# A 3D Visual Security (3DVS) score to measure the visual security level of selectively encrypted 3D objects

Sébastien Beugnon, Bianca Jansen van Rensburg, Naima Amalou, William Puech, Jean-Pierre Pedeboy

# A 3D Visual Security (3DVS) Score to Measure the Visual Security Level of Selectively Encrypted 3D Objects

Sébastien Beugnon[a,b], Bianca Jansen van Rensburg[a,b], Naima Amalou[a], William Puech[a] and Jean-Pierre Pedeboy[b]

[a] *LIRMM Laboratory, UMR 5506 CNRS, University of Montpellier, 860 rue de St Priest, 34095 Montpellier, France*
[b] *Stratégies, Rungis 94510, France*
sebastien.beugnon@lirmm.fr, bianca.jansen-van-rensburg@lirmm.fr, william.puech@lirmm.fr, jp.pedeboy@cadwin.com

*Preprint submitted to Elsevier* *March 18, 2022*

# A 3D Visual Security (3DVS) Score to Measure the Visual Security Level of Selectively Encrypted 3D Objects

Sébastien Beugnon[a,b], Bianca Jansen van Rensburg[a,b], Naima Amalou[a], William Puech[a] and Jean-Pierre Pedeboy[b]

[a] *LIRMM Laboratory, UMR 5506 CNRS, University of Montpellier, 860 rue de St Priest, 34095 Montpellier, France*
[b] *Stratégies, Rungis 94510, France*
sebastien.beugnon@lirmm.fr, bianca.jansen-van-rensburg@lirmm.fr, william.puech@lirmm.fr, jp.pedeboy@cadwin.com

**Abstract**

Today, 3D objects are becoming more commonly used across many domains. However, it is necessary to secure them during their transmission over networks or when archiving them in the cloud. Encryption is a smart solution to protect 3D objects while remaining format compliant. While there exist many methods proposed for 3D quality evaluation, very few have been developed to evaluate the visual security level of encrypted 3D objects. In this paper, we propose an efficient metric, called 3D Visual Security (3DVS) score, to evaluate the visual security level of selectively encrypted 3D objects. First we present a new dataset composed of selectively encrypted 3D objects that have all been evaluated by more than 50 observers in terms of visual security. Secondly, we propose a model to determine the security parameters according to a desired security level. Finally, we detail our proposed 3DVS score which is based on full reference 3D metrics and serves to measure the visual security level of selectively encrypted 3D objects.

*Keywords:* 3D Object, 3D Selective Encryption, Subjective Evaluation, Content Protection, Visual Security Level

## 1. Introduction

In this current decade, 3D objects are widely used in many domains such as digital entertainment, industrial modeling, or the healthcare industry, among others. Moreover, 3D objects have also become more accessible to the general public. With new usages of advanced scanning and printing devices, it has become very easy to produce and copy 3D objects. Virtual, augmented and mixed reality technologies have also developed the need for high quality 3D objects, which are constructed from millions of geometric primitives.

Because of the ease of duplication and production of 3D objects, it is necessary to develop systems in order to guarantee their security. Two main classes of methods have so far been developed to protect 3D objects: data hiding and encryption approaches. The first class of approaches proposes to embed secret messages in 3D objects as imperceptibly and robustly as possible (1).

The second class of approaches is based on encryption methods and proposes to directly protect the geometry of 3D objects (2; 3; 4; 5; 6). Some methods propose to encrypt the geometry of 3D objects by using progressive mesh representation (2), by using geometry-preserving transformations such as permutation (3), or by selectively encrypting bits of the geometry to allow users to view distorted versions of secret 3D objects (4). The advantages of 3D selective encryption approaches are that they allow the visualization of secret 3D objects according to the level of visual security desired by the user. Based on this, Beugnon *et al.* (4) have defined 3 levels of visual security according to the work of Pommer *et al.* (7). These 3 levels are defined as confidential, sufficient and transparent. Recently, secret 3D object sharing, an extension of the secret sharing domain proposed by Shamir (8), has received attention, especially in relation to 3D protection. It is regarded as a new way to insure redundancy and security (5; 6; 9; 10; 11).

Until today, visual security evaluation of encrypted 3D objects for 3D selective encryption approaches has only been carried out visually or by using standard objective 3D metrics such as the Root Mean Square Error (RMSE) (12), the Hausdorff Distance (HD) (13; 14), the PSNR (15), or the Mesh Structural Distortion Measure 2 (MSDM2) (16), which are not very well correlated with the Human Visual System (HVS). Previous work on visual quality assessment methods are mainly focused on the quality of the visual content after watermarking (17; 18; 19) or after various other processing methods (20; 21). During the last decade, visual quality assessment of

3D objects has been widely studied and extensively adapted for 3D objects in order to take into consideration the HVS (22; 23; 24; 25).

Although today there exist visual security metrics for 2D images (26; 27; 28; 29; 30; 31), to the best of our knowledge, no such metric exists for 3D objects. Studying visual security is indeed not at all the same as studying the quality of the 3D object. Visual quality metrics for 3D objects aim to detect whether there is a slight distortion in a 3D object, whereas visual security considers whether users are able to recognize the shape or content of a 3D object and whether a 3D object is considered usable or not.

In this paper, we propose a new 3D visual security metric, called 3D Visual Security (3DVS) score, which is designed to measure the visual security level of selectively encrypted 3D objects. This score is constructed with a combination of classic linear regression and logistic regression. We also construct a polynomial regression model in order to estimate the selective encryption parameters according to the desired visual security level. In order to evaluate our metric, we have developed a new dataset which consists of 50 3D objects which are each selectively encrypted with 10 different encryption levels, based on the visual security levels defined by the work of Beugnon *et al.* (4) and Pommer *et al* (7). This dataset, called *Selectively Encrypted 3D Object* (SE3DO) dataset is composed of 550 3D objects and is accompanied by opinion scores (OS) gathered from 54 different observers.

The main contributions of this paper can be summarized as:

1. A new dataset which consists of 50 3D objects which are each selectively encrypted with 10 different encryption levels. The dataset, called *Selectively Encrypted 3D Object* (SE3DO) is accompanied by a set of OS;

2. A new model to estimate the adequate security parameters according to the desired visual security level;

3. A new metric based on full reference 3D metrics, called 3D Visual Security (3DVS) score, designed to measure the visual security level of selectively encrypted 3D objects.

The rest of this paper is organized as follows. Section 2 presents previous work on 3D selective encryption, 3D quality assessment, image visual security evaluation and the definitions of our three chosen visual security levels. Our proposed SE3DO dataset and the results of our evaluation campaign

are detailed in Section 3. Then, Section 4 presents our new model designed to automatically estimate the adequate security parameters according to the desired visual security level. Our metric 3DVS score, used to measure the visual security level of selectively encrypted 3D objects, is developed in Section 5. Finally, Section 6 concludes and presents future work.

## 2. Previous and Related Work

In this section, we present previous work conducted in 3D selective encryption, 3D quality assessment and visual security level evaluation. In Section 2.1, we present four previous 3D selective encryption methods and, in particular, the method proposed by Beugnon *et al.* (4) which was used to create the dataset presented in this work. In Section 2.2, we focus on existing 3D quality metrics used to assess 3D objects. Finally, in Section 2.3, we detail image visual security evaluation methods as well as three visual security levels which are used to build our proposed 3DVS score.

### *2.1. 3D selective encryption*

The state of the art describes two main classes for securing 3D objects by encryption. The first class concerns full encryption approaches which consider 3D objects as binary data and encrypt them using a standard encryption scheme such as RSA (32) or AES (33). The second class concerns format compliant approaches, these are approaches that maintain the internal structure of the 3D objects.

In this second class, selective encryption approaches (34; 2; 3; 4) are methods that manipulate a specific set of data in order to protect it with a given level of visual security. Cho *et al.* proposed encrypting the 3D object's connectivity in order to generate a surface which contains holes, without modifying the geometry, as well as applying a *fingerprint* to the 3D object (34). Gschwandtner and Uhl proposed using a progressive mesh to represent a 3D object and suggested encrypting a subset of the data (such as positions, colors or indices) in layers of this structure (2). Later, Eluard *et al.* presented multiple geometry-preserving encryption schemes based on permutations of vertices or coordinates (3). Recently, Beugnon *et al.* proposed selectively encrypting the binary representation of floating values used for each coordinate of every vertex of a 3D object (4). In their approach they use a degradation level parameter, which allows them to control the impact of the encryption on the geometry and the security level of the 3D object.

Later, they extended this approach to another set of cryptographic schemes called secret sharing (6).

### *2.2. 3D quality assessment*

Metrics dedicated to evaluating the visual quality of 3D objects are mainly full reference ones. In this section we present five quality metrics specifically applied to 3D objects. These quality metrics are the Root Mean Square Error (RMSE) (12), the Hausdorff Distance (HD) (13; 12), the PSNR (15), the Mesh Structural Distortion Measure (MSDM2) (16) and finally the Dihedral Angle Measure Error (DAME) (35).

The RMSE is computed between two 3D objects $O$ and $O'$ by using a known correspondence between vertices:

$$\mathrm{RMSE}(O, O') = \sqrt{\frac{1}{V}\sum_{i=1}^{V} ||v_i - v'_i||^2}, \tag{1}$$

where $V$ is the set of vertices and $v_i$ (resp. $v'_i$) the coordinates of the $i$-th vertex of $O$ (resp. $O'$).

The HD is based on the distance between a vertex $v$ from a 3D object $O$ to the nearest vertex $v'$ of a second 3D object $O'$:

$$\begin{aligned} \mathrm{HD}(O, O') &= \max(d(O, O'), d(O', O)), & (2)\\ d(O, O') &= \max_{v \in O} d(v, O'), & (3)\\ d(v, O') &= \min_{v' \in O'} \|v - v'\|_2. & (4) \end{aligned}$$

Initially, the PSNR is a reference metric mainly used to evaluate the quality of 2D images. Some authors have proposed using it for 3D objects. Chao *et. al.* (15) proposed quantifying the distortion of 3D vertex positions or vertex normals using RMSE:

$$\mathrm{PSNR}(O, O') = 20 \log_{10} \frac{D_{\max}}{RMSE(O, O')}, \tag{5}$$

where $D_{\max}$ is the length of the diagonal of the bounding box of the reference 3D object $O$.

