Arab Journal of Nuclear Sciences and Applications

Non-Blind Robust 3D Object Watermarking Scheme

Nour N. Ashoub[1], Ahmed A. Emran[2], Mohamed H. Saad[1], Ahmed Y. Morsy[2], Hassan. I. Saleh[1]*

[1] *Radiation Engineering Department , Egyptian Atomic Energy Authority Cairo, Egypt*

[2] *Communication and Electronics Engineering , Al-Azhar university Cairo , Egypt*

Robust digital watermarking is an evolving research area that has received a large amount of attention and became a practical solution to copyright protection. This paper proposes a robust and imperceptible non-blind watermarking method for high rate embedding into 3D polygonal meshes. Our approach consists of vertices selection, embedding and extracting steps. First, the vertices are selected for embedding if they are greater than defined threshold, and then the watermark bits are embedded directly into each vertex in spatial domain. The main attractive features of this approach are flexibility in data embedding technique and fast computation compared to other recent techniques. The experimental results showed that the proposed algorithm provides high robustness against the most common attacks. The applied attacks include connectivity attacks such as mesh smoothing, and mesh cropping and the geometric attacks such as rotations, uniform scaling and their combinations.

Introduction

The fast developments of multimedia and internet enable us to transfer, store and process digital content with less time, better efficiency and lower complexities. The convenience of internet plays a very vital role in illegal and unauthorized copying of digital content. Therefore, the risk of violating owner right and obstructing authenticity of a digital content has increased. Digital watermarking is an effective method to protect digital products. Recently, watermarking techniques have been extended in three dimensions and have involved more attentions. There is urgent need to deal with 3D images and objects, which have many applications such as in medical, geology and industry imaging. The conventional 1D/2D digital watermarking has been developed and their applications appeared in the commercial market.

Conversely, 3D watermarking is still new and there is no effective solution especially for blind and robust 3D watermarking methods. The achievements in 3D watermarking are challenging due to the complexity of representations and the diversity of operations for 3D models [1]. From the view of the embedding domain, the 3D watermarking is classified into spatial domain and transformed domain. The transformed domain methods can be further divide into spectral methods and multi-resolution methods. Watermark can also be classified into blind and non-blind watermark according to whether the original model is required during the extracting process or not. Watermarking algorithms are characterized by the following two important properties; "Imperceptibility" and "Robustness".

The imperceptibility means that the watermarked model should look similar to the original one, while the robustness measures the persistence of the watermark scheme against various types of attacks. On the other hand, the two properties oppose each other because robustness is achieved at the cost of imperceptibility. Therefore, the balance between imperceptibility and robustness is needed while designing a watermarking method in accordance to the practical applications. According to the aimed application, the distinguish is made between the robust watermarking (used for the copyright protection) and the fragile watermarking (used for integrity of content) [2].

Ohbuchi presented some watermarking algorithms for the polygonal mesh [3] and NURBS [4] in the area of ownership proof. Benedens proposed several robust watermarking algorithms that are robust to mesh simplification and affine transform [5,6] and other watermarking technique with high capacity [7].

Wang, et al [8] proposed a robust and blind watermarking scheme for 3D models. His scheme assumed that a good mesh watermarking primitive has to be intrinsically linked to the 3D shape represented by the mesh, the local moments are selected as a promisingly effective primitive. This algorithm ensures that the patches rapidly reach their wanted moment values while not introducing noticeable distortions.

Cho, et al [9] presented a statistical approach that modifies the distribution of vertex norms to hide watermark information into host 3-D meshes. The norms distribution is split into distinct sets called bins, and one bit of the watermark is embedded in each bin. This approach is not applicable to small models, and models with flat regions. It is also very vulnerable to cropping attacks.

Hu, et al. [10] extends Cho's work by minimizing the mean square error between the original mesh and the watermarked mesh under several constraints. The assumption is made that the distortion is the same, but the robustness is improved.

Motwani et al. [10] developed a method for robust non-blind watermarking of 3D models in spatial domain. To select the vertices for embedding, first;

the average normal of all faces formed by a certain vertex are calculated, then the average of angles between each pair of normal is obtained, this process is repeated for all vertices.

