World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:10, No:8, 2016

Identity Management in Virtual Worlds Based on Biometrics Watermarking

S. Bader, N. Essoukri Ben Amara

***Abstract*—**With the technological development and rise of virtual worlds, these spaces are becoming more and more attractive for cybercriminals, hidden behind avatars and fictitious identities. Since access to these spaces is not restricted or controlled, some impostors take advantage of gaining unauthorized access and practicing cyber criminality. This paper proposes an identity management approach for securing access to virtual worlds. The major purpose of the suggested solution is to install a strong security mechanism to protect virtual identities represented by avatars. Thus, only legitimate users, through their corresponding avatars, are allowed to access the platform resources. Access is controlled by integrating an authentication process based on biometrics. In the request process for registration, a user fingerprint is enrolled and then encrypted into a watermark utilizing a cancelable and non-invertible algorithm for its protection. After a user personalizes their representative character, the biometric mark is embedded into the avatar through a watermarking procedure. The authenticity of the avatar identity is verified when it requests authorization for access. We have evaluated the proposed approach on a dataset of avatars from various virtual worlds, and we have registered promising performance results in terms of authentication accuracy, acceptation and rejection rates.

***Keywords*—**Identity management, security, biometrics authentication and authorization, avatar, virtual world.

I. Introduction

IN recent years, virtual worlds have become places of migration for people from the physical world, to spaces such as Second Life, World of Warcraft, and Eve Online. Such virtual environments have gained popularity not only because they offered social entertainment and learning activities, but also in the virtual economy and the rise of the total trading volume and the average income per user [1]. According to eMarketer, global revenues in virtual goods reached $8 billion in 2015, up from $3 billion in 2010 [2]. Actually, most virtual worlds generate revenues from the conducted transactions such as purchasing virtual items, and buying or renting lands. Furthermore, nearly all the virtual worlds have an option of exchanging currency online [2]. Such an economy is based on the activities of its users, who perform economic, social and political transactions as an exchange of values among partners, as in the real world [1].

The existent virtual world access mechanism is only based on using passwords, user names, and avatars. These virtual characters are used by people to represent them in virtual spaces, to depict their digital identity, to build social relationship, to participate in communities, and to collaborate in business activities. Fig. 1 shows samples of some users' avatars in virtual worlds. Today, the users of virtual worlds choose, create and customize their avatars in the form of graphical designs that can take on more and more realistic details, depending on different settings of the virtual space, e.g. skills, style, sex, attire, and race.

Virtual world users have the opportunity to embody multiple avatars that did not necessarily resemble them physically and behaviorally [3]. In fact, avatars can be considered pictures for creating anonymous identities for various purposes, for instance profiles on websites, players in video games, and residents in virtual worlds. Consequently, these virtual characters allow their owners to step outside of their true identity. Thus, users may never know the person behind the digital mask identity provided by avatars, which may eventually represent cybercriminals.

Actually, virtual worlds have attracted the unwanted attention of both hackers and criminal organizations. Several research works have reported an increase in attacks on virtual worlds, in particular the massive online role-playing multiplayer games like Second Life and World of Warcraft [4]. Cybercriminals exploit these environments for fraud and other illegal activities, including money laundering, financial attacks, massive online multiplayer privacy risks, cheating, identity theft, intellectual property crimes [5], cyber-terrorism acts [6], etc.

Due to identity masking, users have created multiple kinds of avatars interacting with other residents to steal their virtual goods and objects, and to acquire fraudulently sensitive information such as usernames, passwords and credit card details. Avatars can also be exploited in virtual worlds to kill users' avatars through swords or weapons and assume their assets, or even to destroy and move objects [4]. Some of the avatars' criminal activities are illustrated in Fig. 2.

Security incidents in virtual worlds can create serious disruption of residents' activities, items and identities. Hence, the security issues within these spaces must be considered. Indeed, several studies [7]-[9] have investigated the need to install security properties in virtual worlds to try to provide solutions for their users' needs with regard to authenticity, privacy, integrity, confidentiality, protection against malicious attacks, risk-free activities, etc.

