



Watermarking in 3D Models Using Depth Path

Nashwan Alsalam Ali

Department of Computer Science, College of Education for Women, University of Baghdad, Baghdad, Iraq

Received: 15/4/ 2019

Accepted: 17/ 7/2019

ABSTRACT

This paper presents a 3D watermarking model based on the nearest distance between two vertices in mesh, where the embedding path moves as deep as possible until the embedding data is completed. The proposed algorithm achieved good results according to invisibility and robustness. The visibility was measured in term of Root Mean Square Error (RMSE) and Hausdroff Distance (HD), which obtained good results. As related to robustness, the proposed method showed resistance to geometrical attack (translation, scaling and rotation) as well as acceptable resistance to signal processing attacks like noise addition and simplification.

Keywords: 3D mesh, digital watermarking, copyright protection, attack, robustness.

العلامة المائية في النماذج الثلاثية الابعاد باستخدام مسار العمق

نشوان السلام علي

قسم الحاسبات، كلية التربية للبنات، جامعة بغداد، بغداد، العراق

الخلاصة

تقدم هذه الورقة نموذجًا للعلامة المائية في النماذج الثلاثية الأبعاد بالاعتماد على المسافة الأقرب بين رأسين في الشبكة الثلاثية الابعاد، يتحرك مسار الاخفاء بأقصى عمق ممكن حتى يكتمل اخفاء جميع البيانات، حققت الخوارزمية المقترحة نتيجة جيدة بالنسبة للاخفاء ومقاومة الهجوم ، مقاييس تأثر الرؤية تم استحصالها اعتمادا على (RMSE) Root Mean Square Error و (HD) Hausdroff Distance وكانت النتيجة جيدة ، وفقاً للمتانة ، والمقاومة الطريقة المقترحة مقاومة للهجوم الهندسي (النقل ، التحجيم ، الدوران) مع المقاومة المقبولة لهجوم معالجة الإشارة مثل إضافة الضوضاء والتبسيط.

1. Introduction

In the last years, the three dimensional (3D) models were spread rapidly due to increased multimedia applications. In any watermarking system, there are two main processes that must be achieved: embedding and extraction. In the embedding process, the information are inserted in the cover media, while in the extraction process, the information extracted from the watermarked model is embedded [1].

There are many different ways to represent 3D models, but the triangle mesh is the most common one. This method contains three points (vertices) and edges that connect these vertices; other types of 3D models include voxel data, trees, and NURBS [2].

In this paper a blind watermarking method to embed a binary data in 3D mesh is proposed, based on the shortest distance between vertices.

The 3D watermarking requirements are the same for the other multimedia (image, audio, and video), which are the invisibility, robustness, and capacity [3].

Concerning 3D watermarking, several techniques have been observed in this field, such as that reported in the study of liu J [1] who proposed a 3D triangle mesh by firstly computing the average normal for each vertices in 3d model, then the vertices are selected for embedding based on the value of the average normal. Another technique was described by Luma and Muna [4] who proposed a method based on a geometrical scheme to embed a watermark in triangle mesh, where the vertices of the 1-ring continue in n-ring and so on until all the binary data are completed. Zainab et al. [5] proposed a 3D watermarking method based on the area of faces and the mean curvature in order to select the best area for embedding.

2. 3D Watermarking

Watermarking means the embedding of information in 3D model, to keep the copyright of 3D digital models. The 3D triangular model with texture consists of the following [6]:

- 1) '**Geometric Mesh**': collection of 3D triangles with vertices and edges.
- 2) '**Texture Image**': consists of 2D image that represents texture information.
- 3) '**Texture Mesh**': the group of 2D triangles.
- 4) '**Triangle Mapping**': Conversion of 3D to 2D triangles?Watermarking algorithms in 3D mesh can be performed either by updating an order of the data in the computer 3D object file, or by changing the topology of the 3D object (i.e., the connectivity of the mesh to embed data, while positions of vertices are not changed).

3. The Proposed Watermarking Algorithm

A new proposed watermarking method is depending on the geometric approach for hiding data in 3D mesh. This approach is performed through moving the 3D mesh to the center of mass to prevent the watermarked model from any geometrical attack (translation, scaling, rotation). Initially, the 3D polygon mesh is shifted to the origin of the rectangular coordinate system by finding the center of gravity of the 3D mesh and then transforming vertices coordinates to be from -1 to $+1$.

