RETHINKING THE HIGH CAPACITY 3D STEGANOGRAPHY: INCREASING ITS RESISTANCE TO STEGANALYSIS

Zhenyu Li[⋆] [*] *Sébastien Beugnon*[†] *William Puech*[†] *Adrian G. Bors*[⋆]

[⋆] Department of Computer Science, University of York, York YO10 5GH, UK
[†] Laboratory LIRMM, UMR CNRS 5506, Université de Montpellier, 34095 Montpellier, France

ABSTRACT

3D steganography is used in order to embed or hide information into 3D objects without causing visible or machine detectable modifications. In this paper we rethink about a high capacity 3D steganography based on the Hamiltonian path quantization, and increase its resistance to steganalysis. We analyze the parameters that may influence the distortion of a 3D shape as well as the resistance of the steganography to 3D steganalysis. According to the experimental results, the proposed high capacity 3D steganographic method has an increased resistance to steganalysis.

Index Terms— 3D steganography, steganalysis, shape distortion, information hiding

1. INTRODUCTION

3D objects are playing a key role in many popular and cutting-edge technologies, such as virtual reality and 3D printing. Crypto-security applications of 3D objects and graphics are increasingly important given the large diversity of ways for generating 3D objects, either by using software or 3D scanning and given their ubiquitous usage in many applications. Information hiding, including watermarking and steganography, is the technique that can conceal the information in the digital files without causing noticeable changes to the carriers. The 3D information hiding started in the late 90s [1], when artists and 3D graphics designers wanted to enforce their copyright. Since then, various 3D information hiding methods have been proposed [2, 3, 4, 5].

High capacity 3D steganography, such as the method from [6], which can embed a payload of 10 Bits Per Vertex (BPV), have been proposed lately. Inspired by [7], Itier *et al*. [8] proposed a 3D steganographic method which hides information following the Hamiltonian path of the 3D point cloud resulting in 3 BPV. Subsequently, Itier *et al*. [9] improved the capacity of the steganography in [8] to 24 BPV and used the static arithmetic coding during embedding.

Nevertheless, the resistance of 3D steganography to steganalysis has not been considered when designing information hiding algorithms. Few papers have discussed so far the challenges in 3D steganalysis [10, 11, 12]. In this paper, we rethink about the high capacity 3D steganography proposed in [9] in the view of enhancing its resistance to steganalysis. We analyze the influence of the parameters in the algorithm on the steganlytic features, as well as that of the domain used for embedding, while attempting to increase the steganography's resistance to steganalysis. Experiments are carried out to evaluate the proposed methodology. Section 2 describes the details of the high capacity 3D steganography proposed in [9]. A brief introduction of 3D steganalysis is given in Section 3. Section 4 presents the proposed 3D embedding approach while increasing the resistance to steganalysis. The experimental results are described in Section 5 and the conclusion is provided in Section 6.

2. HIGH CAPACITY 3D STEGANOGRAPHY

The high capacity 3D steganographic algorithm proposed in [9] utilizes a synchronization technique to guarantee that the order of the embedded data is the same during the embedding and extraction stages. Unlike the steganography for digital images, where the synchronization is based on the existing sequential order of the pixels in the image, there is no such evident sequence for vertices of 3D objects.

The steganographic method from [9] builds the Hamiltonian path over the complete graph of the vertices in the 3D object without using the connectivity information. The Hamiltonian path is a unique traversal of all the vertices in the 3D object, starting from a vertex v_0 chosen by a secret key. For each step, the algorithm chooses the nearest neighbor v_{i+1} of the current vertex v_i. Finally, a Hamiltonian path $\mathbf{P}_n$ is generated. It is noted that there is a chance that some of the edges in the path $\mathbf{P}_n$ may not exist initially in the mesh. In fact, the data is hidden whilst simultaneously ensuring its synchronization with the embedded bit order. The message is embedded by changing the relative position of a vertex v_{i+1} to its predecessor v_i once the vertex v_{i+1} is added to the Hamiltonian path $\mathbf{P}_n$. In order to embed a high bit capacity, the vertex is displaced along three coordinates in the Spherical Coordinate System (SCS) which originates in the location of the vertex's predecessor. In addition, the algorithm partitions

[*]The first author acknowledges the scholarship received from Zhengzhou Institute of Information Science and Technology.

the edge vector into intervals for each coordinate, controlled by the parameter Δ. An interval is subdivided into s sub-intervals which correspond to different words. The vertex is then moved to the new sub-interval within the interval to embed the corresponding word. The new position of the vertex is converted back to the Cartesian coordinate system after the embedding.