Today's virtual world residents need new methods of developing security and trust in these environments. Wherever uncontrolled access is available, illegal activities may occur. However, with expanded access to these spaces, it is becoming

S. Bader is with SAGE Research Unit, National Engineering School of Sousse, University of Sousse, Tunisia (e-mail: samira_bader@yahoo.fr)

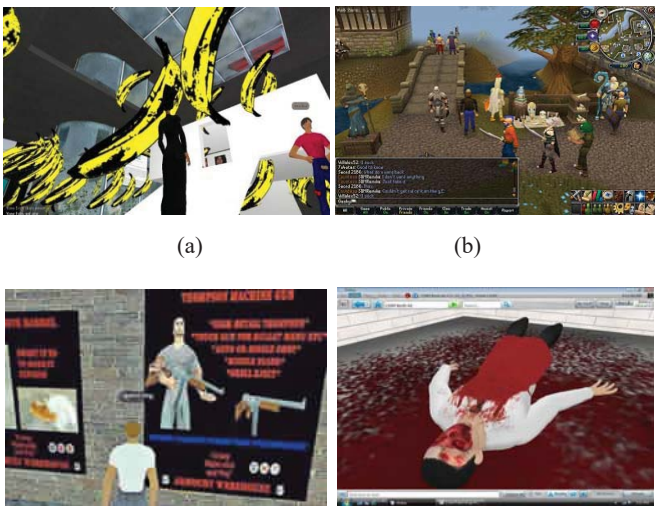
N. Essoukri Ben Amara is with SAGE Research Unit, National Engineering School of Sousse, University of Sousse, Tunisia (e-mail: najoua.benamara@eniso.rnu.tn).

increasingly difficult to authenticate the identity of any virtual- world resident. Doing electronic transactions in the virtual world requires some forms of authentication to ensure that authorized users and their representative avatars are authentic. In any case, such an identity verification system is necessary for security access and trust reasons, which require the implementation of appropriate tools for identity management [1].

(a) (b)

(c) (d)

Fig. 1 Samples of avatars from four popular virtual worlds (a) Second Life, (b) Twinity, (c) The SIMS social, (d) IMVU



(a) (b)

(c) (d)

Fig. 2 Examples of avatars' criminal activities: (a) Grey goo affecting virtual world, (b) Virtual goods property of Jagex theft, (c) Virtual jihadist, (d) Avatar killing

In this paper, we discuss the security issues in virtual worlds related to identity management. We also put forward a solution for virtual identity management and protection based on the integration of biometrics in the authentication and authorization processes.

The rest of the paper is organized as follows. In Section II, we discuss the security of identities in the virtual world. In Section III, we expose the proposed identity management approach. Section IV details the performance evaluation of our approach and the experimentation results. We finish this paper with a conclusion and some perspectives for future works.

II. Securing Virtual World Identities

In virtual worlds, users are anonymously emerged with their virtual identities represented by their avatars. Contrary to a user's real identity, a virtual one does not obey to any rules, e.g. legislative, social or ethical rules. Hence, virtual identities are generally considered unreliable, untrustworthy, and phishing [10]. As a result, criminals are assuming identities to gain access to virtual world resources. The key requirement for secure access into a virtual world is to manage user identities.

Identity management is loosely defined as the process involving emerged technologies for user's identity information handling and resource access controlling [11]. It covers a multitude of solutions that provide a variety of security levels and user administration. It aims to improve security while managing identity attributes and credentials (like identifying who they are, setting the identification/authentication method, defining the roles and rights, etc.) [11]. The access management allows any authentic identity to have access to online resources or services and prevents unauthorized entities from accessing the protected online information, based on previously granted authorizations [12]. Identity and access management includes authentication and authorization procedures, which will be discussed below.

A. Authentication

Authentication is the process of verifying the identity of any individual that requests access. It represents the access control component through which the user gains an initial access to a resource while providing adequate credentials. Identity authentication technologies are diversified and might be known, such as password, personal identification numbers or a secret code, or possessed, like a cryptographic key, digital certificates using a public key infrastructure, an ATM card, a smart card, a cellphone SMS, or a biometric characteristic [13]. Biometric authentication technology is more reliable, safer and more convenient than other classical basic-level authentication techniques. Biometric recognition, as a means of personal authentication, is an emerging area focusing on reinforcing security and convenience. Actually, the biometric recognition of both people and artificial entities is becoming more and more mature and applied in a lot of domains. A variety of biometric features such as fingerprints, iris scans, facial scans, voice, keystroke latencies in word-processing, etc. [14], have been used in order to match individuals to their digital identity ownership.

