MSB-Based Reversible Data-Hiding in Encrypted 3D Object Using a Hamiltonian Path

Erwan Reinders, Bianca Jansen van Rensburg, Pauline Puteaux, William Puech

MSB-based Reversible Data-Hiding in Encrypted 3D Object using a Hamiltonian Path

Erwan Reinders[1] Bianca Jansen van Rensburg[1,2] Pauline Puteaux[3] William Puech[1]

[1] LIRMM, Univ. Montpellier, CNRS, Montpellier, France
[2] Stratégies, Rungis, France
[3] Univ. Lille, CNRS, Centrale Lille, UMR 9189 CRIStAL, F-59000 Lille, France

***Abstract*—Nowadays, 3D objects are frequently stored and shared online, where they become vulnerable to attacks. Therefore, applying security measures such as encryption is crucial. Once the 3D object is encrypted and stored online, a third party who is not authorized to access the content of the 3D object may need to embed hidden data in the 3D object. In this paper, we propose a new MSB-based reversible data-hiding in the encrypted domain method for 3D objects, which uses a Hamiltonian path to establish a unique order for the vertices of a 3D object. For the reconstruction step, we select the smallest distance between vertices to accurately predict the MSB value of the mantissa for each coordinate. Our proposed method is format compliant, avoids any size expansion, and does not require auxiliary file, while guaranteeing the reversibility of the marked encrypted 3D object, even when tested on a large database of 3D objects.**

***Index Terms*—Multimedia security, 3D object, reversible data-hiding in the encrypted domain, Hamiltonian path.**

I. Introduction

Over the last few decades, multimedia data, in particular 3D objects, are transmitted, stored and shared online. They are then vulnerable to attacks such as copying or modification. The security of 3D objects is therefore essential, not to say unavoidable. A 3D object can be secured with encryption methods by converting it to unintelligible ciphertext. Once the multimedia is encrypted and stored online, a third party, for example the server, who does not have the right to access the clear 3D object may need to embed hidden data in the multimedia. Reversible data-hiding in the encrypted domain (RDH-ED) methods can be used to embed data into an encrypted media, without knowing its original content.

In order to reconstruct the original content, many methods for multimedia RDH-ED are based on prediction. The original pixel values, in the case of images, or vertices, in the case of 3D objects, are estimated according to a prediction criteria once the content has been decrypted. In 2018, Puteaux and Puech proposed a high capacity RDH-ED method for images based on MSB prediction [1]. They used the high local correlation between a pixel and its neighbors in the clear domain in order to predict the MSB values of a pixel based on the previously decrypted neighboring pixels. For 3D objects, defining a neighbor is more challenging than for images, as they consist of an unordered set of vertices. Itier *et al.* proposed using a Hamiltonian path to create a unique synchronisation order for the vertices of a 3D object [2]. Itier and Puech then used this Hamiltonian path construction to embed data in the point cloud of a 3D object [3]. Most RDH-ED methods for 3D objects consist of dividing the vertices into an embedding set and a prediction set, where vertices in the prediction set are used to correct the marked vertices in the embedding set. In 2018, Jiang *et al.* proposed the first RDH-ED method for 3D objects, based on LSB substitution, where a vertex is added to the embedding set and its one-ring to the reference set [4]. Xu *et al.* then used the higher correlation between the MSB in the plaintext domain to perform a vertex prediction on the MSB instead of multiple LSB [5]. In 2022, Tsai and Liu proposed randomly choosing a percentage of neighbors according a given threshold and basing the prediction on the center of gravity of the neighboring vertices [6]. Lyu *et al.* proposed optimizing the distribution between the embedding set and the prediction set by using the vertices' parity as the division criteria [7]. In 2020, Tsai proposed a RDH-ED method for 3D objects based on spatial subdivision and space encoding of the 3D object [8]. Some RDH-ED methods for 3D objects are based on the Paillier homomorphic cryptosystem. In 2018, Shah *et al.* proposed a two tier homomorphic RDH-ED scheme method for 3D objects [9]. In 2023, Jansen van Rensburg *et al.* proposed a multi-message RDH-ED method where the 3D object remains watermarked once decrypted [10].

In this paper, we propose a new RDH-ED method for 3D objects which is based on a Hamiltonian path used to define a unique order for vertices in the 3D object. We then use the small distances between the vertices to predict the correct MSB value of the mantissa of each of their coordinates during the reconstruction step. The proposed method is format compliant, has no size expansion and does not require an auxiliary file.

