Secure Virtual World Access Based on Biometric Watermarking of 3D Avatar Face Mesh

Samira Bader and Najoua Essoukri Ben Amara
SAGE Research Unit, National School of Engineering, Sousse, Tunisia

Abstract
Owing to the absence of a reliable access control tool in the virtual worlds, these spaces are more and more exposed to cybercrimes. In the guise of fictive identities, cybercriminals involve multiple avatars to perform illegal activities. To deal with this, setting up an access control mechanism in these digital environments is becoming necessary. In this paper, we propose an original access control solution based on an identity authentication approach that can assure the security of virtual spaces. Thus, only authentic users and respective avatars are allowed to accede into the virtual worlds and exploit their resources. The access control is based on the biometrics technique. The identity of virtual-world users’ is authenticated through their provided fingerprint while requesting the access. These fingerprints are later coded to generate biometric signatures serving as watermarks. In order to join the individual to their respective avatar, these signatures are inserted into the avatars’ face through a watermarking algorithm. The watermarking process is applied to the 3D avatar facial meshes. The embedded watermark is extracted when necessary to authenticate the avatars. The avatar identity is confirmed as authentic on the basis of an acceptance threshold of correlation values computed between the original watermark and the extracted one. The experimental investigations show that the proposed watermarking algorithm can keep a good imperceptibility and is robust facing up most of the attacks that could appear in a virtual environment. The registered authorized-user, FRR and EER rates at different attacks prove that the suggested approach is also efficient to distinguish genuine identities from impostor ones.

Keywords: cybercrime, securing virtual world, access control, authentication, watermarking, biometrics, fingerprint, 3D avatar facial meshes

I. INTRODUCTION
Virtual worlds have initially emerged as means of entertainment and communication, then they have gained not only popularity but also importance in serious application domains such as learning, training, and business [1]. Thanks to the evolution of the Web-based applications which have greatly facilitated the use of these spaces by offering interactive digital spaces for their users who practice, in a simulated reality, more and more activities including sharing data, holding virtual congresses and meetings, networking and hosting virtual seminars and lectures, and running research. In these environments, users incarnate their respective digital representation called avatar. Avatars are virtual characters or personages, which are the residents of the virtual world. They are utilized by their owners not only to interact with others, but also to be used in various activities including money transfer, electronic transactions, selling virtual items, and exchanging virtual currencies for actual money. Table 1 provides examples of application domains into 3D virtual worlds.

Despite the great success of these spaces, they are potentially requiring a constant care to protect them against illegal activities, which are diversified such as money laundering, virtual goods theft, psychological violence, terrorists financing, and identity theft and usurpation. These virtual-world security threats are originally caused by the absence of an efficient access control procedure to these spaces. Currently, during their access into the virtual spaces, the users are only identified through their avatar and their fictive name as their password. These avatars can represent both the real users’ identity in the virtual worlds and their masked ones. With the development of 3D graphics, users have various abilities with regards to their characters, such as changing their body parts, storing artifacts, adapting their appearance by changing clothes, communicating with other avatars, etc. Consequently, the same character can be duplicated and shared between different users, reproduced, falsified, or stolen to be used in spying and other criminal activities. In addition, owing to the variability of the offered design tools and technology of virtual worlds, these characters vary from one space to another depending on the user interfaces, software, and graphic tools. Therefore, cybercriminals have emerged multiple avatars to steal users’ money, virtual goods and objects, sensitive information, and avatars [2].