B. Authorization

Closely associated with authentication is authorization, which determines whether a user is permitted to access a particular resource. Authorization is the core module that implements the level of rights and privileges available to the authenticated entity. It consists in the process of determining what kind of access should be granted to the user based on

their credentials, attributes (information about the user, as membership or role), and trust (agreement between different parties and systems for sharing identity information) [12].

An unauthorized access is the opportunity that an unauthorized entity profits from the illegitimate access to certain resources and the capability to alter with that access. It is also related to impersonation, which means that a person presents credentials to claim an impostor identity [15]. This type of attack in an authorization procedure is due to the lack of a robust access controlling what remains an identity authentication solution. In any case, authentication and authorization are processes setting up an acceptable level of confidence that a unique identifier refers to as an individual entity. The identifier might be a biometric template, a username, a public-key, etc.

III. Proposed Identity Management Approach

In the proposed identity management procedure, both users and their representative avatars in virtual worlds are the subject of authentication and access authorization. Individuals and avatars not only have an identity but also they need to prove it while they are conducting transactions, which rely on authentication. Biometrics is the key component of the authentication process ensuring that only verified identities are able to access the resources in the virtual world. In our study, biometrics can create a strong, non-revocable link between a physical person and the corresponding virtual personage as the owner of a given biometric feature.

The process model for identity management of authenticating both the user and the representative avatar is shown in Fig. 3. This framework shows the basic components of the suggested approach: i) the user verification, enrolment and registration; and, ii) the authentication and authorization requests.

A. Identity Verification and Biometrics Enrollment

Users are enabled to log on within the identity management procedure for account registration and also for access privileges to a specific resource. As shown in Fig. 3, once the account is created, the user must provide their fingerprint image as a biometric authentication method. The employment fingerprint modality for recognition has been widely used in commercial and forensic areas. They have the advantages of both ease of use and low cost. A variety of devise types for fingerprint acquisition are becoming more and more sophisticated, and embedded into mobile phones, laptops, etc. This technology has been applied on people authentication during electronic transactions, access control systems and other application domains. Whereas biometrics contains accurate and sensitive information about people, we have implemented a cryptology protection technique for a fingerprint template, which has been further used for avatar watermarking.

B. Avatar Watermarking

We recall that watermarking consists in embedding a watermark into hosting information. Digital watermarking has been widely used to counter security issues, e.g. property and copyright protection and document and author authentication [16]. In the proposed identity management approach, we have utilized the watermarking technique for authentication of avatars proposed in [17]. In [17], the authors put forward two watermarking approaches of 2D and 3D avatar faces. The discretized fingerprint was used as an embedded watermark in the images and the 3D mesh model faces. The insertion of a binary mark was processed into the 3D mesh of an avatar's face. Fig. 4 shows the main steps in the developed watermarking process of the 3D faces.