The Mesh Structural Distortion Measure 2 (MSDM2) (16) is an improvement of the metric MSDM (36) which adapts the 2D metric Structural SIMilarity (SSIM) (37) for 3D objects. In (16) and (36) Lavoué proposes replacing

pixel values by the mean curvature of a 3D object and proposes a local measure defined as:

$$LMSDM(x,y) = (\alpha L(x,y)^a + \beta C(x,y)^a + \gamma S(x,y)^a)^{\frac{1}{a}}, \tag{6}$$

where $x$ and $y$ are two local 3D windows, $L$ represents a normalized curvature distance, $C$ is based on the standard deviations $\sigma_x$ and $\sigma_y$ which reflect the roughness of the surfaces and $S$, by considering the covariance between local windows, which aims to detect changes in salient features.

Finally, MSDM between two 3D objects $O$ and $O'$ is defined by a Minkowski sum of their local window distances. MSDM2 provides two main improvements. The first allows users to compare 3D objects with different connectivities. It uses a step to determine the correspondence between the vertices of the reference 3D object $O$ and those of the compared 3D object $O'$. The second improvement concerns the evaluation of visual differences by multiresolution. The results of the metric are therefore more correlated with subjective assessments. With this approach, all the scores calculated on the surface area are combined into a single global score.

Finally, DAME proposed by Vása and Rus (35) is used to analyze distortions in the dihedral angles of 3D object triangles with the same connectivity:

$$\mathrm{DAME}(O,O') = \frac{\sum\limits_{\{t_1,t_2\}\in\Omega} ||D_{t_1,t_2} - \overline{D_{t_1,t_2}}||m_{t1,t2}(w_{t_1} + w_{t_2})}{||\Omega||}, \tag{7}$$

where $\Omega$ is the set of all pairs of triangles $t_1$, $t_2$ sharing the same edge, $D_{t_1,t_2}$ the dihedral angle between $t_1$ and $t_2$ in $O$, $\overline{D_{t_1,t_2}}$ the dihedral angle between $t_1$ and $t_2$ in $O'$, and $m_{t1,t2}$ the visual masking coefficient:

$$m_{t_1,t_2} = e^{k \times D_{t_1,t_2}}, \tag{8}$$

where $k = 7$ is chosen empirically by the experiments of Vása and Rus (35).

The visibility terms $w_{t_1}$ and $w_{t_2}$ are deduced by calculating the density of the pixels representing the triangles at different viewing angles. Vása and Rus proposed calculating this term by generating synthetic images of the 3D object from different angles in order to count the number of pixels in each image representing a triangle. The authors also proposed an approximation of this term, which is much faster. It consists of calculating the ratio between the area of the triangle and the area of the surface of the 3D object. For the purpose of our study in Section 4 and Section 5, we chose to use these visual quality metrics.

*2.3. Visual security level evaluation*

In this section, we first present previous methods of visual security level evaluation for images. Then, we present the different levels of 3D visual security we use in this paper.

Regarding the images, in 2009, Yao *et al.* introduced a visual security assessment based on neighbourhood similarity (26). Jenisch and Uhl (38) described a visual security evaluation based on SIFT (39). In 2016, Xiang *et al.* proposed a perceptual visual security index by analyzing the texture and extracted edges of an image (27). Xiang *et al.* later described in 2020 a visual security index based on spatial contrast and texture features of an image (28). Abraham *et al.* suggested a visual security evaluation method using edge, texture and wavelet frequency information from the original and encrypted image (29). In 2020, Guo *et al.* proposed a perceptually encrypted image database for visual security evaluation (30). Even more recently, in 2021, Yang *et al.* described a visual security index based on a convolutional neural network (31).

Inspired by the work of Pommer et Uhl (7) for selective encryption of visual data, in 2019 Beugnon *et al.* defined three distinct visual security levels (4). These three visual security levels correspond to the accessibility of the visual content or the shape of 3D objects for the human visual system (HVS). These three levels are named **transparent**, **sufficient** and **confidential**. To the best of our knowledge, this is the only classification for 3D visual security that exists©.

The **confidential level** defines a level where neither the shape nor the content of a 3D object are accessible to the HVS. As for the **sufficient level**, this defines when users are able to recognize the shape of a 3D object, but not its content. Finally, the **transparent level** corresponds to a 3D object whose content and shape are recognizable, but the quality of the 3D object remains low enough to prevent it from being used, for example, for 3D printing. Fig. 1 illustrates two examples of the three visual security levels applied to two 3D objects of shoes[1]. The first shoe is from the brand *Clarks*© and the second shoe from the brand *New Balance*©. At the **transparent level**, we can recognize that the objects are shoes and recognize the brand, while at the **sufficient level**, the brand is not identifiable. Finally, at the **confidential level**, we cannot even recognize that they are shoes.

[1]Provided by STRATEGIES (https://www.romans-cad.com/)

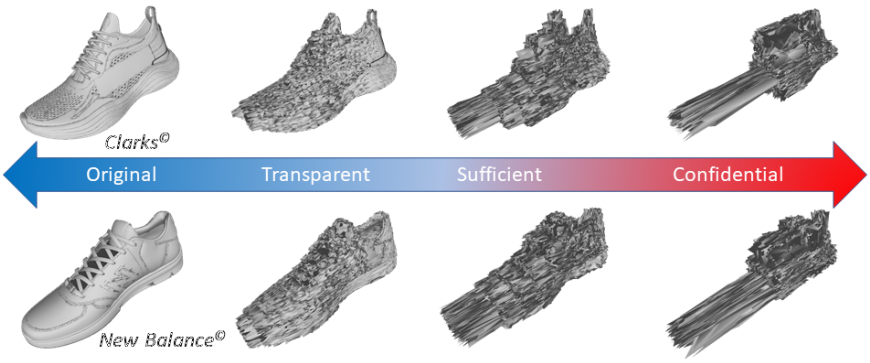



Figure 1: Examples of the three visual security levels: **transparent**, **sufficient** and **confidential** (4) applied to two manufactured 3D objects of shoes provided by STRATEGIES (https://www.romans-cad.com/). The first shoe is from the brand *Clarks*© and the second from the brand *New Balance*©.

Furthermore, visual security assessment is very different from quality assessment. While quality assessment constrains the evaluations to small visual distortions by comparing the visual quality of two 3D objects, visual security assessment tries to study a larger and broader spectrum of 3D objects where distortions intend to hinder the usage or the comprehension of the 3D content.

## 3. The proposed Selectively Encrypted 3D Object (SE3DO) dataset

In this section, we present our proposed Selectively Encrypted 3D Object (SE3DO) dataset. First, in Section 3.1, we explain the differences between visual security metrics and visual quality metrics. Then, in Section 3.2, we present the dataset we have created. Next, in Section 3.3, we describe our evaluation protocol. Finally, in Section 3.4, we analyze our obtained evaluations.

### *3.1. Visual security compared to visual quality*

Measuring the visual security of a 3D object is very different to measuring its visual quality. Visual security metrics seek to evaluate the security of the media, and therefore how accessible the content is to the human visual system (HVS).

In this paper, we propose a metric which classifies 3D objects into five different categories: distortion-less 3D objects, noisy 3D objects, transparent level 3D objects, sufficient level 3D objects and finally confidential level 3D objects. Among these five categories, we consider that only three categories, the **confidential**, **sufficient** and **transparent** levels, are secure.

Visual quality metrics, however, are not designed at all to indicate the security of a 3D object. These metrics indicate the quality of 3D objects which are considered to be distortion-less or noisy. They therefore mainly handle 3D objects which are not at all considered secure. The differences are illustrated in Fig. 2.

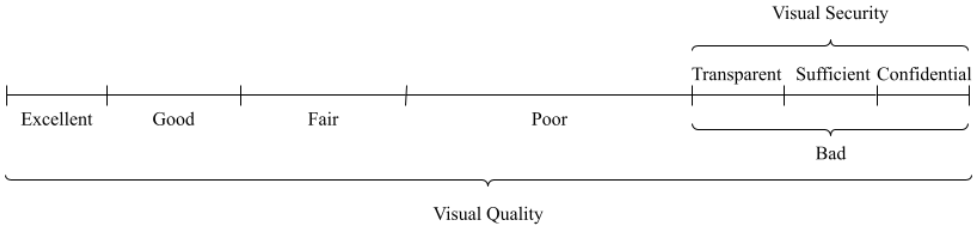



Figure 2: Visual quality compared to visual security.

### *3.2. The SE3DO dataset*

#### *3.2.1. The original 3D objects*

In computer graphics, there is, to the best of our knowledge, no dataset of subjective evaluations of the visual security of encrypted 3D objects. All previous 3D object datasets have been constructed to assess quality (40) in various contexts such as acquisition, processing, compression, watermarking or even segmentation applications (41; 42; 43). Our proposed dataset is constructed with 3D objects from existing datasets, such as *Princeton Mesh Segmentation Project* (41), *SHREC-12* and *SHREC-14* for 3D segmentation (42; 43) and *Thingi10k* (44). From these datasets, we select 50 3D objects which serve as references in the proposed SE3DO dataset. Four examples of these 3D objects are presented in Fig. 3

As illustrated in Fig. 3, the reference 3D objects are either from CAD (Fig. 3.a) or from scanning systems (Fig 3.b). So some of these 3D objects represent living entities named "organic" objects, whereas the complement represents "inert" objects (helmet, statue, vase, *etc.*). By varying the origins of the reference 3D objects, as well as the represented content, we are able to

(a) Object #5 (b) Object #12

(c) Object #24 (d) Object #32

Figure 3: Examples of reference 3D objects from the *Selectively Encrypted 3D Object* (SE3DO) dataset.

