A Novel Approach of 3D Object Watermarking Algorithm using Vertex Normal

Law Kumar Singh
Dept. of CS&E
IET Alwar,Rajsthan (India)

Deepak Chaudhry
Dept. of CS&E
IET Alwar,Rajsthan (India)

Gopalji Varshneya
Dept. of IT
HCST,Mathura (india)

ABSTRACT
The concept of 3D Watermarking algorithm which is non blind and must be robust against different attack is the novel area of research. There are huge requirement of developing a robust and effective watermarking strategies to protect the illegal distribution of proprietary 3D objects. In the proposed algorithm which alter the size of vertex normal according to the digest of watermark bit to be embedded in repeated pattern. In a non-blind watermark detection scheme, this can identify the watermark in referring to the cover mesh model. The proposed technique is evaluated for robustness, experimentally by simulating attacks such as introducing noise, smoothing, cropping.

Keywords
Three dimensional polygon model; Watermarking; Robustness, on blindness watermarking;

1. INTRODUCTION
The watermarking of 3D objects is a new frontier of digital watermarking concerning the embedding of information into 3D objects in an imperceptible way. The scope of interest on 3D watermarking technology is constantly growing in the last few years due to the large applications of 3D models in multimedia technology. There are number of applications where geometrical data are widely used like in mechanical engineering for virtual view and simulation, in cultural heritage to viewing the virtual museums, for movies and video in entertainment industries, the reproduction of archeological sites and in internet to managing virtual world applications and so on. The blow up of this new multimedia data has been supported both by the tremendous graphics power contained by the modern graphics devices and by the effort done to develop efficient technique to build, edit and compress 3D objects. Now this trend has accelerated the digital watermarking technology and the number of works related to 3D watermarking [1].

1.1 Watermarking Properties
There are several properties of digital watermarking. The overall properties of a specific watermarking system determine the context for which a certain algorithm is suitable or not. Properties such as public and private watermark depend on the information carried by the watermark. Inheritability and quasi-invariability properties depend on the application of watermarking as IPR protection. Some properties of watermark depend on the capability to manage multiple watermarks in the same asset.

1.1.1 Readable vs. Detectable
A watermarking system can be either able to read the embedded or only verifies the presence of embedded information. The former case is referred as readable watermarking system and the recovery of the watermark is known as watermark decoding process. In the later case, the recovery process is indicated with watermark detection. The detectable watermarking is also known as 1-bit watermarking as the detector provides only a yes-no answer

1.1.2 Blind vs. Non-blind
Blind watermarking algorithms are able to extract the watermark information without the original data. Blindness is an important property of a watermarking algorithm. A non-blind watermarking system needs to store the original 3D object before the watermarking process, in order to make the recovery of the watermark possible on the other hand blind techniques do not have this necessity that make them more useful for the real applications.

1.1.3 Public vs. Private
A watermark is said to be private if only authorized users can recover it. If assign a different secret key to each user that is called a private, whose knowledge is necessary to extract the watermark from the watermarked asset. This can be accomplished by an appropriate definition of the embedding and detection function public watermark carries public information that anyone can extract to know something about the watermarked digital content. Private watermarking requires being more robust than public watermarking for two reasons. The first one relies on the Kerkhoff''s principle that security must not be based on algorithm ignorance. So if the watermark information can be easily extracted, it is easier for attacker to remove the watermark. Another reason is that there are fewer motivations to eliminate public information from a digital content.

1.1.4 Multiple Embedding
Generally, it is required to insert multiple watermarks inside the host asset. One example could be a copyright protection scheme in which two watermarks co-exist: one identifying the author of the work and another one indicating the name of the customer. All the watermarks contained in the watermark asset must be able to read by detector. In many cases, it is necessary to allow multiple insertions, in fact, if the insertion of a second watermark destroys the first watermark, any attempt to make such watermark robust fails since the pirates can use the watermarking embedding algorithm itself as an attack.