The division into sub-intervals can be done by using either a uniform or a non-uniform distribution. When considering the uniform distribution, every sub-interval is of the same length. Meanwhile, for the non-uniform distribution, the lengths of the sub-intervals are determined by the probability of the occurrence of the corresponding words in the whole secret message, which is coded by the Static Arithmetic Coding.

In order to prevent the displacement of the vertices changing the existing Hamiltonian path and to preserve the synchronization of the bit embedding process, a checking stage is used during the information hiding stage. During the extraction, the Hamiltonian path is built by knowing the starting vertex v_0 and the information is extracted bit-by-bit by detecting the sub-interval where each vertex lies, based on the knowledge of Δ.

3. 3D STEGANALYSIS

In the study from [9], the distortion of the meshes caused by the embedding is analyzed by the Peak Signal-to-Noise Ratio (PSNR) [6] and the Mesh Structural Distortion Measure (MSDM2) [13] which is better correlated with human perception. However, the steganography's resistance to the 3D steganalysis was not considered in [9]. The existing image steganalytic methodology [14, 15] cannot be applied to 3D meshes, because unlike 3D objects, images are represented on regular lattices. The first 3D steganalytic algorithm was proposed in [10]. Then, an improved approach using local feature set for 3D steganalysis was developed by Li and Bors [11]. Both these 3D steganalytic approaches are using the statistics of local 3D features as inputs to machine learning method algorithms which train the steganalyzer for differentiating the cover and stego 3D objects.

Information embedding in 3D objects only change very slightly the mesh surface. According to the studies from [10, 11], statistics of localized 3D features can be successfully used for 3D steganalysis. A 52-dimensional feature vector was proposed for 3D steganalysis in [11]. Before extracting the features, Laplacian smoothing is applied to the meshes of both cover-objects and stego-objects. The features are then extracted from the original and smoothed meshes. Then, the first four moments, representing the mean, variance, skewness and kurtosis, of the difference between the geometrical information of the original and smoothed meshes are used as inputs for the steganalyzer. The 3D features considered for steganalysis in [11], include the following: the vertex position and norm in the Cartesian coordinate system; the vertex position and norm in the Laplacian coordinate system [16]; the face normal; the dihedral angle of two neighboring faces; the vertex normal; the Gaussian curvature and curvature ratio.

4. INCREASING THE RESISTANCE OF 3D STEGANOGRAPHY TO STEGANALYSIS

In this section, we describe a 3D steganographic method which increases the resistance of the 3D steganography [9] to steganalysis. This investigation includes three aspects: the interval parameter Δ, a different selection of the sub-intervals s and a different embedding style in SCS.

In the following we analyze the displacement of a vertex v_i in the context of increasing the resistance to steganalysis. The embedding is applied in the spherical coordinate system, which is illustrated in Figure 1 (a). We consider the displacement of the vertex along the radial coordinate. Assuming that the sub-intervals are characterised by uniform distributions, then the displacement of the vertex in the radial coordinate is defined as

$$D_\rho = \sum_{j=1}^{s}\sum_{k=1}^{s} P_j Q_k |j-k| \frac{\Delta}{s}, \tag{1}$$

where P_j is the probability of the vertex v_i positioned in the j-th sub-interval, Q_k is the probability of the modified position of the vertex v_i being in the k-th sub-interval, and $\frac{\Delta}{s}$ is the length of each sub-interval. We assume that the vertex v_i is randomly located in the interval, so that $P_j = \frac{1}{s}$, $j = 1, 2, \ldots, s$. If the word in the message is uniformly distributed, the modified position of the vertex v_i is accordingly located randomly in the interval, and $Q_k = \frac{1}{s}$, $k = 1, 2, \ldots, s$. So equation (1) is simplified as:

$$D_\rho = \frac{\Delta}{3}\left(1 - \frac{1}{s^2}\right). \tag{2}$$

The equations calculating the displacement of the vertex in the two angle coordinates of SCS are similar to equation (2).