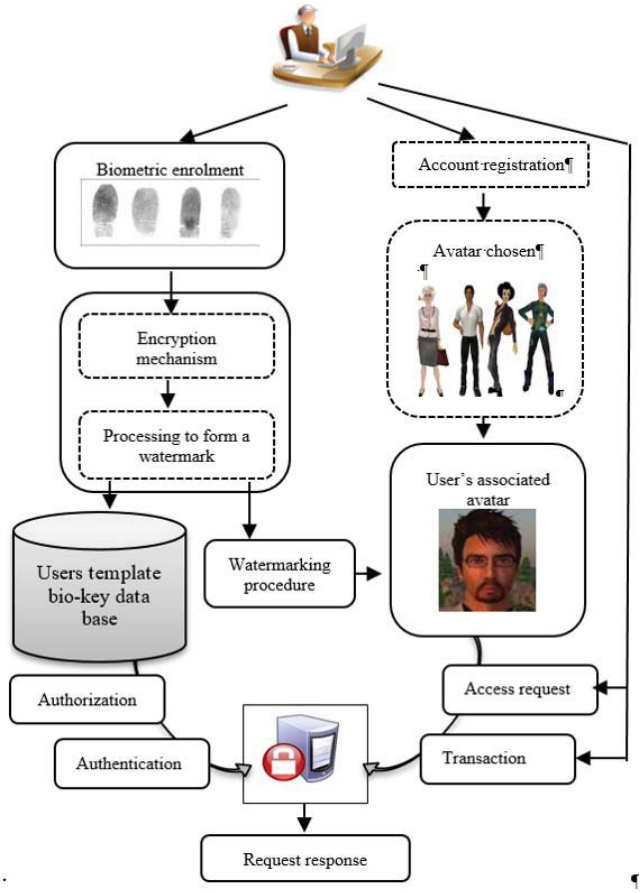


Fig. 3 Identity management and access control

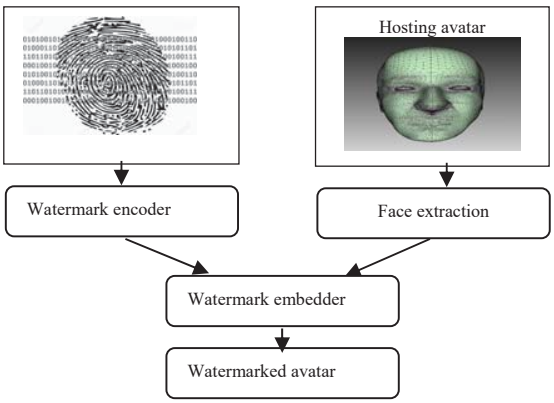


Fig. 4 3D avatar face watermarking

C. Internal Authentication and Authorization

Authentication is the process of verifying the authenticity of any emerged identity. It is based on the extraction of the watermark from the cover asset. Authorization, in our framework, is the act of checking if an avatar has the proper permission to access a particular file or perform a particular action, assuming that the avatar has successfully been authenticated. The authentication aims to verify the identity of the watermarked avatar while acceding into the virtual world. This process requires that the extracted watermark corresponds to the claimed identity of the avatar. The extraction of the embedded mark is performed by our algorithm, which was developed in [17]. For the access control mechanism, typical authorization checks involve querying for approving avatar credential possession. Fig. 5 illustrates the authentication and authorization flowchart.

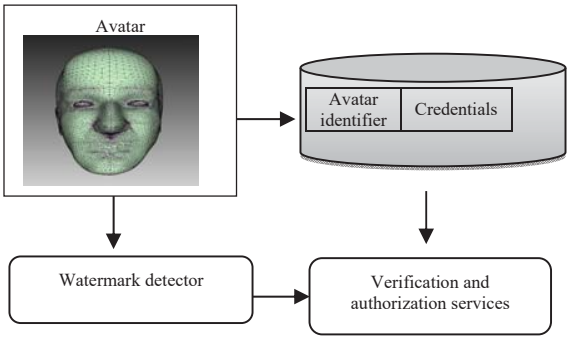


Fig. 5 Authentication and authorization flowchart

IV. Performance Evaluation and Results

The main goal of user and avatar authentication is to validate the identity of any users and their respective avatar. In the proposed identity management approach, access into the virtual world necessitates a strong authentication mechanism based on biometrics. At the same time, attackers attempt to penetrate information resources with their compromised objectives concerning the mechanism that protects the resources from any unauthorized access. While authentication mechanism threats are various, we are interested in the potential attacks possibly occurring in virtual worlds. Most of these attacks were discussed in [17] and could be summed up into biometric template attacks, watermarking attacks, and avatar stealing and exploiting attacks. To evaluate the performance of the identity management approach, we have conducted a series of tests considering the aforementioned attacks in the virtual world.

A. Protection Against Attacks

If an imposter does not have any credentials to access into the virtual world, he may seek to gain unauthorized access by attacking the authentication mechanism. In this case, the biometric template, the watermark and the avatar need a security mechanism that is able to protect them from hackers. For the biometric-template security, we have opted for the cancelable biometrics, which can preserve user privacy, since the original biometric feature is never exposed in the avatars' authentication process. For instance, this method ensures the protection of the biometric template with the generation of an auxiliary and non-invertible data. We have implemented a blind multi-watermarking process for the protection of the watermark against some attacks, which consists of applying some transformation into the watermarked avatars to modify, or destroy their identity's proof. These kinds of attacks can be related to signal processing, like geometric transformation, adding noise and connectivity attacks, or linked to the avatar personalization by adding accessories, for example. We have also verified the reliability of the authenticator while an impostor seeks to gain access into the platform resources. Indeed, we have used dummy fingerprint templates in order to state the level of distinguishing genuine identities from those of impostors.

