Double Security Watermarking Algorithm for 3D Model using IEEE-754 Floating Point Arithmetic

Hitendra Garg
PhD Scholar, Dept.of CSE ,
MNNIT, Allahabad

Suneeta Agrawal
Professor , Dept. of CS&E
MNNIT, Allahabad, India

Gopalji Varshney
Assistant Professor , HCST
Mathura, India

ABSTRACT

Most of the fragile watermarking scheme authenticate the user but unable to locate the region of tampering. The objective of proposed scheme is not only maintaining the quality of watermark 3D object at its acceptable level but also identify the region of tampering. During the process of watermarking embedding the normal distance of each vertex from center of mass is calculated and marked vertices are converted into IEEE-754 floating point representation in double precision. Cryptographic hash function is applied to find the mark vertices. The watermark is inserted in each of the segments of 3D model so that authentication may be done through any of the segment. Fragile watermarking technique is used for authentication in case of multiple user claims for the single object. It is very important to protect and authenticate the 3D model.

Keywords

copyright protection; hash function; payload; cover object.

1. INTRODUCTION

Extensive growth of internet and wide accessibility of data over internet may increase the misuse of data items. These data may be audio, video, text, images or 3D object, etc. Due to the characteristics of easy duplication and modification of these contents, it is necessary to develop a variety of techniques like digital signature and watermarking scheme for various protection, ownership claiming and find the region of content tampering [1].User accesses the data and publishes the same data with slight modification which violations copyright act. The watermarking scheme is designed to check the ownership (robust watermarking) or to verify the authentication (Fragile Watermarking).

Generally these 3D object are of two type synthetic (CAD-generated) and real-world (via 3-D scanning). To protect these objects from intentional change watermarking techniques are used. Watermarking of 3D object is different from the watermarking scheme of image, video audio etc. 3D object watermarking schemes are generally categorized into main three categories: Data file Organization, topological data and geometrical data. During the watermarking process we keep in mind the following parameter like quality of watermarked solution, quality of watermarked process, interaction with standard tools and difficulty of practical implementation /realization. A number of techniques are used for watermarking: Non-Blind /Blind, Fragile/Robust etc. The non-blind watermarking (Private) which requires the original object while detecting watermark is very efficient in terms of image quality and robustness, while blind watermarking (Public) techniques are vice-versa in nature. Fragile watermark vulnerable to slight modification i.e. watermark is destroyed when some attack is done over it. Like digital signature fragile watermarking is used for authentication and localization of modifications. In robust watermarking, watermark should not be easily changed or destroyed by any intentional attack. The Robust scheme is used for copy right and fragile scheme is used for authentication.

Watermarking techniques are used to protect the copy- right and the integrity of digital content. Watermarking is an art of hiding secondary data on the primary data that may be text, audio, video, image, 3D object, etc in such a way that perceived quality of primary data remains at its acceptable level.

This paper is organized as follows. Section 1 introduces section 2 related work done on 3D watermarking. Section 3 basics of proposed watermarking technique, watermark insertion algorithm and watermark retrieval algorithm or watermark object verification process. Section 4 showing the results analysis based on Hausdorff distance and (Peek Signal to Noise Ratio)PSNR. Section 5 explains different attacks on watermarking object. Section 6 explain summary of the properties of proposed watermarking Algorithm. Finally Conclusion and future scope in section 7 and 8 respectively.

