

Invisible Watermarking in 3D models

A robust method of watermarking in 3D models

Modigari Narendra,

Assistant Professor, Department of Computer Science and Engineering,

Sri Ramakrishna Institute of Technology
Coimbatore-641010, Tamilnadu, India.

narendramodigari@gmail.com

K.Thanga Vaila, K.Nandhini, S.A Padmanabhan,
P.Satheesh Kumar

B.E. Computer Science and Engineering,
Sri Ramakrishna Institute of Technology
Coimbatore-641010, Tamilnadu, India.

thangavaila@gmail.com

Abstract—The world is fast growing towards industrialism where every product developed takes huge efforts, man power and time. The products can be represented as a mathematical representation. So industries are adapting to 3D models in manufacturing a product rather than to develop a real one and test it. The 3D models are easy to develop which can be used to represent a real world three dimensional object. They are mainly used in architectural design, manufacturing design etc. But the 3D model is less secure and can be easily pirated. The person who creates the 3D model has no ownership details on the 3D model. To make it secured and make copyright to owner watermarking is embedded in it. Most of the watermarking algorithms are not resistant to attacks like translation, scaling, cropping, rotational, shearing, etc. But the algorithm used in developed by us is resistant to attacks like scaling, translation and the watermarking algorithm is invisible. This ensures that the owner who created it has a control or copyright over it. If the model with watermark is pirated it can be recognized by trying to extract the watermark.

Index Terms—3D models, binary data, frequency, energy, slice, DWT

I. INTRODUCTION

There is a big growth in 3D modeling in production and other fields .But the problem arises when it comes to security. The person who creates the 3D model as no ownership details on the 3D model. So to overcome that problem, embedding a watermarking identity inside the 3D model will help to keep the ownership safe based on some algorithms. This makes the creator to gain ownership on the model he/she created.

The main problem with the present scenario is that there is no security measures to protect the 3D model .Anyone can miss use are make the model and replicate it and make the model their own due to less security and make pattern on them. The work of 3D model owner goes in vain and he/she does not get credit for that.3D models developed by 3D owners are being replicated easily by other users. So securing the work of the owner becomes essential. Watermark embedding in 3D models may create distortion in the model and lead to collapse of the model. The paper emphasizes to develop a robust and invisible watermarking on 3D models. In normal 3D model it can be extracted from original and can be updated to new one this will enforce privacy.

The main scope of the paper is for providing the invisible watermark on 3D model that is robust and does not create any distortion to the actual 3D model which be retrieved by certain algorithm. The present techniques are vulnerable to attacks and this can deform the shape of the 3D model. But in proposed algorithm the defect can be overcome.

The following are the main objectives that can be primarily focused in this work.

- To ensure Copyrights.
- To provide proof of Ownership
- To protect integrity
- To ensure 3D model invisible water marking
- To provide robustness
- For the purpose of copy control

A watermark is an identifying image or pattern in paper that appears as shades of lightness/darkness when viewed by transmitted light caused by thickness or density variations in the paper.

A 3D model is a digital representation of an object in three dimensions without which 3D printing would not be possible. 3D modeling is used in many different industries, including virtual reality, video games, 3D printing, marketing, TV and motion pictures, scientific and medical imaging and computer aided design and manufacturing.

Robust watermarking is a watermarking algorithm that can survive not only general operations such as a compression ,adding noise, filtering, analog to digital or digital to analog conversion, and so forth but also such geomantic attacks such as rotation, scaling, translation, shearing and so forth. The watermarking algorithm presented in this paper is resistant to attacks such as scaling and translation.

II. EXISTING WORKS

Mun et al.[1] proposed the robust watermarking method of a 3D mesh against cropping to obtain a blind watermarking scheme that allowed consistent segmentation and improved the robustness against cropping. For the watermark embedding, Surface Diameter Function(SDF) based segmentation is performed on the face and segment pair known as gain and a watermark bit is inserted into each bin of the histogram of vertex-norm distribution. For watermark extraction, every

segment is used to extract the watermark sequence and the final decision was based on the set of sequences by using majority voting system. Consistent partitioning for 3D mesh watermarking was gained by SDF based segmentation and the watermark sequences were extracted properly. However, the method failed to meet the 100% robustness in general mesh operations such as smoothing, simplification, shape distortions.