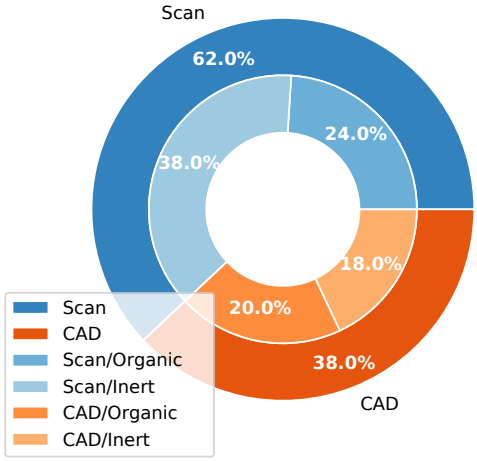
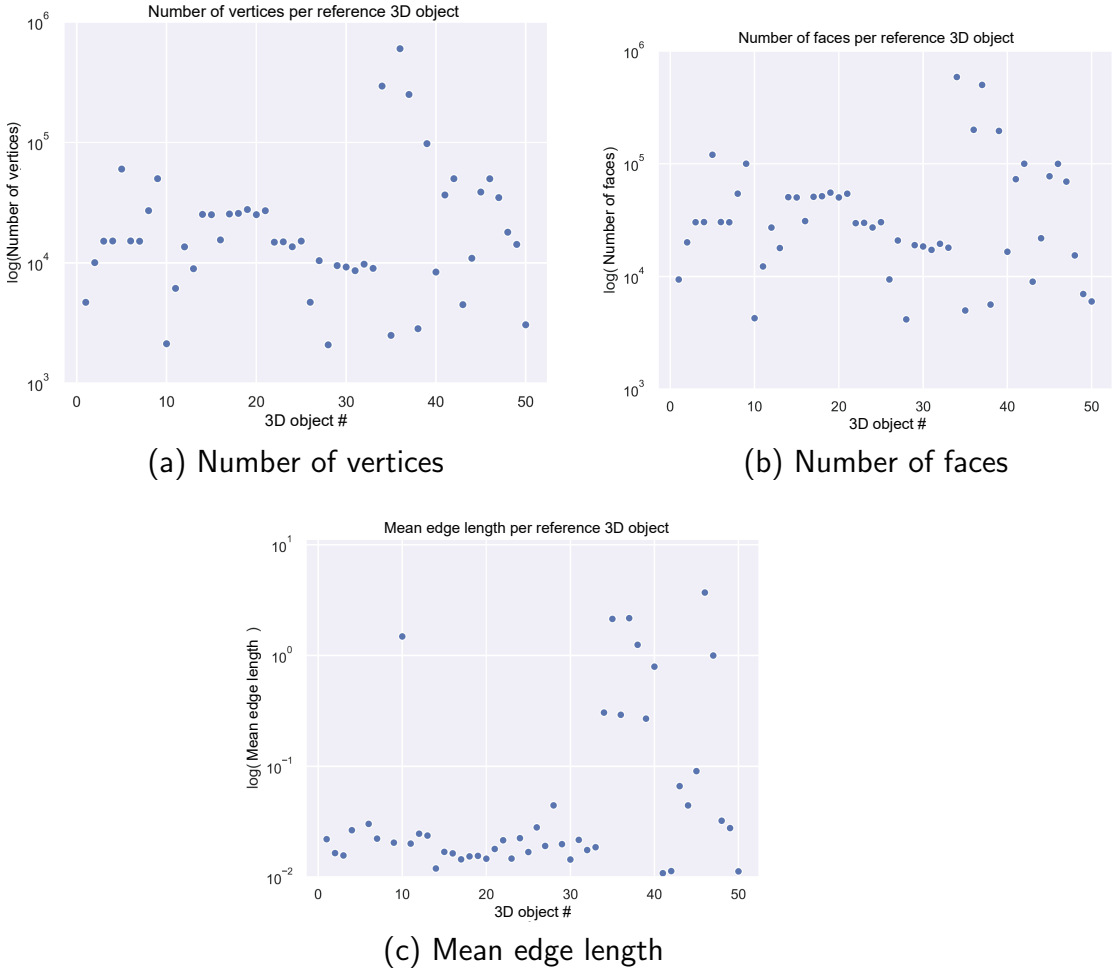



Figure 4: Distribution of reference 3D objects in *the Selectively Encrypted 3D Object* (SE3DO) dataset depending on the origin (CAD or Scan) and type of content (Organic or Inert).

evaluate a wide variety of 3D objects. This is in order to study the effects of 3D selective encryption and to determine not only where it is most effective in protecting the content, but also where it is most adapted to the density of the vertices, the size of the 3D object and the local curvature which can influence its numerical form.




(a) Number of vertices

(b) Number of faces

(c) Mean edge length

Figure 5: Characteristics of reference 3D objects of the SE3DO dataset.

Fig. 4 presents the distribution of the reference 3D objects: 31 are 3D objects generated by scanning, whereas 19 of the 3D objects are produced using CAD tools. Among these 3D objects, 21 of them represent organic 3D objects, while the other 29, represent inert 3D objects. We can note that the

reference 3D objects are distinguished by properties such as the number of vertices, the number of faces, the average length of an edge, as well as other characteristics, as illustrated in Fig. 5.

*3.2.2. The encrypted 3D objects*

We propose encrypting these 50 reference 3D objects using the 3D selective encryption method from (4), which is presented in Section 2. This method considers that each vertex coordinate is represented by a 32 bit floating point, which consists of a single bit sign, an 8 bit exponent and a 23 bit mantissa. It is only the 23 bit mantissa that is encrypted. The degradation level is based on the variable $p$, where $p$ indicates the first bit of the mantissa to be encrypted. Then we encrypt the 50 3D objects using the degradation levels where $p \in [\![13\ ;\ 22]\!]$, as illustrated in Fig. 6 for the 3D object #18. According to a study by Beugnon *et al.*, when the parameter $p < 13$, the RMSE between the original 3D object and the selectively encrypted 3D object is negligible (4). When $13 \leq p \leq 16$, even though there is no visual difference between the original and selectively encrypted 3D object (Fig. 6), the RMSE is no longer negligible. This is why we have chosen to use the degradation levels where $p \in [\![13\ ;\ 22]\!]$. For each encryption, we change the secret key $K$ to avoid bias. Finally, including the reference 3D objects, we obtain our SE3DO dataset which is composed of 550 3D objects, where 500 of them are selectively encrypted.

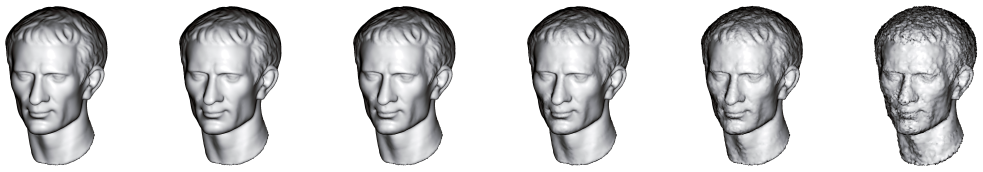
*3.3. Evaluation protocol*

Generally, images are subject to large varieties of distortions related to acquisition, processing, compression, storage, transmission, reproduction or data hiding. This results in a degradation of their visual quality. The same observations can be made for 3D objects. Initially, subjective evaluations are generally used to evaluate the performance of objective metrics. With the arrival of machine learning methods, some metrics are constructed from the data produced by the evaluations (24), as described in Section 2.2.

*3.3.1. Evaluation system*

The most common measurement for creating these metrics is the Mean Opinion Score (MOS) which usually varies between 1 and 5.

Table 1 presents the scale we have defined for the study of the visual security of 3D objects for our subjective evaluations. Values 1, 2 and 3 correspond to the three different security levels defined by (7) and (4) as part



(a) Original (b) $p = 13$ (c) $p = 14$ (d) $p = 15$ (e) $p = 16$ (f) $p = 17$

(g) $p = 18$ (h) $p = 19$ (i) $p = 20$ (j) $p = 21$ (k) $p = 22$

Figure 6: 3D objects representing the selective encryption of the 3D object #18 of the SE3DO dataset, according to the different selective encryption levels where the parameter $p \in [\![13\ ;\ 22]\!]$.

Table 1: Values and significations of the MOS as part of the visual security assessment.

| MOS | Signification | Shape | Content | Quality |
|---|---|---|---|---|
| 1 | **Confidential level** | Confidential | Confidential | Poor |
| 2 | **Sufficient level** | Accessible | Confidential | Poor |
| 3 | **Transparent level** | Accessible | Accessible | Low |
| 4 | Noisy 3D object | Accessible | Accessible | Medium |
| 5 | Distortion-less 3D object | Accessible | Accessible | High |

of the scenarios for selective encryption of visual data, namely the confidential, sufficient and transparent level as defined in Section 2.3. Thus, we have associated a MOS value of 1 with the confidential level, where our selective 3D object encryption methods generate 3D objects whose shape and content are confidentially protected. The MOS value of 2 is associated with the sufficient level, where only the shape of the 3D object is recognizable, but not its content. Finally, a MOS value of 3 corresponds to the transparent level, this allows recognition of the form and the content, but the high quality of the 3D object is protected. A MOS value of 4 allows observers to differentiate between noisy 3D objects and 3D objects that are of high quality with a MOS value of 5. The value of MOS 5 corresponds to 3D objects that obviously have no defects and therefore are high quality, unencrypted 3D objects.

*3.3.2. Stimulus mode*

Among the different subjective quality assessment protocols there are 4 pre-dominant modes, namely *single-stimulus*, *double-stimulus*, *forced-choice pairwise comparison* and *similarity judgments*. Each of these modes has its advantages as well as its disadvantages (40). However, in our subjective assessment, it is very clear that we must use the single-stimulus protocol. Indeed, because we are searching for a metric to encrypt the visual security of a selectively encrypted 3D object, the use of protocols using two 3D objects (the original 3D object and the encrypted one, for example) provides information on the shape and content of the 3D object whose visual security we are trying to analyze. Thus, other modes of *stimulus* seeking to compare two 3D objects of different qualities would not provide us with any information on the visual security. Due to the nature of the data, in our case 3D objects, we allow observers to interact with these 3D objects by authorizing camera motions (translation, rotations, zooms) so that they can observe the shape of the 3D object from all angles.

*3.3.3. Evaluation environment*

Subjective assessments with a standardized protocol to provide correct and universal results. However, they require a controlled environment and many limitations due to human judgment that can vary significantly depending on external conditions and individuals.

Our evaluations are therefore conducted in a specialized room behind closed doors to maintain control over essential elements such as light, screen resolution and distance from the screen. As shown in Fig. 7, the observers

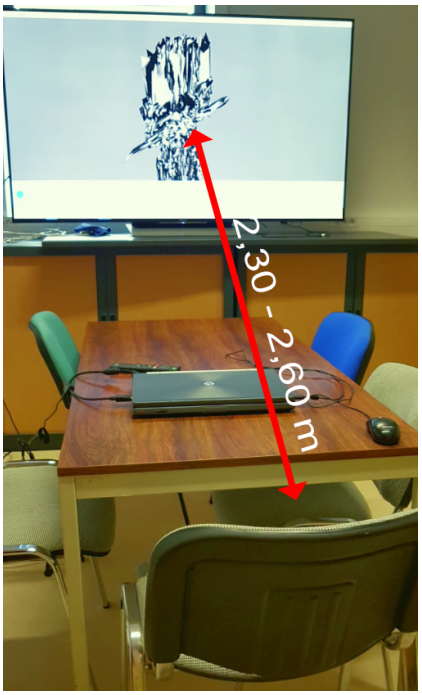



Figure 7: The room used for subjective evaluation of the visual security of selectively encrypted 3D objects.

are positioned in front of a professional LCD screen *Sony FW-75XD8501* 4K Ultra HD of 190.5 $cm$, based on LED technology with a resolution of 3840 $\times$ 2160 pixels and a brightness of about 450 $cd/m^2$. The observers are seated at a distance of between 2.30-2.60 meters from the screen.