2. RELATED WORK

Watermarking of 3D object is different from the watermarking scheme of image, video audio etc. 3D object watermarking scheme are generally categorized into main three categories:- **1. Data file Organization:** encode the information by modifying the organization of the data in file associated with 3D object. **2. Topological data:** The algorithms which operate on mesh data using the topologies of 3D object i.e connectivity of mesh to embed data. The positions of the vertices are not modified. **3. Geometrical data:** These are based on slight modifications performed on geometrical data of 3D object. Ohbuchi et al. [2 ,3] uses NURBS reparameterization by changing the degree of freedom from three to one by imposing some constraints. Ohbuchi et al applies Triangle Strip Peeling Symbol sequence embedding (TSPS), Polygonal Stencil Pattern(PSP),Mesh Density Pattern.Mao et al. triangle subdivision and find new position to insert the watermark[4]. Ohbuchi et al. applies Triangle Similarity Quadruple (TSQ), which was based on modification of the geometry of triangular mesh. Tetrahedral Volume Ratio (TVR) embed the watermark in the triangular mesh by modifying affine-invarient (ratio of volume) value of pair of tetrahedral.[2,3]. Wagner et al. [5] embeds the watermark in the length of the 'normals' defined on each vertex. The use of a norm invariant to affine transformations yields a watermark that is robust to affine transforms of the 3D object.

Lots of work is done in 3D watermarking in both spatial and frequency domain. In frequency domain coefficient of DCT, DFT, and wavelet transformation are used to insert the watermark. Jeonghee et al. [6] algorithm operates in the DCT domain. The 3D mesh is traversed to generate strips of triangles and transform their vertex coordinates into frequency coefficients in the DCT domain. The watermark is then embedded into the mid-frequency band of coefficients for robustness and imperceptibility. Mitrea et al.[7] This NURBS surface watermarking algorithm operates on 2D DCT coefficients by means of a spread spectrum procedure. Firstly, three virtual images are computed from the NURBS representation: the pixel values in these images are the coordinates of the NURBS control points. A 2D DCT is then applied to each image to obtain a vector of characteristics. Then, the secret information (key) and public information (logo) are combined by means of a code division multiple access (CDMA) technique to provide the watermark which is subsequently embedded into the vector of characteristics by means of a weighted addition. Watermark detection is achieved by means of matched filters. Praun et al [9,10] proposed a sophisticated robust watermarking by constructing a set of scalar basis functions over the mesh vertices using multi resolution analysis and then perturbed vertices along the direction of surface normal weighted by basis functions. This algorithm is resistant to common mesh attack such as translation, rotation, scaling, cropping, smoothing, simplification and re-sampling operation.

Yeo and Yeung [11] proposed fragile watermarking by computing two indices for every vertex (location, value indices).Both values are calculated by hash function depending on vertices and their neighbor values. These are public and fragile but having causality and convergence problem. The watermarking techniques uses mesh feature like texture color/intensity associated with each vertices, line and face to insert the watermark.

Chou et al [16] and Wang et al [15] used floating point arithmetic for watermark insertion using different approach like selection of mark vertices, mask selection, insertion of watermark in selected coordinate of vertices rather than all.

3.PROPOSED WATERMARKING TECHNIQUE

In the proposed Non-blind watermarking technique watermark information is embedded into three-dimensional polygonal models geometry by using berry distance , generated by point cloud information of object. The proposed non-blind watermarking system is suitable for embedding private watermarks, which can be used for tracing of copies through embedding a customer related information to identify a valid customer or by embedding an ownership related information to identify a legal owner [1, 2]. In the proposed scheme our object is to maintain the quality of the object at acceptable level. To reduce the amount of payload ,we insert watermark in some place rather than all vertices. This selection of vertices is done using cryptographic security function SHA to generate 128 bits stream. We can provide double security by using cryptographic hash function as well as watermark into the 3D object. Watermark calculation are basically based on floating point or integral arithmetic.[15].In floating point arithmetic method must require appropriate tolerance required for compassion. Some time tolerance is too small to compare which result not equal even if no attack is there while large tolerance is difficult to identify or destroy the shape of the model. So, selection of appropriate tolerance is important.