To address the problems of criminality in the virtual worlds, authenticating and identifying non-biological entities such as intelligent software agents, domestic and industrial robots, and avatars, while requesting the access into virtual world resources, is becoming a challenge. The need of such a recognition and verification mechanism is diversified including: access control to information or system resources, tracing every task, defining an authorization strategy, securing the interaction, etc. The science of recognizing non-biological entities, known as Artimetrics, was firstly introduced in [3]. Since then, some biometric recognition methods have been extended to verify and identify the virtual world avatars [4, 5]. However, the proposed authentication techniques are not efficient enough to secure and control the access into the virtual worlds or to confirm the veracity of any avatar identity. Figure 1 shows the most frequent causes of both 2D and 3D avatar authentication failures.
The purpose of this investigation is to develop a reliable secure access control tool of the virtual worlds that can ensure the protection of private information. The proposed solution is based on exploring the technique of biometrics to join the identity of the virtual world users to their avatars. Our main contribution is to model an adequate watermarking algorithm that embeds in the 3D avatars’ face a signature of the fingerprint trait, which represents the identity of the avatar’s owner. We opt for the biometric characteristics of the fingerprint. This is justified by the frequent use of this biometric modality and the integration of the fingerprint readers into several devices (mouse, iPhone, iPad, etc). The rest of this paper is organized as follows. The second section briefly reviews the main techniques utilized for identity verification based on watermarking and/or biometrics. Our proposed approach is detailed in the third section. The fourth section describes the 3D avatar database used for the experimentation tests. In the fifth section, the experimental results are listed and analyzed. The conclusion and the future work are given in section 6.

Table 1: Selection of applications in 3D virtual worlds

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples of 3D virtual world</th>
</tr>
</thead>
<tbody>
<tr>
<td>Immersive virtual world/reality</td>
<td><img src="image1" alt="Example images" /></td>
</tr>
<tr>
<td>Metavers</td>
<td><img src="image2" alt="Example images" /></td>
</tr>
<tr>
<td>Social virtual world</td>
<td><img src="image3" alt="Example images" /></td>
</tr>
<tr>
<td>Serious virtual world</td>
<td><img src="image4" alt="Example images" /></td>
</tr>
<tr>
<td>Virtual lounge</td>
<td><img src="image5" alt="Example images" /></td>
</tr>
<tr>
<td>Educational / Learning</td>
<td><img src="image6" alt="Example images" /></td>
</tr>
<tr>
<td>Games</td>
<td><img src="image7" alt="Example images" /></td>
</tr>
</tbody>
</table>

Figure 1: Illustrations of some avatar-authentication problematics: (a) avatar physics variability, (b) similarity between avatars (c) duplication of avatars (d) personalization of avatars by adding accessories

II. AUTHENTICATION BASED ON WATERMARKING AND BIOMETRICS

The classical human identification/verification techniques, such as passwords, keys, and smart cards reveal many limitations facing up theft, loss, hacking, and falsification problems. The utilization of the characteristics, proper to each human, known as biometrics, is increasingly used in several application domains to respond to the needs in terms of security, like access control, people and virtual agent recognition, passports, electronic transactions, etc. For a more reliability of these systems, the biometric techniques are usually reinforced with other appropriate methods like steganography, cryptography, watermarking, or a combination of the three techniques [6]. In this section, we recall some basic and useful watermarking and biometric watermarking notions.

A. Watermarking

Watermarking consists in invisibly embedding a watermark in a digital content (an audio, a video, or a 3D object) without altering its appearance. The watermark could be a mark (e.g. image, logo, text) or a biometric signature. The application areas of digital watermarking are numerous: control and copyright protection, broadcast monitoring, fingerprinting, indexing, medical application, content authentication, etc [7]. The watermarking of 2D images and 3D objects has been subject of various research works. The watermark embedding may be carried in the spatial domain or in the transformed ones (spectral and multi-resolution spaces). The suggested methods can be mainly classified into different categories according to the classification criteria, which are namely imperceptible or perceptible, robust or fragile, blind or non-blind, and spatial or spectral.

The watermarking of 3D models was firstly introduced by Ohbuchi and al. [8]. With the widespread use of 3D models on the Internet, computer graphics, acquisition and printing, and CAD technology, the digital right management of the 3D models has become a challenge. Since then, a variety of techniques has been employed to develop watermarking approaches for 3D objects. 3D object watermarking involves embedding the watermark into the 3D object meshes by...
modifying their geometrical or topological primitives. For example, the vertex coordinates can be adjusted to insert the watermark. Alternatively, the mark can be embedded by modifying the 3D model topology, by slightly varying the spectral coefficients, or by organizing the mesh according to the ordered ring facets [9]. In other developed techniques, the merits of both spatial and frequency domains are combined for the watermark insertion [10].

For more information about 3D object watermarking, we invite the reader to consider the more recent references in Table 2.