2. PREVIOUS WORK
Ryutarou Ohbuchi, Hiroshi Masuda, Masaki Aono [2] proposed the techniques for inserting data into three-dimensional (3D) polygonal models of geometry i.e. their vertex topology (connectivity) or both. Three watermark embedding algorithms has been proposed in the paper that are triangle similarity quadruples (TSQ) embedding algorithm, tetrahedral volume ratio (TVR) embedding algorithm and mesh density pattern (MDP) embedding algorithm. These schemes comes under oblivious techniques that can extract the watermark without reference to original mesh model, but this

technique is not more robust against various attacks. In TSQ algorithm, it modifies ratios between the length of triangle edge or basis length and height of the triangle .Other mesh triangles technique is proposed to compute Macro-Embedding Primitives (MEP). Every MEP possesses a quadruple of values (Marker, Subscript, Data1, and Data2). A marker is a particular value that identifies MEPs. The triangle marked M possesses a Marker, S possesses a Subscript and D1 and D2 possesses data values Data1 and Data2. Whereas every MEP is shaped by topology, a set of MEPs are shaped by the quantity of subscript. The TSQ extraction algorithm does not need an escrowed original cover-3D-model for extraction. Though, it needs a pair of values that identifies marker triangles. Watermarks created by the TSQ algorithm are robust to plane to plane transformation of the stego-3D models. The watermarks can be damaged by randomization of coordinates, by geometrical transformation, or by broad topological alteration such as re-meshing. Tetrahedral Volume Ratio (TVR) embedding algorithm uses the ratio of the volumes of a pair of tetrahedrons as an embedding primitive. To embed the watermark, ratios are slightly modified and are invariant to affine transforms. The TVR algorithm does not need a cover-3D-model for extraction. The watermarks that it produces survive affine transformation, but are damaged by topological modifications such as re-meshing, randomization of vertex coordinates. MDP embedding algorithm produces polygonal mesh models. As inputs it takes given curved surface models. As the algorithm tessellates given curved surfaces, it embeds a visible pattern by changing the sizes of triangles in the output mesh. This pattern is only just visible if displayed with smooth shading using proper vertex norms vectors calculated from the original curved surfaces, but it can be visible when displayed by using wire mesh rendering. For every geometrical transformation, this watermarking algorithm is robust. The algorithm is resistant but not immune to polygonal simplification and other topological manipulations. Oliver Benedens [3] presented a watermarking algorithm suitable for embedding private watermarks into three dimensional polygon based models. The information is stored in the geometry of the model by the algorithm modifies the models normal distribution. The watermarks embedded by this algorithm present significant robustness against mesh simplifying techniques. This system uses collections of surfaces as embedding primitives. It proposed modifications in object/model normal distribution to realize independence of one particular mesh representation. The system requires a mesh representation of a 3D model consisting entirely of triangle patches as input. In the algorithm the watermark W, a bit of string is embedded into this mesh by performing certain shifting of vertices. It has arbitrary contents and length. After embedding it introduce specific changes in mesh surface normal distribution. The resultant mesh M once more consists of triangle patches. It must be stressed that the embedding procedure to be described does not change model M regarding the number of vertices and faces, adjacencies, face orientation and topology. Other techniques proposed by Oliver Benedens [4] use the volume of two tetrahedrons as an embedding primitive. The method described can be stacked on a more robust scheme permitting transmission of labeling information to the user or, increasing blind detection abilities of the underlying method. This paper gives two major important significant additions, both driven by real word requirements: the first contribution is that provides the ability to deal with reduce precision of vertex coordinates. The second contribution is that it provides a general technique for reducing the processing requirement, time of watermark (label) extraction and enhancing robustness towards affine

