.
Pakanen et al. (2022)	Describe two studies investigating how physically remote telexistence users wish to see other users visualized as virtual avatar in AR and VR.
Schell et al. (2022)	Present comparisons of different data representations and machine learning architectures for user authentication using movement data.

reality, avatar, or have different interpretations of such concepts), by focus or objectives (study in related domains or topics but lack relevance to our research questions and objectives), by formats (items with only abstract, poster, demo) and by other reasons (retracted items, items not written in English, items with no abstract and full text available).

Thirdly, we examined the remained items for eligibility by browsing the full text or thoroughly and intensively reading if necessary. Those with full text not accessible were excluded; items that are irrelevant to the topic or have a different focus will be excluded; items lacking groundwork and evidence to support their conclusions will be excluded.

Finally, items that remained from the previous process were included and analyzed in this systematic review.

3 Results

As illustrated in Figure 2, we have collected 782 items from database searching and 32 items from additional sources. 658 different works were identified after removing duplicates.

In the level 1 screening, 284 items were rejected by domain or topic, including works that have different definitions of our search terms (for example, “avatar” can be its original concept within Hinduism, the film *Avatar* by James Cameron, or a profile image in early Internet parlance), works that are not related to social virtual reality (e.g., a significant amount of works study virtual characters in MMORPGs) or avatar (e.g., some works use “avatar” to describe the concept that we usually define as “agent,” a virtual character controlled by computer programs). 212 items were rejected by research focus due to the lack of relevance to our research questions and objectives (e.g., many works discussing the “identity” of avatars focus on users’ self-perception of gender and race). 17 items were rejected by format, and six items were rejected for other reasons. Some items have met multiple criteria to be rejected, but they are counted only once with the primary rejection reason. The screening yields 138 items after removal.

In the next level of full-text screening, we applied the eligibility criteria and further excluded 89 items. Five items were eligible according to our criteria, but were already included in a previous review by Jones et al. (2021) which was also one of the selected papers. To avoid repetition, we did not include these items. Finally, 49 papers are included in the results and analysis. An overview of the selected 49 papers can be found in Table 2.

3.1 Preliminary analysis

The selected papers have covered a wide range of topics, research methods and study characteristics. We first provide preliminary observations on selected works according to the published year, related domain, and the social VR platform used, constituting Section 3.1. Then, we present study characteristics and syntheses of results in five categories, namely digital bodies generation (Section 3.2), threats to privacy and identity (Section 3.3), user-avatar relationships (Section 3.4), protections (Section 3.5), and avatar-identity related user study (Section 3.6). The distribution of the selected papers across the five categories and the subtopics under each, as well as the relationship of each category to the Research questions, is shown in Figure 3.

3.1.1 Published year

In Figure 4, we illustrate the number of publications of collected papers, papers after level 1 screening, and papers included in the final results, according to year. Prior to 2009, few relevant studies had emerged. Only six papers show some degree of relevance and passed the level 1 screening, while only one paper fell into our inclusion until 2008. The number of collected papers has a substantial increase in 2009, followed by a gradual upward trend until 2015 except for a slight decline in 2013, which indicates an increase in research interests in relevant topics, such as virtual world, social VR, and avatars. 14 papers published during this period are included in the final results. However, the year 2016 has witnessed a dramatic decrease of interest, only 29 papers from this year were collected, and the number of selected papers shows a similar trend. Since then, attention to this field has steadily increased until it peaked last year when a total of 21 papers passed the level 1 screening. Combined with the observation in Section 3.1.3, such an interesting change in trend may stem from the rise and fall of *Second Life*[8] from Linden Lab, a virtual community that has once received considerable attention, and the popularity of the “metaverse” accompanied by advancements in VR technology in recent years.

3.1.2 Research domains

Due to the relatively liberal eligibility criteria, the included articles cover diverse research domains (Figure 5) range from law (N = 2), medicine (N = 2), education (N = 2), ethics (N = 2), psychology (N = 8), human-computer interaction (N = 15) and computer science (N = 33). On the one hand, the lack of research on the addressed research topics has forced us to broaden the scope of searching; on the other hand, it also reflects the fact that identity and privacy issues arising from the use of digital bodies have received a certain amount of attention from outside of the technical realm.

3.1.3 Social VR platform

We have also counted what kinds of social VR platforms (including early desktop virtual worlds such as *Second Life*) are being used in research to conduct studies, collect data,

[8] https://secondlife.com/.

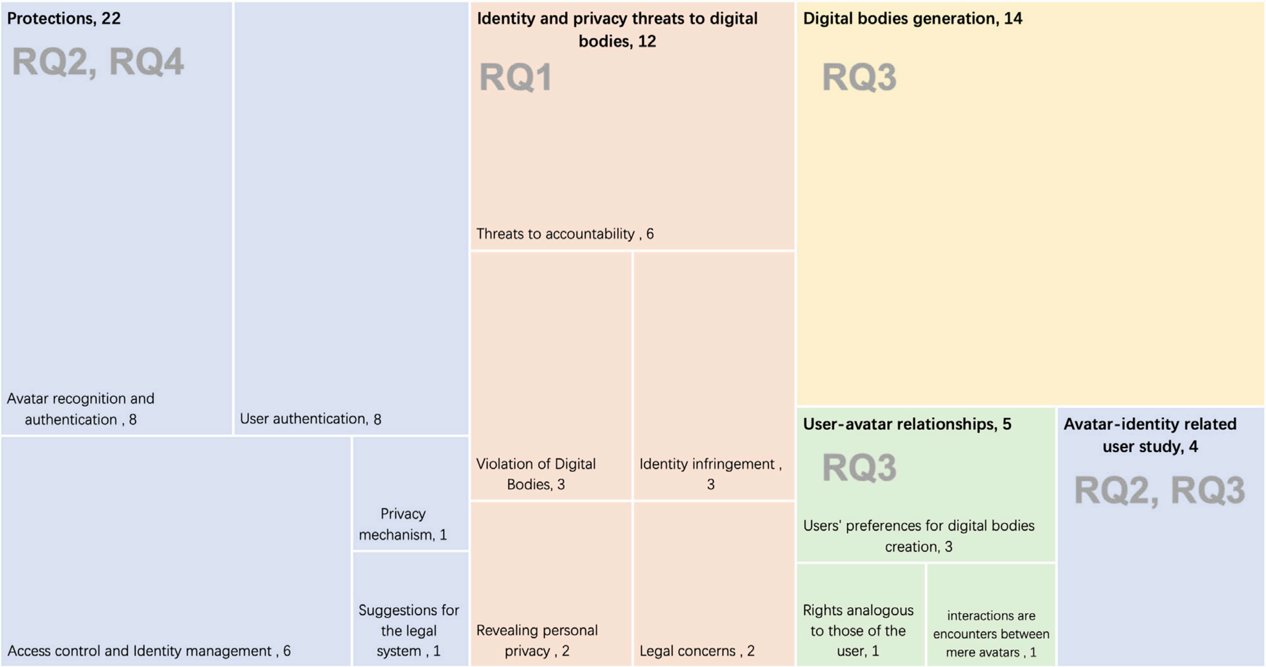
Protections, 22
RQ2, RQ4
Avatar recognition and authentication , 8
User authentication, 8
Access control and Identity management , 6
Privacy mechanism, 1
Suggestions for the legal system , 1
Identity and privacy threats to digital bodies, 12
RQ1
Threats to accountability , 6
Violation of Digital Bodies, 3
Identity infringement , 3
Revealing personal privacy , 2
Legal concerns , 2
Digital bodies generation, 14
RQ3
User-avatar relationships, 5
RQ3
Users' preferences for digital bodies creation, 3
Rights analogous to those of the user, 1
interactions are encounters between mere avatars , 1
Avatar-identity related user study, 4
RQ2, RQ3

FIGURE 3
Distribution of selected papers across categories and subtopics, and their relationship to the research questions. As some papers appear several times, the numbers do not add up to the total number of papers, nor number in each category.

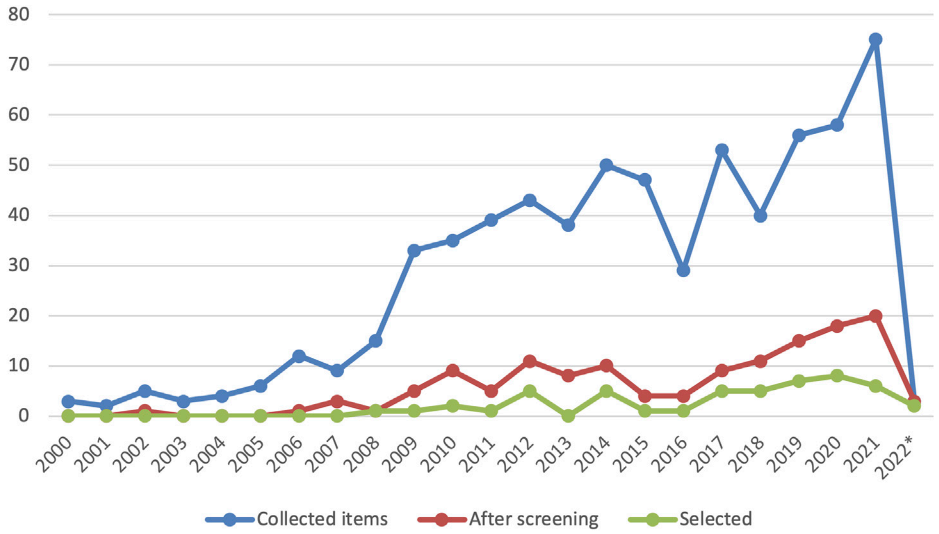

FIGURE 4
Division of collected and selected items according to published year. *Database searching was conducted in January 2022, thus the Year 2022 only yields two selected item.

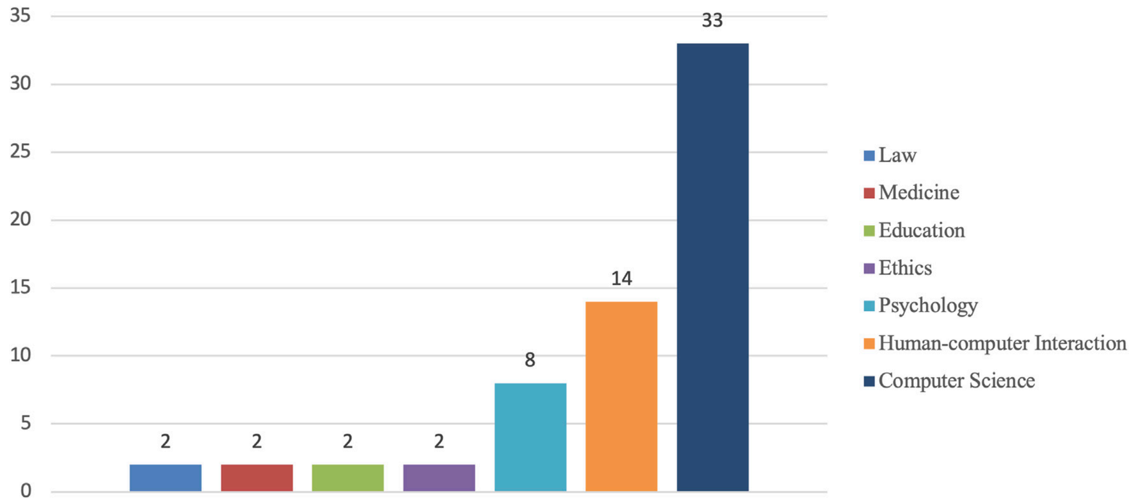

FIGURE 5
The research domains covered by the selected articles and the corresponding number of articles. Some articles cover more than one domain.

recruit participants, or being analyzed. By 2017, *Second Life* was still dominant, and 11 papers conducted studies or collected data on *Second Life*. However, since 2018 *Second Life* has disappeared. Other social VR platforms Include *AltspaceVR* (N = 1), *Entropia Universe* (N = 2), *Reaction Grid* (N = 1), *VRchat* (N = 1), and self-implemented virtual worlds (N = 3).

3.2 Digital bodies generation

While it is true that social VR users can choose between a variety of representations to suit different purpose, a unique personalized realistic avatar that captures the likeness of them is substantial to increasing body ownership, presence, and dominance (Waltemate et al., 2018), and preferred for trust-building (Bente et al., 2014).