Feng, et al [11] presented a 3D model-watermarking scheme based on features recognition. This method presents a good robustness against common attacks, but does not present perceptibility measures. Generally, non-blind watermarking algorithm has better robustness than blind one. However, non-blind watermark requires complicated pre-processing, such as re-sampling and registration, which is the key to extract the watermark successfully.

A non-blind watermarking scheme, which is selected in this paper, needs the original 3D model to extract the embedded watermarks and the original watermarks to measure the robustness. To achieve high robustness with lower computational complexity, we propose a non-blind watermarking algorithm that uses spatial domain for the embedding process. The proposed scheme uses the vertices of the 3D mesh model for their robustness against some attacks such as; translation, rotation, uniform scaling, adding noise, re-meshing, and mesh simplification. These feature points represent the characteristics of 3D models where watermarks are embedded; also the detection used a non-blind method as it is more robust compared to blind methods.

The rest of the paper is structured as follows: section 2 describes the proposed watermarking method and the steps of embedding and extracting the watermark. In section 3 evaluates the robustness of proposed method. The experimental results are provided in section 4 and a conclusion of the paper is presented in section 5.

The proposed watermarking method
This section describes the proposed watermarking scheme for 3D mesh models. The watermarking scheme was designed mainly to reach better robustness of the watermark against various attacks, while enhancing the computation performance. The watermark embedding is carried out in spatial domain, which adds a watermark directly in the original cover content. In general, spatial-domain-based watermarking is fast and less complicated.

The Embedding watermarking

The block diagram of the embedding procedure in the proposed scheme is shown in figure (1.a), the vertices detection is used for original 3D object in order to select the embedding locations by applying the threshold factor L. Then, the values of the selected vertices are modulated by the watermark bits values to create the watermarked 3D object. The values of watermark stream bits are detected row by row. Embedding of '0' varies the value of the original vertex to be scaled down by a factor of (1- *K)*. Similarly, an embedding of watermark bit with value '1' changes the value of the original vertex to be scaled up by a factor of (1+ *K)*. The embedding (modulation) equation is as follows:

$$MWxyz = \begin{cases} Mxyz(1+k) & if\ w=1 \\ Mxyz(1-k) & if\ w=0 \end{cases} \quad \textbf{(1)}$$

Where $\mathbf{Mw_{xyz}}$ the watermarked 3D model vertex values for Cartesian coordinates, $\mathbf{M_{xyz}}$ the original 3D model vertex values for Cartesian coordinates, **K** is the embedding strength (**0≤ K≤ 0.1),** and **w** is the watermark bit value.

For redundancy, each of the three Cartesian coordinates values of the vertex (x, y, z) is modified by the same watermark bit value according to equation (1).

The robustness and distortion varies proportional to the increase of the embedding strength (**k**).Also as the pattern of watermark bit (**w**) values change, so does the robustness and distortion.

The Exrtacting Watermarking

The proposed method applies a non-blind watermarking scheme in which, the original model is needed to extract the watermark from the watermarked model. Figure (1.b) shows the extraction watermarking procedure. The demodulation of watermarked vertices is used to recover the watermark bits from the embedded vertices as shown in equation (2):

$$W_{E=} \begin{cases} 0 & if\ Mxyz-Mwxyz \ge 0 \\ 1 & if\ Mxyz-Mw\ xyz <0 \end{cases} \quad (2)$$

where $\mathbf{W_E}$ the extracted watermark bit

The Evaluation of Robustness

The proposed watermarking method was carried out on five 3D models representing computer graphics models used for testing the watermarking

scheme. Figure (3) displays the five models used in this paper, it is a subset of the dataset defined by Wang's benchmark [8]. The models were selected to provide a diversity of mesh shapes; the Bunny model has many rounded faces, where the dragon shape is very complex. While, the Horse and the Venus objects are quite flat. These models have the characteristics shown in table (1).