B. Biometric watermarking

Biometrics has been successfully employed for trusted human identity recognition using one’s physiological characteristics (the face, the ear, the fingerprint, the palmprint, etc), behavioral characteristics (the gait, the signature, the handwriting, etc) or biological characteristics (the AND, the saliva, etc). Since the biometric approaches can ensure a reliable authentication of legitimate users and identification of imposters, they have been basically applied to control the access, respond to the security threats, and become the most efficient-known way for securing an individual’s identity [11]. Besides, watermarking has been suggested as an efficient solution to enhance the functionality and security of the biometric authentication systems [12] and to secure the access into the digital right management systems [13]. In fact, these systems are potentially exposed to malicious threats such as database system spoofing and biometric template stealing at the communication channel of the biometric system [14]. Watermarking has been also proposed in the multi-biometrics fusion to improve the system performance [15]. In [16] a new approach is suggested for biometric watermarking of avatars. The proposed algorithm was evaluated on a database of 3D avatar facial meshes collected from the virtual world Second Life. The experimental results are promising; however, some details about the attacks and authentication scenarios still need to be elaborated. In this study, we aim to enhance the 3D avatar watermarking algorithm in practical authentication situations. The identity of users is necessarily verified while requesting the application access and also while processing the avatar authentication stage, as well.

III. PROPOSED APPROACH

The proposed approach relies on a reliable access control process, which allows only previously enrolled and authentic users to accede and exploit virtual world resources. The core idea is to authenticate both users and their individual avatars. To deal with this, the users are invited to subscribe via the offered interface and to choose their representative avatar. During the subscription session, users provide their fingerprint image, which will be transformed into the secret message and saved in the watermark database for later identity verification requests. The biometric watermarking technique is utilized for authentication purposes as to identify the avatars’ possessor. After the user chooses an avatar, the biometric signature is inserted into the avatar’s face. Then, the watermarked avatar is merged into the platform environment. When the avatar attempts to access the virtual world resources, the authentication stage appeals the watermark extractor to recover the identity legitimacy information. Based on the computed similarity measure between the loaded watermark from the database and the extracted one, the system authorizes or not the avatar to access the virtual space. The block diagram of the system is outlined in Figure 2. This framework shows the basic components of the system. In what follows, we describe the main modules of the proposed approach.

| Table 2: State of the art of watermarking 3D objects |
|---------|----------------|------|-----------------|
| Ref     | Techniques                          | Characteristics | 3D-model databases               | Tested attacks                              |
| [17]    | Discrete cosine transform            | Robust          | Non-Blind                     | Cropping                                    |
| [18]    | Geometric entity substitution algorithm | Non-Blind       | Robust                        | Translation, Rotation, Scaling, Entity deletion |
| [19]    | Vertex-norms distribution modification and quadratic programming | Robust          | Blind                         | Cropping, Noise, Smoothing, Simplification, Rotation, Scaling, Translation, Vertex reordering |
| [20]    | Vertex curvature 3D mesh watermarking algorithm | Robust          | Blind                         | Cropping, Noise, Smoothing, Simplification, Rotation, Scaling, Translation, Vertex reordering |
| [21]    | Vertex displacement based on surface distortion criterion function minimization | Statistical     | Robust, Blind                 | Smoothing, Simplification, Resampling, Quantization, Affine transformation, Vertex reordering |
| [22]    | Spectral mesh compression and vertex norm distribution modifications with an evolutionary optimizer | Blind           | Good visual quality           | Translation, Scaling, Rotation, Noise, Simplification |
| [23]    | Discrete cosine transform and 3D model information redundancy | Robust          | Blind, Good imperceptibility  | Translation, Rotation, Scaling, File attack, Noising, Smoothing, Vertex coordinate quantization, Cropping |
A. Watermark generation tool
The goal of this phase is to generate the watermark, a binary message extracted from the users’ fingerprint. The algorithm for the fingerprint discretization is developed on the basis of the work in [24, 25, 26, and 27]. Once acquired, the user’s fingerprint images are subjected to required pretreatment operations for image alignment and region-of-interest detection. After that, the Gabor filter technique is utilized to extract energy and amplitude features from the fingerprint images. The obtained feature vector is latterly coded into a binary message by a quantization of the spatial feature distribution. For the reliability of data transmission, a set of parity bits are extracted from the binary feature vector and stored in the database. These bits are utilized to accomplish the recovery of the binary vector. Then, the obtained binary vector is transformed into a hash code using a hash function ensuring its privacy. The generated biometric marks are at last saved in the watermark database to be further used in the authentication process.