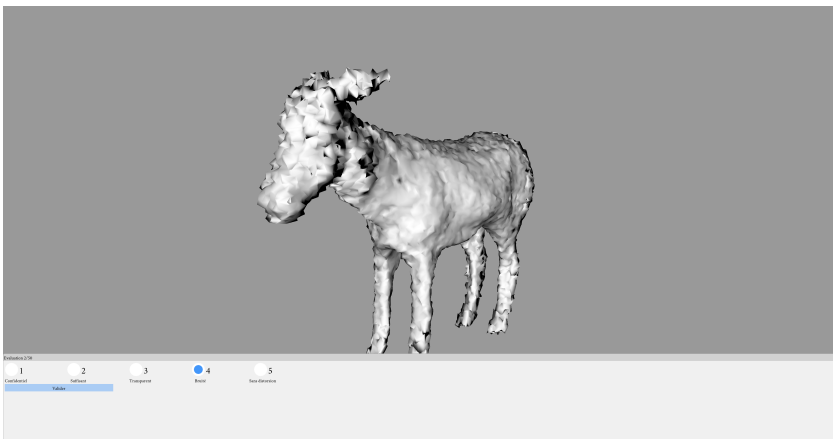


Figure 8: Evaluation of the visual security of selectively encrypted 3D objects. The observer selects an opinion score (OS) value for the selectively encrypted 3D object.

The 3D objects are displayed on a uniform grey background, without texture, using a *shader* based on the Phong model (45) with light grey material turning white in specular areas as illustrated in Fig. 8.

*3.3.4. Evaluation procedure*

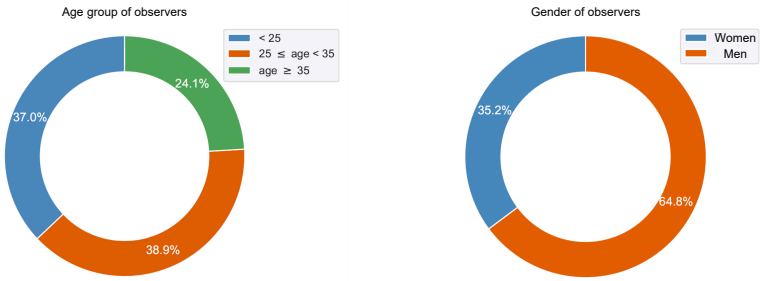
As described in Section 3.2, we have 50 3D reference objects and for each of these objects, 10 additional variations generated with the encryption parameters ($13 \leq p \leq 22$). We decided that each observer evaluates 50 distinct 3D objects which can be original or selectively encrypted with ($13 \leq p \leq 22$). To prevent observers from learning to recognize 3D objects, we decided to show them only one random variant of each of the 50 3D reference objects. Before the evaluation phase, the problematic of visual security of 3D objects is presented to the observers. As illustrated in Fig. 9, observers are introduced to the problematic by presenting a 3D object selectively encrypted with different levels. The order in which the selectively encrypted 3D objects are presented is crucial, as it serves to show the evolution of the shape and content of the 3D object from confidentially encrypted into something recognizable, and how the opinion score (OS) should be assigned during each evaluation phase.

(a) Confidential level ($MOS = 1$) (b) Sufficient level ($MOS = 2$) (c) Transparent level ($MOS = 3$) (d) Noisy 3D object ($MOS = 4$) (e) Distortion-less 3D object ($MOS = 5$)

Figure 9: Selectively encrypted 3D objects for the observer initiation phase at the different levels of visual security of 3D objects.

### *3.3.5. Observer group analysis*

The group of observers who participated in our subjective assessments is diverse. It was composed of experts in the field of computer graphics, image processing, as well as other, so-called non-experts.




(a) Age (b) Gender

Figure 10: Observer distributions by : a) Age, b) Gender.

Fig. 10 represents the distribution of observers by age and gender. As illustrated in Fig. 10.a, our observers are divided into three age groups: under 25 (20), 25-35 (21) and over 35 (13). We note that 19 observers are women and 35 are men according to Fig. 10.b.

*3.4. Evaluation analysis*

The 54 observers generated 2700 OS values distributed over all 550 3D objects in the dataset. Among the 2700 OS, approximately 250 are those of the 3D reference objects. These scores on 3D reference objects are mainly used to identify ambiguous 3D reference objects, *i.e.* objects with a naturally distorted appearance for observers. This makes it possible to analyze the perception of the quality of 3D objects created from the digitization of real-world objects. In addition, we can obtain more information on the threshold of sensitivity to distortions of different observers. The approximate 2450 other OS are those of the evaluation of selectively encrypted 3D objects. On average, each selectively encrypted 3D object has been evaluated 5 times.

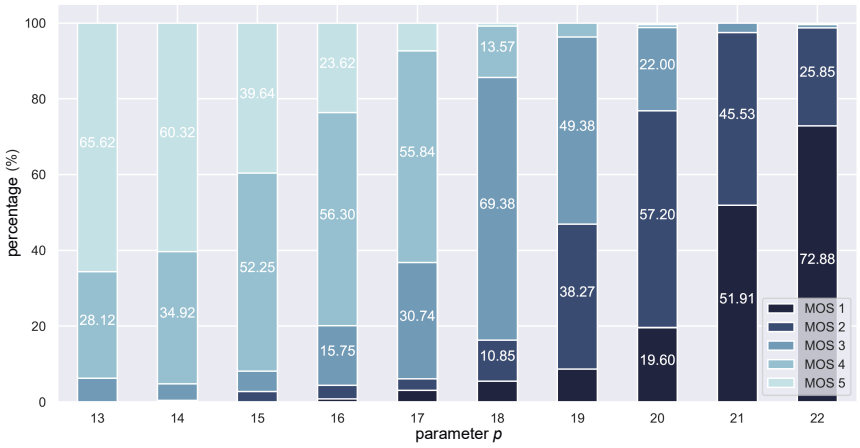



Figure 11: Distribution of the percentages of the opinion score values according to the parameter $p$.

In our SE3DO dataset, for each selectively encrypted 3D object, whatever the value of $p$, we noticed that the assigned OS values can generally vary around two or three values. Thus, we deduce that there is no specific value of $p$ that allows us to obtain a unique value for OS, whatever the encrypted 3D object. Fig. 11 shows the distribution of the percentages of the OS values according to the parameter $p$. More precisely, we note that the majority of observers gave an OS of 5, for $p \in \{13,\ 14\}$ (65.62%, 60.32%), an OS of 4, for $p \in \{\ 16,\ 17\}$ (56.30%, 55.84%), an OS of 3, for $p \in \{18\}$ (69.38%), an OS of 2, for $p \in \{20\}$ (57.20%) and an OS of 1, for $p \in \{\ 22\}$ (72.88%). However, observers are more varied for $p \in \{15,\ 19,\ 21\}$. Indeed, if we look in more detail at $p$ =15, although observers voted for an OS of 4, with 52.25%,

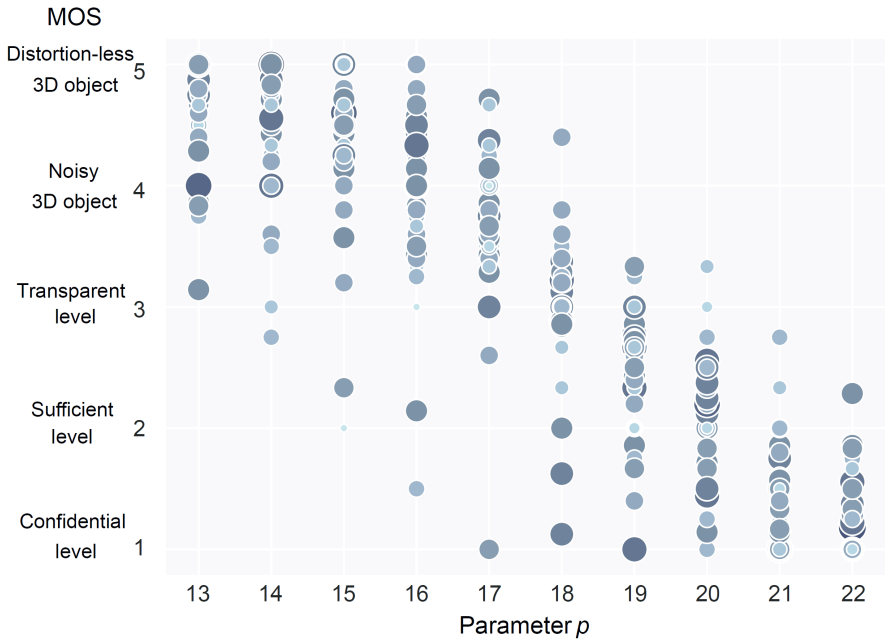



Figure 12: Distribution of the MOS values for each encrypted 3D object according to the parameter $p$.

there are still 39.64% who chose a score of 5. We find a similar situation for $p = 19$ where no OS value exceeds 50%, with 49.38% for an OS of 3, 38.27% for an OS of 2 and 12.35% for the other OS values. Finally, for $p = 21$, an OS of 1 is 51.91%, compared to 45.53% with an OS of 2. From these results, we can begin to see specific intervals representing different levels of visual security. Thus, observers consider objects selectively encrypted with a parameter $p$ equal to 18 or 19 as transparent, 19 or 20 as sufficient and finally 21 or 22 as confidential. Despite an encryption with $p$ equal to 13 or 14, most observers consider that the 3D objects do not have visible geometric distortions and that they only appear from $p = 15$. To summarize we can note, that for $p \in \{13,\ 14\}$, the majority of observers preferred an OS of 5, for $p \in \{15,\ 16,\ 17\}$ an OS of 4, for $p \in \{18,\ 19\}$ an OS of 3, for $p \in \{20,\ 21\}$ an OS of 2 and finally a OS of 1 for $p \in \{22\}$. In addition, we can also note that for some values of $p$, OS values are assigned almost uniformly between two values, particularly for $p \in \{15,\ 19,\ 21\}$. We can deduce that the values of $p$ pivots, where observers consider that a visual change occurs for a large part of the selectively encrypted 3D objects. We still observe that there are

very rare value pairs ($p$, OS), but they do still exist. For example, the first evaluation giving an OS of 1 appears for $p = 16$, while for an OS of 5, the last encryption parameter $p$ is 18.