transformation and specially vertex randomization attacks. Oliver Benedens and Christoph Busch [5] introduced a digital watermarking system dedicated for embedding watermarks into 3D polygonal models. The system proposed three watermarking techniques, one named Vertex Flood Algorithm (VFA) suitable for embedding fragile public readable watermarks with large capacity and giving a method for model authentication, second one, realizing affine invariant watermarks, named Affine Invariant Embedding (AIE) and a third one, named Normal Bin Encoding (NBE) algorithm. The watermarks produced by these algorithms are stackable. Oliver Benedens [6] proposed algorithm for geometry based watermarking of 3 D models using embedding private watermarks by altering normal distribution. The central idea is the observation that the operations mentioned may cause large changes in model vertex and face set configuration, adjacencies, and topology. A 3D object can be utilized as a collection of surfaces with arbitrary size and orientation. There exists nearly an infinite quantity of meshes representing or approximating one particular set of surfaces with variable perceived quality. Oliver Benedens [7] proposed two high capacity methods for embedding public watermarks into 3D polygonal model. First is the vertex flood algorithm that modifies vertices, so their distances to the center of mass of a designated start triangle encode the watermark bits. Since the algorithm operates solely on vertices and does not take topological relationships into account, it does not require connectivity of the faces in the input mesh. Second is the triangle flood algorithm which generates a unique traversal path of triangles, starting from a designated start triangle. Due to the two purposes, vertices of triangles along the path are modified: first to encode watermark bits in the height information, second to order the triangles in a specific way, producing a unique traversal path. Thomas Harte et al.[8] proposed a public blind watermarking scheme for 3D graphical object due to their increasing use in medical imaging, virtual reality, animation, multimedia, computer-aided design (CAD) etc. Digital watermarking schemes for 3D graphics are attracting new challenges due to the specific nature of the information present in 3D graphical object. In the watermarking scheme a sequence of bits is inserted in the geometrical configuration of the graphical 3D object by modifying the locations of certain vertices. Wu Hao-Tian et al. [9] proposed a different fragile watermarking technique for 3D meshes. At First, the watermark data is inserted in the mesh geometry by slightly modifying the vertex positions in adaptive manner but the mesh topology remains the same. The watermark extraction process of this algorithm is of a blind category as during extraction some prior information of the original mesh is required. In the proposed algorithm the inserted watermark is invariant to translation, rotation and uniform scaling. Any attack on the watermarked mesh can be detected using a reference data. In the algorithm the watermark strength is made adjustable so that the inserted watermark gets change after a trivial modification in the watermarked model. The result shows that the distortion produced in the original object after the watermarking process is very nominal. Quan Liu et al. [10] proposed a different watermarking method for the 3D mesh models. In the technique, transformation 3D mesh into planar regularly sampling signals is done using geometric signal processing theory and then singular value decomposition (SVD) technique is used to insert the watermark. The watermarking embedding procedures are as: global planar parameterization, planar regular sampling, SVD decomposition, watermark embedding, SVD inverse operation, re-sampling. Finally the original model is recovered by reconstructing the 3D mesh. A

unique feature of this watermarking technique for 3D meshes is that it uses geometrical signal processing to convert 3D mesh signal into planner regularly sampled signal and then a singular value decomposition (SVD) technique is used to insert the watermark. Simulation results show that this algorithm possess good imperceptibility and a high robustness to unauthorized attacks such as mulltiresolution filtering, adding random noise, cropping and dithering, As recent compression techniques allow a very high compression rate of 3D objects, it is necessary that watermark should also support such compression techniques. Florence Denis et al. [11] proposed a robust watermarking technique for compressed 3D polygonal meshes, by introducing the complete algorithm for this purpose. The basic theme of this approach is to subdivision of surfaces by defining a smooth shape from a coarse polyhedron by repetitively and infinitely inserting new vertices and edges as per certain subdivision rules. Jae-Won Cho et al. [12] proposed two oblivious watermarking schemes for 3D polygonal mesh models, which alter the distribution of vertex norms according to the watermark bit to be embedded. One scheme is to shift the average value of the distribution and another is to modify its variance. Histogram mapping functions are utilized to modify the distribution. These mapping functions are used to decrease the visibility of watermark as far as possible. Due to the statistical characteristics of vertex norms are invariant to the distortion less attacks, the introduced scheme are robust towards such attacks. In addition, these schemes use an oblivious watermark detection method, which can detect the watermark without any reference to the cover mesh model. Simulation results showed that the proposed schemes are remarkably robust towards distortion less attacks. In addition to this, they are highly robust towards various distortive attacks.

3. PROPOSEDAPPROACH

3.1 Watermarking Approch

In the proposed technique watermark information is embedded into three-dimensional (3D) polygonal models of geometry by using vertex normal, generated by point cloud information of object. Hash functions which are used in algorithm, ensure the integrity of the object as well as the watermark.

The following steps are performed during the watermarking process.

1. Volume is computed as absolute pixel distance from origin.

$$V = \sum dis\ i$$

$$dis\ i = \left(Xi^2 + Yi^2 + Zi^2\right)^{0.5}$$

2. Each Cartesian coordinates of a vertex $vi = \left(xi,\ yi,\ zi\right)$ on the cover mesh model are converted into spherical coordinates

$$ci = \left(\rho i,\ \theta i,\ \Phi i\right).$$

By using formula

$$x_g = \left(\sum_{i=1}^{i=n} x\right)/n\ ; \quad Y_g = \left(\sum_{i=1}^{i=n} y\right)/n; \quad Z_g = \left(\sum_{i=1}^{i=n} z\right)/n;$$

$$\rho i = \sqrt{\left(\left(x_i - x_g\right)^2 + \left(y_i - y_g\right)^2 + \left(z_i - z_g\right)^2\right)}$$

Where i is the number of the vertex $(x_i,\ y_i,\ z_i)$ and at $i = g$ there is center of gravity of the mesh model, and ρi is the ith vertex normal. The vertex norm represents the distance between each vertex to the center of gravity.