We looked for recent technical advancements that enable the automatic creation of personalized realistic avatars without the need for complex manual efforts. The generated avatars should not be simply a 3D reconstruction of a human body but should also be animatable and suitable for being used in social VR applications. 14 papers (Ichim et al., 2015; Achenbach et al., 2017; Feng et al., 2017; Hu et al., 2017; Alldieck et al., 2018a, 2018b, 2019a, 2019b; Nagano et al., 2018; Lazova et al., 2019; Zheng et al., 2019; Beacco et al., 2020; Huang et al., 2020; Wenninger et al., 2020) that presented novel methods or end-to-end pipelines are identified. As shown in Figure 6, they can be further classified according to data acquisition, which either use single images (N = 6), multi-view images (N = 1), monocular videos (N = 5), or photogrammetric scanners (N = 2). Three papers only focus on generating the avatar head, while the remaining 11 focus on full-body avatars. All the avatars or characters generated from these methods are animatable. Except for the three methods that generate facial avatars, all methods create rigged avatars, and two methods also enable facial blendshapes. It is also worth mentioning that methods in seven papers are based on the SMPL (Skinned Multi-Person Linear) Model (Loper et al., 2015). A summary of these papers includes their novel features, data acquisition, avatar types, and animation capability listed in Table 3.

3.3 Identity and privacy threats to digital bodies

Despite that the concerns for identity infringement and privacy issues that digital bodies may bring about have been highlighted frequently in literature, they are usually mentioned merely as background information and are rarely described and analyzed comprehensively. The following sub-sections are the syntheses from 12 papers on existing and potential identity and privacy issues that stem from or threaten the use of digital bodies in social VR.

3.3.1 Violation of digital bodies

As the representations of users and the medium of interaction between users and the virtual worlds, avatars as the direct digital proxies of the users are inevitably the target of violence and sexual harassment. Lemley and Volokh in their paper (2018) described a type of assault that are nowadays

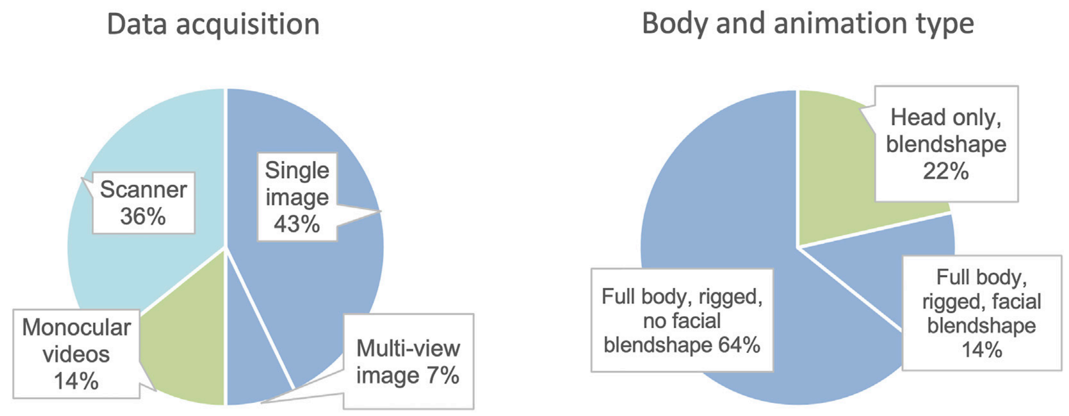

FIGURE 6
Different data acquisition methods and body and animation types of digital body generation pipelines, illustrated as bar charts.

TABLE 3 This table summarizes the papers that presented methods or pipelines to automatically generate personalized (photo)realistic avatar from either images, videos or scanners.

References	Features	Data acquisition	Type	Animation
Ichim et al. (2015)	A complete pipeline for creating fully rigged, personalized 3D facial avatars that recovers facial expression dynamics from hand-held video	Monocular video	head	facial blendshapes
Achenbach et al. (2017)	A complete pipeline for generating high-quality fully-rigged avatar from multi-view stereo reconstruction	Photogrammetric scanner	full-body	fully-rigged facial blendshapes
Feng et al. (2017)	A system that can generate a photorealistic, fully-rigged 3-D character in less than 20 min	Photogrammetric scanner	full-body	rigged; hand rigs and facial blendshapes added manually
Hu et al. (2017)	A fully automatic framework that digitizes a complete 3D head with hair with blendshapes and joint-based rigs from a single unconstrained image	Single image	head	facial blendshapes joint-based rigs
Alldieck et al. (2018a)	A method for high detail-preserving human avatar creation from monocular video	Monocular video	full-body	fully-rigged (SMPL)
Alldieck et al. (2018b)	A method to obtain accurate 3D body models and texture of arbitrary people from monocular video in which a person is moving	Monocular video	full-body	fully-rigged (SMPL)
Nagano et al. (2018)	An end-to-end deep learning approach for facial expression texture synthesis	Single image	head	facial blendshapes
Alldieck et al. (2019a)	A method to infer the personalized 3D shape of people from a few frames (1–8) of a monocular video in which the person is moving with a reconstruction accuracy of 4–5 mm	Monocular video	full-body	fully-rigged (SMPL)
Alldieck et al. (2019b)	A method to infer detailed full human body shape from only a single photograph	Single image	full-body	fully-rigged (SMPL)
Lazova et al. (2019)	A method to generate 3 days avatar from a single image, predict complete segmentation, texture and displacement map from partial texture and segmentation from input view	Single image	full-body	fully-rigged (SMPL)
Zheng et al. (2019)	A deep-learning based framework to reconstruct a 3D human model from a single image	Single image	full-body	fully-rigged (SMPL)
Beacco et al. (2020)	An animatable 3D character reconstruction method from frontal and lateral RGB pictures of the person to reconstruct	Frontal and lateral images	full-body	fully-rigged (SMPL)
Huang et al. (2020)	A novel end-to-end framework for accurate reconstruction of animation-ready 3D clothed humans from a monocular image	Single image	full-body	fully-rigged
Wenninger et al. (2020)	A method to generate high-quality fully-rigged avatar from monocular smartphone video clips	Monocular video	full-body	fully-rigged facial blendshapes

somewhat common: "virtual groping"—the offenders maliciously touching and rubbing body parts of the victim's avatars. Although the victims are not "physically" being touched, they could still be seriously disturbed as if it happened in the real world. Falchuk et al. (2018) also discussed such criminal harassment to avatars targeted at female players, and reported that in *Second Life*, this kind of harassment has become so prevalent that developers need to publish a "primer" on how to avoid harm in such situations. Vanacker and Heider (2012) discussed the ethical issues raised from the harm done to avatars, including a case study of "The upskirt gallery," where a Second Life user took sneak peek photos and exhibited several "upskirt pictures" of other avatars he encountered in the virtual world.

In addition, violation of avatars does not always appear during interactions. Violation can also be the offensive modification of the victim's avatar (Lemley and Volokh, 2018), which includes using certain techniques to make the avatar appear naked, exaggerating the avatar's appearance features to make it a grotesque caricature, to mention a few.

3.3.2 Identity infringement

Identity theft is one of the most common concerns stemming from the use of avatars, especially personalized avatars. Falchuk et al. (2018) have described a kind of "social engineering hacking" in social VR. The offenders could impersonate a player's friend to obtain information and profits, which might have harmed the privacy of both victims.

Lemley and Volokh (2018) discussed, from a legal perspective (based on United States law), whether users are protected when others deliberately use their names and likenesses to create an avatar. They argued that such impersonation may unfortunately be legally permitted, "*especially when it is clear that this is just a pseudonym, can be a useful means of parody, commentary, and entertainment.*" However, they also pointed out that such conduct should perhaps not be allowed without the consent of the impersonated person, for the fact that VR has a much higher visceral quality, and such impersonation may damage others' perception of the impersonated person. Furthermore, they argue that ordinary people are more affected by avatar impersonation than celebrities. Therefore, the right of publicity needs to extend to a broader scope for VR and AR avatars.

Lake (2020) discussed identity infringement more specifically, noting that due to the highly interactive nature of social VR, "*this type of infringement will be far more intimate than the theft of a still image or a static fake Facebook profile.*" Lake further notes that as interactions in social VRs occur in real-time, users lack the means to authenticate offenders' identities in a timely manner; meanwhile, the fluent e-commerce enabled by cryptocurrencies prevalent in social VR often helps offenders instantaneously get money from their victims. Interestingly, when it comes to the legal protection that a user's avatar will receive (based on United States law), Lake believes that there are two scenarios: 1) trademark or copyright law applies to avatars that are unlike the users, and 2) the right of privacy and the right of publicity, should apply to personalized avatars that reflect the identity of users.

3.3.3 Threats to accountability

Anonymity and identity disguise also hinder the track of accountability of avatars in social VR. In their discussion of multi-user virtual worlds in eHealth applications, Gorini et al. (2008) pointed out that anonymity might negatively impact patients during e-therapy, as anyone can interact with the patients and there is no guarantee of who the patients are interacting with. Several papers (Mohamed and Yampolskiy, 2012; Yampolskiy et al., 2012) have revealed that terrorist groups were using virtual communities, such as *Second Life*, for communication and recruitment. Establishing the identity of individuals in such circumstances is challenging. Bader and Ben Amara. (2016) pointed out that identity masking in the virtual worlds allows users to create multiple avatars and exploit the virtual environments for crimes such as money laundering, economic fraud, identity theft, and cyber-terrorism.

In investigating virtual worlds as situated learning approaches, Conrad et al. (2017) raised their concerns about the impact of "fake" accounts. By comparing to "profiling cloning" and fake accounts on social networking sites such as *Facebook*, they suggested that for activities such as education, the necessity for anonymity is no more justified and will make it difficult to trace back to the person that can be accountable when deliberate disturbances and negative intervenes occur.

3.3.4 Revealing personal privacy

While personal privacy leakage is already a prevalent risk in the virtual world, the use of digital bodies may further exacerbate it. Deng and Ruan (2009) pointed out that users' personal information such as name and address might be required in registration for creating an avatar, as many social VR's policies oppose anonymous use. Besides, as the avatar is *"an important extension of the user's own privacy and identity with implication for intimacy and dignity,"* in-world privacy concerns are also being raised as users' daily activities will often be mirrored in their avatars (Deng and Ruan, 2009). Falk et al. (2021) have proposed such an example: a de-anonymization attack that by just secretly recording the movement of an avatar and mapping the correlations with the movement of the user in real life using a bespoke agglomerative clustering algorithm, the identity of the user might be revealed with an accuracy of 89.60%.

3.3.5 Legal concerns

Lemley and Volokh (2018) concluded that existing law could not provide sound solutions against threats posed by VR and AR. They demonstrated the legal dilemma and identified potential questions through several case studies, such as how the law is likely to treat VR "street crimes" and the difficulties in criminal law enforcement and involvement. Thus, they suggested thinking

TABLE 4 We summarized typical user-avatar relationships that were observed or defined in literatures. These help us to understand how user perceive their avatar and how to develop protection mechanism for their digital body.

Types of user-avatar relationships	Literatures describing such relationships
avatar as an extension/part of self	Graber and Graber (2010), Freeman et al. (2020), Freeman and Maloney (2021))
avatar as an alter-ego differs from offline self	Kanamgotov et al. (2014), Freeman and Maloney (2021)
Avatar as a more real version of self	Freeman et al. (2020), Freeman and Maloney (2021)
Avatar as medium between user and virtual world	Kanamgotov et al. (2014)
Avatar as a tool	Kanamgotov et al. (2014)
Users and avatars as distinct entities	Carruth and Hill (2015)

ahead of such issues, and the legal doctrines and rules need to be adjusted to address the new situation. Similarly, Lake (2020) revealed the inconsistencies and procedural barriers brought about by dated Internet laws with a specific focus on identity misappropriation in social VR. According to them, these barriers include 1) Internet personal jurisdiction, 2) strong judicial preference toward protecting the anonymity of anonymous online users, and 3) sweeping immunity for Internet Service Providers (ISP), leaving plaintiffs without a defendant to sue.

3.4 User-avatar relationships

The relationships between users and avatars are central to the understanding of identity and privacy issues and are a prerequisite for ethical and legal discussions. Only when the nature of user-avatar relationship is clarified, can the violations to avatars be characterized and corresponding protection mechanisms be developed. We have selected five papers and further classified different user-avatar relationships described in these papers into six categories in Table 4. Based on the number of articles found and the distribution of their respective topics of interest, we believe that research under this category is underdeveloped. Nevertheless, we summarized their conclusions or key arguments on user-avatar relationships.