II. The proposed 3D data-hiding method in the encrypted domain

In this section, we present the proposed RDH-ED method based on an MSB prediction using a Hamiltonian path.

A. Overview of the proposed encoding phase

Fig. 1 presents an overview of the encoding phase of our proposed method. First, the 3D object undergoes a preprocessing step. Then, the spatial processing order of the vertices of the 3D object needs to be established in order to accurately predict the value of the next vertex during the decoding phase. We note that this is more challenging than in 2D images, as

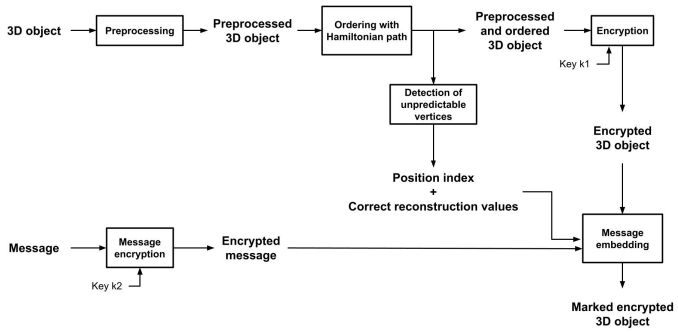


Fig. 1: General overview of the encoding phase of the proposed RDH-ED method.

3D objects are composed of an unordered set of vertices. We therefore use a Hamiltonian path to order the vertices of the 3D object [2]. The Hamiltonian path guarantees that the next vertex in the path has the smallest Euclidean distance to the previous vertex, among the remaining vertices. This property is used to accurately predict the value of the vertices during the decoding phase, as the 3D object's vertices are ordered directly in its file when the encoded object is saved. Then, the vertices that cannot be predicted during the reconstruction step are identified. The preprocessed and ordered 3D object is encrypted with a secret encryption key K_1 and both the positions and the values of the incorrectly predicted vertices, called auxiliary information, are embedded by substitution of the MSB values of the first encrypted vertices coordinates. During the data-hiding step, a secret message (encrypted with a secret data-hiding key K_2) can be embedded in a similar way in all remaining encrypted vertices of the 3D object.

B. Hamiltonian path construction

We note the original 3D object O, which is represented by a set of n vertices $V = \{v_1, ..., v_n\}$ and l binary associations between these vertices, a set of edges $E = \{e_1, ..., e_l\}$. Each vertex consists of three coordinates x, y and z, where each of which can be represented by a 32-bit floating point fp, which consists of a sign s (1 bit), an exponent e (8 bits) and a mantissa $mant$ (23 bits) where: $fp = (-1)^s \times mant \times 2^{e-127}$.

In this paper, we propose constructing the Hamiltonian path [3] of a 3D object in order to define the processing order of the vertices. We rely on this order to predict the reconstruction of the vertices during the decoding phase. The construction of a Hamiltonian path is described in Algorithm 1. For each vertex v_i in the Hamiltonian path, the vertex v_{i+1} is the closest to v_i in terms of the Euclidean distance, where v_{i+1} is not already in the Hamiltonian path ($v_{i+1} \notin HPath$). During the decoding phase, we exploit this property in order to predict each vertex value and thus accurately reconstruct the original 3D object. We note that the Hamiltonian path produces a single vertex order for the 3D object for every given starting vertex v_k. We define μ_H as the average Euclidean distance of a connection $v_i \rightarrow v_{i+1}$ in the Hamiltonian path, and σ_H the standard deviation of the Euclidean distance distribution for all Hamiltonian connections.

Algorithm 1 Hamiltonian path construction

Require: A 3D object $O = \{V, E\}$, a starting vertex v_k and a function $nearestNeighbor(v, X)$ to get the nearest neighbor of v in the set X.
Ensure: A 3D Hamiltonian path of the 3D object O

$HPath \leftarrow \{v_k\}$
$V' \leftarrow V$
$E' \leftarrow E$
$v_i \leftarrow v_k$
while $V' \neq \emptyset$ **do**
  $V' \leftarrow V' \setminus \{v_i\}$
  $v_{i+1} \leftarrow nearestNeighbor(v_i, V')$
  $HPath \leftarrow HPath \cup \{v_{i+1}\}$
  $v_i \leftarrow v_{i+1}$
end while
return $HPath$

C. Vertex prediction

During the data-hiding step, the p MSB of the mantissa of each encrypted coordinate are substituted with the message (auxiliary information + secret message) to be embedded. Therefore, during the 3D object reconstruction step, the correct MSB values of each vertex need to be predicted. In this paper, we present a p MSB prediction for each vertex in the 3D object, based on the constructed Hamiltonian path.