Lavoue et al.[2] investigated the use of image metrics for assessing the visual fidelity of 3D graphical objects. Image-based metrics perform very well in evaluating the quality of different versions of a same object under a single type of distortion. For simple use cases or in cases when model-based metrics cannot be applied, image-based metrics will work very well. Rendering algorithms are less accurate in comparing different distortions or distortions applied to different 3D models. In complex scenarios involving the ranking of different distortions applied on different 3D objects the model-based approaches perform better. Due to variations in methods applied for both simple and complex objects, evaluating the visual quality of 3D models was not efficient.

Yang et al.[3] proposed the extended version of his own research and a robust method that is modification of Cho et al.'s mean and variance based watermarking algorithm. The algorithm embeds the watermark into the histogram of the radial coordinates of the mesh vertices embedding each watermark bit inside a discrete statistic of the model in the number of elements of two adjacent bins. The proposed discrete statistic offers improved performance against both the proposed steganalytic attack and standard watermark removal attacks. The embedding algorithm is based on histogram shape modification, similarly to some existing image watermarking algorithms. It provides robustness against malicious watermark removal attacks and against steganalytic attacks and also offers improvement in terms of embedding distortion. But the embedding distortion was still present in the method.

Molaei et al.[4] proposed a method in which a pre-processing is applied on the 3D model to make it robust against geometric transformation attacks. Then, a number of triangle faces are determined as mark triangles using a novel systematic approach in which faces are categorized and sorted robustly. In order to enhance the capability of information retrieval by attacks, block watermarks are encoded using Reed-Solomon block error-correcting code before embedding into the mark triangles and the encoded watermarks are embedded in spherical coordinates. This method is robust against additive noise, mesh smoothing and quantization attacks. But a negligible visual distortion is observed in host model using this method.

Chou et al.[5] investigated about the important technologies that were present for the watermarking of 3D models and compared their performance a decade ago. The robust and fragile watermarking methods are compared and it is that concluded the robust method to be more useful to claim the ownership. The three requirements for 3D robust watermark embedding are unobtrusive, robust, and space efficient. Unobtrusive means the embedding must not interfere with the intended use of a model. Robust means the embedded watermarks should remain detectable after being maliciously attacked. Space efficient means an embedding method should be able to embed sufficient amount of information into models. The major functions in 3D fragile watermarking:

integrity checking and changed region locating. The Triangle Similarity Quadruple (TSQ) extraction algorithm does not require the original 3D model for extraction of watermark. Watermarks embedded by the TSQ algorithm remain detectable against translation, rotation, and uniform-scaling transformations of the marked 3D models. But the watermarks will be destroyed by randomization of coordinates, or by topological alteration such as re-meshing, smoothing, and simplification operations.

Hou et al.[6] proposed a blind estimation algorithm for 3D printed model that can be helpful in the real world. The Blind estimation algorithm for printing direction that starts from analysis of the layering artifact. The watermark from the printed-and-scanned model is synchronized to the original orientation. After testing with many 3D models and the mesh attacks, the method does not lose embedded pattern during the 3D print-scan process. This algorithm achieved robustness against a small amount of cropping attack. Embedded watermark can survive local loss of the surface, because the frequency domain was exploited for the watermarking. However, the proposed method cannot guarantee perfect invisibility under current printing technology, even though the current 3D printing technology creates models with relatively high accuracy and resolution.

Jang et al.[7] proposed SDF based segmentation for watermark embedding into the 3D models. For the embedding process, consistent segmentation is performed based on calculation of SDF and roughness. Then, the watermark is inserted for each segment. A watermark bit is inserted in each bin of each segment using the improved Histogram Mapping Functions (HMF), with consideration of the roughness of the surface. This HMF has been used for statistical watermarking. For the extraction process, a watermarked mesh is segmented and the vertices of the segment are divided. Then, the mean of vertex norms is calculated, and the watermark bit is extracted from each bin of each segment. Watermark Trace Energy (WTE) of each segment is calculated and the extracted bit-sequence of the segment with the largest WTE is determined as the final watermark. The proposed method can extract the final watermark even if a large amount of the mesh has been cropped. This method is not applicable to very small models because the watermark system needs sufficient numbers of vertices to divide segments effectively. It is also vulnerable to severe distortions that change the histogram of the shape diameter function values.