Fig. 12 represents the MOS values calculated from the OS values provided by the observers for each encrypted 3D object in our SE3DO dataset. We note in Fig. 12 that, despite the OS given mainly by observers for each value of the encryption parameter $p$ presented in Fig. 11, some 3D objects are considered highly encrypted despite a low $p$ value. Or on the contrary, 3D objects are considered to be of a transparent or sufficient level, despite a high value of $p$.

## 4. Security parameter estimation

In this section, we present our method to estimate the visual security parameter for 3D objects which we wish to selectively encrypt. An overview of the method is illustrated in Fig. 13. The visual security parameter is estimated using a polynomial function obtained by regression based on the desired security level $MOS_{desired} \in [\![1\ ;\ 5]\!]$, where 1 corresponds to a confidential level, 2 a sufficient level, and 3 a transparent level. The estimated visual security parameter $p$ is then used to selectively encrypt the 3D object.

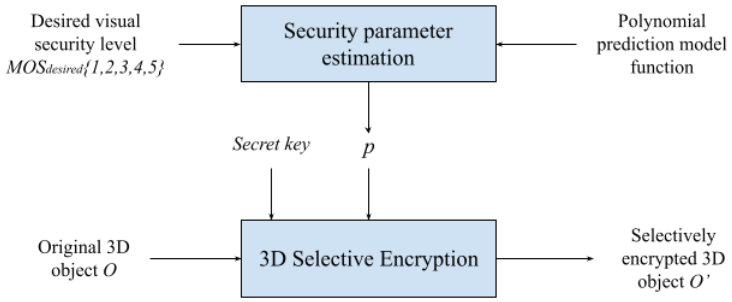



Figure 13: Overview of the visual security parameter estimation.

In order to be able to estimate the encryption parameter $p$, we calculate correlations between the values of $p$ and the values of the MOS obtained from the observers. A correlation coefficient is a statistical measurement describing the linear relationship between two variables. These correlation coefficients are between $-1$ and $+1$. A correlation coefficient close to $+1$ indicates that the two variables have a very high positive linear relationship, while a correlation coefficient close to $-1$ shows that the two variables

have a very high negative linear relationship. A correlation coefficient close to 0 indicates that the variables are independent and therefore there is no relationship between the two.

Table 2: Correlation coefficients between the parameter $p$ and the MOS values obtained from the observer evaluations of the SE3DO dataset.

| Correlation coefficients | Visual security parameter $p$ |
|---|---|
| Pearson | -0.906 |
| Spearman | -0.904 |

Table 2 presents the obtained correlation coefficients between parameter $p$ and the MOS values of the observers. At first we chose to use the data from the evaluations in three different ways: by directly using all the values of OS given by observers (raw values), by using the median values of OS for each 3D object, and finally by using the MOS values for each 3D object. The first approach (raw values) uses all the OS given (approximately 2450 evaluations) which makes it possible to calculate a value as close as possible to reality. The other two approaches (median and mean values) use the OS values assigned to the 500 selectively encrypted 3D objects. We find that there is a strong relationship between the parameter $p$ and the OS values of the observers. With this analysis, we observe that the parameter $p$ is strongly correlated to the OS values of the observers. As a result, we can build a model to estimate the value of $p$ based on a desired level of visual security. To do this, we have decided to apply a polynomial regression in order to build a statistical learning model. So, we separate the data from the SE3DO dataset into two distinct 3D object datasets, namely a 3D object dataset for the training phase and a 3D object dataset for the test phase. The goal is to train the model on a representative subset of the data and test the validity of the model on the rest of the 3D objects, which have never been observed by the model. To do this, we use 30 3D reference objects (and their 300 associated encrypted versions) for the training phase and 20 3D reference objects (and their 200 associated encrypted versions) for the testing phase.

Table 3 presents the results of the estimation models of the parameter $p$ as a function of the MOS values for the training base and the test base. We test our model on the MOS obtained for each 3D object. We first calculate

Table 3: Results of the polynomial regressions according to the MOS values of the observers on both datasets.

| Regression metrics | Train | Test |
|---|---|---|
| $R^2$ score | 0.8651 | 0.7443 |
| Explained Variance Score | 0.8651 | 0.7508 |
| Mean Absolute Error | 0.7774 | 1.0745 |
| Mean Squared Error | 1.1128 | 2.1094 |
| Max Error | 4.7248 | 5.2846 |
| Median Absolute Error | 0.5838 | 0.7303 |

Table 4: Estimations of the parameter $p$ according to the desired level of visual security for the 3D object #18 shown in Fig. 6.

| Visual security parameter $p$ | 13 | **14** | 15 | **16** | 17 | **18** | **19** | 20 | 21 | **22** |
|---|---|---|---|---|---|---|---|---|---|---|
| Observed MOS | 5.0 | 5.0 | 4.7 | 4.0 | 3.6 | 3.2 | 2.6 | 1.0 | 1.0 | 1.0 |
| $f(D)$ | 13.55 | 13.55 | 14.06 | 15.66 | 16.49 | 17.63 | 19.00 | 21.61 | 21.61 | 21.61 |
| $[f(D)]$ | 14 | **14** | 14 | **16** | 16 | **18** | **19** | 22 | 22 | **22** |

the determination coefficient (or $R^2$ score):

$$R^2(y, \hat{y}) = 1 - \frac{\sum_{i=0}^{n-1} (y_i - \hat{y}_i)^2}{\sum_{i=0}^{n-1} (y_i - \overline{y})^2}, \tag{9}$$

where $y$ is the score vector of the field truth, $\hat{y}$ the score vector obtained by the model and $\overline{y}$ the mean of the scores of $y$.

The $R^2$ score gives information about the quality of the model, for example a model giving the right predictions without taking into account the input data receives a score of 0.0. The score can become negative if the model is bad, while a model giving good results by taking into account the input data has a score that tends towards 1.0.

The explained variance score is a metric used to evaluate the quality of predictions based on a relationship between the difference in variances of the prediction and the field truth:

$$EVS(y, \hat{y}) = 1 - \frac{\text{variance}(y - \hat{y})}{\text{variance}(y)}, \tag{10}$$

where variance is the square of the standard deviation for $y$ and $\hat{y}$, respectively variance($y$) and variance($\hat{y}$).

We also calculate the mean absolute error (Mean-AE), the mean squared error (MSE), the maximum absolute error (Maximum-AE), and the median absolute error (Median-AE).

Table 3 presents the results when we train our model with the MOS values to estimate the value of $p$ according to a $MOS_{desired}$ between 1 and 5. Indeed, the $R^2$ score has a value around 0.8651. In addition, we note that the median absolute error is only 0.5832, which means that the estimated values of $p$ are mostly close to what is expected. Table 3 also presents the results of the estimation models of the parameter $p$ as a function of MOS for the test data. We observe a decrease in scores during the test phase. Indeed, the best results obtained, with the mean values, are 0.7443 compared to 0.8651 during the training phase for the $R^2$ score and the explained variance score is about 0.7508, compared to 0.8651 during the training phase. These results show the robustness of the model using the MOS values for learning.

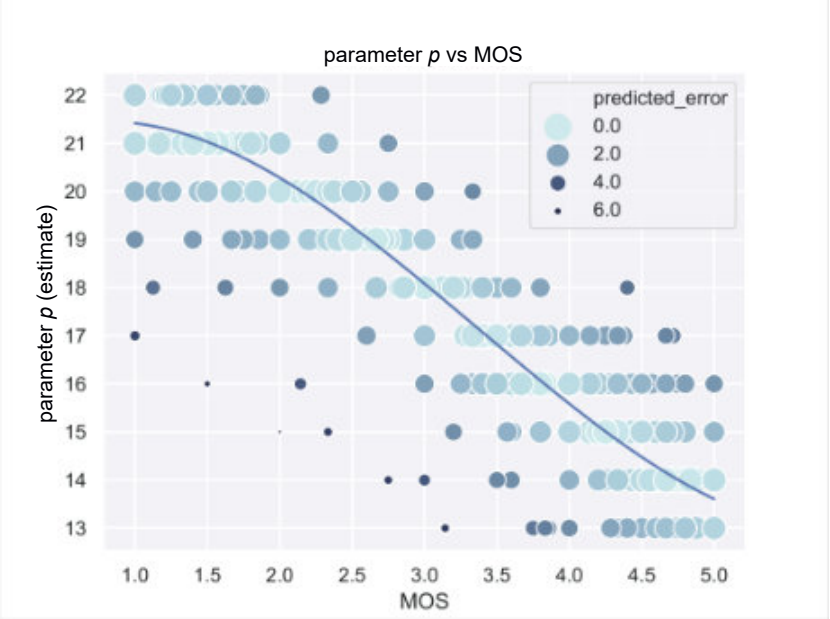



Figure 14: Polynomial regressions for estimating the visual security parameter $p$.

In Fig. 14, we present the polynomial regressions for the estimation of $p$ as a function of the desired visual security level and the MOS values of the 3D object used to train the model. The blue curve represents the obtained polynomial following the polynomial regression for each model. The size of

the markers and their color correspond to the absolute error of the estimation, so the smaller and darker the circle, the higher the error. The coefficients of the polynomial obtained by regression are:

$$f(D) = 21.0404 + \begin{bmatrix} \mathrm{D} & \mathrm{D}^2 & \mathrm{D}^3 \end{bmatrix} \times \begin{bmatrix} 1.6931 \\ -1.2442 \\ 0.1212 \end{bmatrix}. \tag{11}$$

So, thanks to our subjective evaluations we were able to establish a model for the estimation of the encryption parameter $p$ according to a desired level of visual security. We note that the best way to estimate $p$ is obtained with a model using MOS values due to the high scores for $R^2$ and the explained variance, this method also benefits from low errors, as is presented in Table 3.

Table 4 compares the results obtained for the estimations of the parameter $p$ with the model $f(\cdot)$ according to the MOS values for the 3D object #18 of the SE3DO dataset and its 10 encrypted versions with $p$ ranging from 13 to 22, as shown in Fig. 6. We find that we can estimate an encryption parameter $p$ that is relatively close to the one used during the construction of the dataset from the desired level of visual security. The various estimations give slightly lower values for $p$ when the desired level of visual security is greater than or equal to 3. From a desired visual security level of 2, the estimated parameters are higher than the expected encryption parameter. So, our models are able to offer adapted values for the encryption parameter, especially when the desired visual security score is less than or equal to 2. Indeed, the estimated value of $p$ is greater than the expected value.