3.4.1 Users' preferences for digital bodies creation

To a certain extent, users' creation and customization of their digital bodies implicate how they perceive their avatars and how the user-avatar association is built. According to the evidence found, the creation of avatars reflects different preferences.

Kanamgotov et al. (2014) investigated different identity attributes during avatar creation and how avatar customization influences the degree of user-avatar association. In their first experiment—an unstructured interview with 16 computer science students, they discovered that experienced users tend to create an alter ego/false identity that is different from themselves with a higher level of customization and shares fewer identity similarities with their avatars. Besides, many participants prefer creating multiple avatars with different identities rather than using a single identity; Some chose to mask their own identities for privacy concerns. In their second experiment on a virtual campus, 12 participants customized their avatars and explored the virtual environment, followed by a semi-structured interview. They further conclude that users portray social identities through the creation of avatars. Most users prefer fabricating identities depending on the objects and environments they are exposed to rather than their own identities. We identified three types of user-avatar relationships from the study of Kanamgotov et al.: avatar as an alter-ego differs from offline self, avatar as medium between user and virtual world, and avatar as a tool.

Freeman et al. (2020) provide a different observation. A qualitative analysis was carried out on 30 semi-structured interviews of participants recruited from different social VR platforms. As a result, they identified three key themes that differentiate social VR avatars from those in traditional virtual worlds and online games. Firstly, avatar creation in social VR is considered challenging but fun and emotionally fulfilling. Secondly, higher engagement, intimacy, and personal feelings towards their avatar were provoked as users' physical bodies became the immediate and sole interface between them and their avatars (avatar as an extension/part of self). Lastly, experiencing social VR avatars also encourage users to explore their own identity (avatar as a more real version of self), especially for those who might struggle with their gender or sexual identity. Their participants also show a stronger identification with their digital bodies in social VR than in other virtual worlds, as they have a stronger desire to make their digital bodies similar to themselves, which is inconsistent with the observation of Kanamgotov et al. (2014). The same data was further analyzed by Freeman and Maloney (2021), adding that the construct of avatars in social VR is normally based on consistency with the users' physical selves or the social atmospheres of specific platforms. Besides, aesthetics, gender, race, and age/maturity play an essential role for users to perceive and interact with each other in social VR.

The inconsistent observations between (Kanamgotov et al., 2014) and (Freeman et al., 2020; Freeman and Maloney, 2021) may stem from the difference in their recruitment targets. Participants in the study of Freeman et al. (2020) were recruited from different social VR platforms, who might be more comfortable with socializinghe virtual world and more open to presenting their authentic selves on such platforms, comparing to participants recruited from school in the study of Kanamgotov et al. (2014). Both articles (Kanamgotov et al., 2014; Freeman and Maloney, 2021) highlight that environment or social atmospheres in social VR can impact users' choice of avatar identity. In addition, only customizable avatars were considered in these studies, while personalized avatars, which reproduce the appearance of the user's physical self, were not an option.

3.4.2 Rights analogous to those of the user

From an ethical perspective, Graber and Graber (2010) discussed whether an avatar shares rights analogous to the rights of the user. They started their argument "*A Physical Body is Not Necessary for Legal Protection and Having Rights as a Person*" with the evidence of psychological abuse and a will. Further, they argued that rights are already assigned to representations of an individual without biological corporeal such as prosthetic limbs, or without biological consciousness such as people in a permanent vegetative state, therefore could as well be assigned to digital bodies. Lastly, they presented a thought experiment to argue that avatars are appropriate candidates for rights and conclude that an avatar has rights analogous to the rights of the user, *if* a user considers an avatar an extension of the self.

3.4.3 Avatar-mediated interactions are encounters between mere avatars

In contrast, Carruth and Hill (2015) argued that users and their avatars should be considered to be distinct. Without *further grounding,* online avatar-mediated interactions should not be considered as encounters *between users* but rather merely *between avatars*. They investigated different accounts of identity and distinctness between users and avatars, concluding that they should be considered distinct as they instantiate distinct sets of properties. They then argued that user-avatar identification that is only relevant to their own avatar first-personally, is not sufficient to ground encounters between users. Therefore, they suggested that social and ethical issues described in literature (many have been described above) under the notion of the encounter between users, should be reconsidered.

3.5 Protections

In response to the problems mentioned above, we hope to find corresponding protection mechanisms or potential countermeasures in the literature. While 13 papers (Gavrilova and Yampolskiy, 2010; Boukhris et al., 2011; Mohamed and Yampolskiy, 2012; Yampolskiy et al., 2012; Bader and Ben Amara, 2014a; Bader and Ben Amara, 2014b; Bader and Ben Amara, 2016; Bader and Ben Amara, 2017; Falchuk et al., 2018; Pfeuffer et al., 2019; John et al., 2020; Lake, 2020) have explicitly addressed one or several identity and privacy issues and proposed corresponding protection mechanisms, works that have presented techniques or design guidelines that provide potential solutions in the area of virtual reality are also included and analyzed. Based on their characteristics and objectives, we have subdivided them into the following categories.

3.5.1 Avatar recognition and authentication

The traceability of an avatar is crucial to its acceptability in the social VR. Gavrilova and Yampolskiy (2010) are the first to investigate the field of automatic visual or behavioral authentication of non-biological entities (as they call *Artimetrics*), including software agents, avatars, and hardware robots. They have outlined the state-of-the-art visual and behavioral authentication and multi-modal system for avatar authentication. In another work (Yampolskiy et al, 2012) that was later published, they further defined and gave examples of six scenarios requiring *Artimetrics*, namely 1) matching a human face to an avatar face and 2) *vice versa*, 3) matching the face of one avatar to another avatar, 4) matching an avatar's face from one virtual world to the same avatar represented in a different virtual world(s), and 5) matching a sketch of an avatar to an avatar's face and 6)*vice versa*.

Following this field of study, Boukhris et al. (2011) presented a biometric identification system of avatar faces using support vector machines (SVM), and wavelet transforms, and achieved a 4.22% Equal Error Rate (EER) on a dataset of 100 samples collected from *Second Life*. Mohamed and Yampolskiy (2012) introduced two algorithms, Principal Component Analysis (PCA) and Wavelet PCA (WPCA), for avatar face recognition and tested them on two datasets of avatars from *Second Life* and *Entropia Universe*. Yampolskiy et al. (2012) described an avatar face recognition framework, including a set of algorithms to perform face detection and image normalization, face representation, and matching. Two scenarios within-virtual-world (avatar-to-avatar matching) and inter-reality-based (photo-to-avatar matching) was tested. In order to create a standard for evaluating avatar face authentication algorithms, Bader and Ben Amara (2014b) have developed the SID-Avatar database, a collection of 50 3D avatars from *Second Life*.

In contrast to automatic recognition, Tummon et al. (2019) were interested in avatar facial recognition by humans in a virtual airport passport control. A series of experiments were conducted to assess the feasibility of face-matching performed by participants in VR. In a follow-up work, Tummon et al. (2020) have further investigated how body language of avatars influences facial identification in the same scenario.

3.5.2 User authentication

User authentications are the key to combating identity theft and achieving secured identity management. In their review of virtual reality authentication, Jones et al. (2021) identified and provided a comprehensive overview of 29 papers until October 2020. They categorized the authentication methodologies of selected works into four types: knowledge-based authentication, biometric authentication, multi-model authentication and gaze-based authentication. With further analysis of the performances and

TABLE 5 An overview of six papers focusing on VR identification and/or authentication, that are not included in the reviewed of (Jones et al., 2021).

References	Type	Data acquisition and device	Algorithms	Dataset and results
Pfeuffer et al. (2019)	Biometric: head, hand and eye movement	Collect users' head, hand, and eye motion data on a HTC Vive while they performed controlled VR tasks (pointing, grabbing, walking, typing)	random forest, SVM	N = 22 Pointing: 63.55% Grabbing: 45.84% Walking: 49.67% Typing: 54.27%

Miller et al. (2020a)	Biometric: head and hand movement	Collect tracking data on a HTC Vive while participants watched 360-degree videos and answered questionnaires in VR.	kNN, random forest, and GBM	N = 511
				Accuracy = 95.3%

Miller et al. (2020b)	Biometric: head and hand movement, trigger positions for the dominant hand controller	Collect multi-system dataset consisting of 46 users performing a ball-throwing interaction using the Oculus Quest, HTC Vive, and HTC Vive Cosmos	nearest neighbor point position matching	N = 41, within-system Vive: 97% Quest: 91% Cosmos: 91% Cross-system Quest-Cosmos: 58% Vive-Cosmos: 70% Vive-Quest: 85%
(Miller et al., 2021))	Biometric: head and hand movementtrigger positions for the dominant hand controller	Collect multi-system dataset consisting of 46 users performing a ball-throwing interaction using the Oculus Quest, HTC Vive, and HTC Vive Cosmos	Siamese neural networks	N = 41 Authentication Quest-Vive EER = 1.39% Quest-Cosmos EER = 3.13% Vive-Cosmos EER = 3.86% Identification Quest-Vive: 98.53% Quest-Cosmos: 88.84% Vive-Cosmos: 87.82%
Liebers et al. (2021)	Biometric: head and hand movement	Collect tracking data on an Oculus Quest while participants performed a bowling and an archery task in two sessions recorded on different days	LSTM, MLP	N = 16 Bowling: 68% Archery: 90%
Schell et al. (2022)	Biometric: head and hand movement	3-point tracking data from publicly available full body mocap "Talking With Hands" dataset (Lee et al., 2019) with three different pre-processing techniques: scene-relative (SR), body-relative (BR), and body-relative velocity (BRV).	Random forest, MLP, FRNN, LSTM, GRU	N = 34 Top mean accuracies: RF+BR: 84% MLP+BR: 82% FRNN+BR: 82% LSTM+BR: 85% LSTM+BRV: 82% GRU+BR: 83% GRU+BRV: 86% Sequence lengths to achieve 100% mean accuracies: LSTM+BR: 150s GRU+BRV: 150s FRNN+BRV: 160s RF+BR: 240s LSTM+BRV: 280s

user studies of proposed protocols, they outlined the pros and cons of different authentication methodologies, pointed out the lack of study in this area and called for more investigation into multi-model schemes.

Additionally, we found six papers (Pfeuffer et al., 2019; Miller M. R. et al., 2020; Miller R. et al., 2020; Liebers et al., 2021; Miller et al., 2021; Schell et al., 2022) focusing on VR authentication that are not included in the review of Jones et al. An overview of these papers is listed in Table 5.

Notably, a latest work (Schell et al., 2022) compares different data representations and machine learning architectures for user authentication using movement data. By comparing three data representations: scene-relative, body-relative, and body-relative velocity data, the authors highlighted the importance of data pre-processing and concluded that scene-relative encoded data is not ideal, as it reflects session specific characteristics (i.e., position and orientation of the users) that could easily lead to overfitting of the models. In the comparison between five different prominent machine learning techniques (i.e., random forest, multilayer perceptron (MLP), and three RNNs: fully recurrent neural network (FRNN), long short-term memory (LSTM) and gated recurring unit (GRU)), RNN architectures outperformed random forest and MLP.

On the other hand, instead of seeking to improve the performance of authentication, John et al. (2020) implemented and evaluated a hardware-based eye-tracking defocus configuration that prevents biometric leaking during eye animation and iris authentication. Their evaluations reveal the security-utility trade-off between iris authentication and eye animation performance and suggest two different defocus configurations for each preference.

3.5.3 Access control and identity management

Another research direction is how to ensure that avatars themselves, as digital entities, can be protected from unauthorized access by imposters, and how the identity of the users can be managed within the social VR system. Although some authors have called for access control and identity management for avatars in social VR (Gavrilova and Yampolskiy, 2010; Yampolskiy et al., 2012; Bader and Ben Amara, 2014a; Bader and Ben Amara, 2016; Bader and Ben Amara, 2017; Freeman et al., 2020) are the only authors we found that explored this topic and proposed technical solutions.