B. Authentication Accuracy Evaluation

When biometrics are used for authentication for controlling physical or logical access, the objective of the application is to prevent unauthorized access under all circumstances. The key metrics for a biometric-solution evaluation are the False Accept Rate (FAR), which is also called the False Match Rate (FMR), and the False Reject Rate (FRR), sometimes referred to as the False Non-Match Rate (FNMR). In biometrics recognition, both of the FRR and the FAR are important. In our application, the authorized-user acceptance rates, FAR and FRR, are used to indicate whether the secret watermark is correct or not. The authorized-user acceptance rates and the FNMR might verify accuracy. Otherwise, these metrics measure the exactitude of the matching process. FAR expresses the ability degree of distinguishing a genuine identity from an imposter. Indeed, the authenticator process has to allow access to only legitimate users who are previously registered in the database.

C. Results

The accuracy of the access control is based on the rate in which geniuses and impostors are accepted or rejected. The authorized-user acceptance rates, the FAR and the FRR are respectively calculated according to (1)-(3). The authentication process is based on the similarity level between the original biometric template and the extracted one. Thus, we have utilized the Normalized Cross Correlation (NCC) to quantify this similarity degree. For the experimentation tests, we have disposed of the digital fingerprint database (DBII-PolyU database) and the 3D avatar mesh database [18]. We have conducted various tests. Table I summarizes the obtained values of the authorized-user acceptance rates and the FRR in the case of the absence and presence of signal processing attacks and geometric ones. Fig. 6 shows the FAR values corresponding to an attack for different NCC thresholds using the dummy fingerprint template.

$$Authorized-user\ acceptance\ rate\ \% = \frac{Number\ of\ correct\ acceptance}{Number\ of\ authorized\ user\ attempts} * 100 \quad (1)$$

$$FAR\ \% = \frac{Number\ of\ false\ acceptance}{Number\ of\ impostor\ user\ attempts} * 100 \quad (2)$$

$$FRR\ \% = \frac{Number\ of\ false\ rejection}{Number\ of\ authorized\ user\ attempts} * 100 \quad (3)$$

TABLE I
AUTHORIZED USER, FRR AND FAR FOR DIFFERENT ATTACKS

		NCC threshold	Authorized- user acceptance rates	FRR	FAR
No attacks		1	100	0	-
Signal processing and geometric attacks	Rotation	1	100	0	-
	Translation	1	100	0	-
	Scaling	1	100	0	-
	Noise value <0.3 %	1	99.5	0.45	-
	Noise value <0.5 %	1	98.5	1.55	-
		0.8	100	0	-
Impostor attacks	Dummy fingerprint	1	-	-	0
	Modifying a stolen avatar (BER <0.5)	1	-	4.87	0

The suggested approach is robust against geometric and signal processing attacks and impostor phishing. Actually, we have registered authorized user rates of 100 % in the case of the absence and presence of the majority of attacks. In addition, the authentication process does not permit rejecting an authentic identity according to the obtained the FRR values at an NCC threshold value equal to 0.8. Furthermore, the authenticator is reliable in distinguishing genuine identities from impostors, when a hacker uses a dummy fingerprint or a stolen impression. Hence, attackers cannot access the contents of the virtual world server.