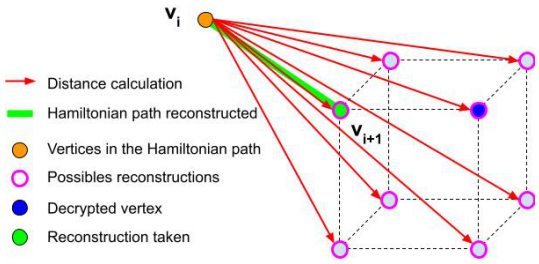


Fig. 2: Prediction example, with $p = 1$, on a predictable vertex.

Fig. 2 illustrates the prediction step for a vertex v_{i+1} in the Hamiltonian path, based on the previous vertex v_i. We assume that all previously predicted vertices in the Hamiltonian path are correct. As p MSB of the mantissa of each coordinate need to be predicted, the vertex v_{i+1} has $2^{3\times p}$ possible reconstructions.

According to Algorithm 1, v_{i+1} is the vertex with the minimum Euclidean distance from v_i among these $2^{3\times p}$ possible reconstructions. In order to increase the probability that the correct reconstruction of v_{i+1} is the possible reconstruction with the minimum Euclidean distance to v_i, and consequently avoid incorrect predicted values, the 3D object is first translated by a twice the value of the diagonal of the bounding box during the processing step:

$$D = \sqrt{(x_{max} - x_{min})^2 + (y_{max} - y_{min})^2 + (z_{max} - z_{min})^2}, \quad (1)$$

where x_{min} is the minimum x coordinate among all x coordinates of all vertices (similarly for y_{min} and z_{min}, but with

y and z coordinates respectively). The values of x_{max}, y_{max} and z_{max} are obtained in the same way, but for maximum x, y and z coordinates respectively. This translation increases the value of the exponent e of the coordinates and consequently increases the impact of the MSB in the mantissa. Therefore, the probability of selecting the correct predicted value of v_{i+1} during the reconstruction step is increased, as the correct predicted vertex is more likely to be the closest predicted vertex to the previous vertex v_i. In order for the translation to be most effective, we assume that the 3D objects are centered on $(0, 0, 0)$ (*i.e.* $-x_{min} \simeq x_{max}$, $-y_{min} \simeq y_{max}$, $-z_{min} \simeq z_{max}$).

However, while the translation operation increases the chances of a correct prediction, some vertices v_{i+1} in the Hamiltonian path remain unpredictable. There are two categories of unpredictable vertices. There are **topological discontinuities** when two consecutive vertices v_i and v_{i+1} do not share an edge. If all the vertices that share an edge with v_i are already in the Hamiltonian path, then a vertex v_{i+1} which does not share an edge is selected. This type of connection produces topological discontinuities in the Hamiltonian path. It is also common in 3D objects where different sections of the 3D object's geometry are close and do not share a direct connection, such as, for example, a 3D object representing a hand with closely spaced fingers. We define **large distances connections** when the distance between v_i and v_{i+1} is greater than $(\mu_H + k \times \sigma_H)$, where $k \in \mathbb{N}$ is a threshold. These connections may or may not share an edge. They are more common at the end of the Hamiltonian path, however may also appear earlier in the Hamiltonian path, depending on the shape of the 3D object. These connections are more difficult to predict in the reconstruction step. To ensure the reversibility of our method, the first bits of the embedded message are dedicated to highlighting all the unpredictable vertices, by storing both their positions and their values as auxiliary information.

D. Data-hiding in the encrypted domain

After the detection of all the unpredictable vertices, the preprocessed and ordered 3D object is encrypted. With the help of a secret encryption key K_1, a pseudo-random binary sequence is generated. This sequence is used for the encryption of each vertex by performing an exclusive-OR operation with the bits of the mantissa of each coordinate. During the data-hiding step in the encrypted domain, the embedded message is composed of two different parts:

- The **auxiliary information** (*i.e.* unpredictable vertex information): binary information used to reconstruct the n' unpredictable connections.
- The **secret message**: the message embedded by the user.