The proposed system selects the center of the 3D object as a starting point for the path using the the following equations (1, 2, and 3).

$$X_c = \sum_{k=1}^n \frac{X_k}{n} \quad \dots (1)$$

$$Y_c = \sum_{k=1}^n \frac{Y_k}{n} \quad \dots (2)$$

$$Z_c = \sum_{k=1}^n \frac{Z_k}{n} \quad \dots (3)$$

X_c , Y_c , Z_c represent the center of the 3D mesh; (n) is the counter of the vertices in the 3D mesh; X_k , Y_k , and Z_k are the coordinates of the vertex [4].

The path of embedding generated by moving from one vertex to another vertex depends on the minimum distance between each vertex and all the vertices connected with it. The distance between any two vertices is calculated by Euclidean distance. The Euclidean distance between any two points (such as p and q) is the distance for the line between them. In 3D space, the distance between any two points that have positions (x_1, y_1, z_1) and (x_2, y_2, z_2) is

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2 + (z_2 - z_1)^2} \quad \dots (4)$$

To explain how the embedding process is achieved, Figure-1 shows a part of the Venus mesh to explain an example for the embedding path. As a first step, the center of the mesh is computed as shown in (V_1) , the position value of vertices is used for embedding by least significant bits, then the

distance from V_1 to all the neighbouring vertices is considered as the child generated for this vertex is found and selected the vertex with shortest distance for embedding.

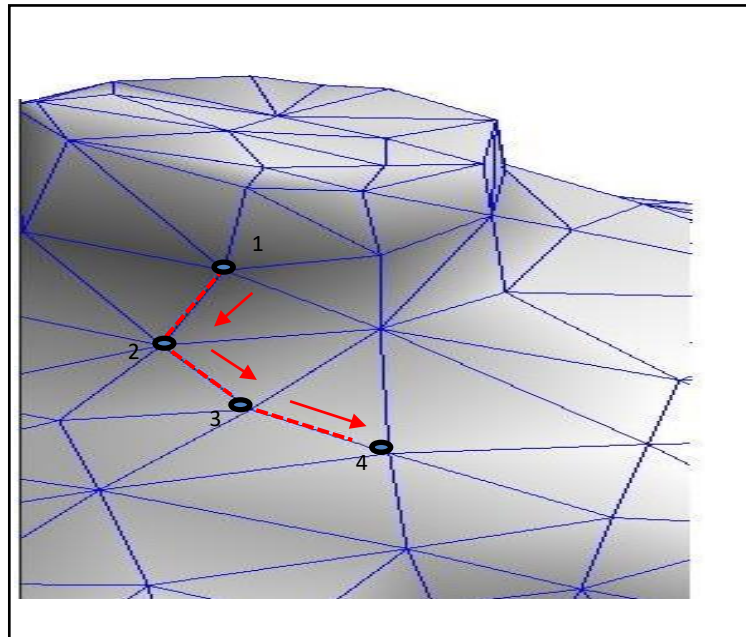


Figure 1- A part of the mesh explaining the starting point

This process is repeated until complete embedding of all the data is achieved. The following algorithm describes head line steps for embedding text in a 3D mesh using nearest neighbour.

Embedding algorithm

Input: 3D model, text

Output: watermark model

Step1: Read 3D model of '.OFF' File format (M).

Step2: Read Vertices (V) and Edges (E) from file.

Step3: Read the data and convert it to binary.

Step4: Choose the center of the mesh based on equations (1-3).

Step5: Generate the entire child for the center vertex (the neighbor vertices).

Step6: Select the path based on the shortest distance by applying (Eq. 4) between the center and all child vertices.

Step7: Choose the vertex on the other side of edge for embedding, convert it to the vertex location to binary and used least significant bit for embedding.

Step8: Repeat the above step 5, 6, 7 until complete embedding process.

Step9: View the watermark model.

In order to extract the watermark from the watermark model, the following steps have been applied:

Extracting algorithm

Input: watermark model

Output: text

Step1: Load 3D watermark model of '.OFF' File format (M).

Step2: Read vertices and edges from file store in (V) and (E).

Step3: Choose the center of the mesh based on equations (1-3)

Step4: Convert the vertex location to binary, extract the first binary bit using the LSB.

Step5: Generate the entire child for the center vertex (the neighbor vertices).

Step6: Select the closet vertex to the center based on the shortest distance.

Step7: Convert the binary to ASCII code.

Step8: Check if it reach end of bits then go to step10.

Step9: Repeat the above step 5, 6.

Step10: Convert from ASCII to text (the watermark).