B. Hosting data extraction
The 3D meshes of the avatar face represent the host data that is used later for watermarking processing. The literature shows that the 3D mesh face extraction has been addressed in the development of a biometric system based on 3D face modality [28, 29]. There are different approaches for cropping the face surface from the head, which utilize the sphere technique centered at the noise tip [30, 31]. Another suggested technique is based on the clustering of a 3D point utilizing the texture information available in the texture map [32]. A further method consists in the extraction of the frontal face area exploiting the ordered-facets ring [33]. In the proposed approach, the extended multi-ring neighborhood based on a 3D mesh segmentation algorithm is utilized to extract the avatar face meshes. This technique decomposes the object into meaningful regions [34]. First of all, the avatar’s head mesh is segmented to extract its different parts like the face, the ears, the eyes, and the profiles. Then, the boundaries corresponding to the polygons’ union of each part are localized. Afterwards, we extract the mesh part representing the hosting information, as it is illustrated in Figure 3.

C. Watermark embedding
The watermark embedding step consists in inserting the mark bits into the corresponding face mesh. In the suggested approach, the ring structure of the facial mesh is exploited to insert the watermark in an iterative process. In fact, the watermark is repetitively embedded according to the number of rings, so the number of repetitions depends on the ring size of the hosting mesh. The payload capacity also depends on the number of rings in the mesh. Therefore, the number of embedded watermarks changes from one avatar face to another. The embedding stage is firstly performed by changing the order of the triangles’ vertices according to the distance between each triangle vertex and the facet center, and secondly by using the Least Significant Bit (LSB) technique. This technique originally designed to work with 2D images, is easily extended to 3D object watermarking [35].

There corresponds for each avatar face a mesh M (F, V), which is composed of a set of facets and vertices. The facets F = \{f_1, f_2,...,f_m\} of the m triangles f_i are described by their connectivities (v_{i1}, v_{i2} and v_{i3}) of the k^th triangle. The vertices V = \{v_1, v_2,...,v_n\} of the n vertices v_i are described by their 3D coordinates (v_{ix}, v_{iy} and v_{iz}). The detailed embedding steps are summarized below.

**Step 1:** Extract the left and right j^th rings from the facial mesh representing the hosting data.

**Step 2:** For the k^th triangle of this ring, compute its centroid coordinates.

**Step 3:** Calculate the distances value (dv_{k1}, dv_{k2} and dv_{k3}) between the connected vertices (v_{k1}, v_{k2} and v_{k3}) and the centroid of the corresponding triangle f_k.

**Step 4:** Read the k^th secret bit from the binary watermark.

**Step 5:** Adjust the order of the three vertices of the k^th triangle with respect to the values of the watermark and their distances dv_{kj}.

If the watermark secret bit is equal to 1, we rearrange the vertices (v_{k1}, v_{k2} and v_{k3}) according to the increasing distance order (dv_{k3}, dv_{k2}, dv_{k1}) and we substitute the three LSBs of the vertex v_{k1} coordinates by the sequence 111. Otherwise, we rearrange the vertices (v_{k1}, v_{k2} and v_{k3}) according to the decreasing distance order (dv_{k1}, dv_{k2} and dv_{k3}) and we substitute the three LSBs of the vertex v_{k3} coordinates by the sequence 000.
Step 6: Repeat steps 2-5 until all the watermark bits are embedded.

Step 7: Repeat all the steps until the number of the watermark bits exceeds the number of facets.

D. Watermark extraction and classification

The verification of the identity of the resident during its access to various resources of the virtual world and during the establishment of electronic transactions is to find the watermark that was inserted into the mesh of the face of the corresponding avatar. To extract the embedded bits, the avatar face meshes are scanned in the same order as in the insertion process on a blind mode. The watermark extraction and classification steps are listed below:

Step 1: Do the same instructions as in steps 1-3 in the watermark embedding procedure.