3. Find m such that $m = n/128$. Where n is the total number of vertices.

The volume of original object and watermarked object is used to authenticate the watermarked object. Any tampering would result in change of the pixel values hence altering the volume.

4. Divide W in m small patches if $W < m$ make $W = m$.

5. A cryptographic hash function *H is* applied to compute the hash

$$H\ (m,\ G_m)\ = \left(p_1,\ p_2,\ --,\ p_{l28}\right).$$

Where Gm denotes the sum of vertex normal in one group and *pi* denotes the output of the hash function in bits, and L is its length. MD5 will be used as a hash function, and hence L will be 128 for implementation if $L < 128$ then make it 128 by adding 1 as binary bit at remaining places.

Hence, let *Pi be* a stream of 128 bits for Gi.

$$P_i = P_{i,1},\ P_{i,2},\ --P_{i,128}$$

6. Combine *P* with the corresponding watermark binary block *W,* using the exclusive OR operation to obtain the data block D.

7. Embed the each bit of D into the ρi of Gm in sequence by increasing ρi by unit 1 if bit of D is 1 and no change in ρi if bit of D is 0.

8. A mesh model of object consisting of vertices represented in spherical coordinate is now converted in Cartesian coordinates.

3.2 Watermarking Extraction Approach

The following steps are performed during de-watermarking process (A)Steps performed on watermarked object during de-watermarking

1. For each vi Cartesian coordinates of a vertex vi= $(x_i,\ y_i,\ z_i)$ on the cover mesh model are converted into spherical coordinates $ci = \left(\rho i,\ \theta i,\ \Phi i\right)$, by using formula

$$\rho i = \sqrt{\left(\left(x_i - x_g\right)^2 + \left(y_i - y_g\right)^2 + \left(z_i - z_g\right)^2\right)}$$

Where i is the number of the vertex $(x_i,\ y_i,\ z_i)$ and at i=g there is center of gravity of the mesh model, and ρi is the ith vertex normal. The vertex norm represents the distance between each vertex and the center of gravity.

2. Find m such that $m = n/128$. Where n is the total no of vertices.

3. Follow the steps1, 2 and 3 for original object and find group of vertex norm Co for original object.

4. Compare for changes and extract the 128 bit from each group to find D.

(B) Steps performed on original object during de-watermarking process

5. Divide Watermark W in m small patches.

6. A cryptographic hash function *H is* applied to compute the hash

$$H\ (m,\ G_m)\ = \left(p_1,\ p_2,\ --,\ p_{l28}\right)$$

Where Gm denotes the sum of vertex normal in one group and *pi* denotes the output of the hash function in bits, and L is its length. MD5 will be used as a hash function, and hence L will be 128 for implementation if L<128 then make it 128 by adding 1 as binary bit at remaining places.

Hence, let Pi be a stream of 128 bits for Gi.

$$P_i = P_{i,1},\ P_{i,2},\ --P_{i,128},$$

7. Combine *P* with the corresponding watermark binary block *W,* using the exclusive OR operation to obtain the data block D_o.

8. Compare D_o of original object computed from step 7 with D of step 4 to identify the watermark embedded in 3D object by finding statistical correlation.

4. Experimental Results

This section present experiment which evaluates Visual quality of embedded watermark and robustness of watermark. Robustness of the watermark object can be measured by correlating some properties of original object and watermarked object. Robustness is also evaluated under various attack operations and the simulation results shows that proposed algorithm will able to detect up to 99% of watermark data after applying different attack operations on watermarked objects.