It can be inferred from equation (2) that if the interval parameter Δ is decreased, then the displacement of the vertex will be reduced as well. At the same time, when the number of sub-intervals s increases, increasing the embedding capacity, the displacement would increase as well. However, the influence of the number of sub-intervals on the displacement is very small, because $dD_\rho/ds = 2\Delta/3s^3$ is very small when s is large. According to this analysis, it is worthwhile to make the interval parameter Δ as small as possible in order to limit the effect of the distortions, produced by the information embedding, on those features used for steganalysis.

In the following we analyze the influence of the distortion produced by the information embedding on the features used for 3D steganalysis. The original version of the HPQ steganography [9] embeds in all three coordinates of the edge vector in SCS. However, changes in the two angle coordinates

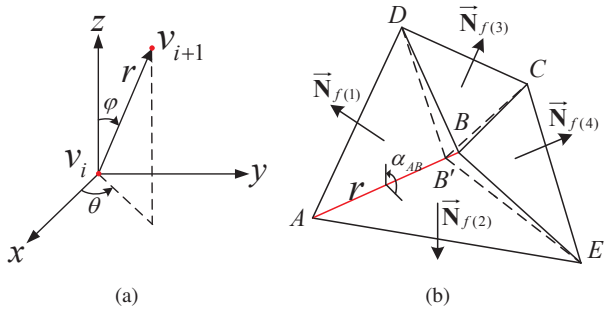

Fig. 1. Illustration of the embedding changes in SCS. (a) The edge vector $\overrightarrow{v_i v_{i+1}}$ represented in SCS as (r, θ, φ). (b) The changes produced by HPQ in the radial coordinate of the edge vector in SCS.

of SCS, θ and φ , may provide a more significant influence on the steganalytic features than changes in the radial coordinate, r.

Figure 1 (b) illustrates how the change produced by the information embedding is only applied in the radial coordinate of the edge vector $\overrightarrow{AB}$ between the vertices A and B. The new position of the vertex B is B', which is not moved from the direction of the edge $\overrightarrow{AB}$. The face normals of the faces $\triangle ABD$ and $\triangle ABE$, $\vec{\mathbf{N}}_{f(1)}$ and $\vec{\mathbf{N}}_{f(2)}$, are not affected by the displacement of the vertex B. The dihedral angle between the faces $\triangle ABD$ and $\triangle ABE$, which is shown in Figure 1 (b), is:

$$\alpha_{AB} = \arccos \frac{\vec{\mathbf{N}}_{f(1)} \cdot \vec{\mathbf{N}}_{f(2)}}{|\vec{\mathbf{N}}_{f(1)}||\vec{\mathbf{N}}_{f(2)}|}. \quad (3)$$

The dihedral angle α_{AB} is not influenced by the modification of the vertex B either. However, the displacement of the vertex B changes the direction of the face normals $\vec{\mathbf{N}}_{f(3)}$ and $\vec{\mathbf{N}}_{f(4)}$, except when all the faces are on the same flat surface. In practice, lots of flat regions exist in Computer Aided Design 3D objects. Smooth regions look locally flat in 3D objects of high resolution. Consequently, the subsequent edge vector is only slightly affected by the displacement from its predecessor edge.

It can be observed that any modification of the edge vector $\overrightarrow{AB}$ in any of the two angle coordinates of SCS, would result in changes in the face normals $\vec{\mathbf{N}}_{f(1)}$, $\vec{\mathbf{N}}_{f(2)}$ and in the dihedral angle α_{AB}. Such features are used for steganalysis and their modifications would be identified by the steganalyzer.

According to this analysis, the 3D embedding's resistance to steganalysis is improved when modifying only the radial component of a edge vector's representation in SCS. However, the edges used by the steganography are generated during the construction of the Hamiltonian path, and some of them may actually not exist in the original mesh. Nevertheless, the overlap between the edges of the original mesh and those in the Hamiltonian path is quite high, so eventually this issue does not significantly influence the steganalysis result.