Rolland et al.[8] introduced a method to enhance the radial distance-based framework to 3D mesh watermarking. It was based on the spread transform and perceptual shaping on the basis of roughness information and the formulation of quadratic programming problem to minimize the geometric distortion. However the method failed in terms of security and was vulnerable because it was not aligned with the steganalysis resistance.

Chen et al.[9] described a novel blind and robust digital watermarking method for the 3D meshes using geometry image technique and spherical parameterization. The experimental results showed that the watermark is robust enough to survive from the attacks such as common geometric transforms, crop, re-sampling and simplification. It was a GPU (Graphics Processing Unit) -accelerated blind and robust watermarking approach to the 3D polygon meshes on the basis of the geometry image transform and image watermarking, which

performs watermark embedding and detection on the basis of the geometry image derived from a spherical parameterization of the input mesh with the help of massive-parallel processing power of the GPUs on the display card. Since the watermark embedding and detection of the system are implemented on GPU, it is computation efficient than the other approaches to 3D mesh watermarking. However due to their very generic approach to embedding or detection by bit replacement is vulnerable to quantization attacks.

Singh et al.[10] suggest embedding the watermark bits by altering the length of vertex normal. The pattern of watermark bits is repeatedly embedded into the cover object to increase the robustness. The algorithm is invariant to uniform scaling, translation, rotation and reordering point information of watermarked object. Due to repeatability of the pattern, the cover object cannot be easily damaged by quantization attacks. However the algorithm suffers from noise attacks.

Garg et al.[11] proposed a method in which the embedding of watermark in deeper surface in a 3D polygon mesh has less distortion compared to watermark insertion in flat and peak surfaces. The method begins with classifying the vertices into three mutually exclusive groups corresponding to the vertices of concave, flat, and protrusive areas. The watermark bits are embedded by relocating the selected vertices in accordance with their category. This method is vulnerable to attacks such as additive noise and mesh smoothing.

The above works gave an overview on how the watermarks are embedded into and extracted from the 3D models and the advantages and the disadvantages of each technique and the attacks such as noise, quantization attacks, etc that are encountered in each technique. In our watermarking technique we ensure the integrity, proof of ownership and copy control of the 3D model. The 3D watermarking algorithm developed will have improved robustness trade-off.

III. PROPOSED WORK

The embedding process starts by loading the 3D object and have to slice is selected every pixel in a 2D image has a frequency related to them and after slicing the 3D model it is converted to 2D model and to make the embedding process in the slice the pixel are selected using frequency and mentioning the radius of the area where the watermark is embedded then the frequency is taken in 1:10 ratio.

The embedding bit of the size is 10 bit and 2D image has both frequency and energy associated with it and binary data is embedded into the area that is calculated from the frequency values and then the XOR with the energy and 10 bit binary data to generate a secret key and the secret key is generated for security reason without this extraction cannot be possible. The watermark embedding process is shown in the Fig 1. and the step by step procedure for embedding is given.

Step 1:

The 3D model with the extension .obj and 10 bit binary data (watermark) are taken as inputs.

Step 2:

The 3D model is sliced, the subX, subY, subZ for all slices are separated using the following function.

[slice,sliceInd,subX,subY,subZ]=extractslice(obj,obj.f.v(1),obj.f.v(2),obj.f.v(3), inv(1), inv(2), inv(3),64)

Where inv() is inverse of the vertices and slice is used to slice the volumetric slice part.