4.1 Simulations without attack

Baseline simulations are done in absence of any external attack on the watermarked object. Fig (1) shows 3D face Watermarked object which performed on different key value. Table (1) show the different parameter which is calculated after simulation. The centre of gravity allows robustness against translation of watermarked object and volume provides the measure of robustness against various transformations done on the watermarked object. In the proposed algorithm both of these parameters depend upon the additive unit used in the algorithm, which is defined as:

$$\text{Additive unit } = \left(Xg + Yg + Zg\right)/\text{key value}$$

It is obvious from above expression that the additive unit is inversely related to the key value. Higher is the key value lower is the additive unit. Simulation results demonstrate that at very high key values, the robustness of the watermarking algorithm becomes very low and it is found that a key value equal to 3000 (the key value is inversely prepositional to the additive quantity) is most suitable for watermarking with respect to robustness and visual quality.

4.2 Attack simulation

It is difficult to imagine all possible attacks on a polygonal mesh, some of these are:

• Translation/Rotation/Uniform Scaling. These geometric transformations are very used in computer graphics to position a 3D model inside a scene.

• Noise. For noise attack we intend the random perturbation of mesh vertices.

• Polygonal simplification. This operation is often used to transmit a low-level version of the model or to optimize a model eliminating most of the non-salient faces.

• Cropping. An attacker can discard the part of the model that he does not need.

• Remeshing. This operation can be described as a geometric resampling of the shape of the mesh followed by a re-definition of the connections between vertices. Many of the attacks are simulated on the Watermarked 3D objects. Face.obj having 10976 vertices and 3855 faces. Fig 2 shows the various attacks performed on the watermarked 3D models. Robustness is also evaluated under various attack operations and Table 2 shows the simulation results shows that proposed algorithm will able to detect up to 99% of watermark data after applying different attack operations on watermarked objects. In Laplacian Smooth, Color Noise, Cropping and

Two Step Smooth Attack, the volume of watermark object is changed by 188.85, 21.36, 1.36 and 19.62 respectively still the dewater-marking algorithm identified watermark in the object. So this can conclude that proposed algorithm shows good robustness against those attacks. To evaluate the robustness, perceptual quality the simulation is performed on the 3D object models.
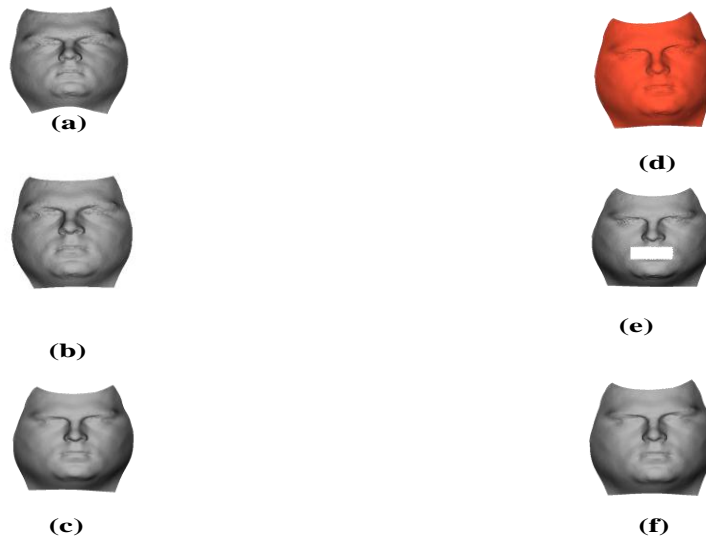

(a)

(b)

(c)

Fig 1: Face watermarked object with different Keys (a) Watermarked3D face with key=3000, (b) Watermarked 3D face Key=500 and (c) Watermarked 3D Face with key=30

Table 1. Simulation result of 3D face object on different Key

Key	Centre of body of original object (x,y,z)	Centre of Body of Watermarked object (x,y,z)	Volume of original object	Volume of watermarked object	Time for water –marking msec.
30	14.939751855394235 -72.36885224272672 0.9258057290114582	14.922471227841005 -72.46742317148875 1.0539214553601068	1109586.180930741	1123430.4417944427	33750
500	14.939751855394235 -72.36885224272672 0.9258057290114582	14.93968964513502 -72.36920709806996 0.9262669456263137	1109586.180930741	1109635.3073995812	36453
3000	14.939751855394235 -72.36885224272672 0.9258057290114582	14.93975012733148 -72.36886209981928 0.9258185405841038	1109586.180930741	1109587.545483716	36250

Fig 2: Watermarked 3D Face after different Attack(a)Original 3D face ,(b) Watermarked 3D Face, (c) Laplacian Smooth Attack (d)Color Noise Attack,(e) Cropping Attack and (e)Two Step Smooth Attack