They initially proposed a watermarking blind algorithm of an avatar's face for securing access to virtual worlds (2014a). Biometric information (fingerprint) will be coded as a 128-bits sequence and inserted into the avatar's face as an invisible watermark, by altering the vertex ordering of the mesh without changing the geometry. The watermark can be later extracted with a blind algorithm and compared with the original one according to Normalized Cross Correlation (NCC) for authentication. The method was proved robust to similarity transformations and signal processing attacks.

Bader and Ben Amara further describe an identity management framework relying on cancelable biometrics authentication (Bader and Ben Amara, 2016). This work is based on their previously mentioned watermarking schema but integrated with authorization mechanisms. A process model including components for 1) Identity Verification and Biometric Enrollment, 2) Avatar Watermarking, and 3) Internal Authentication and Authorization, was described.

In another paper (Bader and Ben Amara, 2017), they presented a virtual world platform for implementing and deploying biometrical access control against identity attacks from cybercriminals. They put forward a detailed methodology guide for designing such a virtual world equipped with a user interface for registration and biometric enrollment, simulation of 3D scenes, avatars, and objects, and a biometric-based logical access control framework.

3.5.4 Privacy mechanism

Falchuk et al. (2018) presented design guidelines for privacy mechanisms in social VR (social metaverse as they call it) that help protect avatars from several threats with a focus on harassment and observation, as addressed in Section 3.3.1. They defined "privacy plan" as "*A particular set of steps, initiated by an avatar, that enacts changes in the social metaverse such that the avatar has less risk of privacy intrusion when the plan is enac,*" and gave several logical design examples of these privacy plans, such as "Creating a crowd of clones" identical to the avatar to confuse attackers about its actual activities, and "Private Copy" of a part of the virtual world that user can temporarily have exclusive access. To offer privacy plans to users, they have further designed a privacy framework with interactive menus that allow the user to select and control these privacy plans.

3.5.5 Suggestions for the legal system

Targeting the procedural hurdles by dated Internet laws addressed in Section 3.3.5, Lake (2020) proposed several suggestions, which include revamping to what amount cyber interactions in VR reach a minimum contact that satisfies personal jurisdiction, and removing the shield of online anonymity when a certain IP address is involved in cybercrimes.

3.6 Avatar-identity related user study

We were also curious if there is empirical research evaluating the interplay between social interaction and avatar-related identity manipulation, as these are the fundamental to trust-building in social VR.

To investigate the response to identity disguise, Segovia and Bailenson (2012) studied ostracism during avatar-based interaction, and manipulated ostracizers' avatars to be either physically similar or dissimilar to the ostracizers. In their experiments during a ball-tossing game, participants who were ostracized from the game showed significantly higher aggressiveness towards unidentifiable ostracizers whose avatars are dissimilar to themselves, and higher aggressiveness towards ostracizers who have chosen to disguise their identity rather than have been assigned to. Their results indicate that identity manipulation might not be easily accepted during social interaction in VR.

Feng et al. (2014) presented their avatar generation method from the body scan, and in their experiments incorporated both the original scanned subjects' and other people's gestural styles into the avatars. Participants who know the subjects evaluated the subjects' avatars with original gestural style as more recognizable than those without. They also suggested that their framework could be used to investigate the impact of gestural style on the trust and liking towards avatar. This study sheds light on whether people can recognize identity misappropriation when encountering imposter avatars.

Fysh et al. (2021) provided a user-friendly photorealistic avatar generation method for the psychological research community, and demonstrated a series of studies exploring the identification of the avatar faces with respect to the correspondence of the avatars with their real-life counterparts. Their research provides off-the-shelf workflows and research methodologies for future psychological research on digital bodies and identity.

Pakanen et al. (2022) presented two studies on how users want to see other users in VR and AR multi-user systems, focusing on avatar visual designs. They created 36 comparable avatars with six styles ranging from Photorealistic, Hologram, Cartoon, Shadow, Robot, to Furry, and six body alterations from full body to only eye and mouth. In the first study, semi-structured interviews were conducted with 16 participants after they experienced a multi-user system in VR or AR; a follow-up online survey further collected 43 participants' preferences for avatar designs. Results from these studies suggested a preference for seeing other users with photorealistic avatars in both VR and AR scenarios due to their humanlike representation and affordances for interaction. They further inferred that use cases influence how users want to see others. Recognizable avatars in professional use cases are desired, as trust-building for users is highly impacted by the certainty of knowing whether the avatars they are interacting with are who they expect to be. Hearing the voice of the avatar will further enhance the trust that the avatar is really the person that it is supposed to be and not an artificial agent.

4 Discussion

This work aimed to give an overview of threats to users' identity and privacy in social VR with a specific focus on the digital bodies. We tried to collect relevant research, discussion and identify potential solutions. 49 studies were selected, analyzed, and presented according to five topics: 1) digital bodies generation, 2) threats to privacy and identity, 3) user-avatar relationships, 4) protections and 5) avatar-identity related user study.

Firstly, research into personalized avatar generation has produced significant results. Many proposed approaches are able to generate personalized avatars that can directly be animated and used as digital bodies in social VR in a short period of time. These approaches also vary in data acquisition, from requiring photogrammetric scanners to using single image. Secondly, we extracted and summarized existing and potential threats to users' privacy and identity described in literature. While the violation of digital bodies is most severe in current social VR, identity infringement such as identity theft raises most concerns from the use of personalized avatars. Meanwhile, the accountability of social VR citizens is being threatened by the anonymity. Besides, the use of digital bodies may also increase the risk of personal privacy leakage. Thirdly, we classified different user-avatar relationships, in order to better understand the nature of threats to identity and privacy. Then, we presented several potential countermeasures in response to the threats that we identified, including avatar recognition, user authentication, access control and identity management, and privacy mechanisms. Lastly, we presented several empirical research that evaluate the interplay between social interaction and avatar-related identity manipulation.

The initial results have revealed a severe lack of research and attention on the addressed topic. Although some inspiring works were found, the focuses and contributions of most related research appear to be scattered. Apart from avatar generation and user authentication, many reviewed subtopics lack comprehensive research and influential results.

One of our initial objectives of this work was to find research in the field of information security and human-computer interaction on the issue of identity theft as addressed in Section 3.3.2. Surprisingly, not only has the issue received little attention, but almost all in-depth discussion has come from the legal perspectives only (Lemley and Volokh, 2018; Lake, 2020). The reason for this might be that the technology for photorealistic avatar creation is still in its early stage. Despite that many believe users entering virtual worlds as themselves and in their own likeness is the future trend of social VR (O'Brolcháin et al., 2016), this is not yet the reality. Naturally, there are few real-life cases of such identity theft.

Although violations against digital bodies and the threats to accountability addressed in Section 3.3.1 and Section 3.3.3 have been widely reported by the media (Basu, 2021), it is worrying that this has not received sufficient attention from the academic community, and that the relevant discussion seems to be still at the level of the *Second Life* era.

In contrast, the industry seems to be devoting more attention to these issues. For example, social VR developers have started implementing protection mechanisms against harassment (Kelly, 2016; Kaleem, 2022). In addition, with the development of blockchain technologies and Web 3.0, related concepts such as self-sovereign identity (SSI) and Non-Fungible Token (NFT), have emerged and are being "touted" as perfect answers to the future of the "metaverse" (Tweeddale and Yumasheva, 2021; Sawers, 2022).

Nevertheless, we will still attempt to answer the research questions as initially posed, given the available information at hand.

4.1 RQ1: What are the existing and potential threats to privacy and identity when using digital bodies in social VR?

These threats to privacy and identity include the violation of the digital bodies, identity infringement, threats to accountability, and the risk of revealing personal privacy. The lack of protection and procedural barriers in existing law has also exacerbated the issues.

Some of these threats have long been prevalent in traditional social networking services (SNS). Identity infringement has long plagued social media such as *Facebook*. Many fake accounts have been created through stolen profiles and photos to engage in fraudulent activities (Picchi, 2018). In comparison, in social VR, not only does the high interactive nature lead to identity infringement being more intimate (Lake, 2020), but the presence of digital bodies may also result in more disorienting and contagious fraudulent activities. Similarly, in traditional SNS, the reveal of personal privacy remains a big issue, not only in terms of what users consciously provide but also what they unconsciously provide, such as their online activities. In the case of social VR, users' daily activities could be reflected through their digital bodies in the virtual world and lead to a higher level of revealing. In addition, online games and social media are under threats to accountability. With the protection of anonymity, malicious attacks and defamation are commonplace. In social VR, a salient issue resulting from these threats is the violation of digital bodies.

These similarities and differences are also reflected in practices. Combined with relevant media reports, violations to the digital bodies have occurred the most commonly. Based on the current state that social VR is being used more for leisure and socializing, the damages are mostly psychological and emotional. However, suppose social VR would play an essential role in our life and even become an alternative realm for human social activities in the foreseeable future, identity infringement might prevail and cause more substantial harm, such as the defamation of personal reputation and theft of property.

As we have remarked previously, such threats and issues were mostly mentioned merely as background information and comprehensive description and analysis from technical background is still inadequate. Therefore, we look forward to systematic discussions and analyses of threats as well as reasonable predictions of potential problems that have not yet occurred, by researchers who have extensive experience and sufficient knowledge in this field. As an example, Adams et al. (2018) have presented grounded work on VR security and privacy perceptions, which provides an extensive understanding of perceived risks in VR and detailed analyses of the state of VR privacy policies. Similar works on digital bodies would be very rewarding, as they would raise the awareness of users, developers, and researchers and provide accurate and comprehensive understandings for interdisciplinary research.

4.2 RQ2: How can we protect digital bodies and users from those threats?

Research directions we have identified so far include in-world avatar recognition, user authentication, access control and identity management, and other privacy mechanisms against harassment. Unfortunately, the presented works are not sufficient for the threats mentioned above.

4.2.1 In-world avatar recognition

In-world avatar recognition provides the possibility to identify and trace avatars involved in cybercrimes and other malicious activity. At the current stage, most works have been done in avatar face recognition, and have achieved promising performance. As the reviewed works in this area date from 2011–2014, we expect that developments in AI technology over the last few years will lead to further performance breakthroughs. However, in our opinion, avatar face recognition alone might have its limitation in practical application. At a system level, user activity can easily be tracked based on back-end data such as user id without using graphics as a medium; attackers can also use generic self-presentations or steal other's avatars to mask their identities.

Thus, in order to improve the usability, more investigation to other recognition modalities, such as behavioral recognition, is desired. The legitimacy of tracking avatar activities may also raise legal and ethical concerns, and a future research direction could be about how such tracking can be done legally while guaranteeing the citizens' privacy in the virtual world.

4.2.2 User authentication

Currently common social VR applications are no different from traditional SNS, and generally use accounts with passwords, or bind with VR device accounts, to authenticate users. Such methods could be vulnerable to observation attacks and unrealistic for instant checks. On the other hand, biometrics such as fingerprint, voice recognition, and camera photo ID have proved to be reliable for identity verification in virtual interaction (Semple et al., 2010), many services are already offering multi-factor authentication (MFA) (Ometov et al., 2018) using biometrics, such as fingerprint on mobile platforms. The use of VR devices, on the other hand, offers more options for biometrics acquisition than other platforms.

With the advancing artificial intelligence technology, promising progress has been made on novel authentication algorithms and mechanisms for VR in the past few years. With the various sensors of VR devices and users' unique biometrics, these authentication methods, although not yet mature, have achieved a high degree of accuracy. However, most current methods still require specific scenarios or tasks, and the way forward should be continuous authentication of users regardless of the environment and their activities. Additionally, research such as John et al. (2020) that considers the trade-off between the use of biometrics and potential privacy breaches deserves more attention.

In addition, we cannot ignore the potential problems arising from the use of artificial intelligence in social VR, such as bias in AI. It has been widely reported (Siwicki, 2021; Dilmegani, 2022) and researched (Ferrer et al., 2021) that the prejudiced assumptions in the algorithm development or prejudices in the training data could contribute to bias in the output of machine learning algorithm, and causing discrimination. For instance, a face recognition algorithm trained with a dataset containing mainly Caucasian people may perform poorly in recognizing people of other races. Similar bias could also exist when utilizing AI for VR authentication. For example, algorithms based on movement or physiological biometrics may be impractical or even discriminatory to people with disabilities. In human-centered social VR, it will be essential to consider the needs of different groups of people and ensure that viable alternatives are available to the appropriate technology.