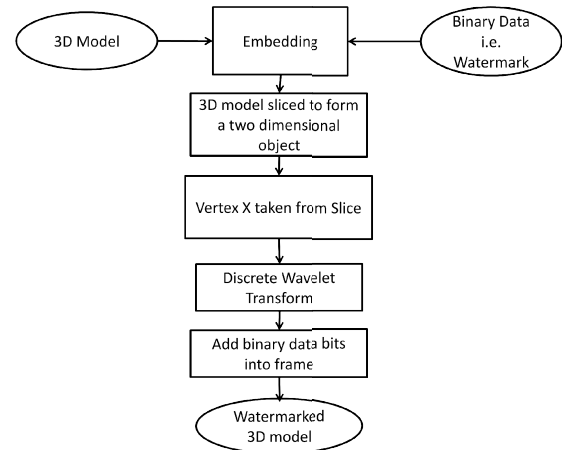


Fig 1. Embedding Process

Step 3:

After slicing the 3D model is converted into 2D slice frame. Every pixel in a 2D image has a frequency related to them. One of the slices is selected where frequency is calculated for that coordinate subX by splitting the subX into 1:10 ratio up to 100 using equation (1).

$$I_{i+1} = I \left[\left((i \times 10) + 1 \right) : \left((i + 1) \times 10 \right) \right] \quad (1)$$

$$\text{Where } 0 \leq i \leq 9$$

where I is subX and I_{i+1} contains 1/10 of subX.

Step 4:

The one level DWT is applied for calculating the frequency to each part of the split subX by specifying the wavelet name using the equation (2). The wavelet used in this algorithm is db2 which means Daubechies 2 wavelet.

$$\text{Approximate_Coefficient_Frequency, Detail_Coefficient_Frequency}_i = \text{dwt}(I_i, \text{wavelet_name}) \quad (2)$$

$$\text{Where } 1 \leq i \leq 10$$

$$\text{wavelet_name} = \text{db2}$$

The function dwt returns the approximate coefficient and the detail coefficient of the frequency.

Step 5:

Energy coefficients are calculated for each frequency approximate coefficient by squaring it and summing all the approximate coefficients then range given using equation (3). Then the absolute value of the energy coefficient is taken and stored as in the equation (4). The energy coefficients are calculated using the below formula.

$$\text{Temp_Energy_Coefficient} = \sum_{j=1}^6 (\text{Approximate_Coefficient_Frequency}_i(j, 1))^2 \quad (3)$$

$$\text{Energy_Coefficient}_i = \text{ABS}(\text{Temp_Energy_Coefficient}) \quad (4)$$

$$\text{Where } 0 \leq i \leq 9$$

Step 6:

Energy coefficient is converted into binary form by comparing the energy coefficient by using the following

condition.

$$\text{Energy_in_binary}[i] = \begin{cases} \text{Energy_coefficient}_i & \geq \text{Energy_coefficient}_{i+1} \\ 0 & \text{otherwise} \end{cases}$$

Where $1 \leq i \leq 9$

$$\text{Energy_in_binary}[10] = \begin{cases} \text{Energy_coefficient}_{10} & \geq \text{Energy_coefficient}_1 \\ 0 & \text{otherwise} \end{cases}$$

Step 7:

The exclusive OR operation is performed on 10 bit binary data taken as input along with the energy in binary form relational array using the equation (5). Thus the embedding is done and secret key is generated.

$$\text{Secret_Key} = \text{XOR}(\text{Energy_in_binary_form}, \text{Input_data}) \quad (5)$$

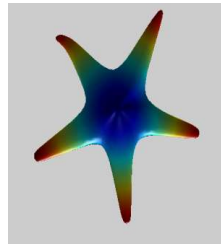
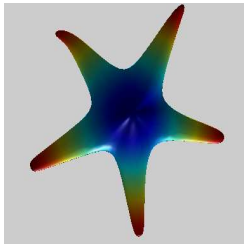