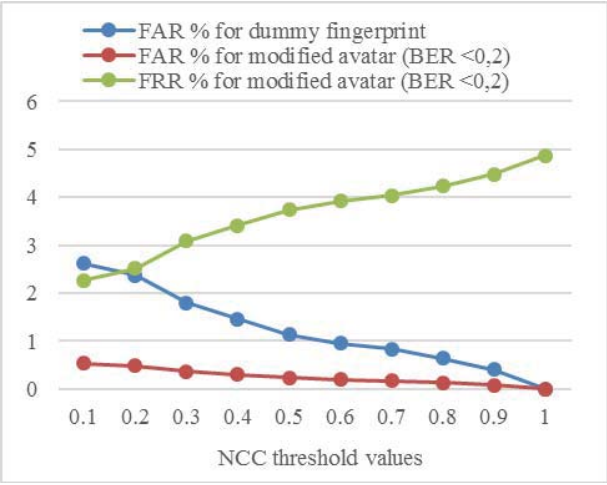


Fig. 6 FAR and FAR for different threshold values

V. CONCLUSION

This paper introduces a method for securing virtual identities and access into virtual worlds through an identity management solution. This technique is based on the integration of a strong biometrical authentication and authorization mechanism. This enables only genuine users who have an authentic identity to gain access. We have evaluated the performance of the developed approach considering attacks that occurred in virtual worlds. The authentication accuracy has been quantified utilizing three key metrics: the authorized-user acceptance rate, the FAR and the FRR. In our experimentation, we studied the impact of the NCC threshold value on the FAR and the FRR, which are always correlated. The approach shows promising results at a high level of an NCC threshold. As a future work, we are constructing our virtual space that will integrate our proposed identity management approach.

REFERENCES

[1] M. Buzinkay, *Commercial Transactions in the Virtual World: Issues and Opportunities*, City University of HK Press, pp. 245-260.
[2] C. Pearce, B. R. Blackburn, C. Symborski, "Virtual worlds survey report: a trans-world study of non-game virtual worlds – demographics, attitudes, and preferences," 2015.
[3] H. Lin, H. Wan, "Avatar creation in virtual worlds: behaviors and motivations", Computers in Human Behavior, vol. 34, pp. 213-218, 2014.
[4] C. Mettouris, V. Maratou, D. Vuckovic, G. A. Papadopoulos, and M. Xenos, "Information security awareness through a virtual world: an end-user requirements analysis," in Proc. 5th International Conference on Information Society and Technology – ICIST 2015, Kopaonik, 2015, pp. 273-278
[5] F. Farahmand, A. Yadav, and E. H. Spafford, "risks and uncertainties in virtual worlds: an educators' perspective," Journal of Computing in Higher Education, vol. 25, no. 2, pp 49-67, 2013.
[6] A. Ar-Raqib, E. Mozley Roche, "Virtual worlds real terrorism," Den Haag: Aardwolf Publications, 2010, pp. 75-85.
[7] C. Y. Lee, M. Warren, "Security issues within virtual worlds such as Second Life," in Proc. 5th Australian Information Security Management Conference, Perth, 2007, pp. 44.
[8] A. Dudley, J. Braman, Y. Wang, G. Vincenti, and D. Tupper, "Security, legal, and ethical implications of using virtual worlds," in Proc. 14th World Multi-Conference on Systemics, Cybernetics and Informatics, Orlando, 2010.
[9] B. Carminati, E. Ferrari, and M. Viviani, "Security and trust in online social networks," Synthesis Lectures on Information Security, Privacy, & Trust, vol. 4, no 3, pp. 1-120, 2013.
[10] J. Kultan. P. Schmidt "Identity and threats in the virtual world," Management Information Systems. vol. 7, No. 4, pp. 021-025, 2012.
[11] R. Cowles, C. Jackson, and V. Welch," Identity management for virtual organizations: a survey of implementations and model," in Proc. 9th IEEE International Conference on e-Science, 2013.
[12] G. Cruz, A. Costa, P. Martins, R. Gonçalves, and J. Barroso, "Toward educational virtual worlds: should identity federation be a concern?" Educational Technology & Society, vol. 18, no 1, pp. 27–36, 2015.
[13] Y. Liu, Y. Chai, and Y. Liu, "Study on the model and algorithm of Internet trusted identity authentication system," in Proc. IEEE 12th International Conference on e-Business Engineering, 2015
[14] W. A. Shier, S. N. Yanushkevich, "Biometrics in human-machine interaction," in Proc. IEEE International Conference on Information and Digital Technologies, 2015, pp. 305-313.
[15] T. A. P. Sidhi, "Enhancing the network security with gray code," World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, vol. 10, no 3, pp. 1-5, 2016.
[16] Y. WU, "Data hiding by vector quantization in color image," World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, vol. 9, no 5, pp. 1155-1162, 2015.
[17] S. Bader, N. E. Ben Amara, "A securing access approach to virtual worlds based on 3D mesh watermarking of avatar's face," in Proc. 4th International Conference on Image Processing Theory, Tools and Applications, Paris, 2014, pp. 1-6.
[18] S. Bader, N. E. Ben Amara, "SID-avatar database: a 3D avatar dataset for virtual world research," in Proc. First International Conference Image Processing, Applications and Systems, Hammamet, 2014, pp. 1-5.