Nowadays, privacy preserving security has become a key focus of information security and biometrics technologies, but in the VR domain, very little consideration has been given. In this regard, we expect authentication research in VR to be on par with mainstream security research, and possible directions include cancelable biometrics, homomorphic encryption, secure two-party computation, and so forth (Baig and Eskeland, 2021).

On the other hand, VR authentication can also be used without being restricted to existing VR sensors. Authentication modalities such as physiological biometrics (iris, fingerprint, EEG, ECG) (Ryu et al., 2021) with the support of additional wearables could also be considered. With VR devices such as the *HP Reverb g2 Omnicept* equipped with pupillometry, heart rate measure and face camera entering the market, there are reasons to believe that future VR devices will offer more authentication possibilities.

4.2.3 Access control and identity management

The protection of identity and the protection of digital bodies might be two separate aspects of the problems that together form a link between users, digital identities, and digital bodies. The idea of utilizing watermarking for avatar protection proposed by Bader and Ben Amara (2014a) deserves further exploration, and some recent studies on 3D mesh watermarking can be referred to (Ali, 2019; Malipatil and Shubhangi, 2020; Beugnon et al., 2022; Yoo et al., 2022).

NFTs, on the other hand, might have provided a different direction and have received a lot of attention in the identity management of the "metaverse." As a token stored on the blockchain which represents a unique entity, an NFT can establish a verified and public proof of ownership of a digital item, as well as a digital identity or an avatar (Sawers, 2022). However, since what an NFT provides is merely proof of ownership and the avatar itself remains unchanged, it is still questionable how a social VR system can verify and secure such ownership. Nevertheless, nowadays, there are already productions in the form of cross-platform avatars created based upon such concepts, such as *Ready Player Me*[9].

VR involves a lot of sensitive information about users, such as biometric information and personal activities. The leakages of such information will no doubt threaten users' privacy and increase the risk of identity theft, as profiles of victims can be generated from such personal information. Therefore, it is important for identity management to minimize the risk of leaking such, and federated identity (Jensen, 2011) and self-sovereign identity (SSI) (Preukschat and Reed, 2021) are worth explorations. Traditional identity management processes and stores personal data in centralized databases, and the verification and authentication process are operated with a central authority, which "*increases the risks of abuse and more easily rouses desires to use the system beyond the purposes for which it was originally intended* (The European Data Protection Supervisor (EDPS), 2018)." In order to deal with such issues, decentralization has been a visible trend in identity management (Allen, 2016). SSI is a concept for digital identity driven by the development of cryptography, distributed networks, cloud computing and blockchain technologies (Preukschat and Reed, 2021). SSI allows individuals to fully own and manage their digital identities that exist independently from services (Mühle et al., 2018). The implementation of SSI should allow the digital bodies as part of the identity data to be persistent and verify and authenticate the identity using decentralized identifiers (DIDs) (W3C Community Group, 2020) without giving away the control of their personal data. However, there is still a long way to go before these theories can actually be applied to the social VR.

[9] https://readyplayer.me/.

4.2.4 Privacy mechanisms

Privacy mechanisms are tools for users to protect their avatar and personal space in the virtual world, especially against harassment. Falchuk et al. (2018) in their protection mechanisms, have designed a privacy framework with interactive menus that allow users to customize their privacy settings. Many social VR applications such as *Horizon Worlds* and *AltspaceVR* have implemented "personal bubble" and similar features to prevent strangers from intruding personal space (Kelly, 2016; Kaleem, 2022).

In addition, adjusting the rendering of avatars could also provide options for users to protect themselves. For instance (Wolf et al., 2021), propose interaction techniques that allow users to actively control the transparency of other avatars, in order to reduce occlusion in overcrowded space. Such techniques could also be a good practice to mitigate the impact of harassment on victims, or to make unwanted users disappear. Alternatively, users could be given the option to blur their own avatars in untrusted environments, similar to the effect presented by Wang et al. (2021) in their experience-sharing reconstruction methods. Allowing users to switch self-avatar among different levels of fidelity (e.g., sketch-like rendering vs. cartoon-like rendering vs. realistic rendering, as Volonte et al. (2016) present in their study) could also be an option, for users to keep their personalized presentations while hiding identifiable details. We believe there are still many possibilities worth exploring.

On the other hand, empirical studies focusing on such privacy mechanisms are still inadequate. Further investigation should be conducted to quantify the effectiveness of privacy mechanisms and impact to user experience.

4.2.5 AI in social VR

Despite that no relevant research has been found, it is reasonable to assume that AI technology will have massive potential for the prevention and remediation of various threats and cybercrimes in social VR. Many video game developers have started to use AI algorithms to detect cheating (Sreedhar, 2020; Jonnalagadda et al., 2021) or other abnormal activities. *Facebook* uses AI to detect and label harmful content and misinformation generated on its platform (Schroepfer, 2019). Similarly, AI can also be applied in social VR systems to identify irregularities, including identity theft, the violation of digital bodies, and so on. Furthermore, AI-based credit systems can be applied to determine the trustworthiness score of users by combining user authentication, user behavior analysis and other user data.

However, such monitoring is often accompanied by controversy, and the above scenario is perhaps reminiscent of the future portrayed by many anti-utopian science fictions. AI can be valuable tools to protect users' privacy and security, but excessive and inappropriate use of AI can also lead to social surveillance and pose threats to autonomy (O'Brolcháin et al., 2016). Algorithm-based personalization contents in the virtual world could isolate users in their "filter bubbles," and the analysis of users' activities and behaviors could also enhance the manipulation of users. While exploring how AI technology can be used to protect users and to build intelligent human-centered social VR, discussion and awareness should also be raised to prevent social VR itself from posing threats to privacy and autonomy.

4.3 RQ3: What is the current stage of digital bodies usage in social VR, in terms of usability and user acceptance?

Personalized avatars can nowadays be created without complex manual efforts and highly capture the likeness of users. However, these technical advancements mostly remain as prototypes and not yet been deployed in commercialized social VR platforms. On the other hand, social VR users also tend to hide their real-life identities in virtual communities. As a results, personalized avatars as digital bodies are not yet popular among users.

Despite much progress in the generation of personalized avatars, they are still not readily accessible to the general public. One reason lies in that some of the methods required expensive equipment and setup, such as camera rigs (Achenbach et al., 2017; Feng et al., 2017). Another reason might be that most research focus more on the reconstruction realism and performance, while paying less attention to the deployment and the acquisition of users' data. Additionally, most generation pipelines applied AI automation, which again could lead to bias in outputs. Whether the realism in appearance reproduction varies across gender, age, or race, remains to be explored. It is also worth considering and exploring whether these avatar generations can serve people with disabilities.

User acceptance also play an essential role. Firstly, the use of avatars is perceived differently by users. While many people see avatars as an extension or part of themselves, others might see them as only communication tools. Although some suggest that many social VR users tend to use avatars that are consistent with their offline selves (Freeman and Maloney, 2021), sharing real-life identities in public virtual environments may raise privacy concerns and may still not be preferred (Kanamgotov et al., 2014). The change of virtual environments might also be relevant to user acceptance. In the case of customizable avatars, the creation of avatars is strongly related to the virtual environments and usage scenarios (Kanamgotov et al., 2014; Freeman and Maloney, 2021). Whether specific scenarios of social VR (such as education and work collaboration) encourage the usage of personalized avatars remains to be explored. Meanwhile, we recognize that digital bodies also have the potential to help users in their exploration of self-identification, such as gender (Freeman et al., 2020; Freeman and Maloney, 2021). It also raises the question of whether digital bodies necessarily need to resemble their users? Perhaps for some people, a unique and identifiable digital body created in accordance with their ideal self could better represent their identity in the virtual world.

Therefore, we have identified the following research gaps. In term of usability, the deployment of personalized avatar generation should be further considered, and we look forward to non-biased, low-cost and user-friendly pipelines to be deployed on social VR platforms that allow users to generate and use their own avatars. In term of user acceptance, it would be worthwhile to investigate further what external factors influence the way users perceive their avatars. Different usage scenarios may strongly influence the willingness of users to use personalized avatars and to reveal their self-identity in the virtual world.

4.4 RQ4: How to indicate the authenticity of social VR citizens' identity?

Protecting social VR citizens from the threats of privacy and identity issues will encourage them to enter the virtual world as themselves. However, how can users tell whether the avatars they encounter can be trusted? The appropriate way of indicating the identity authenticity of social VR citizens is yet another research gap that has not been explored.

Some traditional SNS such as *Twitter* and *Facebook* usually provide a "badge" for accounts that have the owners' identities verified, and users tend to give higher credibility to these "verified accounts" (Vaidya et al., 2019). Similar mechanism can be adapted to social VR communities that provides identity status for authenticated users. It is also worthwhile marking social VR citizens who have suspicious identities or activities. One the other hand, Pakanen et al. (2022) suggests that visual designs of avatars will influence how other users perceive them and might have an impact on trust-building. It will be interesting to find out whether explicit information of authenticity (e.g., an identity status) or implicit indicators (e.g., the designs or rendering styles of the avatars) can effectively communicate the trustworthiness of social VR citizens and influence their trust among each other. We can also adapt certain UI designs from video games. For instance, in many video games, enemy and friendly characters are often highlighted in certain way (e.g., outlined) and distinguished by colors. Similar approach can be applied for trustworthy and untrustworthy social VR citizens.

Research in this direction can aim at identifying the factors that influence users' trust during social interaction and creating a design guideline that gives requirements and recommendations for a social VR system that can effectively communicate the authenticity and trustworthiness level of its citizens.

4.5 RQ5: How do we evaluate the trust among social VR citizens?

The efforts of building authenticity and preventing identity infringement are not just to protect the user from potential harm, but ultimately to enhance the trust among social VR citizens. To that end, it is of great importance to evaluate the trust.

Self-reporting questionnaires are the dominant methods for measuring trust. However, most self-reporting methods may not be ideal for measuring specific trust and can reflect the internal feelings less accurately (Chan, 2010), and behavioral measurement are sometime preferred. Bente et al. (2014) investigate how photorealistic avatars and reputation scores affect trust-building in online transactions by letting participants perform the *Trust Game* online with a static avatar image. Hale et al. (2018) use a *Virtual Maze* experiment, in which participants need to navigate through a virtual 3D maze, and they can seek advice about which door to choose from two virtual characters. Perceived trustworthiness is measured by how often participants seek and follow advice from each character along. In addition, other behavioral clues are also investigated to measure trust or perceived trustworthiness, such as collaborative behavior in a shared virtual environment (Pan and Steed, 2017) and duration of mutual gaze in conversation (Aseeri and Interrante, 2021).

Unfortunately, apart from the study mentioned above, there has rarely been research on the measurement of the trust among social VR users. Future research can further aim at creating trust measurement paradigms that are specific for social VR citizens. Physiological data acquired by VR sensors might also provide the potentials for trust measurement.

4.6 Future research directions

In previous sub-sections, several research gaps have been identified, and several future research directions have been pointed out. In this sub-section, we aim to summarize and call for attention to these research directions, which include novel research directions waiting for exploration in the field of social VR, as well as technical advances in relevant areas that show potential to solve addressed issues.

4.6.1 Summaries and analysis of threats to digital bodies in social VR

To raise the awareness of issues and provide extensive background for relevant research, We need more comprehensive discussions and analyses of threats and violations to digital bodies in social VR. Such studies can come not only from technical perspectives but also from ethical and legal perspectives.

4.6.2 Low-cost and user-friendly digital body generation

Currently, most photorealistic avatar generation techniques are not easy to be deployed and brought to the market, as they may require expensive equipment or complex processes. Easy-to-use generation pipeline and friendly user interfaces will make photorealistic avatar generation more accessible to the public. For instance, with a few clicks on a cellphone application, users should be able to scan and generate their digital bodies with the cellphone camera and upload them to the virtual world. Additionally, to avoid bias evaluation of performance across different groups such as gender, age and race, need to be made. Similarly, research should look into the applicability of these generation pipelines to people with disabilities.

4.6.3 Virtual world citizen recognition and tracking

In previous research, the tracking of virtual world citizens (including avatars and agents) is mostly based on visual recognition, such as facial recognition of their digital faces. With the advances of AI algorithms, behavioral recognition (such as movement patterns and in-world activities) and multimodal recognition, should be further explored. Meanwhile, another research focus could be on tracking virtual world citizens without violating the privacy of users.