4. Experimental Results

Many experiments have been performed to show the implementation of the proposed method according to invisibility and robustness against types of attack. Table 1 shows the models that have been used as examples for the experience in a Standford library [7]. "Venus", "Nefertiti", "Mannequin", and the watermark are "Copyright Protection".

Table 1- The test 3D objects.

No	Name	Test models from different position	Faces	Vertices
1	Venus		1396	711
3	Nefertiti		562	299
4	Mannequin		839	428

In this paper, the invisibility of the proposed system has been measured by Root Mean Square

Error (RMSE) which represents the difference between the original and the watermark model. RMSE determined the error generated from the square root between every pair of vertices for the two objects before and after embedding, so that the two meshes must have the topology. RMSE is calculated as follows [8]:

$$RMSE = \sqrt{\sum_{i=1}^n ||v_i - v'_i||^2} \quad \dots (5)$$

Where: n represents the number of vertices in the mesh, v_1 : vertex of object before embedding, and v_1' : a vertex corresponding in the watermarked object [8].

Another measurement of visibility called Hausdroff Distance (HD) has been used to test the proposed system. HD compares between two models and finds the error between them through calculating the minimum distance for any point in the first model to all points in the watermarked model [9].

$$HD(M, N) = \max_{m \in M} \{ \min_{n \in N} \{ d(m, n) \} \} \quad \dots (6)$$

Where: M and N are the meshes before and after embedding, $d(m, n)$ is the Euclidean distance for (m and n) in 3D domain, and the value of HD should be equal to zero if there is no difference between two meshes. Figure-2 illustrates the 3D models before embedding (original), a 3D mesh model to clarify each face with its vertices, and the watermarked model. There is obviously no difference in the eyes, this is confirmed by the values of the objective test based on RMSE and (HD), as shown in Table 2. In Table-2, their values approaches zero, which reflects little difference between the original model and the 3D watermarking model

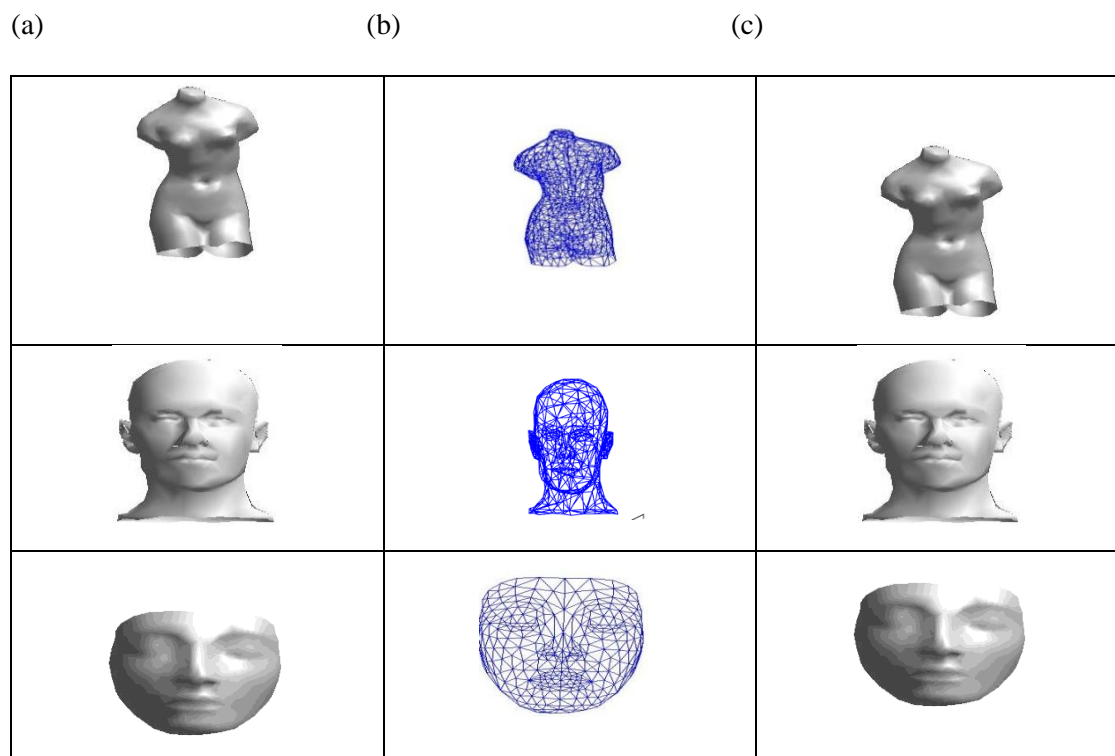


Figure 2-(a) the original model, (b) the mesh for 3D model, and (c) The watermarked model.