Table 2. Simulation result on 3D face object after applying attacks

Attack	Centre of Body of Original object (x,y,z)	Centre of Body of Watermarked object (x,y,z)	Volume of Original Object	Volume of Watermarked Object after attack	Time for Water-marking msec.	Time for Dewater marking msec.
Laplacian Smooth Attack	14.939751855394235 -72.36885224272672 0.9258057290114582	14.9401157592201863 -72.36113240460993 0.9204359744897869	1109586.180930741	1109397.3306475144	447782	25407
Color Noise Attack	14.939751855394235 -72.36885224272672 0.9258057290114582	14.939750132744198 -72.36886209839692 0.9258185351676389	1109586.180930741	1109567.545525655	447782	27125
Cropping Attack	14.939751855394235 -72.36885224272672 0.9258057290114582	14.939750132744198 -72.36886209839692 0.9258185351676389	1109586.180930741	1109587.545525655	447782	25844
Two Step Smooth Attack	14.939751855394235 -72.36885224272672 0.9258057290114582	14.939848047740524 -72.37760459684749 0.9193817201166393	1109586.180930741	1109605.8022706895	447782	25594

5. CONCLUSION

A new robust watermarking scheme has been proposed for 3D polygonal models. The watermark is embedded into vertex normal calculated by a point cloud model of the 3D object. Reason for choosing point cloud model is that it provides more robustness against reordering of file compared to mesh models. A point cloud model can be generated from a mesh model and vice versa. The .obj files contain both the point cloud information and the corresponding facet information, thus allowing the 3D model to be used by algorithms using either of the information models. The proposed algorithm introduces a very minute distortion, depends upon the user select key value so that user can identify the key value against robustness and visual quility. The algorithm provides a great flexibility in achieving desired results in the watermarked object considering the trade off between originality and robustness. The visual quality can be varied for the same watermark after varying the size of additive unit. Also different visibility is achieved by varying the weight of the watermark keeping the same length. The proposed algorithm is invariant to translation, rotation, uniform scaling and reordering point information of watermarked object

6. ACKNOWLEDMENT

7. REFERENCES

[1] Boon-Lock, Y. and Minerva, Y.M., 1999. Watermarking 3D objects for verification. *IEEE Computer Graphics and Applications Magazine,* January/February, 36-45.

[2] Ohbuchi, R., Masuda, H., Aono, M. May 1998.Watermarking three-dimensional polygonal models through geometric and topological modifications. *IEEE Journal on Selected Areas in Communications*, Vol. 16, no 4, 551–559

[3] Oliver, B. 1999.Watermarking of 3D polygon based models with robustness against mesh simplification. *in Proceedings of SPIE: Security and Watermarking of Multimedia Contents*, vol. 3657, 329–340.

[4] Oliver, B. 2000. Affine invariant watermarks for 3D polygonal and NURBS based models. *in proceedings of the Third International Workshop on Information Security ISW2000*, 15 – 29.

[5] Oliver, B. 1999, Geometry based watermarking of 3D models. *IEEE Magazine,* Jan/Feb, 46-55.

[6] Oliver, B. and Christoph B. 2000 Towards blind detection of robust watermarks in polygonal models. *in proceedings Euro graphics 2000*, C199-C208.

[7] Oliver, B. 1999, Two high capacity methods for embedding public watermarks into 3D polygonal models. *in Proceedings of the Multimedia and Security-Workshop at ACM Multimedia 99, Orlando, Florida*, 95–99.

[8] Harte T. and Bors A.G. 2002. Watermarking graphical objects. Department of Computer Science, University of York, York YO10 5DD, U.K.

[9] Hao-Tian W. and Yiu-Ming C. August 2005. A Fragile watermarking scheme for 3D meshes. *in proceeding of MM-SEC'05*, 1-2, ACM, 117-123.

[10] Liu Q. and Zhang X. 2006, A SVD-based digital watermarking algorithm for 3D mesh models. *in proceeding of the 8th International Conference on Signal Processing ACM. Vol. 4,* 16-19.

[11] Denis F. et al. 2005. Digital watermarking of compressed 3D meshes. Dans International Conference on Machine Intelligence (ACIDCA-ICMI), Tozeur, Tunisia.

[12] Won C. J. et al. Jan 2007. An oblivious watermarking for 3-D polygonal meshes using distribution of vertex norms. *IEEE Transactions on Signal Processing*, Vol. 55(1), 142-155.