For each vertex v_i, the message is embedded in the mantissa of each coordinate by means of an MSB substitution, as proposed by Puteaux and Puech for data-hiding in encrypted images [1]. We note p the number of MSB per coordinate substituted during the embedding process. Therefore, the embedding rate, which is determined by the total number of bits per vertex (bpv) reserved for the message embedding, is noted $3 \times p$ bpv. Consequently, the maximum message length is:

$$m_{length} = (n-1) \times (3 \times p), \tag{2}$$

where n is the number of vertices in the 3D object. We note that $(n-1)$ vertices are used for embedding, as the first vertex needs to be intact in order to predict the second vertex. Fig. 3 illustrates the data-hiding step. The auxiliary information includes the number of unpredictable vertices, as well as their position and their values.

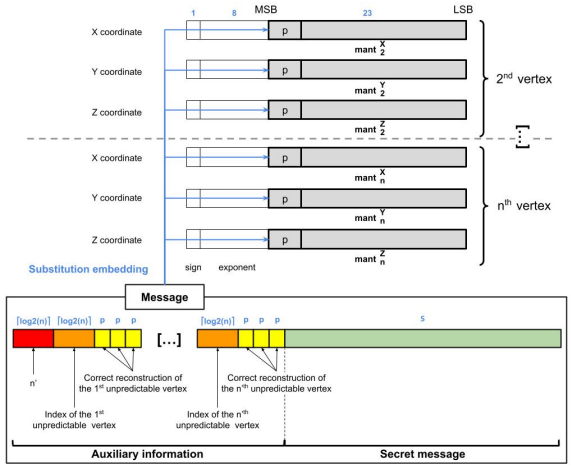


Fig. 3: Message embedding step.

The number n' of unpredictable vertices, as well as their positions, is embedded using $\lceil log2(n) \rceil$ bits, as the maximum value of a vertex position is n. This size is also useful during the decoding phase, as n is known in the file format. The bit size A of the auxiliary information is given by:

$$A = \lceil log2(n) \rceil + (\lceil log2(n) \rceil + (3 \times p)) \times n'. \tag{3}$$

After the embedding of the auxiliary information, one can embed bits of the secret message in every remaining encrypted vertex, without knowing the original 3D object in clear nor the secret encryption key K_1. Note that, for the sake of confidentiality, this secret message is encrypted using a secret data-hiding key K_2 before being embedded. The bit size S of this secret message part is given by: $S = m_{length} - A$. The payload, corresponding to the number of bits of the secret message embedded in a vertex is:

$$payload = \frac{S}{n} = \frac{(n-1) \times (3 \times p) - A}{n}. \tag{4}$$

We observe that when n is large, $payload \approx$ 3 bpv. This is also true when A is null. We can also compute the maximum value of n', which depends on n and p:

$$n'_{max} = \frac{(n-1) \times (3 \times p) - \lceil log2(n) \rceil}{\lceil log2(n) \rceil + (3 \times p)}. \tag{5}$$

E. Message extraction and object reconstruction

To extract the message, the p MSB of each coordinate of every vertex are read, with the exception of the first vertex. If we possess the secret data-hiding key K_2, the secret message

(after the auxiliary information) is then decrypted using K_2 to reconstruct the secret message in clear. Note that, in this case, the content of the original 3D object remains protected.

If we possess the secret encryption key K_1, then for each coordinate of each vertex in the 3D object, the mantissa is decrypted using K_1. The decrypted vertices can then be reconstructed. For the unpredictable vertices, we read the auxiliary information from the extracted message and reconstruct them with Eq. 3. In order for all the remaining vertices to be reconstructed, their $2^{3\times p}$ possible reconstructions are calculated. In this paper, we take $p = 1$ and therefore there are 8 possible combinations for the reconstruction. To select the right reconstruction, we refer to the same Hamiltonian path of the 3D object as the encoding phase, deduced from the 3D object file due to the vertex reordering. The vertex v_{i+1} is considered to be the possible reconstruction with the minimum Euclidean distance from v_i. Once all the vertices are reconstructed, the bounding box of the reconstructed 3D object is calculated, and inverse translation is performed.

If we possess both keys, then the secret message can be retrieved and the 3D object can be reconstructed.