5. EXPERIMENTAL RESULTS

In this section, we test the proposed 3D steganography's resistance to steganalysis. In the experiments, we use 354 cover 3D objects from the Princeton Mesh Segmentation project [17] database. Then, we set different values for the parameters in the high capacity 3D steganography [9] based on the Hamiltonian Path Quantization (HPQ), and embed the information as described in Section 4. The steganalytic features used for training the steganalyzers are the 52-dimensional Local Feature Set (LFS52) proposed in [11]. For each setting of the information algorithm, a steganalyzer is trained over 260 pairs of cover and their corresponding stego objects and tested over the other 94 pairs. The machine learning method that we used to train the steganalyzers is the Fisher Linear Discriminate (FLD) ensemble [18], which is the most popular method used in the field of steganalysis. The training and testing sets are independently split for 30 times, and the median value of the detection errors is considered as the final result. The detection error ratio is the sum of the false alarms and miss detections divided by the size of the testing set.

In order to observe the influence of the interval parameter Δ on the resistance of the 3D steganography based on HPQ [9] to steganalysis, we set the values of $\Delta \in \{10^{-4}, 10^{-5}, 10^{-6}, 10^{-7}\}$. The embedding domains are the three coordinates of SCS. The payload rate is 24 BPV, consisting of 8 BPV for each coordinate of SCS, which means that the number of sub-intervals is $s = 2^8$. The final results of the detection errors for the steganalysis of the HPQ based steganography with different values for the interval parameter Δ are provided in Figure 2. These results indicate that a smaller value of the interval parameter Δ leads to a higher detection error, corresponding to higher resistance to steganalysis. In the case when $\Delta = 10^{-4}$, the interval becomes too large to find enough available edges for embedding, so the actual payload is less than 24 BPV, which explains why the detection error goes up.

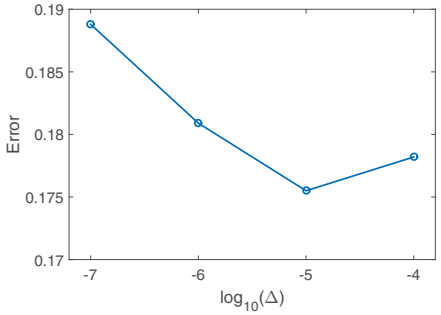

Fig. 2. Detection errors for the steganalysis of the high capacity 3D steganography HPQ [9] when varying the interval parameter Δ.

Table 1. Median values and the standard deviations of the detection errors for the steganalysis of the 3D steganography (HPQ) [9] and its variants, $\Delta = 10^{-7}$.

	HPQ (24 BPV)	HPQ-PA (8 BPV)	HPQ-R (8 BPV)	HPQ-R (24 BPV)
LFS52	0.1888 ($\pm$.0253)	0.2553 ($\pm$.0242)	0.3112 ($\pm$.0259)	0.3085 ($\pm$.0246)
Dihedral Angle	0.1866 ($\pm$.0174)	0.3431 ($\pm$.0222)	0.4400 ($\pm$.0197)	0.4441 ($\pm$.0156)
Laplacian	0.3545 ($\pm$.0168)	0.3750 ($\pm$.0227)	0.3800 ($\pm$.0276)	0.3803 ($\pm$.0197)
Curvature	0.3563 ($\pm$.0232)	0.3963 ($\pm$.0190)	0.4033 ($\pm$.0253)	0.4069 ($\pm$.0212)

In the following, we provide the steganalysis results for the high capacity 3D steganography based on HPQ [9] and its variants designed according to the approach from Section 4. The results are summarized in Table 1, in which HPQ represents the original method introduced in [9] that embeds information in all three coordinates of SCS with a payload rate at 24 BPV, HPQ-PA represents the variant that embeds only in the Polar Angle coordinate (φ) of SCS with a payload rate at 8 BPV, HPQ-R represents the variant that embeds only in the Radial coordinate of SCS. For HPQ-R, two payload rates are considered, namely, 8 BPV and 24 BPV, corresponding to different sub-intervals $s = 2^8$ and $s = 2^{24}$. In all these methods, the interval parameter is set as $\Delta = 10^{-7}$.