4.WATERMARK INSERTION ALGORITHM:

The 3D object is mesh G(V,F) where V $=\{v1, v2, v3 \ldots\ldots vn\}$set of all vertices and F=$\{f1, f2, f3 \ldots\ldots fn\}$ is set of all faces describing the topologies of the mesh. To insert the watermark into the 3D mesh, calculate the centre of mass (Xcm, Ycm, Zcm) also known as berry center of the mesh computed as

$$\mathrm{Xcm}=\sum_{i=1}^{n} Xi/\mathrm{n} \qquad (1)$$

$$\mathrm{Ycm}=\sum_{i=1}^{n} yi/\mathrm{n} \qquad (2)$$

$$\mathrm{Zcm}=\sum_{i=1}^{n} Zi/\mathrm{n} \qquad (3)$$

After calculating the center of mass, find the

$$Vn = \sqrt{(Xi - Xcm)^2 + (Yi - Ycm)^2 + (Zi - Zcm)^2}$$

where Vn={V1,V2……. Vn } represents the distance between each vertex to the center of mass/berry center. Then apply hash function SHA on any watermark string, which produces bits stream of 128 bits. Divide the set of vertices in a group of 128 each from starting to end. Then modify the Vn to obtain updated Vn'. Now re-calculate the coordinate $(Xi^{'}, Yi^{'}, Zi')$ from updated Vn' considering same berry centre (Xcm, Ycm, Zcm) using equation 4-8.

$$\theta = \tan^{-1}\left[\frac{\mathrm{Y-Ycm}}{\mathrm{X-Xcm}}\right] \qquad (4)$$

$$\Phi = \cos^{-1}\left[\frac{\mathrm{Z-Zcm}}{\mathrm{V}}\right] \qquad (5)$$

$$\mathrm{X'} = \mathrm{V^{'}n} * \cos(\theta) * \sin(\Phi) + \mathrm{X} \qquad (6)$$

$$\mathrm{Y'} = \mathrm{V'n} * \sin(\theta) * \sin(\Phi) + \mathrm{Ycm} \qquad (7)$$

$$\mathrm{Z'} = \mathrm{V'n} * \cos(\Phi) + \mathrm{Zcm} \qquad (8)$$

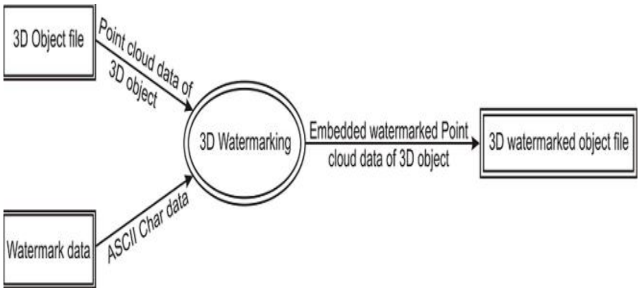
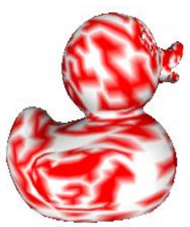

3D Object file
Point cloud data of 3D object
3D Watermarking
Embedded watermarked Point cloud data of 3D object
3D watermarked object file
Watermark data
ASCII Char data

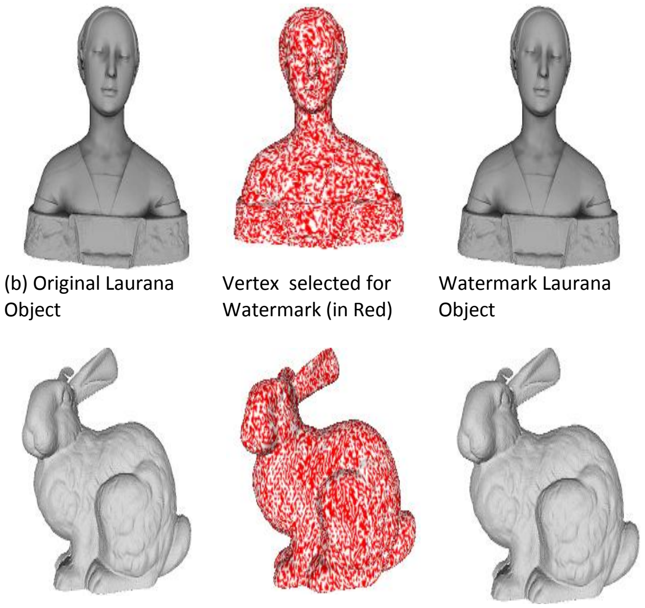
Fig 1 Context diagram for watermarking System