In this section, we have shown that it is possible to estimate the parameter $p$ from a desired visual security level. We can therefore automatically propose a value for this encryption parameter.

## 5. The proposed 3DVS score

In this section, we develop our proposed regression based 3D Visual Security (3DVS) score, illustrated in Fig. 15. In Section 5.1, we detail the correlation between the MOS values and our different metrics. Then in Section 5.2, we construct a regression model based on the MOS values. In Section 5.3, we present the construction of our 3DVS score based on regression, and finally in Section 5.4 we apply the proposed 3DVS score to another 3D selective encryption method in order to verify its effectiveness.

Still based on our subjective evaluations, we can now build a metric to estimate the level of visual security of selectively encrypted 3D objects as a score. As explained in Section 3.1, estimating the visual security level is very different to estimating the visual quality. Each 3D object in the dataset is studied using the objective metrics with full reference, as presented in Section 2. Each object is then compared to its reference 3D object. Then we can analyze the efficiency of the metrics used to study the visual security level of selectively encrypted 3D objects.

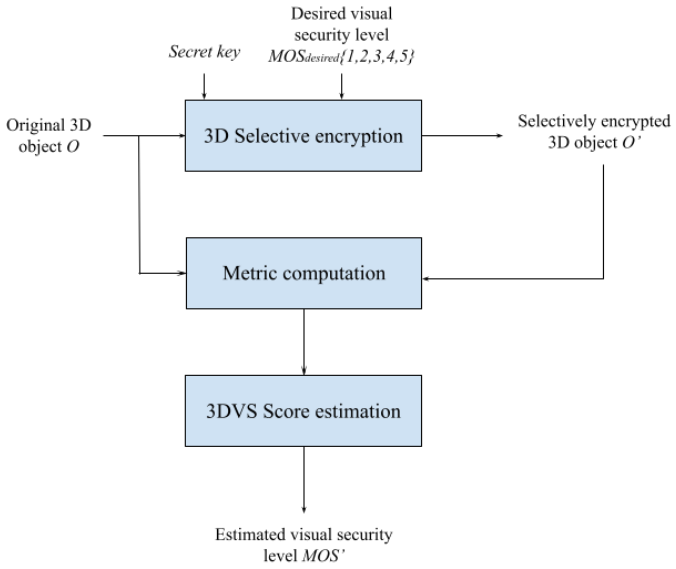



Figure 15: Overview of the proposed 3D-Visual security (3DVS) score.

### *5.1. Correlation*

Table 5 shows the correlation coefficients calculated for the objective metrics log(RMSE), log(HD), DAME, MSDM2 and PSNR, when using the MOS values of each 3D object of our SE3DO dataset.

We can clearly see in Table 5 that the PSNR metric has the highest correlation with a Pearson value of 0.903 and a Spearman value of 0.930. The log(RMSE), log(HD) and MSDM2 metrics also have interesting correlation coefficients (above 0.70 in absolute terms), with the log(RMSE) being the highest. Only the DAME metric is totally independent of the scores given by the observers. We suspect that this is because the DAME metric is based

Table 5: Correlation coefficients between the observers' MOS values and objective metrics.

| | Objective metrics | | | | |
|---|---|---|---|---|---|
| Correlation coefficients | log(RMSE) | log(HD) | DAME | MSDM2 | PSNR |
| Pearson | -0.775 | -0.743 | -0.032 | -0.757 | 0.903 |
| Spearman | -0.815 | -0.794 | -0.116 | -0.776 | 0.930 |

on the mean of the differences in dihedral angles weighted by the area of the triangles. Seeing as how the geometric positions of the vertices vary greatly, we can assume that the areas of the triangles formed by these vertices also vary greatly.

*5.2. Regression model construction*

We notice that the MOS values are distributed in the form of a sigmoid function, in particular in relation to the PSNR which has the highest correlation with the MOS out of all the full reference metrics used. It is for this reason that we wish to construct our linear regression model using a sigmoid function. We therefore use a combination of classic linear regression and logistic regression. We do this by fitting a sigmoid function to the data, without classifying the data into binary categories.

In order to fit the sigmoid, and consequently construct our model, the MOS values which vary between 1 and 5 have to be mapped to values between 0 and 1:

$$y' = \frac{(y-1)}{4}, \tag{12}$$

where $y$ is the original MOS and $y'$ the mapped MOS.

The input data is normalised in order for it to be possible to construct a multi-feature regression model. The sigmoid function is then fit to the data in the same way as is logistic regression:

$$\hat{y'} = \frac{1}{1+\exp^{-z}}, \tag{13}$$

where $\hat{y'}$ is the output value of our model, $z = w_0 + w_1 \times x_0 + w_2 \times x_1 ...$, with $w$ the weights and $x$ the features, and $w_i \in w$ and $x_i \in x$.

Instead of interpreting $\hat{y'}$ as a percentage likelihood as we would in logistic regression, we convert $\hat{y'}$ to a value between 1 and 5, which represents the

Table 6: Results of the polynomial regressions of the selected metrics for the MOS values.

| | 3D metrics | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Training | | | | Testing | | | |
| Regression metrics | log(RMSE) | log(HD) | MSDM2 | PSNR | log(RMSE) | log(HD) | MSDM2 | PSNR |
| $R^2$ score | 0.6450 | 0.5971 | 0.6482 | **0.8991** | 0.6641 | 0.6533 | 0.5582 | **0.9166** |
| Explained Variance Score | 0.6450 | 0.5971 | 0.6482 | **0.8991** | 0.6696 | 0.6653 | 0.5583 | **0.9197** |
| Mean Absolute Error | 0.1509 | 0.1627 | 0.1527 | **0.0794** | 0.1435 | 0.1490 | 0.1693 | **0.0733** |
| Mean Squared Error | 0.0395 | 0.0449 | 0.0390 | **0.0112** | 0.0363 | 0.0375 | 0.0477 | **0.0090** |
| Max Error | 0.6578 | 0.6521 | 0.6155 | **0.4439** | 0.7850 | 0.7437 | 0.6346 | **0.2808** |
| Median Absolute Error | 0.1180 | 0.1232 | 0.1302 | **0.0629** | 0.1137 | 0.1290 | 0.1451 | **0.0572** |

MOS estimated by our model:

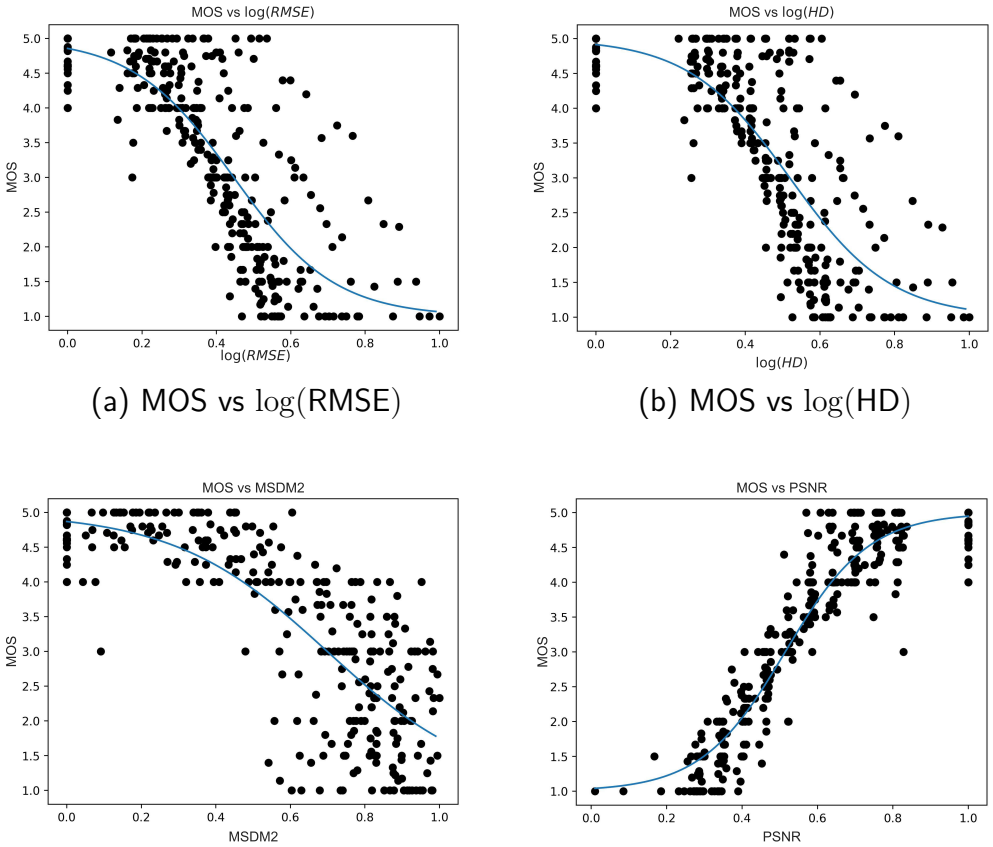
$$\hat{y} = 1 + 4 \times \frac{1}{1 + \exp^{-z}}. \tag{14}$$

*5.3. Construction of the proposed 3DVS score*

We use the sigmoid-based regression model described in Section 5.2 to construct the proposed 3DVS score. Fig. 16 illustrates the sigmoid-based regression model fit to the MOS values for each 3D object of the SE3DO dataset that we have used to train our model. Visually, we observe that the curves closely fit the given data, especially in the case of the PSNR.

In Table 6, we present the different regression metric scores obtained from the training and test phases of the regression models constructed with log(RMSE), log(HD), PSNR and MSDM2. We note that while the PSNR has the best scores for $R^2$ with 0.9166 and for the explained variance with 0.9197, the other three metrics produce interesting results. Therefore, our metric is largely based on the PSNR, but we use the other three metrics in order to render the 3DVS score more robust.

Fig. 17a shows the calculated visual security levels in relation to the ground truth MOS values of the 3D objects of the test dataset (20 reference 3D objects and their 200 variations) according to a regression based on log(RMSE), log(HD), PSNR and MSDM2. Visually, determined visual security levels seem to correspond well to the MOS values of the observers.




(a) MOS vs log(RMSE)

(b) MOS vs log(HD)

(c) MOS vs MSDM2

(d) MOS vs PSNR

Figure 16: Distribution and regression of the MOS values for each encrypted 3D object according to the metric values log(RMSE), log(HD), MSDM2 and PSNR.