III. Experimental results

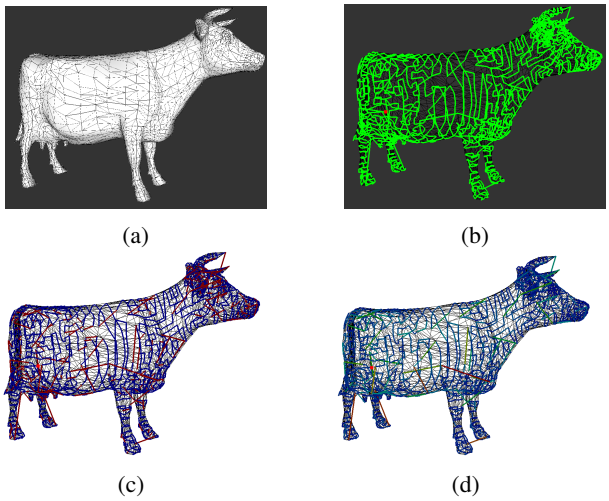
In this section, we present experimental results of the proposed RDH-ED method.

A. A full example on a single 3D object

We present a full example of our proposed method when applied to the 3D object *Cow* from the Stanford database [11]. The 3D object *Cow*, illustrated in Fig. 4a, is composed of 2,903 vertices and is approximately centered in zero, with a bounding box of: $x_{min} = -0.690$, $y_{min} = -0.583$, $z_{min} = -0.272$, $x_{max} = 0.980$, $y_{max} = 0.440$ and $z_{max} = 0.272$. We note that the mean Euclidean distance between two vertices that share an edge is 34.934×10^{-3}.

In our experimental results, we set the embedding parameter $p = 1$ which means that the message is embedded in one MSB of the mantissa per coordinate. The message has then a length of $2,902 \times 3 = 8,706$ bits (according to Eq. 2), and therefore during the reconstruction step there are $2^3 = 8$ possible values for a vertex v_{i+1} to be predicted. We note that in this case, the maximum number of unpredictable vertices allowed is $n'_{max} = \frac{2,902\times3-12}{12+3} = 579$ vertices (according to Eq. 5).

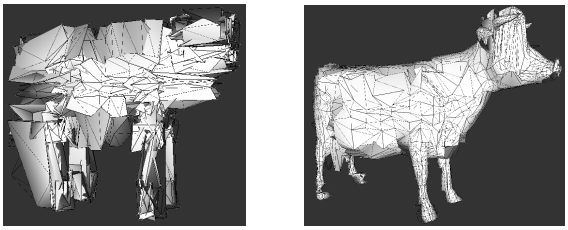
Fig. 4b illustrates the results of the constructed Hamiltonian path, starting at the vertex #546 (red dot) of the 3D object *Cow* (Fig. 4a). The mean Euclidean distance between two connected vertices in the Hamiltonian path is $\mu_H = 25.092 \times 10^{-3}$ and the standard deviation is $\sigma_H = 23.935 \times 10^{-3}$. The minimum distance between two connected vertices is 3.271×10^{-3} and the maximum is 0.345. We note that for this 3D object, the value of μ_H is similar to the mean length of an edge. Fig. 4c illustrates the various topological discontinuities in the Hamiltonian path (in red). With vertex #546 as the starting vertex for the Hamiltonian path, we have 269 (9.266%) topological discontinuities. Fig. 4d presents, with colors, the Euclidean distances of the vertex connections in the Hamiltonian path. The smallest connections tend towards blue, while the larger connections tend towards red. We can observe from the many dark blue vertex connections that most vertex connections have a distance close to the minimum distance.



(a) (b) (c) (d)

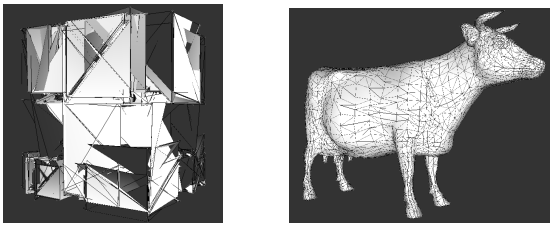
Fig. 4: a) The original 3D object *Cow* [11], b) The Hamiltonian order starting from the vertex #546 (red dot), c) Topological discontinuities (red) in the Hamiltonian path, d) Distances between connected vertices in the Hamiltonian path (from blue to red).