4.6.4 Biometrics identification and authentication

Firstly, we believe that researchers should pay more attention to physiological biometrics (such as iris, EEG and ECG) for VR identification and authentication, considering that VR devices have been equipped with more and more physiological sensors. Secondly, continuous authentication and periodic authentication should be developed to improve usability. Lastly, the use of user information such as biometrics for authentication inevitably leads to privacy and security issues, and we have yet to see privacy-preserving authentication (concepts such as cancelable biometrics, homomorphic encryption, secure two-party computation, and so on) applied to the field of VR. It is worth noting that relevant concepts and techniques have been well developed in biometrics and security research, and it is essential to introduce them into the field of VR.

4.6.5 Decentralized identity management

With the development and popularity of blockchain technology in recent years, the concept of decentralization has also been applied to identity management. These include federated identity and self-sovereign identity (SSI), among others. While these concepts have received much attention in the discussion of the "metaverse," we believe there is an urgent need for grounded research and evaluation of their usability.

4.6.6 Privacy mechanism

Several mechanisms and designs for protecting users' digital bodies from violation and identity infringement have been applied to social VR platforms. We hope that not only will more such privacy mechanisms be proposed, but also that there will be more empirical research focusing on evaluating the effectiveness of these mechanisms.

4.6.7 AI in social VR

Artificial intelligence technologies show great potential to be used to build intelligent human-centered social VR. These technologies can be involved in detecting abnormal activities, protecting users from violation, assessing user trustworthiness, and so on. On the other hand, excessive use of AI in social VR can also result in ethical and legal issues, which should receive considerable attention and extensive discussion before they emerge.

4.6.8 Identity and authenticity indicating system

How to effectively inform social VR users whether other citizens are trustworthy, for example, whether they are truly who they claim to be or not, should be valuable to protect users from threats such as identity theft during social interaction in the virtual world. Related research could create design guidelines for an identity and authenticity indicating system that could provide additional identity information of social VR citizens, or even incorporate such information into their representations when rendering their digital bodies.

4.6.9 Study of users' acceptance of digital bodies

To raise the overall acceptance of digital bodies, especially personalized digital bodies that capture the likeness of users, more research needs to be conducted to understand how social VR users perceive and utilize their digital bodies, and to investigate the influence of external factors (such as scenarios and environment) on their acceptance.

4.6.10 Trust measurement paradigms

We need reliable methods to measure and evaluate users' trust towards the system and each other, with consideration of the differences and similarities between the real and virtual worlds. These include subjective measurements such as self-report questionnaires designed for social VR scenarios or for trust towards avatars, and behavioral paradigms to measure trust using behavioral clues. Furthermore, although there is no yet reliable physiological measurement for trust, we believe this direction is worth exploring, given the ability of VR devices to collect physiological information such as eye movement, heart rate, facial expression, and so on.

4.7 Limitation

While this work provides a good overview of the existing discussion and countermeasures against the threats to identity and privacy stemming from the use of digital bodies in social VR, it still has certain limitations in the following ways. Firstly, although we target relevant research from different disciplines, our information source might show a preference for Computer Science and Psychology. The relatively liberal eligibility criteria might also result in certain subjectiveness during data screening. Meanwhile, due to the diversity of research methods and focus on the selected literature, it is difficult to conduct a comprehensive meta-analysis of them, and some individual study characteristics could not be effectively presented. In addition, the scope of our concerns is limited to issues related to digital bodies only, some other highly relevant privacy issues in social VR discussed in selected literature may have been overlooked. Finally, regarding research gaps identified during the discussion, we have proposed several recommendations for future studies and call for interdisciplinary collaboration. These recommendations might turn out to be rather uncomprehensive and biased based on the limitation of our own knowledge.

5 Conclusion

With the development and widespread of social VR technologies and applications, threats to users' privacy and identity have also emerged. This work presents a systematic review of the protection of users' identity and privacy in social VR with a focus on the use of digital bodies. Out of 814 items collected, 49 papers were selected and analyzed. In the structured overview of these papers, their study characteristics were categorized into five focuses: digital bodies generation, threats to privacy and identity, user-avatar relationships, protections, and avatar-identity related user study. A severe lack of relevant research was noticed. During our review, we identified several research gaps to be filled, including the further analysis of identity and privacy threats, new directions for protection mechanisms, how to encourage the use of digital bodies, how to best communicate the authenticity and trustworthiness of social VR citizens, and how to measurement trust among them.

Despite the fact that privacy and identity issues such as identity theft and the threats to accountability were mentioned from time to time in literature, there is a lack of systematic research and analysis of these issues from a technical background. Regarding the protection against such threats, while there has been impressive progress in certain areas such as user authentication, in most other areas, there has been a lack of significant and influential results. In addition, we have noted that academia is lagging behind industrial inquiry on this topic. In the discussion, we respond to the research questions posed at the outset based on knowledge obtained from the review, point to some future directions for research with relevant literature, and call for interdisciplinary collaboration. We envision this work to raise awareness of addressed issues and facilitate the development of social VR toward a direction that highlights security and trustworthiness. We believe this to be a necessity to build trustworthy, intelligent and human-centered social VR, and raise the acceptance of social VR as an alternative realm for human activities.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

Author contributions

JL conducted the search, processing, and analysis of the literature and took the lead in writing. ML has initiated the idea and goals, motivated the main questions and categories, and edited and refined the manuscript.

Funding

This work is part of the Privacy Matters (PriMa) project. The PriMa project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 860315.

Acknowledgments

Special thanks to Johrine Cronjé for proofreading and feedback.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Achenbach, J., Waltemate, T., Latoschik, M. E., and Botsch, M. (2017). “Fast generation of realistic virtual humans,” in Proceedings of the 23rd ACM Symposium on Virtual Reality Software and Technology VRST ’17, New York, NY, USA (New York, NY: Association for Computing Machinery), 1–10. doi:10.1145/3139131.3139154

Adams, D., Bah, A., Barwulor, C., Musaby, N., Pitkin, K., and Redmiles, E. M. (2018). “Ethics emerging: The story of privacy and security perceptions in virtual reality,” in Fourteenth Symposium on Usable Privacy and Security (Baltimore, MD: SOUPS 2018), 427–442.

Ali, N. A. (2019). Watermarking in 3D models using depth path. *eijs.*, 2490–2496. doi:10.24996/ijs.2019.60.11.21

Alldieck, T., Magnor, M., Bhatnagar, B. L., Theobalt, C., and Pons-Moll, G. (2019a). “Learning to reconstruct people in clothing from a single RGB camera,” in 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (Long Beach, CA: CVPR), 1175–1186. doi:10.1109/CVPR.2019.00127

Alldieck, T., Magnor, M., Xu, W., Theobalt, C., and Pons-Moll, G. (2018a). “Detailed human avatars from monocular video,” in 2018 International Conference on 3D Vision (3DV), 98–109. doi:10.1109/3DV.2018.00022

Alldieck, T., Magnor, M., Xu, W., Theobalt, C., and Pons-Moll, G. (2018b). “Video based reconstruction of 3D people models,” in 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, 8387–8397. doi:10.1109/CVPR.2018.00875

Alldieck, T., Pons-Moll, G., Theobalt, C., and Magnor, M. (2019b). “Tex2Shape: Detailed full human body geometry from a single image,” in 2019 IEEE/CVF International Conference on Computer Vision (ICCV). doi:10.1109/ICCV.2019.00238

Allen, C. (2016). The path to self-sovereign identity. Available at: https://www.coindesk.com/markets/2016/04/27/the-path-to-self-sovereign-identity/(Accessed October 18, 2021).

Aseeri, S., and Interrante, V. (2021). The influence of avatar representation on interpersonal communication in virtual social environments. *IEEE Trans. Vis. Comput. Graph.* 27, 2608–2617. doi:10.1109/TVCG.2021.3067783

Bader, S., and Ben Amara, N. E. (2014a). “A securing access approach to virtual worlds based on 3D mesh watermarking of avatar’s face,” in 2014 4th International Conference on Image Processing Theory, Tools and Applications (IPTA), 1–6. doi:10.1109/IPTA.2014.7001949

Bader, S., and Ben Amara, N. E. B. (2017). “Design of a 3D virtual world to implement a logical access control mechanism based on fingerprints,” in 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA) (Hammamet: IEEE), 1239–1246. doi:10.1109/AICCSA.2017.147

Bader, S., and Ben Amara, N. E. (2016). Identity management in virtual worlds based on biometrics watermarking. *Int. J. Comput. Syst. Eng.* 10, 1478–1482.

Bader, S., and Ben Amara, N. E. (2014b). “SID-avatar database: A 3D avatar dataset for virtual world research,” in International Image Processing, Applications and Systems Conference, 1–5. doi:10.1109/IPAS.2014.7043319

Baig, A. F., and Eskeland, S. (2021). Security, privacy, and usability in continuous authentication: A survey. *Sensors* 21, 5967. doi:10.3390/s21175967

Bailenson, J. N., Beall, A. C., Loomis, J., Blascovich, J., and Turk, M. (2004). Transformed social interaction: Decoupling representation from behavior and form in collaborative virtual environments. *Presence. (Camb).* 13, 428–441. doi:10.1162/1054746041944803

Bary, E. (2020). Zoom, Microsoft Teams usage are rocketing during coronavirus pandemic, new data show. *MarketWatch*. Available at: https://www.marketwatch.com/story/zoom-microsoft-cloud-usage-are-rocketing-during-coronavirus-pandemic -new-data-show-2020-03-30 (Accessed March 8, 2022).

Basu, T. (2021). The metaverse has a groping problem already | MIT Technology Review. *MIT Technol. Rev*. Available at: https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/(Accessed May 10, 2022).

Beacco, A., Gallego, J., and Slater, M. (2020). “Automatic 3D character reconstruction from frontal and lateral monocular 2D RGB views,” in 2020 IEEE International Conference on Image Processing (Abu Dhabi: ICIP), 2785–2789. doi:10.1109/ICIP40778.2020.9191091

Bente, G., Dratsch, T., Rehbach, S., Reyl, M., and Lushaj, B. (2014). “Do you trust my avatar? Effects of photo-realistic seller avatars and reputation scores on trust in online transactions,” in HCI in business *lecture notes in computer science*. Editor F. F.-H. Nah (Cham: Springer International Publishing), 461–470. doi:10.1007/978-3-319-07293-7_45

Beugnon, S., Itier, V., and Puech, W. (2022). “3D watermarking,” in *Multimedia security 1* (John Wiley & Sons), 219–246. doi:10.1002/9781119901808.ch7

Boukhris, M., Mohamed, A. A., D’Souza, D., Beck, M., Ben Amara, N. E., and Yampolskiy, R. V. (2011). “Artificial human face recognition via Daubechies wavelet transform and SVM,” in 2011 16th International Conference on Computer Games (Louisville, KY: CGAMES), 18–25. doi:10.1109/CGAMES.2011.6000330

Carruth, A. D., and Hill, D. W. (2015). Identity and distinctness in online interaction: Encountering a problem for narrative accounts of self. *Ethics Inf. Technol.* 17, 103–112. doi:10.1007/s10676-015-9364-y

Chae, S. W., Lee, K. C., and Seo, Y. W. (2016). Exploring the effect of avatar trust on learners’ perceived participation intentions in an e-learning environment. *Int. J. Human–Computer. Interact.* 32, 373–393. doi:10.1080/10447318.2016.1150643

Chan, D. (2010). “So why ask me? Are self-report data really that bad?” in *Statistical and methodological myths and urban legends* (Abingdon-on-Thames: Routledge), 329–356.

Chen, Y., Dang, G., Cheng, Z.-Q., and Xu, K. (2014). Fast capture of personalized avatar using two Kinects. *J. Manuf. Syst.* 33, 233–240. doi:10.1016/j.jmsy.2013.11.005

Cole, S. (2020). “This open-source program deepfakes you during Zoom meetings,” in *Real time. Vice*. Available at: https://www.vice.com/en/article/g5xagy/this-open-source-program-deepfakes-you-during-zoom-meetings-in-real-time (Accessed March 9, 2022).