Step 2: If the three vertices of the \( k \)th triangle are increasingly ordered according to their distances to the centroid, we assume that the bit is equal to 1 and we find it out in the LSB of the first vertex. Otherwise, we assume that the bit is 0 and we find it out in the LSB of the last vertex.

Step 3: Repeat steps 1 and 2 until all the binary messages are extracted.

Step 4: Load the watermark from the database corresponding to the claimed identity.

Step 5: Calculate the Normalized Cross Correlation (NCC) between the stored watermark and the extracted one.

\[
NCC(W, W^*) = \frac{\sum_{i=1}^{M} W(i) W^*(i)}{\sqrt{\sum_{i=1}^{M} W(i)^2 \sum_{i=1}^{M} W^*(i)^2}}
\]  

(1)

where and W are \( W^* \) respectively the embedded and extracted watermark, M and i are respectively the length and the index of the watermark.

Step 6: Classify the obtained NCC according to the defined acceptance threshold.

Step 7: Accept or deny the claimed identity.

IV. DATABASE

Considering that the research area of identity management in virtual worlds is recent and due to the lack of public databases, we have invested in the development of a dataset for the evaluation of the proposed approach. The database is available for virtual-world research area purposes [36]. It currently includes two sets of avatar file formats. We used the sets A and B for the experimentations detailed in this paper.

The dataset A was collected from the Second Life virtual world. Each avatar was composed by a set of meshes relative to every part of its body. The dataset B was created within the website Mixamo, which offered the opportunity to create, animate and rig 3D characters for project designing. The created avatars could be coded into various formats corresponding to the game software, which were mainly Fbx, Dae, and Bvh. Figure 4 depicts examples of the avatar head meshes from the datasets A and B.

The utilized 3D avatars were coded into the OBJ file format that describes their geometry. These OBJ files have a line-by-line organization of data; i.e., each line corresponds to a description of the geometric form by the vertex coordinates, the normal vectors by the triplet of values, the texture coordinates by odd values and the corner of the triangle by the number of correspondent vertices. Table 3 demonstrates the statistics concerning the utilized dataset for analyzing all the experiments. The digital fingerprint database DBII-Poly U was utilized for the watermark generation.

Figure 4: Examples of avatar head meshes from the (a) set A and (b) set B

Table 3: Dataset statistics utilized in the experiments

<table>
<thead>
<tr>
<th>Avatar database</th>
<th>Dataset A</th>
<th>Dataset B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of avatars</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>Mean number of vertices per face mesh</td>
<td>1132</td>
<td>2500</td>
</tr>
<tr>
<td>Mean number of facets per face mesh</td>
<td>1844</td>
<td>3000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fingerprint DBII-PolyU database</th>
<th>Number of fingerprint images for watermark generation</th>
<th>Number of fingerprint images for authentication test</th>
<th>Number of impostor fingerprint images</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>600</td>
<td>400</td>
<td>100</td>
</tr>
</tbody>
</table>

V. EXPERIMENTATIONS AND RESULTS

This study has focused upon verifying the identity of both users and their representative avatars using the embedded fingerprint features watermark. The experiments were conducted to evaluate two aspects of the proposed framework: the watermarking scheme and the authentication accuracy while controlling the access into virtual world resources. This section explores the performance of the suggested watermarking algorithm and depicts some experimental results to demonstrate its robustness. The developed algorithms were programmed with Matlab 2015a and the operating system was Windows 7.
A. Watermarking evaluation

In order to evaluate the performance of the developed watermarking scheme, three different challenging criteria, which are invisibility, distortion and robustness against attacks, are investigated.