(a)Original Duck Object



Vertex selected for Watermark (in Red)

Watermark Duck Object



(b) Original Laurana Object

Vertex selected for Watermark (in Red)

Watermark Laurana Object

c)Original bunny Object

Vertex selected for Watermark (in Red)

Watermark bunny Object

Fig 2 (a) Original, Marked and Watermark Duck
(b) Original, Marked and Watermark Laurana Model
(c) Original, Marked and Watermark Bunny Model

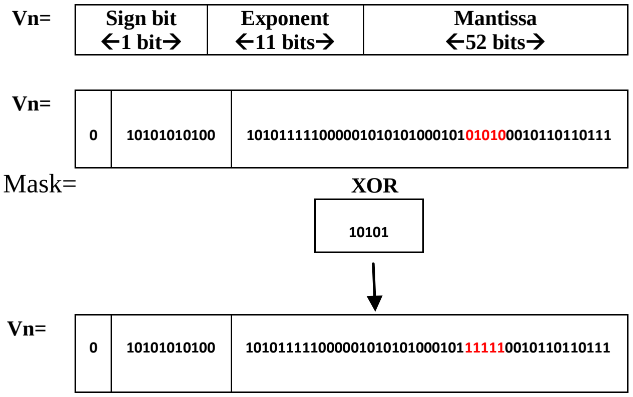


Fig 3 Operation on mantissa part of Vn of mark vertices to obtained updated Vn’

The amount of change in Vn is the watermark. Vn is updated such that perceivable quality of the object remains at its acceptable label. To update the Vn ,first find the IEEE -754 floating point representation in double precision which gives three part of Vn :1 bit sign , 11 bits exponent,52 bits mantissa. then select a 5 bits mask 10101 and apply XOR operation of mask with selected 5 bits of mantissa.

5.WATERMARK EXTRACTION ALGORITHM

The proposed algorithm is non-blind by nature as it required original cover model, watermarked inserted and watermarked model. To verify the model and region of tampering of the watermark model ,first convert all vertices V_i from cartesian to spherical coordinates $ci = (Vn_i, \theta_i, \Phi_i)$using $Vn = \sqrt{(Xi - Xcm)^2 + (Yi - Ycm)^2 + (Zi - Zcm)^2}$. where (Xcm, Ycm , Zcm) is same as calculated during watermark insertion. Follow the same step as insertion process to find the bits stream of 128 bits by applying hash function over watermark string. Then calculate the Vn' i.e berry distance from center of mass of the original object to the vertices of the watermark object.compare the Vn and Vn Obtained from watermark which gives a bits stream. The bit stream is compared with the result of the hash function for verification and identify the resign of tampering.

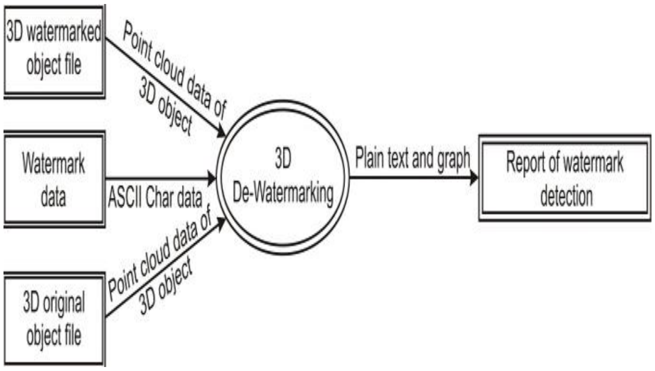

3D watermarked object file
Point cloud data of 3D object
Watermark data
ASCII Char data
3D original object file
Point cloud data of 3D object
3D De-Watermarking
Plain text and graph
Report of watermark detection