Table-2 displays the experimental results for the proposed algorithm. The results show that the method of creating watermark models does not generate any distortion in the components of the image, where the values of RMSE and HD are very low and close to zero.

Table 2-The RMSE and HD for watermarked model

Model	RMSE	HD
Mannequin	0.00000094	0.0039
Nefertiti	0.00000002	0.0039
Venus	0.00000005	0.002

5. Robustness against Attack

One of the important requirements that must be achieved by any watermarking system is robustness against attack. In this paper, the Correlation Factor is used to measure the difference between the embedding and the extracted watermark.

Correlation Factor (CF) is the ratio of the recovered watermark to the embedding watermark bits, its value range between -1 to $+1$, and can be expressed as follows [2]:

$$CF = \frac{\sum_{i=1}^{N-1} (b'_i - \bar{b}') (b_i - \bar{b})}{\sqrt{\sum_{i=1}^{N-1} (b'_i - \bar{b}')^2 \sum_{i=1}^{N-1} (b_i - \bar{b})^2}} \quad \dots (7)$$

Where: indicates the averages of the extracted watermark bit , while the embedded watermark bit. Generally, the acceptable value of CF is higher than 0.75. When the value approaches 1, it indicates an ideal result (i.e. watermark extracted is completed without any loss).

In this paper, two types of attack have been used to check the robustness. The first type is the geometrical attack which includes translation, scaling and rotation. The second type of attack is signal processing that includes noise addition and smoothing. The noise is inserted in the normal direction for every element of the vertices, while the smoothing occurs on the original objects by subdividing the mesh specified by the “Vertices” and “faces”, such that each face of the mesh has been subdivided into N^2 smaller faces. Table 3 below shows the effect of these different types of attack on the watermarked model that depends on the value of CF which represents the ratio of the extracted watermark bit after attack as the value high this mean good robustness against attack.

Table3-CF values after different types of attack.

Model	Translation	Scaling	Rotation	Noise level 0.001	subdivision
Venus	1	1	1	0.89	0.1
Nefertiti	1	1	1	0.6352	-0.21
Mannequin	1	1	1	0.904	0.22

6. Conclusions

The proposed method is efficient in terms of non-observation and robustness. The selection of embedding area in 3D mesh increased the invisibility which is one of the most requirements of any watermarking system, where it based on the minimum distance between vertices (the area with most intensity of vertices).

The experimental results showed that the proposed algorithm is resistant to any geometrical attack (rotation, scaling, and translation) with acceptable value at adding noise, while the resistance had weakness at the more complex attack which is subdivision that change the topology of the 3D mesh by increasing the number of faces in 3D model.

References

- Liu, J. **2014**. A new watermarking method of 3D mesh model. *Telkomnika Indonesian Journal of Electrical Engineering*, **12**(2): 1610 -1617.
- El Zein, M., Basyoni, L., El Bakrawy, G. **2016**. Non-Blind Robust Watermarking Approach For 3D Mesh Models. *Journal of Theoretical and Applied Information Technology*, **83**(3).
- Rolland,X., **2014**. Robust 3D Watermarking, PhD dissertation, University Nice Sophia Antipolis,HAL Id.
Available at: <https://tel.archives-ouvertes.fr/tel-01127191>
- Luma, F. and Muna M. **2016**. Text Hiding in 3D Object, *Eng. &Tech.Journal*, **34**(5).

5. Zainab N. Al-Qudsy¹, Shaimaa H. Shaker, and Nazhat Saeed Abdulrazzqu, **2018**. Proposed an efficient blind digital 3D model watermarking algorithm using geometrical properties, *interciencia journal*, **43**(11), ISSN: 0378-1844.
6. Yang, Y. **2013**. "Information Analysis for Steganography and Steganalysis in 3D Polygonal Meshes". School of Engineering and Computing Sciences University of Durham United Kingdom.
7. The Stanford 3D scanning repository. URL <http://www-graphics.stanford.edu/data/3dscanrep>
8. Muna M. and Luma F. **2015**. Watermarking in 3D Model Using Dihedral Angle, *Iraqi Journal of Science*, **56**(4C): 3546-3553.
9. Hitendra, G. **2013**. A Secure Image Based Watermarking for 3D Polygon Mesh. *Romanian Journal of Information Science and Technology*, **16**(4): 287–303.