Text Hiding in 3D Object

Dr. Luma Fayeq Jalil
Computer Science Department, University of Technology/ Baghdad.
Email: dr_lumafaik79 @yahoo.com
Muna M. Laftah
Computer Science Department, University of Technology/ Baghdad.
Email: muna_majeed@yahoo.com

Received on:1/9/2015 & Accepted on:7/4/2016

ABSTRACT

In this research was to propose a new way to hide data from the text in the tri-dimensional images type depending on the geometric style is proposed, this can be done via the manipulation of the location of the (vertex) in most areas of softness in the triangular object dimensions of any of the many details areas so we make sure not to detect the presence of the data eye human. The experimental results showed, a high rate of failure note the presence of hidden data depending on the scale "RMS" Tripartite-dimensional images, and the way showed good resistance to the types of geometric attack such as "translation"," rotation" and "scaling" and out where he was retrieving a full hidden data without any destruction and this is what boosted "BER".

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

INTRODUCTION

Hide information has recently become the subject of research; it is important to put a lot of attention. Hide information includes a wide range of applications that are an integral part of messages to the media of confidential part for different purposes [1].Personal computers and internet connections made the distribution of digital data (text, sound, and image)and applications easy and fast that leads to appear the problem of copying and transmitting of the digital products illegally without any authentication[2].

The main types of hiding data either watermarking or what is called concealing information, and all of those methods are used to express the progressive private information by integrating data in many types of digital media. The main important difference between the watermarking and steganography is that the first focuses on water property authentication (ratification in deep description) , at the other hand the steganography hides the information such that there is no one in the sender part or receiver can suspect of having the information[1].

These items may be text, audio, video or3-dimensional data (3D) objects. Due to the misuse of data, security has become an important issue to protect them. 3Dobjects can be viewed from any angle, such as the highest bid, side view; vision etc. Less 3Dobjects has a large number of applications in the field of design and architecture, machine design, cultural heritage and recreation. 3Dobjectsare classified into two groups based size objects "voxels, constructive solid geometry" surface-based and things(the surface of the implicit, parametric surfaces, polygon mesh) [3]. In this paper, we are concerned with the3Dpolygon mesh only.

A mesh is a group of polygonal aspects of targeting constitute an appropriateapproximationObjectreal3D.It holds three different combinatorial components: vertices, edges, and facets. From The other point of view, a network can also be completely explained by two types of information: Engineering the informationattitudes3D"coordinates"ofallvertices, while the contact information it supported neighborly relations between the different elements [4]. Mathematically, a 3D polygonal mesh containing N vertices and M edges can be constructing as a signal.

M = {G,C}, such that
G = {vi}i=1,2,...,N ,
vi = (xi, yi, zi)
C = {(vk1 , vk2)} , 1 ≤ k1 ≤N, 1 ≤ k2 ≤N, k1 ≠k2
In figure (1) shows the bunny3D object and its triangle mesh [4].

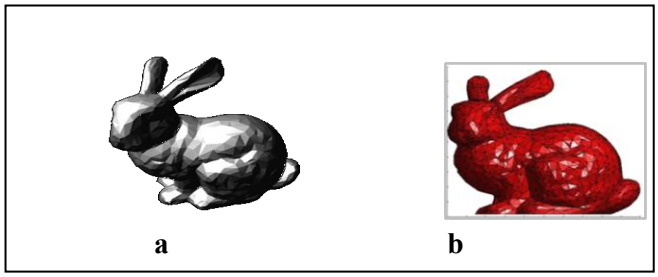


Figure (1): a: bunny3D object b: triangle mesh

Watermark proposed in this paper takes into account the geometric characteristics of theobject3D mesh vertices to choose to include the watermark. Vertices are selected considering the distortion perceivable, which is defined as distortion is observed by humans visual system. Because it cannot be modeled mathematically, and therefore cannot be automated. It was a personal assessment used to evaluate the distortion perceivable due to the various processes 3D processing (pressure, smoothing, and simplify and division). Geometric attacks only modify the geometric region of the watermarked mesh model. No matter what is the kind of the geometric alteration, the attack is reflected by an adjustment of positions. A similarity transformation is considered to be a common operation rather than an attack, against which even a fragile watermark should be ambidextrous to stand. It comprises, rotation, translation, uniform scaling, and combinations of the above three operations.
Watermarking of 3D object is different from the watermarking scheme of image, video or audio [5].
The hidden information called watermark may be a serial number , random number sequence, copyright messages, ownership identifiers, control signals, transaction dates, creators of the work, text, bi-level or grey-level image, or other digital formats[6].