Conrad, M., Hassan, A., Koshy, L., Kanamgotov, A., and Christopoulos, A. (2017). Strategies and challenges to facilitate situated learning in virtual worlds post-second life. *Comput. Entertain.* 15 (3), 1–39. doi:10.1145/3010078

Deng, X., and Ruan, J. (2009). “Users’ privacy in the second life library,” in 2009 IEEE International Symposium on IT in Medicine Educat, 337–340. doi:10.1109/ITIME.2009.5236404

Dilmegani, C. (2022). Bias in AI: What it is, types, examples & 6 ways to fix it in 2022. *AI Mult*. Available at: https://research.aimultiple.com/ai-bias/(Accessed September 22, 2022).

Dionisio, J. D. N., Iii, W. G. B., and Gilbert, R. (2013). 3D Virtual worlds and the metaverse: Current status and future possibilities. *ACM Comput. Surv.* 45, 1–38. doi:10.1145/2480741.2480751

Falchuk, B., Loeb, S., and Neff, R. (2018). The social metaverse: Battle for privacy. *IEEE Technol. Soc. Mag.* 37, 52–61. doi:10.1109/MTS.2018.2826060

Falk, B., Meng, Y., Zhan, Y., and Zhu, H. (2021). “Poster: ReAvatar: Virtual reality de-anonymization attack through correlating movement signatures,” in Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security CCS ’21, New York, NY, USA (New York, NY: Association for Computing Machinery), 2405–2407. doi:10.1145/3460120.3485345

Feng, A., Lucas, G., Marsella, S., Suma, E., Chiu, C.-C., Casas, D., et al. (2014). “Acting the part: The role of gesture on avatar identity,” in Proceedings of the Seventh International Conference on Motion in Games MIG ’14, New York, NY, USA (New York, NY: Association for Computing Machinery), 49–54. doi:10.1145/2668064.2668102

Feng, A., Rosenberg, E. S., and Shapiro, A. (2017). Just-in-time, viable, 3-D avatars from scans. *Comput. Animat. Virtual Worlds* 28, e1769. doi:10.1002/cav.1769

Ferrari, A. (2021). *DIGITAL HUMANITY. Do users’ gaming habits affect the perceived human- likeness of virtual agents in a simulated human interaction?*

Ferrer, X., Nuenen, T. V., Such, J. M., Coté, M., and Criado, N. (2021). Bias and discrimination in AI: A cross-disciplinary perspective. *IEEE Technol. Soc. Mag.* 40, 72–80. doi:10.1109/MTS.2021.3056293

Foerster, K., Hein, R., Grafe, S., Latoschik, M. E., and Wienrich, C. (2021). “Fostering intercultural competencies in initial teacher education. Implementation of educational design prototypes using a social VR environment,” in *Innovate learning summit (association for the advancement of computing in education* (Chesapeake: Association for the advancement of computing in education (AACE)), 95–108.

Freeman, G., and Maloney, D. (2021). Body, avatar, and me: The presentation and perception of self in social virtual reality. *Proc. ACM Hum. Comput. Interact.* 4, 239–23927. doi:10.1145/3432938

Freeman, G., Zamanifard, S., Maloney, D., and Adkins, A. (2020). “My body, my avatar: How people perceive their avatars in social virtual reality,” in Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems CHI EA ’20, New York, NY, USA (New York, NY: Association for Computing Machinery), 1–8. doi:10.1145/3334480.3382923

Fribourg, R., Argelaguet, F., Lecuyer, A., and Hoyet, L. (2020). Avatar and sense of embodiment: Studying the relative preference between appearance, control and point of view. *IEEE Trans. Vis. Comput. Graph.* 26, 2062–2072. doi:10.1109/TVCG.2020.2973077

Fysh, M. C., Trifonova, I., Allen, J., McCall, C., Burton, A. M., and Bindemann, M. (2021). Avatars with faces of real people: A construction method for scientific experiments in virtual reality. *Behav. Res. Methods* 54, 1461–1475. doi:10.3758/s13428-021-01676-5

Gavrilova, M. L., and Yampolskiy, R. V. (2010). "Applying biometric principles to avatar recognition," in 2010 International Conference on Cyberworlds, 179–186. doi:10.1109/CW.2010.36

Gorini, A., Gaggioli, A., Vigna, C., and Riva, G. (2008). A second life for eHealth: Prospects for the use of 3-D virtual worlds in clinical psychology. *J. Med. Internet Res.* 10, e21. doi:10.2196/jmir.1029

Graber, M. A., and Graber, A. D. (2010). Get your paws off of my pixels: Personal identity and avatars as self. *J. Med. Internet Res.* 12, e28. doi:10.2196/jmir.1299

Hale, J., Payne, M. E., Taylor, K. M., Paoletti, D., and De C Hamilton, A. F. (2018). The virtual maze: A behavioural tool for measuring trust. *Q. J. Exp. Psychol.* 71, 989–1008. doi:10.1080/17470218.2017.1307865

Heath, A. (2021). Inside Facebook's metaverse for work. *Verge*. Available at: https://www.theverge.com/2021/8/19/22629942/facebook-workrooms-horizon-oculus-vr (Accessed October 12, 2021).

Hu, L., Saito, S., Wei, L., Nagano, K., Seo, J., Fursund, J., et al. (2017). Avatar digitization from a single image for real-time rendering. *ACM Trans. Graph.* 36, 1–14. doi:10.1145/3130800.31310887

Huang, Z., Xu, Y., Lassner, C., Li, H., and Tung, T. (2020). "Arch: Animatable reconstruction of clothed humans," in 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 3090–3099. doi:10.1109/CVPR42600.2020.00316

Ichim, A. E., Bouaziz, S., and Pauly, M. (2015). Dynamic 3D avatar creation from hand-held video input. *ACM Trans. Graph.* 34, 1–14. doi:10.1145/2766974

Jensen, J. (2011). "Benefits of federated identity management - a survey from an integrated operations viewpoint," in *Availability, reliability and security for business, enterprise and health information systems lecture notes in computer science*. Editors A. M. Tjoa, G. Quirchmayr, I. You, and L. Xu (Berlin, Heidelberg: Springer), 1–12. doi:10.1007/978-3-642-23300-5_1

John, B., Jorg, S., Koppal, S., and Jain, E. (2020). The security-utility trade-off for Iris authentication and eye animation for social virtual avatars. *IEEE Trans. Vis. Comput. Graph.* 26, 1880–1890. doi:10.1109/TVCG.2020.2973052

Jones, J. M., Duezguen, R., Mayer, P., Volkamer, M., and Das, S. (2021). "A literature review on virtual reality authentication," in *Human aspects of information security and assurance IFIP advances in information and communication technology*. Editors S. Furnell and N. Clarke (Cham: Springer International Publishing), 189–198. doi:10.1007/978-3-030-81111-2_16

Jonnalagadda, A., Frosio, I., Schneider, S., McGuire, M., and Kim, J. (2021). Robust vision-based cheat detection in competitive gaming. *Proc. ACM Comput. Graph. Interact. Tech.* 4, 1–18. doi:10.1145/3451259

Kaleem, K. (2022). How meta is dealing with sexual harassment in VR. *MUO*. Available at: https://www.makeuseof.com/meta-sexual-harassment-vr-personal-boundary/(Accessed May 10, 2022).

Kanamgotov, A., Koshy, L., Conrad, M., and Prakoonwit, S. (2014). "User avatar association in virtual worlds," in 2014 International Conference on Cyberworlds, 93–100. doi:10.1109/CW.2014.21

Kelly, K. (2016). Introducing space bubble. *AltspaceVR*. Available at: https://altvr.com/introducing-space-bubble/(Accessed May 10, 2022).

Kim, J. (2021). Advertising in the metaverse: Research agenda. *J. Interact. Advert.* 21, 141–144. doi:10.1080/15252019.2021.2001273

Lake, J. (2020). Hey, you stole my avatar!: Virtual reality and its risks to identity protection. *EMORY LAW J.* 69, 48.

Latoschik, M. E., Kern, F., Stauffert, J.-P., Bartl, A., Botsch, M., and Lugrin, J.-L. (2019). Not alone here?! scalability and user experience of embodied ambient crowds in distributed social virtual reality. *IEEE Trans. Vis. Comput. Graph.* 25, 2134–2144. doi:10.1109/TVCG.2019.2899250

Latoschik, M. E., Roth, D., Gall, D., Achenbach, J., Waltemate, T., and Botsch, M. (2017). "The effect of avatar realism in immersive social virtual realities," in Proceedings of the 23rd ACM Symposium on Virtual Reality Software and Technology, Gothenburg Sweden (New York, NY: Association for Computing Machinery), 1–10. doi:10.1145/3139131.3139156

Lazova, V., Insafutdinov, E., and Pons-Moll, G. (2019). "360-Degree textures of people in clothing from a single image," in 2019 International Conference on 3D Vision (Quèbec: 3DV), 643–653. doi:10.1109/3DV.2019.00076

Le, Q. T., Pedro, A., and Park, C. S. (2015). A social virtual reality based construction safety education system for experiential learning. *J. Intell. Robot. Syst.* 79, 487–506. doi:10.1007/s10846-014-0112-z

Lee, G., Deng, Z., Ma, S., Shiratori, T., Srinivasa, S. S., and Sheikh, Y. (2019). "Talking with hands 16.2 m: A large-scale dataset of synchronized body-finger motion and audio for conversational motion analysis and synthesis," in Proceedings of the IEEE/CVF International Conference on Computer Vision, 763–772.

Lemley, M., and Volokh, E. (2018). *LAW, virtual reality, and augmented reality*, 166. UNIVERSITY OF PENNSYLVANIA LAW REVIEW, 1051–1138.

Li, J., Chen, G., de Ridder, H., and Cesar, P. (2020). "Designing a social VR clinic for medical consultations," in Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems CHI EA '20, New York, NY, USA (New York, NY: Association for Computing Machinery), 1–9. doi:10.1145/3334480.3382836

Liebers, J., Abdelaziz, M., Mecke, L., Saad, A., Auda, J., Gruenefeld, U., et al. (2021). "Understanding user identification in virtual reality through behavioral biometrics and the effect of body normalization," in Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (Yokohama Japan: ACM), 1–11. doi:10.1145/3411764.3445528

Liu, Q., and Steed, A. (2021). Social virtual reality platform comparison and evaluation using a guided group walkthrough method. *Front. Virtual Real.* 2, 668181. doi:10.3389/frvir.2021.668181

Lohle, M., and Terrell, S. (2014). Real projects, virtual worlds: Coworkers, their avatars, and the trust conundrum. *Qual. Rep.* 19.

Loper, M., Mahmood, N., Romero, J., Pons-Moll, G., and Black, M. J. (2015). Smpl: A skinned multi-person linear model. *ACM Trans. Graph.* 34(6), 1–16. doi:10.1145/2816795.2818013

Lucas, G., Szablowski, E., Gratch, J., Feng, A., Huang, T., Boberg, J., et al. (2016). "The effect of operating a virtual doppleganger in a 3D simulation," in Proceedings of the 9th International Conference on Motion in Games MIG '16, New York, NY, USA (New York, NY: Association for Computing Machinery), 167–174. doi:10.1145/2994258.2994263

Malipatil, M., and Shubhangi, D. C. (2020). "An efficient 3D watermarking algorithm for 3D mesh models," in 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 1–5. doi:10.1109/I-SMAC49090.2020.9243381

Maloney, D., Freeman, G., and Robb, A. (2021). *Social virtual reality: Ethical considerations and future directions for an emerging research space*. Available at: http://arxiv.org/abs/2104.05030 (Accessed May 19, 2021).

Marinussen, M., and de Rooij, A. (2019). "Being yourself to be creative: How self-similar avatars can support the generation of original ideas in virtual environments," in Proceedings of the 2019 on Creativity and Cognition C& C '19, New York, NY, USA (New York, NY: Association for Computing Machinery), 285–293. doi:10.1145/3325480.3325482

McElroy, R. (2021). Deepfakes in cyberattacks aren't coming. They're already here. VentureBeat. Available at: https://venturebeat.com/2021/08/28/deepfakes-in-cyberattacks-arent-coming-theyre-already-here/(Accessed March 9, 2022).