1) Without the preprocessing step: We first present the results obtained for the encoding and reconstruction step, without the preprocessing step, the detection of the unpredictable vertices or the threshold on the distance connections. Fig. 5a presents the marked encrypted 3D object *Cow*. We can notice that the 3D object does not have a confidential visual security level [12], as the form of the 3D object is still visually accessible. Fig. 5b presents the results of the vertex prediction without any preprocessing steps. In this case, we have 994 incorrect reconstructions (34.24%) and obtain an RMSE of 40.104×10^{-3} and a Hausdorff distance of 0.102 between the original 3D object and the reconstructed version. There is no auxiliary information embedded and so the embedded message is actually the secret message. Therefore the payload is $\frac{2,902\times3}{2,903} = 2.99$ bpv (according to Eq. 4).



(a) (b)

Fig. 5: Illustration of the encoding phase and the reconstruction step of our proposed method without the preprocessing step, the detection of the unpredictable vertices or the threshold on the distance connections: a) Marked encrypted *Cow*, b) Reconstructed *Cow*.

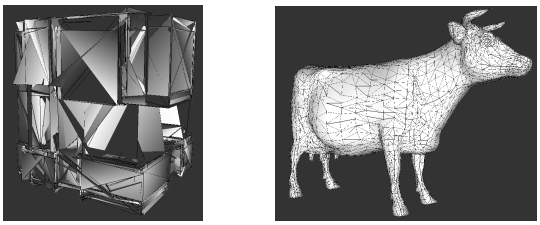


(a) (b)

Fig. 6: Illustration of the encoding phase and the reconstruction step of our proposed method with a translation and a topological discontinuity detection: a) Marked encrypted *Cow*, b) Reconstructed *Cow*.

2) With a translation and a topological discontinuity detection: In order to correctly reconstruct the 3D object, we perform a translation, as well as a topological discontinuity detection (Fig. 4c). These topological discontinuities constitute the auxiliary information of the embedded message. Fig. 6a presents the visual results of the encryption. We can observe that the visual security level of the marked encrypted 3D object is confidential because no information about the original content at all can be recognized. The reconstruction of the 3D object *Cow* is presented in Fig. 6b with an RMSE of 0.2×10^{-6} and a Hausdorff distance of 0.373×10^{-6} between the original 3D object and its reconstructed version. In this case, 269 vertices are unpredictable, and therefore the size of the auxiliary information is equal to $A = 4,047$ bits (Eq. 3). Thus, we have a lower payload of: $payload = 1.60$ bpv. We observe that the RMSE and Hausdorff distance of the reconstructed 3D object are very small. This is due to the translation, which increases the exponent of the floating point coordinate values.

3) With a translation and a large distance detection: In order to reduce the size of the auxiliary information, we perform a large distance detection according to a threshold on the distance connections. Only the vertex connections whose distance is greater than the threshold are included in the auxiliary information. Indeed, we can observe in Fig. 4d that some large distances (green and red vertex connections) exist. However, the distribution of these vertex connection distances is not as sparse, with only a few values above the mean value. For the 3D object *Cow*, they are a subset of the topological discontinuities illustrated in Fig. 4c. These topological discontinuities represent all possible vertex connections that could be difficult to reconstruct. In order to reduce the number of unpredictable vertex connections, we can then apply a threshold to these distances. This allows for a greater payload and then, a larger secret message can be embedded, as the size of the auxiliary information is smaller than when we detect all the topological discontinuities. Fig. 7a presents the marked encrypted 3D object *Cow*, where a threshold on the distance connections is applied. The visual security level of the marked encrypted 3D object is also confidential. For a threshold parameter $k = 1$, we have $n' = 205$ vertices, $A = 3,087$ bits and $payload = 1.96$ bpv. For a threshold parameter $k = 2$, we have $n' = 64$ vertices, $A = 972$ bits and $payload = 2.66$ bpv. Finally, if we take $k = 3$, then we have $n' = 40$ vertices, $A = 612$ bits and $payload = 2.79$ bpv (Fig. 7b). The RMSE and the Hausdorff distance between the original 3D object and the associated reconstructed 3D objects are 0.2×10^{-6} and 0.373×10^{-6} respectively, which are also the same values as for the reconstruction without using a threshold. The threshold allows us to increase the payload without changing the quality of the reconstructed 3D object.