During the testing, we consider the features from the LFS52 steaganalytic feature set in order to observe the influence of embedding in different coordinates of SCS on the steganlytic features. The "Dihedral Angle" represents the 4-dimensional feature subset corresponding to the dihedral angles in the 3D objects. The "Laplacian" represents the 16-dimensional feature subset corresponding to the vertex position and norm in the Laplacian coordinate system. The "Curvature" represents the 8-dimensional feature subset corresponding to the curvature information of the vertex as in [11]. After comparing the steganalysis results for HPQ, HPQ-PA and HPQ-R, it is obvious that by embedding only in the radial coordinate of SCS increases the steganography's resistance to steganalysis to the largest extent, representing an increase of more than 12% in the detection error. The dihedral angle features are very effective when detecting HPQ, but they are almost useless when detecting HPQ-R, which implies that the dihedral angles in 3D objects are quite well preserved when embedding only in the radial coordinate. Furthermore, even when the payload is tripled for HPQ-R, its resistance to steganalysis is only about 0.3% lower than embedding at the payload rate of 8 BPV.

We also compared the proposed steganography, HPQ-R, to several other 3D information hiding algorithms, namely, Multi-Layer Steganography (MLS) [6], the watermarking algorithm that modifies the Mean of the distribution of the vertices' Radial distances in the Spherical coordinate system (MRS) [3], Steganalysis-Resistant Watermarking (SRW) [19], and the original version of HPQ [9], with respect to the resistance to the steganalysis. The number of embedding layers is considered as 10 and the number of intervals is chosen as 10^4 in MLS [6] whose payload rate is nearly 10 BPV. The payload embedded in MRS [3] is 64 bits and the watermarking strength is 0.04. The parameter K in SRW [19] is set to 128, while the algorithm's upper bound for the embedding capacity is $\lfloor (K-2)/2 \rfloor$ bits. The final detection errors of the five information hiding algorithms when using LFS52 for steganalysis are shown in Figure 3. It can be observed that the proposed steganoraphy, HPQ-R, has the strongest resistance to steganalysis when using the LFS52 to train the steganalyzers, providing a reduction of 9-15% in the ability of the steganalyzers to detect the hidden information.

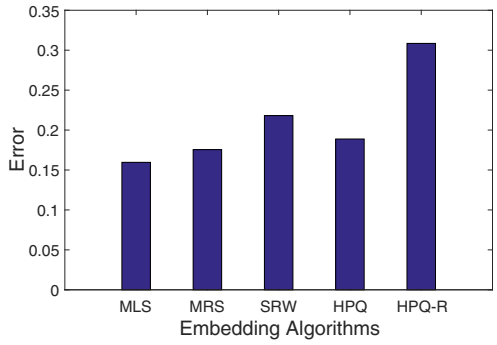

Fig. 3. Detection errors for the steganalysis of several information embedding algorithms in 3D objects when using the LFS52 feature set for training of the steganalyzers.

6. CONCLUSION

The contribution of the paper is a rethinking of the high capacity 3D steganography based on the Hamiltonian path quantization, in order to improve its resistance to steganalysis. We analyze the influence of the interval parameter and the number of sub-intervals with respect to the displacement of the vertex. It is also pointed out that by embedding in the radial coordinate of the spherical coordinate system we achieve lower distortions in the steganalytic features when compared to embedding in the angle coordinates. The experimental results assess these ideas by testing the proposed 3D steganography with the steganalyzers trained with the steganalytic feature set, LFS52. By increasing the resistance to 3D steganalysis we increase the protection of the information stored in 3D objects.

7. REFERENCES

[1] Ryutarou Ohbuchi, Hiroshi Masuda, and Masaki Aono, "Embedding data in 3D models," in *Interactive Distributed Multimedia Systems and Telecommunication Services*. Springer, 1997, pp. 1–10.

[2] François Cayre and Benoît Macq, "Data hiding on 3-D triangle meshes," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 939–949, 2003.