McVeigh-Schultz, J., Kolesnichenko, A., and Isbister, K. (2019). "Shaping pro-social interaction in VR: An emerging design framework," in Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow Scotland Uk (New York, NY: Association for Computing Machinery), 1–12. doi:10.1145/3290605.3300794

McVeigh-Schultz, J., Márquez Segura, E., Merrill, N., and Isbister, K. (2018). "What's it mean to "Be social" in VR?: Mapping the social VR design ecology," in Proceedings of the 2018 ACM Conference Companion Publication on Designing Interactive Systems, Hong Kong China (New York, NY: ACM), 289–294. doi:10.1145/3197391.3205451

Miller, M. R., Herrera, F., Jun, H., Landay, J. A., and Bailenson, J. N. (2020a). Personal identifiability of user tracking data during observation of 360-degree VR video. *Sci. Rep.* 10, 17404. doi:10.1038/s41598-020-74486-y

Miller, R., Banerjee, N. K., and Banerjee, S. (2021). "Using siamese neural networks to perform cross-system behavioral authentication in virtual reality," in *2021 IEEE virtual reality and 3D user interfaces* (Lisbon: VR), 140–149. doi:10.1109/VR50410.2021.00035

Miller, R., Banerjee, N. K., and Banerjee, S. (2020b). "Within-system and cross-system behavior-based biometric authentication in virtual reality," in 2020 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Atlanta, GA, USA (IEEE), 311–316. doi:10.1109/VRW50115.2020.00070

Mohamed, A. A., and Yampolskiy, R. V. (2012). "Using discrete wavelet transform and eigenfaces for recognizing avatars faces," in 2012 17th International Conference on Computer Games (Louisville, KY: CGAMES), 143–147. doi:10.1109/CGames.2012.6314566

Mühle, A., Grüner, A., Gayvoronskaya, T., and Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Comput. Sci. Rev.* 30, 80–86. doi:10.1016/j.cosrev.2018.10.002

Nagano, K., Seo, J., Xing, J., Wei, L., Li, Z., Saito, S., et al. (2018). paGAN: Real-time avatars using dynamic textures. *ACM Trans. Graph.* 37, 1–12. doi:10.1145/3272127.3275075

Neustaedter, C., and Fedorovskaya, E. (2009). "Presenting identity in a virtual world through avatar appearances," in GI '09: Proceedings of Graphics Interface 200, 183–190.8.

O'Brolcháin, F., Jacquemard, T., Monaghan, D., O'Connor, N., Novitzky, P., and Gordijn, B. (2016). The convergence of virtual reality and social networks: Threats to privacy and autonomy. *Sci. Eng. Ethics* 22, 1–29. doi:10.1007/s11948-014-9621-1

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., and Koucheryavy, Y. (2018). Multi-factor Authentication: A survey. *Cryptography* 2, 1. doi:10.3390/cryptography2010001

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* 372, n71. doi:10.1136/bmj.n71

Pakanen, M., Alavesa, P., van Berkel, N., Koskela, T., and Ojala, T. (2022). Nice to see you virtually": Thoughtful design and evaluation of virtual avatar of the other user in AR and VR based telexistence systems. *Entertain. Comput.* 40, 100457. doi:10.1016/j.entcom.2021.100457

Pan, Y., and Steed, A. (2016). A comparison of avatar-video-and robot-mediated interaction on users' trust in expertise. *Front. Robot. AI* 3. doi:10.3389/frobt.2016.00012

Pan, Y., and Steed, A. (2017). The impact of self-avatars on trust and collaboration in shared virtual environments. *PLoS ONE* 12, e0189078. doi:10.1371/journal.pone.0189078

Pfeuffer, K., Geiger, M. J., Prange, S., Mecke, L., Buschek, D., and Alt, F. (2019). "Behavioural biometrics in VR: Identifying people from body motion and relations in virtual reality," in Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow Scotland Uk (New York, NY: Association for Computing Machinery), 1–12. doi:10.1145/3290605.3300340

Picchi, A. (2018). A problem for Facebook users: Identity scams. Available at: https://www.cbsnews.com/news/a-growing-problem-for-facebook- users-identity-scams/(Accessed September 13, 2022).

Preukschat, A., and Reed, D. (2021). *Self-sovereign identity: Decentralized digital identity and verifiable credentials.* Shelter Island, NY: Manning Publications.

Ripka, G., Grafe, S., and Latoschik, M. E. (2020). "Preservice teachers' encounter with social VR–exploring virtual teaching and learning processes in initial teacher education," in SITE Interactive Conference (Association for the Advancement of Computing in Education (Chesapeake: Association for the advancement of computing in education (AACE)), 549–562.

Roth, D., Kleinbeck, C., Feigl, T., Mutschler, C., and Latoschik, M. (2018). "Beyond replication: Augmenting social behaviors in multi-user virtual realities," in 2018 IEEE Conference on Virtual Reality and 3D User Interfaces (VR), Tuebingen/Reutlingen, Germany, 18-22 March 2018 (IEEE). doi:10.1109/VR.2018.8447550

Roth, D., and Latoschik, M. E. (2020). Construction of the virtual embodiment questionnaire (VEQ). *IEEE Trans. Vis. Comput. Graph.* 26, 3546–3556. doi:10.1109/TVCG.2020.3023603

Roth, D., Latoschik, M. E., Vogeley, K., and Bente, G. (2015). Hybrid avatar-agent technology – a conceptual step towards mediated "social" virtual reality and its respective challenges. *i-com* 14, 107–114. doi:10.1515/icom-2015-0030

Roth, D., Waldow, K., Latoschik, M. E., Fuhrmann, A., and Bente, G. (2017). "Socially immersive avatar-based communication," in 2017 IEEE Virtual Reality (Los Angeles, CA: VR), 259–260. doi:10.1109/VR.2017.7892275

Ryu, R., Yeom, S., Kim, S.-H., and Herbert, D. (2021). Continuous multimodal biometric authentication schemes: A systematic review. *IEEE Access* 9, 34541–34557. doi:10.1109/ACCESS.2021.3061589

Sawers, P. (2022). Identity and authentication in the metaverse. *VentureBeat.* Available at: https://venturebeat.com/2022/01/26/identity-and-authentication-in-the-metaverse/(Accessed May 9, 2022).

Schell, C., Hotho, A., and Latoschik, M. E. (2022). "Comparison of data representations and machine learning architectures for user identification on arbitrary motion sequences," in Proceedings of the IEEE International conference on artificial intelligence and Virtual Reality (IEEE AIVR) (New York, NY: IEEE).

Schroepfer, M. (2019). New progress in using AI to detect harmful content. *Meta AI.* Available at: https://ai.facebook.com/blog/community-standards-report/ (Accessed September 22, 2022).

Schuemie, M. J., Straaten, P. V. D., Krijn, M., and Mast, C. A. P. G. V. D. (2001). *Research on presence in virtual reality: A survey.*

Schultz, A., and Parikh, J. (2020). Keeping our services stable and reliable during the COVID-19 outbreak. *Meta.* Available at: https://about.fb.com/news/2020/03/keeping-our-apps-stable-during-covid-19/(Accessed March 8, 2022).

Segovia, K. Y., and Bailenson, J. N. (2012). Virtual imposters: Responses to avatars that do not look like their controllers. *Soc. Influ.* 7, 285–303. doi:10.1080/15534510.2012.670906

Semple, M., Hatala, J., Franks, P., and Rossi, M. A. (2010). Is your avatar ethical? On-line course tools that are methods for student identity and verification. *J. Educ. Technol. Syst.* 39, 181–191. doi:10.2190/et.39.2.h

Shao, D., and Lee, I.-J. (2020). Acceptance and influencing factors of social virtual reality in the urban elderly. *Sustainability* 12, 9345. doi:10.3390/su12229345

Siwicki, B. (2021). How AI bias happens – And how to eliminate it. *Healthc. IT News.* Available at: https://www.healthcareitnews.com/news/how-ai-bias-happens-and-how-eliminate-it (Accessed September 22, 2022).

Slater, M., Perez-Marcos, D., Ehrsson, H. H., and Sanchez-Vives, M. V. (2008). Towards a digital body: The virtual arm illusion. *Front. Hum. Neurosci.* 2, 6. doi:10.3389/neuro.09.006.2008

Sreedhar, N. (2020). A new AI innovation aims to stop cheating in multiplayer video games. Mintlounge. Available at: https://lifestyle.livemint.com//smart-living/innovation/a-new-ai-innovation-aims-to-stop-cheating-in-multiplayer-video-games- 111605612437694.html (Accessed September 22, 2022).

The European Data Protection Supervisor (EDPS) (2018). *Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems.*

Triberti, S., Durosini, I., Aschieri, F., Villani, D., and Riva, G. (2017). Changing avatars, changing selves? The influence of social and contextual expectations on digital rendition of identity. *Cyberpsychology, Behav. Soc. Netw.* 20, 501–507. doi:10.1089/cyber.2016.0424

Tummon, H., Allen, J., and Bindemann, M. (2020). body language influences on facial identification at passport control: An exploration in virtual reality. *I-PERCEPTION* 11, 204166952095803. doi:10.1177/2041669520958033

Tummon, H. M., Allen, J., and Bindemann, M. (2019). Facial identification at a virtual reality airport. *I-Perception* 10, 204166951986307. doi:10.1177/2041669519863077

Tweeddale, A., and Yumasheva, E. (2021). Metaverse and self-sovereign identity (SSI): New superpower? *cheqd.* Available at: https://www.cheqd.io/blog/metaverse-and-self-sovereign-identity-new-superpower (Accessed May 9, 2022).

Vaidya, T., Votipka, D., Mazurek, M. L., and Sherr, M. (2019). "Does being verified make you more credible?: Account verification's effect on tweet credibility," in Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow Scotland Uk (New York, NY: Association for Computing Machinery), 1–13. doi:10.1145/3290605.3300755

Vanacker, B., and Heider, D. (2012). Ethical harm in virtual communities. *Convergence.* 18, 71–84. doi:10.1177/1354856511419916

Volonte, M., Babu, S. V., Chaturvedi, H., Newsome, N., Ebrahimi, E., Roy, T., et al. (2016). Effects of virtual human appearance fidelity on emotion contagion in affective inter-personal simulations. *IEEE Trans. Vis. Comput. Graph.* 22, 1326–1335. doi:10.1109/TVCG.2016.2518158

W3C Community Group (2020). A primer for decentralized identifiers. Available at: https://w3c-ccg.github.io/did-primer/(Accessed October 18, 2021).

Waltemate, T., Gall, D., Roth, D., Botsch, M., and Latoschik, M. E. (2018). The impact of avatar personalization and immersion on virtual body ownership, presence, and emotional response. *IEEE Trans. Vis. Comput. Graph.* 24, 1643–1652. doi:10.1109/tvcg.2018.2794629

Wang, C. Y., Sriram, S., and Won, A. S. (2021). Shared realities: Avatar identification and privacy concerns in reconstructed experiences. *Proc. ACM Hum. Comput. Interact.* 5(CSCW2), 1–25. doi:10.1145/3476078

Wang, M. (2020). Social VR : A new form of social communication in the future or a beautiful illusion? *J. Phys. Conf. Ser.* 1518, 012032. doi:10.1088/1742-6596/1518/1/012032

Wenninger, S., Achenbach, J., Bartl, A., Latoschik, M. E., and Botsch, M. (2020). "Realistic virtual humans from smartphone videos," in 26th ACM Symposium on Virtual Reality Software and Technology, Virtual Event Canada (ACM), 1–11. doi:10.1145/3385956.3418940

Wong, A., Ho, S., Olusanya, O., Antonini, M. V., and Lyness, D. (2021). The use of social media and online communications in times of pandemic COVID-19. *Journal of the Intensive Care Society* 22, 255–260. doi:10.1177/1751143720966280

Yampolskiy, R. V., Klare, B., and Jain, A. K. (2012). "Face recognition in the virtual world: Recognizing avatar faces," in 2012 11th International Conference on Machine Learning and Applications, 40–45. doi:10.1109/ICMLA.2012.16

Yoo, I., Chang, H., Luo, X., Stava, O., Liu, C., Milanfar, P., et al. (2022). *Deep 3D-to-2D watermarking: Embedding messages in 3D meshes and extracting them from 2D renderings.* Available at: http://arxiv.org/abs/2104.13450 (Accessed May 9, 2022).

Zheng, Z., Yu, T., Wei, Y., Dai, Q., and Liu, Y. (2019). DeepHuman: 3D human reconstruction from a single image in 2019 IEEE/CVF International Conference on Computer Vision (ICCV), 7738–7748. doi:10.1109/ICCV.2019.00783