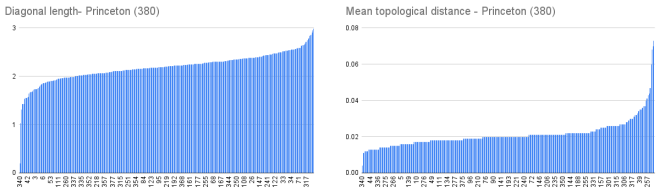


(a) (b)

Fig. 7: Illustration of the encoding phase and the reconstruction step of our proposed method with a translation and a large distance detection: a) Marked encrypted *Cow*, b) Reconstructed *Cow*.

B. Results on an entire database: Princeton [13]

The Princeton database is composed of 380 3D objects, ranging from $1,343$ to $27,824$ vertices ($10,224$ on average) [13].



(a) (b)

Fig. 8: Statistical analysis of the Princeton database [13]: a) Diagonal length, b) Mean distance between vertices sharing an edge.

All the 3D objects of the Princeton database [13] are more or less centered on zero, with diagonal sizes ranging from 0.199 to 2.994 (Fig. 8a). For these 3D objects, the mean Euclidean distance between two vertices sharing an edge ranges from 3.563×10^{-3} to 74.385×10^{-3} (Fig. 8b) and the standard deviation ranges from 1.536×10^{-3} to 77×10^{-3}. We also observe that the distance between two vertices sharing an edge in a 3D object is uniform over the same 3D object.

By applying our RDH-ED method to the entire database, we can embed an average of 2.838 bpv (± 0.046 bpv). We reconstruct these 3D objects with an RMSE of 0.581×10^{-6} and a Hausdorff distance of 0.79×10^{-6} on average. These values are very close to zero indicating near-perfect reconstruction, whatever the considered 3D object. Fig. 9 presents the 3D object #317 from the Princeton database (left-hand image), and the results we obtained after applying the encoding phase of

our RDH-ED method on this object with a threshold parameter $k = 3$ (right-hand image). The 3D object #317 is the head *Max*, which has a large number of vertices $(27,726)$ and triangular faces $(55,448)$, in comparison with the other 3D objects in the Princeton database. The two images in the center correspond to the Hamiltonian path constructed for this 3D object, starting from the vertex displayed in red. At the top, the distance between connected vertices in the Hamiltonian path are represented from blue to red. Below, the topological discontinuities are illustrated in red.

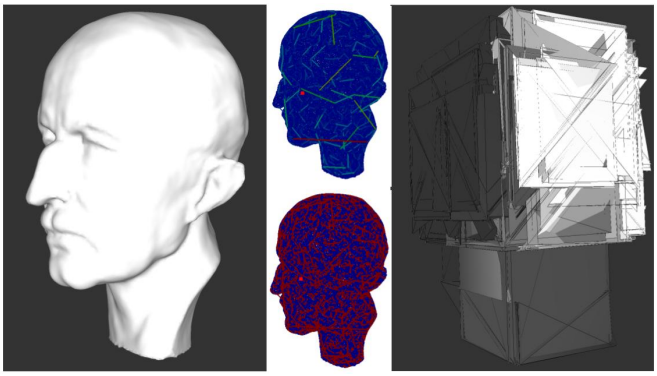


Fig. 9: Illustration of the encoding phase of our proposed method applied to the 3D object #317 of the Princeton database [13].

It has an Euclidean diagonal size of 2.487, for $n'_{max} = 4,620$ vertices. If we take the vertex #11,400 as the starting vertex of the Hamiltonian path (in red), we have $\mu_H = 16.882 \times 10^{-3}$ and $\sigma_H = 14.941 \times 10^{-3}$, for $2,746$ topological discontinuities (9.904%). We have $n' = 278$, $A = 5,019$ bits, $S = 78,156$ bits and obtain a $payload = 2.901$ bpv. We observe for this 3D object that the large distance connections (green and red connections in the top-middle image) are not a subset of the topological discontinuities (in red in the bottom-middle image). This is due to the circularly divided form of this object. We have $n' = 16$, $A = 252$ bits, $S = 7,449$ bits and obtain a $payload = 2.901$ bpv.