RELATED WORK

Algorithms watermarking of 3D objects can be grouped on a large scale on the basis of a file.

1. Data organization, where is inserted watermark by modifying the organization associated with the data file of the object.
2. Datatopographical3D,whichis used to connect from a polygon mesh of the watermark insertion maintain position Tops. It is not modified the geometry of the network any positions of the peaks during the embedding of the watermark. The watermark is included by modifying the edges of the network.
3.Geometricaldata,wherethe watermark is inserted through minor modifications performed on the geometric data of the object3D [4].
There are many means of concealing information and methods of watermarking to a polygon3Dmodelsproposal. The main purpose of the watermarking is strongly withstanding various malicious attacks to certify ownership or content protection. In this section, we refer only to the methods of concealing informationabout3Dpolygonmodels.

Liu, 2014 [5] proposed a new method for embedding a watermark into a 3D model, based on triangular meshes. First, put the frame of reference by taking advantage of the usual average in the region, which has ageometric feature obvious. Each component of the projectheadcoordinationvertexseparatelyon the orthogonalcoordinateaxesin the framework

ofreference; has been selected positionsan integral part of the information in accordance with the area of the neighbors2-ring from every vertex.

Based Hitendra Garg,
2012 [3] algorithm was proposed watermark on the geometrical properties of the 3D mesh, and classified peaks 3D surface mesh to an apartment, and the height of the region and deeper. These peaks are classified into three groups of mutually exclusive. The first group is composed (S1) through the peaks of the deepest area. For the peaks of the second set (S2), and the top of the head is normal in the IEEE-754 is a little representation thousandths of a decimal as '1'. Group C (S3) contains the remaining peaks. They are selected from the peaks S1 and S2 to include the watermark and safe according to the law, and the watermark is included through the re-positioning of selected peaks from their original locations according to the category to which they belong. The evaluation of the robustness against various attacks distortion and less distortion.

Proposed Watermarking Algorithm
The proposed watermarking algorithm is to hide data of type text in 3dtriangle object, such that there is no difference to the eyes between the original and the watermarked object, and can recover the watermark after an attack to destroy it. It is based on the geometrical approach; by selecting the area with the smoothest of mesh based on the more details that imperceptible for the human eyes to detect any change in the object, and then start embedding process as described in the following:

Selection The Vertices for Embedding
In the proposed watermarking algorithm, watermark is embedded by re-location of some selected vertices, so that first step in embedding algorithm specify the location of vertices which are used for embedding , the area with more details in object, which is more smooth than another place is chosen because imperceptible to human visual, suppose via belong to 3D model M, F the number of faces surrounding to each vertex as a ring, so we start by selection the vertex with largest number of faces around then move to the next vertex with smaller number of faces after visit all faces of the first one.

Preprocessing Steps
3D triangle mesh model used for embedding of type (.obj)file which the most common file type of 3D file content.

Step1: Firstly convert polygon to 3D mesh triangle that is mean each face of three edges.

Step2: Choose pivot point v_p (x_p, y_p, z_p)

For every vertex in the object shift all vertices in the object to the origin, assume v_i (x_i, y_i, z_i)

$x_{i+1}=x_i-x_p$

$y_{i+1}=y_i-y_p$

$z_{i+1}=z_i-z_p$

Step3: Translate the object to origin after choosing pivot point and shift the object according to this point, to ensure that the object not affected by the translation, scaling and rotation attack.