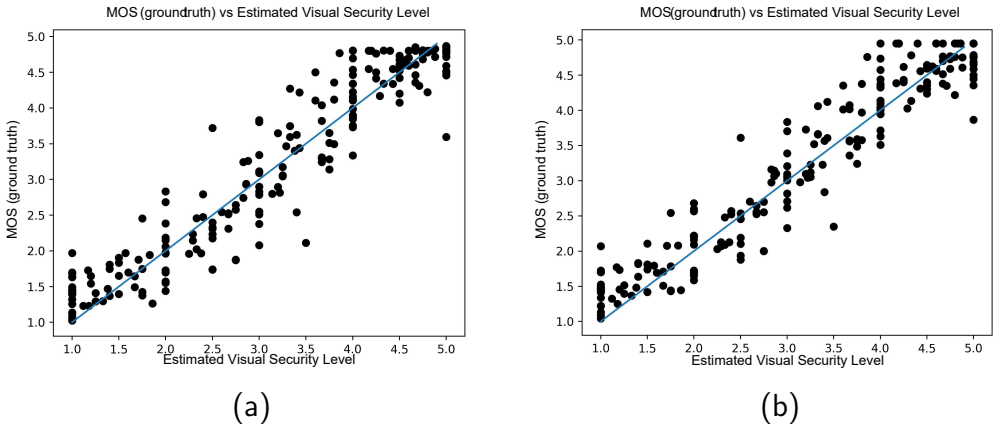



Figure 17: Results from the measurement of the visual security levels from a regression based on the metrics: a) log (RMSE), log (HD), PSNR and MSDM2, b) PSNR and log(RMSE).

This model, noted $g_{All}$, can be formulated as:

$$\begin{cases} g_{All}(O,O') = \alpha + \beta \times \text{PSNR}(O,O') \\ +\gamma \times log(\text{RMSE}(O,O')) + \delta \times log(\text{HD}(O,O')) \\ +\eta \times \text{MDSM2}(O,O'), \\ \alpha = -2.4087, \\ \beta = 6.8352, \\ \gamma = -1.3183, \\ \delta = 0.4188, \\ \eta = -1.0538. \end{cases} \tag{15}$$

Fig. 17b illustrates the determined visual security levels in relation to the ground truth MOS values of the 3D objects of the test base (20 reference 3D objects and their 200 variations) according to a regression based only on the metrics PSNR and log(RMSE). Visually, the determined visual security levels seem to correspond well to the MOS values of the observers. So, this

second model, noted $g_{\text{PSNR,log(RMSE)}}$ can be formulated as:

$$\begin{cases} g_{\text{PSNR},log(\text{RMSE})}(O,O') = \alpha + \beta \times \text{PSNR}(O,O') \\ +\gamma \times log(\text{RMSE}(O,O'), \\ \alpha = -4.0341, \\ \beta = 8.3373, \\ \gamma = -0.5585. \end{cases} \tag{16}$$

Table 7 presents the results of the regression constructed with the four metrics, as well as those constructed with only the PSNR and log(RMSE). We observe that the regression using the PSNR and log(RMSE) gives the best all round results during the testing phase, but in order for our model to be as robust as possible, we can also construct our 3DVS score using $g_{All}$ as it produces similar results.

Table 8 details the visual security level estimated with the proposed regression model for the object #18 from the SE3DO dataset, based on the different full reference metrics. We note that it is mostly the PSNR as well as the combined PSNR and log(RMSE) that produce the most accurate results.

Table 7: Results of the regression constructed with the MOS values of the observers and the different combinations of metrics.

| | 3D metrics | | | |
|---|---|---|---|---|
| | Training | | Test | |
| Regression metrics | $g_{\text{All}}$ | $g_{\text{PSNR,RMSE}}$ | $g_{\text{All}}$ | $g_{\text{PSNR,RMSE}}$ |
| $R^2$ score | **0.8993** | 0.8966 | 0.9127 | **0.9168** |
| Expl. Variance Score | **0.8993** | 0.8966 | 0.9142 | **0.9201** |
| Mean Absolute Error | **0.0792** | 0.0801 | 0.0754 | **0.0728** |
| Mean Squared Error | **0.0112** | 0.0115 | 0.0094 | **0.0090** |
| Max Error | 0.4540 | **0.4412** | 0.3192 | **0.2833** |
| Med. Absolute Error | **0.0624** | 0.0641 | 0.0596 | **0.0589** |

### *5.4. Application of the proposed 3DVS score to another 3D selective encryption method*

In this section, in order to verify the effectiveness of the proposed 3DVS score, we propose to apply it to another 3D selective encryption method.

Table 8: Determined visual security levels based on the MOS values and the metrics for the 3D object #18 shown in Figure 6.

| | Observed MOS | | | | | | |
|---|---|---|---|---|---|---|---|
| $p$ | MOS | $PSNR$ | $MSDM2$ | $log(RMSE)$ | $log(HD)$ | $All$ | $PSNR/RMSE$ |
| 0 | 5.00 | **4.95** | 4.87 | 4.86 | 4.92 | **4.95** | **4.95** |
| 13 | 5.00 | **4.75** | 4.27 | 4.49 | 4.46 | 4.73 | **4.74** |
| 14 | 5.00 | **4.59** | 3.86 | 4.34 | 4.33 | 4.54 | **4.58** |
| 15 | 4.71 | **4.35** | 3.32 | 4.15 | 4.15 | 4.26 | **4.34** |
| 16 | 4.00 | **4.01** | 2.73 | 3.92 | 3.94 | 3.85 | **4.01** |
| 17 | 3.67 | 3.57 | 2.28 | **3.66** | 3.73 | 3.35 | **3.58** |
| 18 | 3.22 | 3.06 | 2.09 | **3.37** | 3.44 | 2.87 | **3.08** |
| 19 | 2.40 | **2.54** | 2.03 | 3.06 | 3.09 | **2.43** | 2.58 |
| 20 | 1.00 | 2.08 | **2.01** | 2.76 | 2.83 | **2.05** | 2.12 |
| 21 | 1.00 | **1.71** | 2.07 | 2.46 | 2.50 | **1.76** | **1.76** |
| 22 | 1.00 | **1.45** | 2.11 | 2.17 | 2.26 | 1.52 | **1.48** |

Indeed, while the proposed dataset is constructed using the selective encryption method developed by Beugnon *et al.* (4), the proposed 3DVS score is able to evaluate the visual security level of 3D objects selectively encrypted using other methods.

Another 3D selective encryption method is used to perform a comparison. This selective encryption method encrypts the vertices of a 3D object by adding pseudo-random values to the three coordinates of each vertex $v_i\{x_i, y_i, z_i\}$. These pseudo-random values have a Gaussian distribution centered in 0 with a standard deviation $\sigma$. From a 3D object $O$ which is composed of $V$ vertices $v_i$, a selective encrypted 3D object $O'$ is obtained by adding a pseudo-random Gaussian noise to each vertex:

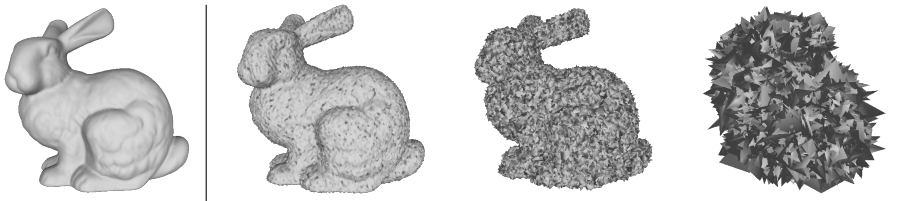
$$v'_i = E_K(v_i), \tag{17}$$

where $E_K()$ is the encryption function, with $K$ the secret key and $i \in [0, V-1]$ such as:

$$\begin{cases} x'_i = x_i + \mathcal{N}_{K,\sigma}(i \times 3) \\ y'_i = y_i + \mathcal{N}_{K,\sigma}(i \times 3 + 1) \\ z'_i = z_i + \mathcal{N}_{K,\sigma}(i \times 3 + 2), \end{cases} \tag{18}$$

where $\mathcal{N}_{K,\sigma}()$ is a pseudo-random Gaussian number generator with a standard deviation $\sigma$ and based on the secret key $K$. This method is fully reversible. For the decryption, the same sequence of pseudo-random values is

generated again using the same key, and are subtracted from the encrypted 3D object. The level of selective encryption depends on the value of $\sigma$ used for the Gaussian distribution.



(a) Original (b) Transparent (c) Sufficient (d) Confidential

Figure 18: Selectively encrypted 3D object *Bunny* (Object #44) with the encryption method based on a pseudo-random Gaussian number generator.

Fig. 18 presents the 3D object *Bunny*, which is selectively encrypted with this method. The visual security level is increased by increasing the standard deviation $\sigma$ of the pseudo-random Gaussian number generator. Fig. 18.a. presents the original 3D object included in the proposed dataset. Fig. 18.b. illustrates the selectively encrypted 3D object when using a standard deviation $\sigma$ $3 \times 10^{-3}$. In this case, the obtained 3DVS score is $[3.163] = 3$, which corresponds to a transparent level. Fig. 18.c. illustrates the selectively encrypted 3D object with a standard deviation $\sigma$ of $10 \times 10^{-3}$. In this case, the obtained 3DVS score is $[1.657] = 2$, corresponding to a sufficient level. Finally, Fig. 18.d. illustrates the selectively encrypted 3D object with a standard deviation $\sigma = 100 \times 10^{-3}$. In this case the obtained 3DVS score is 1, meaning that we have a confidential level.

These experimental results confirm that our 3DVS score performs well on 3D objects which were selectively encrypted with another encryption method.

## 6. Conclusion

In this paper, we proposed a new dataset of selectively encrypted 3D objects and their opinion scores (OS). Based on the dataset and full reference metrics, we used a polynomial regression model to estimate the encryption parameter for selectively encrypted 3D objets Then we developed a new metric, 3DVS score, which serves to evaluate the visual security level of selectively encrypted 3D objects.

Methods based on selective encryption approaches generate 3D objects that can have a transparent, sufficient or a confidential visual security level.