Fig 2. Original 3D model Fig 3. Watermarked 3D model

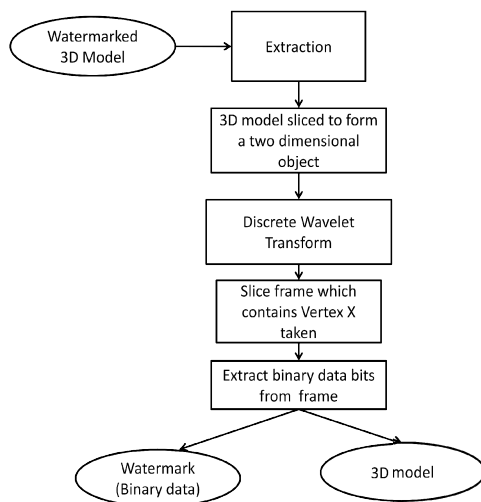


Fig 4. Extraction Process

Extraction in Fig 4. is as same as the approach of the embedding process. Extraction process is similar to that of the embedding process. To get the 3D object and have to slice is selected every pixel in a 2D image has a frequency related to them and after slicing the 3D model it is converted to 2D model and to make the embedding process in the slice the pixel are selected using frequency and mentioning the radius of the area where the watermark is embedded then the frequency is taken in 1:10 ratio and the embedding bit of the size is 10 bit and 2D image has both frequency and energy associated with it and binary data is embedded into the area that is calculated from the frequency values and then the XOR with the energy and secret key for getting an embedding data that is the watermark is being extracted from the 3D model.

IV. PERFORMANCE ANALYSIS

The performance of the algorithm can be calculated by using the geometric measures such as Mean Squared Error (MSE) and Peak Signal-to- Noise Ratio (PSNR). The two geometric measures are used to find the difference between original 3D model and the watermark embedded 3D model.

The algorithm is checked for performance after embedding the watermark without any attacks being performed on the watermarked 3D model. The following TABLE I. contains the PSNR and MSE values of the 3D models without any attacks being performed.

TABLE I. Performance without any attacks

3D Model Name	MSE	PSNR
Cow	0.7706	86.6867
Dragon	0.403	92.021
Horse	0.4181	91.997
Rabbit	0.4181	91.997
Starfish	0.5559	89.524
Venus	2.9107	76.57

After embedding the watermark, scaling attack is performed on the watermarked 3D model. The scaling attack affects the watermarked model to an extent. But still the 3D model resists attack and is robust that is the 3D model is not delicate and is not easily broken. The following TABLE II contains the PSNR and MSE values of the 3D models after performing scaling attack.

TABLE II. Performance after Scaling

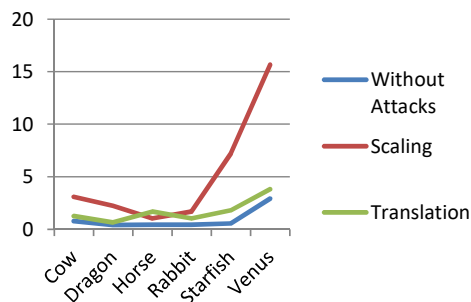
3D Model Name	MSE	PSNR
Cow	3.0825	74.6545
Dragon	2.2234	77.4831
Horse	1.0372	84.105
Rabbit	1.6726	79.955
Starfish	7.2141	67.2599
Venus	15.6426	60.537

After embedding the watermark, the translation attack is performed on the watermarked 3D model. The translation attack affects the watermarked model to an extent. But still the 3D model resists attack and is robust that is the 3D model is not delicate and is not easily broken. The TABLE III contains the PSNR and MSE values of the 3D models after performing the translation attack.

TABLE III. Performance after translation

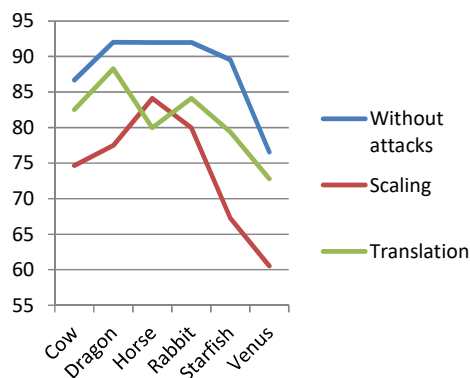
3D Model Name	MSE	PSNR
Cow	1.2450	82.520
Dragon	0.6412	88.28
Horse	1.672	79.955
Rabbit	1.0372	84.105
Starfish	1.7928	79.353
Venus	3.8109	72.802

The following Graph 1 contains the comparison made between Mean Squared Error values of the watermarked 3D model. The comparison is made between 3D models without attacks, scaling and translation attacks performed.



Graph 1 MSE values comparison

The following Graph 2 contains the comparison made between Peak Signal-to-Noise Ratio values of the watermarked 3D model. The comparison is made between 3D models without attacks, scaling and translation attacks performed.