Figure 4 Context diagram for de-watermarking system

6. RESULTS ANALYSIS

To measure the effect of watermarking over the 3D model, Peek Signal to Noise Ratio (PSNR) and Hausdroff distance are considered as below:

Hausdorff Distance: The Hausdorff distance measure the extent to which each point of a model set lies near some point of another model set and vice versa. This distance can be used to determine the degree of resemblance between two objects that are superimposed on one another.

$$H(A,B) = max\big(h(A,B), h(B,A)\big) \qquad \textbf{(9)}$$

where h(A,B)=max min | a-b |

Peek Signal to Noise Ratio: The PSNR measure the noise inserted into the vertices. The watermark inserted is type of noise which changes the shape of the object to some extent.

$$MSE = \boldsymbol{1/n}\left(\sum_{\boldsymbol{i}=\mathbf{0}}^{\boldsymbol{n}} \frac{Vgi^2}{(Vgi-Vg'i)^2}\right) \qquad \textbf{(10)}$$

The V_g and V_{gi}’ represent the distance between each vertex to the center of mass and modified distance between each vertex to the center of mass and modified after watermarking.

$$PSNR=\log_{10}(MSE) \qquad \textbf{(11)}$$

TABLE I Test Results For 3 Different Models

Model	Duck	Laurana	Bunny
No. of vertices	2108	27861	17446
No. of vertices watermarked	730	12873	9259
PSNR	156.25	101.25	123.54
Hausdorff Distance(dH)	0.325	0.487	0.354

7.ATTACKS ON MODEL

The attack on the fragile watermarked 3D model deals with unauthorized tampering /modification of any region in the model. The unauthorized modification can be detected by analyzing both cover model and watermarked model. Another simple way to find the tampering is by means of correlation between suspicious and watermarked model. [14]

$$Correlation = \sum_{i=0}^{n}(Vi * Vi^{'})/(|\ Vi\ |*|\ Vi'\ |) \qquad (12)$$

$$\text{Correlation Factor} = \frac{\text{w} + \text{w}'*\text{Correlation}}{\text{W}} \qquad (13)$$

Where Vi and Vi', are the vertex in attacked and watermark model. w and w' are no of vertices not modified and no of vertices modified. We total number of vertices in the watermark model.

If the Correlation between watermark model and attacked model is 100 signifies that model has not been tampered otherwise compare model is to find the resign of tamper.

Correlation is also 100 for affine transformation as objects are normalized in preprocessing step. The embedding of watermark is secured against translation, rotation uniform scaling and other affine transformation. While considering 3D graphical objects, it is common to have some translational, rotational uniform scaling transformations on it. Any attacker may perform such transformations for tampering watermarked 3D object, resulting in the de-watermarked object, different from the original object. The algorithm suggested need no to register against uniform scaling, as any such change is adjusted in the watermark embedding and detection process itself. The watermark information embedded in proposed method is invariant to translation, rotation and uniform scaling because the ratio between the distances from the mesh centroid to each vertex remains the same after the model is translated, rotated or uniformly scaled [12][13].

5.1 Scaling, Translation and Rotation

Let initial co-ordinates of a point are (x, y, z).

So $Vn = \sqrt{(Xi - Xcm)^2 + (Yi - Ycm)^2 + (Zi - Zcm)^2}$

After embedding the watermark, it becomes (Vn')

$$Vn' = Vn + \alpha \qquad (14)$$

After scaling, the watermarked vertex norm becomes (Vn'*t)