However, it is difficult to establish the pivotal thresholds for change between these three levels when using objective methods. Furthermore, depending on the encryption parameters, the geometry, and the connectivity of the 3D object, the results can vary significantly. To address this we have built a dataset of 550 3D objects, 500 of which are selectively encrypted and used within a subjective evaluation campaign. We have named this new dataset the SE3DO dataset. This includes the OS collected from 54 different observers and is dedicated to selectively encrypted 3D objects (4). Using our SE3DO dataset, we then created a linear regression model designed to estimate encryption parameters according to the desired visual security level for selectively encrypted 3D objects. Finally, with the SE3DO dataset, we developed a new visual security metric 3DVS score for selectively encrypted 3D objects. The 3DVS score was constructed with sigmoid-based regression models and remains effective when used with another 3D selective encryption method.

In future work, we wish to further exploit subjective data assessment by using learning-based approaches such as neural networks, convolutional neural networks (2D and 3D) and by taking advantage of the inherent characteristics of 3D objects. This type of approach should allow us to propose solutions in the case of encrypted 3D objects desynchronized with the original 3D object.In future work, we propose also to develop new visual security metrics for encrypted 3D objects based on metrics with reduced-reference or no-reference methods.

## References


[1] B. L. Yeo, M. M. Yeung, Watermarking 3D objects for verification, IEEE Computer Graphics and Applications 19 (1) (1999) 36–45.

[2] M. Gschwandtner, A. Uhl, Protected Progressive Meshes, in: Advances in Visual Computing, Springer, 2009, pp. 35–48.

[3] M. Éluard, Y. Maetz, G. J. Doërr, Impact of geometry-preserving encryption on rendering time, in: 2014 IEEE International Conference on Image Processing (ICIP), IEEE, 2014, pp. 4787–4791.

[4] S. Beugnon, W. Puech, J. Pedeboy, From Visual Confidentiality To Transparent Format-Compliant Selective Encryption Of 3D Objects, in:

2018 IEEE International Conference on Multimedia and Expo Workshops (ICME Workshops), IEEE Computer Society, 2018, pp. 1–6.

[5] S. Beugnon, W. Puech, J. P. Pedeboy, A Format-Compliant Selective Secret 3D Object Sharing Scheme Based on Shamir's Scheme, in: IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2019, pp. 2657–2661.

[6] S. Beugnon, W. Puech, J.-P. Pedeboy, Format-Compliant Selective Secret 3D Object Sharing Scheme, IEEE Transactions on Multimedia 21 (9) (2019) 2171–2183.

[7] A. Pommer, A. Uhl, Application Scenarios for Selective Encryption of Visual Data, in: Multimedia and Security Workshop (ACM Multimedia), 2002, pp. 71–74.

[8] A. Shamir, How to share a secret, Communications of the ACM 22 (11) (1979) 612–613.

[9] E. Elsheh, A. B. Hamza, Secret sharing approaches for 3D object encryption, Expert Systems with Applications 38 (11) (2011) 13906–13911.

[10] Y.-Y. Tsai, A Secret 3D Model Sharing Scheme with Reversible Data Hiding Based on Space Subdivision, 3D Research 7 (1) (2016) 1.

[11] S.-S. Lee, Y.-J. Huang, J.-C. Lin, Protection of 3D models using cross recovery, Multimedia Tools and Applications 76 (1) (2017) 243–264.

[12] N. Aspert, D. Santa-Cruz, T. Ebrahimi, Mesh: Measuring errors between surfaces using the hausdorff distance, in: Proceedings of the 2002 IEEE International Conference on Multimedia and Expo (ICME), Vol. 1, IEEE, 2002, pp. 705–708.

[13] P. Cignoni, C. Rocchini, R. Scopigno, Metro: Measuring error on simplified surfaces, in: Computer Graphics Forum, Vol. 17, Wiley Online Library, 1998, pp. 167–174.

[14] N. Aspert, E. Drelie, Y. Maret, T. Ebrahimi, Steganography for three-dimensional polygonal meshes, in: International Symposium on Optical Science and Technology, International Society for Optics and Photonics, 2002, pp. 211–219.

[15] M.-W. Chao, C.-h. Lin, C.-W. Yu, T.-Y. Lee, A high capacity 3D steganography algorithm, IEEE Transactions on Visualization and Computer Graphics 15 (2) (2009) 274–284.

[16] G. Lavoué, A Multiscale Metric for 3D Mesh Visual quality assessment, Computer Graphics Forum 30 (5) (2011) 1427–1437.

[17] J. Bennour, J. L. Dugelay, Toward a 3D watermarking benchmark, in: 2007 IEEE 9th Workshop on Multimedia Signal Processing, 2007, pp. 369–372.

[18] K. Wang, G. Lavoué, F. Denis, A. Baskurt, X. He, A Benchmark for 3D Mesh Watermarking, in: 2010 Shape Modeling International Conference, 2010, pp. 231–235.

[19] Y. Nehmé, J.-P. Farrugia, F. Dupont, P. Le Callet, G. Lavoué, Comparison of subjective methods, with and without explicit reference, for quality assessment of 3D graphics, in: ACM Symposium on Applied Perception 2019, (SAP), ACM, 2019, pp. 17:1–17:9.

[20] E. D. Gelasca, T. Ebrahimi, M. Corsini, M. Barni, Objective evaluation of the perceptual quality of 3D watermarking, in: IEEE International Conference on Image Processing (ICIP), IEEE, 2005, pp. 241–244.

[21] K. Vanhoey, B. Sauvage, P. Kraemer, G. Lavoué, Visual Quality Assessment of 3D Models: On the Influence of Light-Material Interaction, ACM Transactions on Applied Perception 15 (1) (2017) 1–18.

[22] G. Lavoué, M. Corsini, A Comparison of Perceptually-Based Metrics for Objective Evaluation of Geometry Processing, IEEE Transactions on Multimedia 12 (7) (2010) 636–649.

[23] K. Wang, F. Torkhani, A. Montanvert, A fast roughness-based approach to the assessment of 3D mesh visual quality, Computers & Graphics 36 (7) (2012) 808–818.

[24] G. Lavoué, I. Cheng, A. Basu, Perceptual Quality Metrics for 3D Meshes: Towards an Optimal Multi-attribute Computational Model, in: IEEE International Conference on Systems, Man, and Cybernetics (SMC), IEEE, 2013, pp. 3271–3276.

[25] L. Dong, Y. Fang, W. Lin, H. S. Seah, Perceptual Quality Assessment for 3D Triangle Mesh Based on Curvature, IEEE Transactions on Multimedia 17 (12) (2015) 2174–2184.

[26] Y. Yao, Z. Xu, J. Sun, Visual Security Assessment for Cipher-Images based on Neighborhood Similarity, Informatica (Slovenia) 33 (2009) 69–76.

[27] T. Xiang, S. Guo, X. Li, Perceptual Visual Security Index Based on Edge and Texture Similarities, IEEE Transactions on Information Forensics and Security 11 (5) (2016) 951–963.

[28] T. Xiang, Y. Yang, H. Liu, S. Guo, Visual Security Evaluation of Perceptually Encrypted Images Based on Image Importance, IEEE Transactions on Circuits and Systems for Video Technology 30 (11) (2020) 4129–4142.

[29] A. S. Abraham, L. R. Nair, M. S. Deepa, A novel method for evaluation of visual security of images, in: 2017 International Conference on Networks Advances in Computational Technologies (NetACT), 2017, pp. 387–391.

[30] S. Guo, T. Xiang, X. Li, Y. Yang, PEID: A Perceptually Encrypted Image Database for Visual Security Evaluation, IEEE Transactions on Information Forensics and Security 15 (2020) 1151–1163.

[31] Y. Yang, T. Xiang, H. Liu, X. Liao, Convolutional neural network for visual security evaluation, IEEE Transactions on Circuits and Systems for Video Technology 31 (8) (2021) 3293–3307.

[32] R. L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21 (2) (1978) 120–126.

[33] J. Daemen, V. Rijmen, The design of Rijndael: AES –the Advanced Encryption Standard, Springer–Verlag, Berlin, 2002.

[34] M. Cho, S. Kim, M. Sung, G. On, 3D Fingerprinting and Encryption Principle for Collaboration, in: International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution (AXMEDIS), IEEE, 2006, pp. 121–127.

[35] L. Vása, J. Rus, Dihedral Angle Mesh Error: a fast perception correlated distortion measure for fixed connectivity triangle meshes, Computer Graphics Forum 31 (5) (2012) 1715–1724.

[36] G. Lavoué, E. Gelasca, F. Dupont, A. Baskurt, T. Ebrahimi, Perceptually driven 3D distance metrics with application to watermarking, Proceedings of SPIE - The International Society for Optical Engineering 6312.

[37] Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, Image quality assessment: from error visibility to structural similarity, IEEE Transactions on Image Processing 13 (4) (2004) 600–612.

[38] S. Jenisch, A. Uhl, Visual Security Evaluation Based on SIFT Object Recognition, in: Artificial Intelligence Applications and Innovations, Springer Berlin Heidelberg, 2014, pp. 624–633.

[39] D. Lowe, Distinctive image features from scale-invariant keypoints, International Journal of Computer Vision 60 (2004) 91.

[40] J. Guo, Contributions to objective and subjective visual quality assessment of 3D models. (contributions à l'évaluation objective et subjective de la qualité visuelle des modèles 3D), Ph.D. thesis, University of Lyon, France (2016).

[41] X. Chen, A. Golovinskiy, T. Funkhouser, A Benchmark for 3D Mesh Segmentation, ACM Transactions on Graphics (TOG) 28 (3) (2009) 73.

[42] G. Lavoué, J. Vandeborre, H. Benhabiles, M. Daoudi, K. Huebner, M. Mortara, M. Spagnuolo, SHREC'12 Track: 3D Mesh Segmentation, in: Eurographics Workshop on 3D Object Retrieval 2012, Eurographics Association, 2012, pp. 93–99.

[43] D. Pickup, X. Sun, P. L. Rosin, R. R. Martin, Z. Cheng, Z. Lian, M. Aono, A. B. Hamza, A. M. Bronstein, M. M. Bronstein, S. Bu, U. Castellani, S. Cheng, V. Garro, A. Giachetti, A. Godil, J. Han, H. Johan, L. Lai, B. Li, C. Li, H. Li, R. Litman, X. Liu, Z. Liu, Y. Lu, A. Tatsuma, J. Ye, Shape Retrieval of Non-Rigid 3D Human Models, in: Eurographics Workshop on 3D Object Retrieval, Eurographics Association, 2014, pp. 101–110.

[44] Q. Zhou, A. Jacobson, 2018 Cover Image: Thingi10K, Computer Graphics Forum 37 (1) (2018) 451–452.

[45] B. T. Phong, Illumination for Computer Generated Pictures, Communications of the ACM 18 (6) (1975) 311–317.