[3] Jae-Won Cho, Rémy Prost, and Ho-Youl Jung, "An oblivious watermarking for 3-D polygonal meshes using distribution of vertex norms," *IEEE Transactions on Signal Processing*, vol. 55, no. 1, pp. 142–155, 2007.

[4] Ming Luo and Adrian G Bors, "Surface-preserving robust watermarking of 3-D shapes," *IEEE Transactions on Image Processing*, vol. 20, no. 10, pp. 2813–2826, 2011.

[5] Adrian G Bors and Ming Luo, "Optimized 3D watermarking for minimal surface distortion," *IEEE Transactions on Image Processing*, vol. 22, no. 5, pp. 1822–1835, 2013.

[6] Min-Wen Chao, Chao-hung Lin, Cheng-Wei Yu, and Tong-Yee Lee, "A high capacity 3D steganography algorithm," *IEEE Transactions on Visualization and Computer Graphics*, vol. 15, no. 2, pp. 274–284, 2009.

[7] Philippe Amat, William Puech, Sébastien Druon, and Jean-Pierre Pedeboy, "Lossless 3D steganography based on mst and connectivity modification," *Signal Processing: Image Communication*, vol. 25, no. 6, pp. 400–412, 2010.

[8] Vincent Itier, William Puech, Gilles Gesquière, and Jean-Pierre Pedeboy, "Joint synchronization and high capacity data hiding for 3D meshes," in *SPIE/IS&T Electronic Imaging*. International Society for Optics and Photonics, 2015, pp. 9393, 05–15.

[9] Vincent Itier and William Puech, "High capacity data hiding for 3D point clouds based on static arithmetic coding," *Multimedia Tools and Applications*, 2016, doi:10.1007/s11042-016-4163-y.

[10] Ying Yang and Ioannis Ivrissimtzis, "Mesh discriminative features for 3D steganalysis," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 10, no. 3, pp. 27:1–27:13, 2014.

[11] Zhenyu Li and Adrian G. Bors, "3D mesh steganalysis using local shape features," in *Proc. of IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, 2016, pp. 2144–2148.

[12] Zhenyu Li and Adrian G. Bors, "Selection of robust features for the cover source mismatch problem in 3D steganalysis," in *Proc. of the 23rd Int. Conf. on Pattern Recognition*. IEEE, 2016, pp. 4251–4256.

[13] Guillaume Lavoué, "A multiscale metric for 3D mesh visual quality assessment," in *Computer Graphics Forum*. Wiley Online Library, 2011, vol. 30, pp. 1427–1437.

[14] Zhenyu Li, Zongyun Hu, Xiangyang Luo, and Bin Lu, "Embedding change rate estimation based on ensemble learning," in *Proc. of the 1st ACM workshop on Information Hiding and Multimedia Security*. ACM, 2013, pp. 77–84.

[15] Hasan Abdulrahman, Marc Chaumont, Philippe Montesinos, and Baptiste Magnier, "Color image steganalysis based on steerable gaussian filters bank," in *Proc. of the 4th ACM Workshop on Information Hiding and Multimedia Security*. ACM, 2016, pp. 109–114.

[16] Ying Yang and Ioannis Ivrissimtzis, "Polygonal mesh watermarking using Laplacian coordinates," *Computer Graphics Forum*, vol. 29, no. 5, pp. 1585–1593, 2010.

[17] Xiaobai Chen, Aleksey Golovinskiy, and Thomas Funkhouser, "A benchmark for 3D mesh segmentation," *ACM Transactions on Graphics*, vol. 28, no. 3, pp. 73:1–73:12, 2009.

[18] Jan Kodovskỳ, Jessica Fridrich, and Vojtěch Holub, "Ensemble classifiers for steganalysis of digital media," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 432–444, 2012.

[19] Ying Yang, Ruggero Pintus, Holly Rushmeier, and Ioannis Ivrissimtzis, "A 3D steganalytic algorithm and steganalysis-resistant watermarking," *IEEE Transactions on Visualization and Computer Graphics*, vol. 23, no. 2, pp. 1002–1013, Feb 2017.