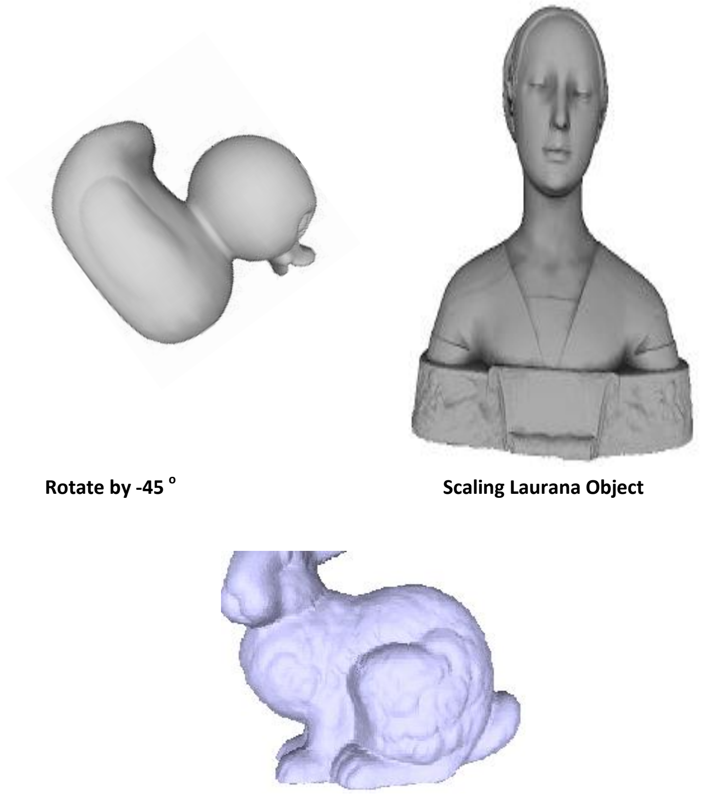
So $$Vn'' = (Vn + \alpha)*\text{t} \qquad (15)$$

After de-watermarking the corresponding obtained coordinate will be reflected in constant ratio which is computable. Thus the watermark is not degraded by uniform scaling.

In the preprocessing step Objects are normalized and their center of mass is shifted to origin. During the transformation of the object the normal distance of the vertices from new center of mass will be same. This preserves translation and rotation attack on the model.

5.2 Cropping

Cropping is the removal of any part of a model. The amount of watermark destroyed depends on the extent of cropping. Since watermark insertion is uniformly repeated throughout the model, the remaining part of model (after cropping) also contain the watermark. Applying the watermark extraction process model can be authenticated.



Rotate by -45 ° **Scaling Laurana Object**

Cropping Bunny Object

Figure 5 Showing various attack on 3D object

8.PROPERTIES OF PROPOSED ALGORITHM

The characteristics of the proposed watermarking algorithm are*:*

1. It is the simplest watermarking algorithm for 3D object but because of the non-blind nature of algorithm it expansive in term of time.
2. Embedded watermark is invariant to translation, rotation, uniform scaling and operations like re-meshing, mesh smoothing cut operations and reordering of the points.

3. Any tampering with the watermark can be detected by comparing data bits of groups extracted from both watermarked and cover object.
4. The strength of the watermark can be adjusted by varying the value and weight of the watermark used.
5. The watermark is inserted such that quality of cover object remains at its acceptable level.
6. The integrity of watermark is very high due to the use of SHA hash function.
7. Reduces payload in watermarking i.e all the vertices are not watermarked.

9.CONCLUSION

In this paper, we have proposed a Non-blind watermarking of 3D mesh models for authentication purpose. The watermarking process is conducted in spatial domain and applies to all the mesh models without any restriction. The experimental results have demonstrated that the proposed method is able to adaptively embed a considerable amount of information into the mesh model. The embedded watermark can be extracted from the watermarked mesh model with prior knowledge of cover model, watermark and cryptographic hash function. In our method, the distortion introduced by the encoding process is quite small and can be adjusted by assigned the parameter *N* a proper value, providing a trade-off between imperceptibility and the precision of 3D data. Compared with previous works, the embedded watermark by our approach is invariant to translation, rotation and uniformly scaling, but sensitive to other operations. Furthermore, the proposed method can also be enhanced to detect those operations besides other processing that might have been applied to the watermarked mesh. Therefore, unauthorized modifications on the mesh model can be detected and classified. Proposed watermarking scheme provide double security by introducing cryptographic hash function. This scheme also reduces data payload. Being a Non-blind watermarking algorithm is expensive in terms of time.