EMBEDDING ALGORITHM
In the following the main steps of embedding algorithm is described
Input: 3D obj, watermark secret data
Output: 3D watermarked model
Step1: Read 3D model, store faces and vertices in a list.
Step2: convert secret data to binary.
Step3: convert 3D model polygon to triangle mesh model.
Step4: compute the edges.
Step5: compute the 1-ring (the faces surrounding for every vertex) and sort the vertices according to the number of faces around each vertex.

Step6: start embedding by selecting the suitable region, the region with the more details (triangles) than others, the smoothness region.
Step7: from ring list choose the vertex with the largest number of faces around it, mark it as used, if there are more than one number of vertices have the same number of faces, test the area of these faces around these vertices and choose the vertex with the smallest area around it, start with the first face in the ring list if it used before, move to the next face, else take the rest of vertices in the face and check if it is not visited before, because sometimes there is an edge belong to two adjacent faces.
Step8: embedding the first bit of text in the selected vertex by convert the (z-coordinate) value of the vertex to binary 64-bit, then test if the input bit is 1, and the selected vertex bit is 0 then convert bit to 1, else leave it, otherwise, if input bit is 0 and bit is 1 convert bit to 0, else leave it.
Step9: move to the next vertex with the lower number of vertices around it and continue until all the input binary is completed
Step10: save the watermarked object

Graphical Example for embedding steps

Figure 2 explains the path drawing for embedding process for part of the mesh.