A.1. Invisibility and distortion

The distortion of a watermarked 3D mesh comparing to the original one should be perceptually invisible. The transformation of the 3D model structure while applying the watermarking algorithm, a minimum distortion should be guaranteed. The metric used to measure the invisibility of the watermark and the distortion of the mesh is the Mesh Structural Distortion Measure (MSDM) between the original mesh and the watermarked one, defined by equation (2).

\[
MSDM(W, W') = \frac{1}{M} \left( \sum_{i=1}^{\text{LSM}} LMSD M(x_i, y_i) \right)^{\frac{1}{2}}
\]

where \( W \) and \( W' \) are respectively the embedded and extracted watermark. \( M \) is the number of local windows in the meshes and \( x_i \) and \( y_i \) are the local contents of the \( i \)th 3D local windows. In this work, one local window was considered per vertex and was associated with a radius \( r = 0.02 \) (meshes are normalized in a unit bounding box). Thus, the meshes to compare must have the same connectivity. After several experiments, we have chosen \( a = 4 \), which provides the best results. The MSDM values are distributed within the interval of \([0, 1]\), where 0 implies total imperceptibility and 1 means that the original mesh is different from the watermarked one. As shown in Table 4, the recorded values show that the developed method preserves the invisibility of the watermark.

A.2. Robustness

A watermarking scheme should exhibit the more robustness against different attacks. We conducted a study to determine the potential attacks occurring in a virtual world. We found that some attacks are related to the mesh transformations resulting from the avatar positioning, displacement view, adding noise and its expression variation. Another attack known as file attack aims to destroy the watermark by modifying the file content. Furthermore, a hacker may use a falsified fingerprint in order to overcome the access control mechanism.

In what follows, we give a description of these attacks as well as their modeling in terms of implementation methods.

A.2.1. Similarity transformation

It consists in affine transformations such as rotation, translation, scaling, etc. In the virtual worlds, these attacks appear while modifying the displacement and the positioning of the avatars (Figure 5). The robustness of the developed watermarking technique was evaluated against translation, rotation, scaling, and adding noise attacks. For the last one, a uniform noise was added on the coordinates of the vertex without exceeding the permitted maximum; i.e., the value that did not provide a visually stunning distortion. The similarity criterion NCC was calculated between the original and the extracted watermark. Table 5 demonstrates the mesh modification after attack and the obtained NCC values.

A.2.2. Facial Expression variation attack

This attack is related to the avatars face personalization by the offered tools in 3D virtual worlds. To study the effect of the different facial expression variation, the modified vertices were detected. The Bit Error Rate (BER) metric was also calculated in order to define the rate of erroneous bits in the extracted watermark compared to the original one. Table 6 exposes the face parts corresponding to seven expressions and the BER between the original watermark and the extracted one. The BER, which is given by equation (3).

\[
BER = \frac{1}{M} \sum_{i=1}^{\text{LSM}} W(i) \oplus W'(i)
\]

According to the BER values, the expression variation could inhibit the authentication system and could reject a true identity. To solve this problem, an avatar facial recognition module was designed to distinguish between a veritable attack and an expression one. The problem of avatar facial expression recognition was addressed using the 3D geometry information extracted from the 3D shape of the face. To this end, the Mesh SIFT approach was adapted for the avatar face expression recognition. This relied on identifying a set of facial key points, computing SIFT feature for 3D facial-mesh avatar expression characterization, and training a K-means algorithm for each facial expression to be recognized.

A.2.3. File attack

It is about reordering the vertices and/or the facets in the mesh description file. The data file content is consequently modified, which can affect the watermark if the hosting data is altered. To implement this attack, we apply a random rearrangement to the watermarked avatar 3D mesh file content by reordering its facets’ vertex. At the watermark extraction process, we compute the distances value \( (dv_{k1}, dv_{k2} \text{ and } dv_{k3}) \) between the connected vertices \( (v_{k1}, v_{k2} \text{ and } v_{k3}) \) and the centroid of the corresponding triangle \( f_k \). If the vertices are not arranged in the right order according to the calculated distances, we can confirm the presence of the file content attack. Thus, we proceed to extract the watermark bits from the first vertex LSB of each triangle.
Table 4: MSDM values for a set of faces from the datasets A and B

<table>
<thead>
<tr>
<th>Watermarked mesh</th>
<th>Dataset A</th>
<th>Dataset B</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSDM</td>
<td>0.020394</td>
<td>0.033630</td>
</tr>
<tr>
<td></td>
<td>0.005019</td>
<td>0.0371</td>
</tr>
<tr>
<td></td>
<td>0.0364</td>
<td>0.0367</td>
</tr>
<tr>
<td></td>
<td>0.0364</td>
<td>0.0037</td>
</tr>
</tbody>
</table>