To conclude our experimental results, our proposed RDH-ED method achieves a payload close to the maximum value (which is very close to 3 bpv) that can be obtained for $p = 1$. The part of the message that is sacrificed is allocated to the embedding of auxiliary information, useful for the reconstruction of the original 3D object from the marked encrypted 3D object. We observe that considering large distance connections (*i.e.* those greater than $\mu_H + 3 \times \sigma_H$) as unpredictable connections, always allows for a correct reconstruction, with low RMSE and Hausdorff distance values, while minimizing the size of the auxiliary information. Note that the reconstruction is reversible regardless of the 3D object geometry or shape. If we compare the results we obtained with those achieved by the current methods of the state-of-the-art, even if we do not manage to improve the payload value, we achieve a much better visual quality during the original 3D object reconstruction phase.

IV. Conclusion

In this paper, we proposed a new RDH-ED method for 3D objects based on an MSB prediction. First of all, we construct a Hamiltonian path to define an order for the vertices of the 3D object. This path allows us to accurately predict each vertex during the reconstruction phase. The unpredictable vertices are identified by observing the topological discontinuities and the large distance connections between two consecutive vertices in the Hamiltonian path. Then, the preprocessed and ordered 3D object is encrypted and both the positions and the values of the unpredictable vertices are embedded by a MSB substitution in the coordinates of the first vertices as auxiliary information. A secret message can then be embedded in the remaining vertices, just after the auxiliary information, directly in the encrypted domain. Note that our proposed method is fully format compliant, size preserving and the visual security level of the marked encrypted 3D object is confidential. Finally, a very good reconstruction of the original 3D object in terms of RMSE and Hausdorff distance values (less than 0.5×10^{-6}) is achieved.

References

[1] P. Puteaux and W. Puech, "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 7, pp. 1670–1681, 2018.

[2] V. Itier, W. Puech, J.-P. Pedeboy, and G. Gesquière, "Construction of a unique robust Hamiltonian path for a vertex cloud," in *2013 IEEE 15th International Workshop on Multimedia Signal Processing (MMSP)*, 2013, pp. 105–110.

[3] V. Itier and W. Puech, "High capacity data hiding for 3D point clouds based on static arithmetic coding," *Multimedia Tools and Applications*, vol. 76, pp. 26421–26445, 2017.

[4] R. Jiang, H. Zhou, W. Zhang, and N. Yu, "Reversible data hiding in encrypted three-dimensional mesh models," *IEEE Transactions on Multimedia*, vol. 20, no. 1, pp. 55–67, 2018.

[5] N. Xu, J. Tang, B. Luo, and Z. Yin, "Separable reversible data hiding based on integer mapping and MSB prediction for encrypted 3D mesh models," *Cognitive Computation*, vol. 14, pp. 1172–1181, 2022.

[6] Y.-Y. Tsai and H.-L. Liu, "Integrating coordinate transformation and random sampling into high-capacity reversible data hiding in encrypted polygonal models," *IEEE Transactions on Dependable and Secure Computing*, 2022.

[7] W.-L. Lyu, L. Cheng, and Z. Yin, "High-capacity reversible data hiding in encrypted 3D mesh models based on multi-MSB prediction," *Signal Processing*, vol. 201, pp. 108686, 2022.

[8] Y.-Y. Tsai, "Separable reversible data hiding for encrypted three-dimensional models based on spatial subdivision and space encoding," *IEEE Transactions on Multimedia*, vol. 23, pp. 2286–2296, 2020.

[9] M. Shah, W. Zhang, H. Hu, H. Zhou, and T. Mahmood, "Homomorphic encryption-based reversible data hiding for 3D mesh models," *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 8145–8157, 2018.

[10] B. Jansen van Rensburg, P. Puteaux, W. Puech, and J.-P. Pedeboy, "3D object watermarking from data hiding in the homomorphic encrypted domain," *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 19, no. 5, pp. 1–20, Oct. 2023.

[11] M. Levoy, J. Gerth, B. Curless, and K. Pull, "The Stanford 3D scanning repository," *URL http://graphics.stanford.edu/data/3Dscanrep/*, vol. 5, no. 10, 2005.

[12] S. Beugnon, B. Jansen van Rensburg, N. Amalou, W. Puech, and J.-P. Pedeboy, "A 3D Visual Security (3DVS) score to measure the visual security level of selectively encrypted 3D objects," *Signal Processing: Image Communication*, vol. 108, pp. 116832, 2022.

[13] P. Shilane, P. Min, M. Kazhdan, and T. Funkhouser, "The Princeton shape benchmark," in *Proceedings Shape Modeling Applications, 2004.* IEEE, 2004, pp. 167–178.