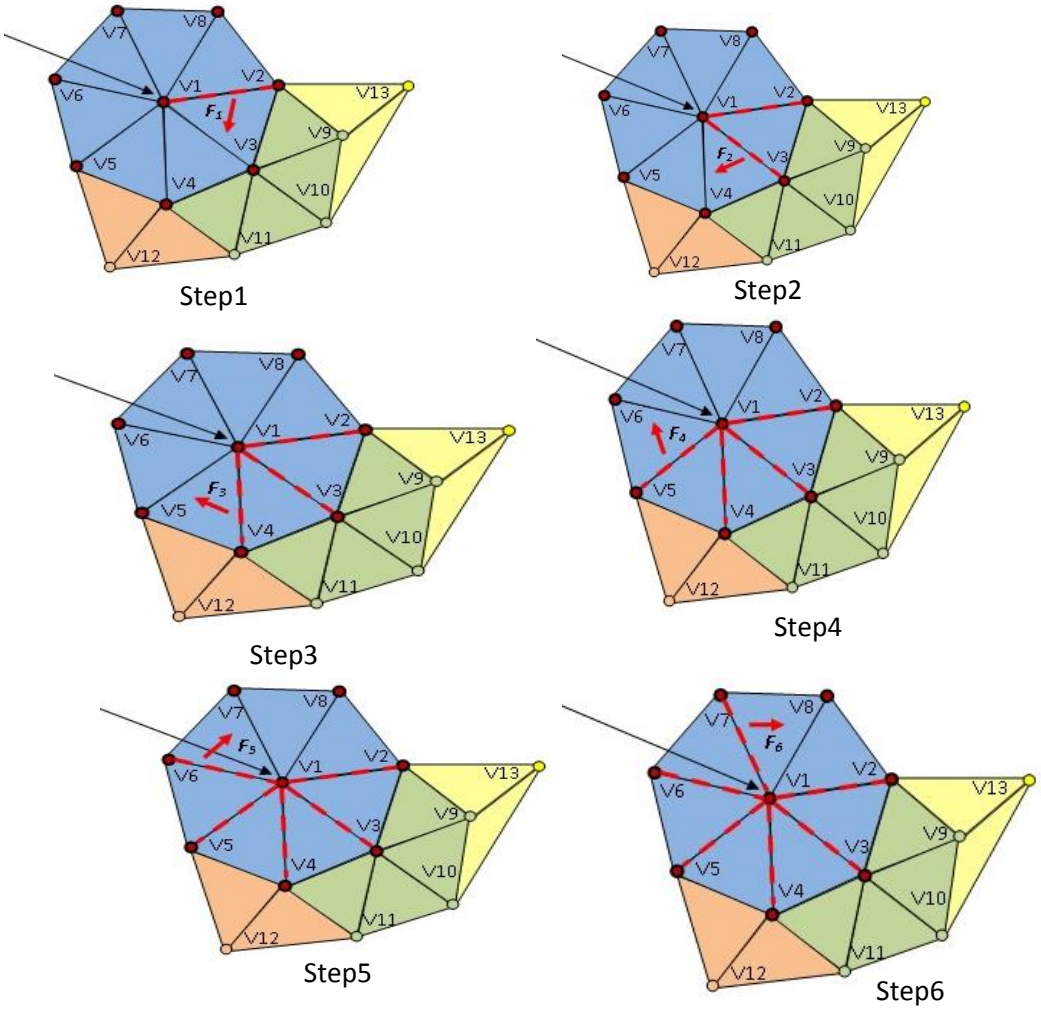


Figure (2): path drawing for embedding process

Suppose v1...v13 are subset of mesh vertices, f is face number
1-Scanning each vertex of mesh and choose the vertex v1 because has seven faces, start embedding in v1 and mark it as used, next move to v2 check it is marked before embedding.
2-Take v3, repeat checking and embedding.
3-Move to the next face (f2) in 1-ring, leave v1 and v2 because it is selected before, use only v4 for embedding and mark it, then move to the next face. Repeat the same operation until reach f6 leave it because all vertices used before.
4-After complete the first ring, move to the vertex v6 that has six faces around it, in this ring surrounding vertex. There is no embedding to vertices (v1,v2,v3,v4) because they are marked in first iteration and also belong to this ring, vertices v9,v10,v11 used for embedding.

Extraction watermarking algorithm
The same steps of embedding but in reverse order
Input: 3D watermarked model '.obj' file
Output: secret data
Step1: load 3D model.
Step2: compute the edges for the 3d model.
Step3: compute the 1-ring list (the faces surrounding for every vertex).
Step4: start extraction by selecting the smoothness region based on the number of faces around each vertex.
Step5: choose the vertex, start with the first face test if it is used before (by checking all vertices in the face if it is marked), move to the next face, else take vertices,used for extraction, and continue until completed extraction all the secret binary data.
Step6: extraction processes such that, extract the binary bits of secret data after convert the (z-coordinate) value of vertex to 64-bit binary.
Step7: move to the next vertex with the lower number of faces around it;continue until all the binary secret data is extracted.
Step8: display the secret data.

4-EXPERIMENTAL RESULT

We have implemented our proposed algorithm on different 3D polygon mesh model as shown in the figure (3).

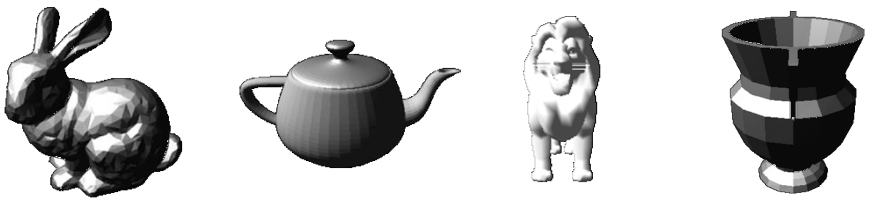


Figure (3): The test 3D objects

Figure (4) shows the objects before and after embedding, we see there is no difference to the eyes, that is mean there is no visual effect on the object.

Object before embedding	Object after embedding	Object after embedding	Object before embedding
			
			

Figure (4): The3D objects before embedding and after embedding the watermark

Evaluation The Proposed Method

"Root Mean Square Error" (RMS) and "Bit Error Rate"(BER) used as matrices to detect the distortion between the original and the watermarked object which is considered as the evaluation method to measure the performance of the proposed algorithm.

Root Mean Square Error (RMS)

The average error is based on the square root of correspondence between every pair of vertices of the two objects before embedding and after embedding for comparison, and therefore it is limited to the comparison between the two meshes sharing the same topology. The root mean square error as follows rating:

RMS=$\sqrt{\sum_{l=1}^{n} ||v_{l-} v_l' ||^2}$...1

n is the number of vertices of mesh and v_l is a vertex of object before embedding and v_l' is a vertex corresponding to the watermarked object.