Graph 2 PSNR values comparison

V. CONCLUSION AND FUTURE WORK

Several methods are there to watermark the 3D model which are fragile and are resistant to attacks and does not contain security keys. In this paper we have addressed the problem that is prevailing while using 3D models. 3D models are widely used in medical and industrial fields. So it should have security for preventing piracy or damage of model. To make it secured, the algorithm embeds a watermark to a slice from the 3D model and creating a security key for the embedding process. Using this extraction is done so it is not vulnerable to piracy. We have used DWT algorithm for watermarking the 3D model.

The algorithm used in this paper supports security of the 3D model, and it also ensures that the binary data is extracted using proper measures. This algorithm can be expanded to make it more resistant to attacks like scaling, translation. In this paper, the algorithm accepts only a single slice but for more accuracy and safety it can be done with multiple slices. DWT algorithm used in our algorithm was single level a one dimensional wavelet algorithm. It can be changed to higher level and can be used for improving the robustness of the algorithm. Watermarking in 3D model is very important to prevent copyrights, ownership etc. The watermarks can be embedded and extracted in different ways to improve the robustness of the model.

ACKNOWLEDGMENT

This work is done as a part of the final year project for the under graduation degree in the course Computer Science and Engineering at Sri Ramakrishna Institute of Technology, Coimbatore by the students K.Thanga Vaila, K.Nandhini, P.Satheesh Kumar, S.A. Padmanabhan and was guided by Modigari Narendra.

REFERENCES

- [1] Seung-Min Mun, Han-Ui Jang, Do-Gon Kim, Sunghye Choi and Heung-Kyu Lee (2015) "A Robust 3D Mesh Watermarking Scheme Against Cropping", IEE.
- [2] Guillaume Lavoue, Mohamed Chaker Larabi and Libor Vasa (2016) "On the Efficiency of Image Metrics for Evaluating the Visual Quality of 3D Models", IEEE August, Vol. 22, No.8.
- [3] Ying Yang, Ruggero Pintus, Holly Rushmeier, and Ioannis Ivrissimtzis (2017) "A 3D Steganalytic Algorithm and Steganalysis-Resistant Watermarking", IEEE February, Vol. 23, No. 2.
- [4] Amir Masoud Molaei, Hossein Ebrahimzad and Mohammad Hossein Sedaaghi (2016) "Robust and Blind 3d Mesh Watermarking in Spatial Domain based on Faces Categorization and Sorting", Springer April.
- [5] Chang-Min Chou and Din-Chang Tseng (2007) "Technologies for 3D Model Watermarking", IEEE May, Vol. 7, No.2.
- [6] Jong-Uk Hou, Do-Gon Kim and Heung-Kyu Lee (2017) "Blind 3D Mesh Watermarking for 3D Printed Model by Analyzing Layering Artifact", IEEE August, Vol. 3, No. 5.
- [7] Han-Ui Jang, Hak-Yeol Choi, Jeongho Son, Dongkyu Kim, Jong-Uk Hou, Sunghye Choi and Heung-Kyu Lee (2017) "Cropping-resilient 3D mesh watermarking based on consistent segmentation and mesh steganalysis", Springer March.
- [8] Rolland-Neviere X, Doerr G and Alliez P (2014) "Triangle surface mesh watermarking based on a constrained optimization framework", Vol. 9, No. 3, Page no.82 to 91.
- [9] Hung-Kuang Chen and Wei-Sung Chen (2015) "GPU-accelerated blind and robust 3D mesh watermarking by geometry image", Vol. 12, No. 5.
- [10] Singh LK, Chaudhry D and Varshney G (2012) "A Novel Approach of 3D Object Watermarking Algorithm using Vertex Normal", Vol. 14, No. 6.
- [11] Garg H and Agarwal S (2013) "A secure image based watermarking for 3D polygon mesh", Vol. 16, No. 4, Page no.288 to 303.
- [12] L. Jani ANbarasi and Modiagri Narendra (2017), "Robust watermarking scheme using Weber Law for 3D mesh models", The imaging Science Journal.