Table 5: NCC values for similarity transformation attacks

<table>
<thead>
<tr>
<th>Initial</th>
<th>Rotation</th>
<th>Translation</th>
<th>Scaling</th>
<th>Noise value &lt;0.5%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacked watermarked avatars</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 6: BER values for different facets expression variation

<table>
<thead>
<tr>
<th>Expression</th>
<th>Frowning</th>
<th>Surprised</th>
<th>Laughing</th>
<th>Crying</th>
<th>Winking</th>
<th>Smiling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variable facets</td>
<td>0</td>
<td>0.5924</td>
<td>0.7600</td>
<td>0.7640</td>
<td>0.7567</td>
<td>0.7819</td>
</tr>
</tbody>
</table>

B. Authentication accuracy

When biometrics are utilized for authentication purposes to control a physical or a logical access, the main goal of the application is to disallow an 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). The FAR expresses the ability degree of distinguishing a genuine identity from an imposter one. The authorized-user acceptance rates, the FAR and the FRR are respectively calculated according to equations (4), (5) and (6).

Authorized − user acceptance rate %

\[
= \frac{\text{Number of correct acceptance}}{\text{Number of authorized user attempts}} \times 100
\]

(4)

FAR% = \[
\frac{\text{Number of false acceptance}}{\text{Number of impostor user attempts}} \times 100
\]

(5)

FRR% = \[
\frac{\text{Number of false rejection}}{\text{Number of authorized user attempts}} \times 100
\]

(6)
In this research, the authorized-user acceptance rates, the FAR and the 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. Indeed, the authenticator process has to allow access only for legitimate users who are previously enrolled in the database. Table 7 summarizes the obtained values of the authorized-user acceptance rates and the FRR in the case of signal processing and geometric attacks and using a dummy fingerprint.

Table 7: Experiment results corresponding to the authorized user, FRR, and FAR rates

<table>
<thead>
<tr>
<th>NCC threshold</th>
<th>Authorized-user acceptance rates (%)</th>
<th>FRR (%)</th>
<th>FAR (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No attacks</td>
<td>1</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>Face expression variation</td>
<td>1</td>
<td>94.80</td>
<td>3</td>
</tr>
<tr>
<td>File</td>
<td>1</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>Rotation</td>
<td>1</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>Translation</td>
<td>1</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>Scaling</td>
<td>1</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>Noise value &lt;0.3%</td>
<td>1</td>
<td>99.5</td>
<td>0.45</td>
</tr>
<tr>
<td>Noise value &lt;0.5%</td>
<td>0.8</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>Dummy fingerprint</td>
<td>1</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Modifying a stolen avatar (BER&lt;0.5)</td>
<td>1</td>
<td>-</td>
<td>4.87</td>
</tr>
</tbody>
</table>

As shown by the different recorded results, the suggested approach is robust against all the considered attacks. Actually, an authorized user rate of 100% is registered in most of the experiments. Furthermore, the authentication process does not permit rejecting an authentic identity according to the obtained FRR values at an NCC threshold value equal to 0.8. Moreover, the authenticator is reliable to distinguish the genuine identities from the impostor ones when a hacker uses a dummy fingerprint or a stolen one. Hence, attackers are unauthorized to accede into the contents of the virtual world server.

VI. CONCLUSION

This paper presents a novel approach to secure virtual worlds by authenticating users and their respective avatars. The suggested 3D avatar face authentication method is based on biometric watermarking, which employs the signature of the user's fingerprint to watermark their personal avatar face. The watermark is embedded in the spatial domain by ordering the facet vertex while the first vertex is adjusted according to the embedded information bit. The proposed technique ensures a good perceptually quality of the watermarked 3D meshes. The experimental results show that the developed algorithm is robust against several attacks specific to the virtual worlds such as similarity transformation, content file reordering, and adding noise. The registered authorized-user, FRR and EER rates at these attacks prove the efficiency of the suggested approach to distinguish genuine from impostors. The developed watermarking algorithm was also evaluated against the expression variation attack. This type of attack thus forms the main focus of the future work to improve the robustness of our method.

REFERENCES