Bit Error Rate (BER)

The BER is the ratio between the numbers of bits that are detected correctly the total number of bits included. BER values lie between [0-1]. Link"1" means that the value of100% of the watermarked is extracted information, table below the result of RMS and BER for the original and the watermarked object [5].

Table (1). The result of RMS and BER for the original and the watermarked object

Model name	no of vertex	face	RMS	BER
bunny	1355	2641	8.2774774062e-08	1.0
simba	2478	1950	0.012207425343019	1.0
teapot	7850	12152	2.2672422375e-05	1.0
Planter flower	594	571	8.6851834448e-04	1.0

The results in Table 1 show that there is no perceptible distortion on the watermarked model and that is one of the most requirements of watermarking based on the RMS values.

Robustness of the Proposed Method

Because of the processing step by converting the object to the origin so that no translation, scaling, and rotation attack affected on the watermarked object. Figure (4) shows the geometrical attack (translation, rotation, scaling) for the watermarked object to test the robustness of the proposed method.

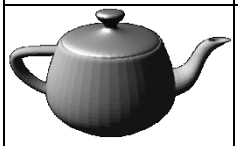
Original object	scaling	rotation	translation	BER
				1.0
				1.0
				1.0
				1.0

Figure (4): The attack on the watermarked object

The BER object watermarked after geometrical attack is to stay 1.0, bit quite a correct detection. Table 2 shows the theoretical comparison of the proposed system with watermarking system approach in [3].Table 2 shows the bit error rate (ρ) of extraction watermark from the various attacks; the proposed system gives the best result from robustness based on the bit error rate.

Table (2) Comparison between the proposed system and existing systems.

Author	System type	translation	Rotation		Scaling		
			1^0	2^0	0.90	0.99	0.001
Liu, 2014	**blind**	ρ>0.95	ρ>0.89	ρ>0.66	ρ<0.53	ρ>0.73	ρ>0.81
Proposed system	**blind**	**1**	**1**	**1**	**1**	**1**	**1**

CONCLUSION

In this paper new blind "3D watermarking" is introduced based on geometrical approach, from the result of the above, we conclude that the proposed algorithm can meet the requirements of concealing information, capacity, strength. Invisibility achieved by choosing the more smooth area for embeddingas a result more complicated hiding in more details which can be found in object, by shifting the object to the original the robustness against geometrical attack is accomplished, so that all the hidden data is retrieved correctly after scaling, translation, and rotation attack.

We can increase the capacity by using x-coordinate and y-coordinate for embedding because only z-coordinate was used in the proposed algorithm.

REFERENCES

[1]Chao-Hung Lin.2013. A high-capacity distortion-free information hiding algorithm for 3D polygon models International Journal of Innovative Computing, Information and ControlCIC, Volume 9, Number 31349-4198.

[2] Bashar S Mahdi ,Alia K. Abdul Hassan .2014. Hybrid Techniques for Proposed Intelligent Digital Image Watermarking,Eng. &Tech.Journal, Vol.33,Part (B), No.4, 2015

[3] Hitendra GARG.2013. A Secure Image Based Watermarking for 3D Polygon Mesh, ROMANIAN JOURNAL OF INFORMATIONSCIENCE AND TECHNOLOGY, Vol. 16, 4, 287–303.

[4] Dugelay J.-L. 2008.Baskurt A., Daoudi M., 3D Object Processing: Compression, Indexingand Watermarking, Wiley.

[5].Liu Jing. 2014. A New Watermarking Method of 3D Mesh Model, TELKOMNIKA Indonesian Journal of Electrical Engineering, Vol.12, 2, 1610 -1617.

[6]Nidaa F. Hassan ,RuaaKadhimJaber .2014. Proposed Algorithm for Digital Image Watermarking Survival against JPEG Compression, Eng. & Tech. Journal .Vol.32,Part (B), No.1 .