10.FUTURE SCOPE

The difficulty with this algorithm is amount of data inserted .Some time inserted data increases hausdroff distance ,PSNR which results distortion in shape of the object.

11.ACKNOWLEDGEMENT

The authors would like to thank University of Stanfort California and Open-source Meshlab sample for providing 3-D model for experiments.

12.REFERENCES

[1].Chang-Min Chou , Din-Chang Teeng " A public fragile watermarking scheme for 3-D model authentication " ELSEVIER , Computer-Aided Design 38(2006) 1154-1165.

[2].Ohbuchi R, Hiroshi Masuda, Masakionom " Watermarking

Three-Dimensional Polygonal Models Through Geometric and opological Modifications" IEEE J Sel Areas Common 1998;16:551-60.

[3].Ohbuchi R, Hiroshi Masuda, MasakiAono".Watermarking Three-Dimensional Polygonal Models" ACM Multimedia 1997-0-89791- 991-2/97/11.

[4] Mao X, Shiba M and Imamiya A" Watermarking 3D geometric models through triangle subdivision "Proceedings of the SPIE, Security and Watermarking of Multimedia Contents III (ed.Wong PW and Delp EJ), **4314**, 253–260.

[5]. Wagner et al. "Robust watermarking of polygonal meshes ". *Geometric Modeling and Processing*, 2000 Hong Kong.

[6]. Yin K, Pan Z, Shi J and Zhang "Robust mesh watermarking based on multiresolution processing." *Computers & Graphics D2001* **25**, 409–420.

[7].Jeonghee J, Lee SK and Ho YS "A three-dimensional watermarking algorithm using the DCT transform of triangle strips" Digital Watermarking Second International Workshop, IWDW,Berlin. 2003.

[8]. Mitrea M, Zaharia T and Preteux F 2004 Spread spectrum robust watermarking for NURBS surfaces.WSEAS Transactions on Communications **3**(2), 734–740.

[9].Paun E , Hoppe H, Finkestein A " Tobust mesh Watermarking" In ACM siggraph proc 1999.

[10]. Hoppe H " Progressive mesh" In ACM siggraph proc 1996

[11] Yeo BL , Yeung MM " Watermarking 3D object for verification" IEEE Computer Graph Appl 1999;19:36-45

[12] Besl P. and McKay N. (1992) "A method for registration of 3D shapes" *IEEE Trans. on Pattern Analysis and Machine Intelligence*, Vol.18 (14), pp. 239–128.

[13] Chen Y. and Medioni G. (1992) "Object modelling by registration of multiple range images" *Image and Vision Computing*, April, Vol.10(3), pp. 145–155.

[14]. M. Barni, F. Bartolini, V. Cappellini, M. Corsini, and A. Garzelli : "Digital watermarking of 3D meshes," *SPIE proceedings series, SPIE,* Bellingham WA, 2004 [15]T.O.Wells, "Electronic and digital signatures: in search of a standard," IT Professional, Vol.2, Issue 3, pp.24-30, 2000.

[15]. Chou CM , Tseng DC "A Public Fragile Watermarking Scheme for 3D model authentication" Computer-Aided Design 2006;38(11):1154-65

[16]Wei-Bo Wang et al "A numerically stable fragile watermarking scheme for authenticating 3D model" ELSEVIER , Computer-Aided Design 40(2008) 634-645

[17] W. Diffie and M. E. Hellman, "Privacy and authentication:An introduction to cryptography," Proceedings of the IEEE,Vol.67, Issue 3, pp. 397-427, 1979.

[18].W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans. Information Theory, Vol.22, Issue 6, pp.644-654, 1976.

[19].L. Xie and G. R. Arce, "A class of authentication digital watermarks for secure multimedia communication," IEEE Trans. Image Processing, Vol.10, No.11, pp.1754-1764, 2001.