The watermark embedding process presents certain distortion to the original cover mesh. This distortion can be measured using many evaluation metrics such as the Root Mean Square Error (RMS), Bit Error Rate (BER) and correlation coefficient (r) . This work uses the RMS between two 3D-surfaces; original model and its watermarked model. The RMS is defined in the following equation [9]:

$$\mathbf{d_{RMS}(S\,,s')} = \sqrt{\frac{\mathbf{1}}{|S|}\sum_{\mathbf{p}\in S}\mathbf{d(p,s')^2}} \quad \textbf{(3)}$$

Where **p** is a point on surface **S, s`** is the surface to measure the distance to, |**S**| is the area of **S**, and **d(p, s`)** is the distance between p and S`. The amount of distortion introduced by a watermarking technique is one of the evaluation factors, The RMS measure is not similar, which means that $d_{RMS}(S',S) \ne d_{RMS}(S,S')$ **t**he MRMS can be defined as follows [12, 13]:

$d_{MRMS}(S,S') = \max\{d_{RMS}(S',S), d_{RMS}(S,S')\}$(4) MRMS is more accurate than simple vertex-to-vertex measures. BER is used for measuring the robustness of the watermark after the model being attacked which defined as: **BER = Errors / Total number of bits.**

The Similarity Measure (SM) represents the correctness ratio of the extracted watermark with respect to the original one, which is calculated using the Bit Error Rate (BER) which defined as: **SM=1-BER**.

By using the SM, we measured the robustness of each extracted watermarks as shown in Figure (2). The correlation coefficient measures the similarity between the original and the extracted watermark evaluates the robustness of the proposed scheme and a non-blind 3D mesh watermarking schemes [14, 15]. The correlation coefficient evaluated by the following equation:

$$r = \frac{\sum_{i=1}^{n-1} (w^*_i - \overline{w}^*)(w_i - \overline{w})}{\sqrt{\sum_{i=1}^{n-1} (w^*_i - \overline{w}^*)^2 \sum_{i=1}^{n-1} (w_i - \overline{w})^2}} \quad (5)$$

Where w^* and $\overline{w}$ denote respectively the averages of the extracted watermark bit sequence w^*_i and the inserted watermark bit sequence w_i. The robustness of the method is verified by applying different attacks on the watermarked model. This includes geometrical deformation and connectivity attacks. The geometrical deformation such as rotation, translation and scaling only change the location of the model not the actual contents of the vertices and faces so the watermarked model is robust and invariant to rotation and translation transformation. The connectivity attacks as Smoothing, Cropping and Subdivision attacks. The Laplacian-surface smoothing attack with different iteration degrees is applied on the watermarked models. The cropping with different degrees (10%, 30%, and 50%) which is applied on the watermarked model but it has not fully destroyed the watermark because the watermark is spread uniformly in the original model at insertion process. The subdivision attacks are applied with Midpoint, loops and LS3 surface algorithms and simplification attacks as shown in figure (4).
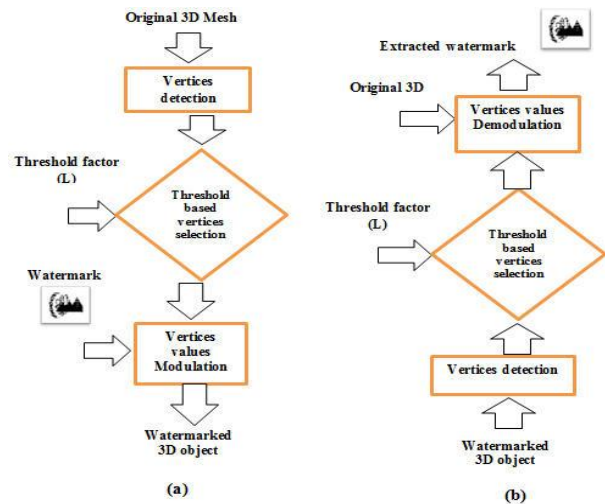

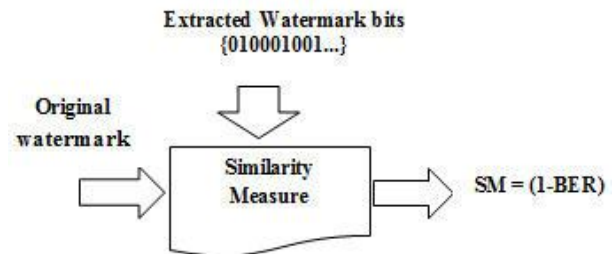**Figure 1: The watermarking processes, (a) embedding process and (b) extraction process.**

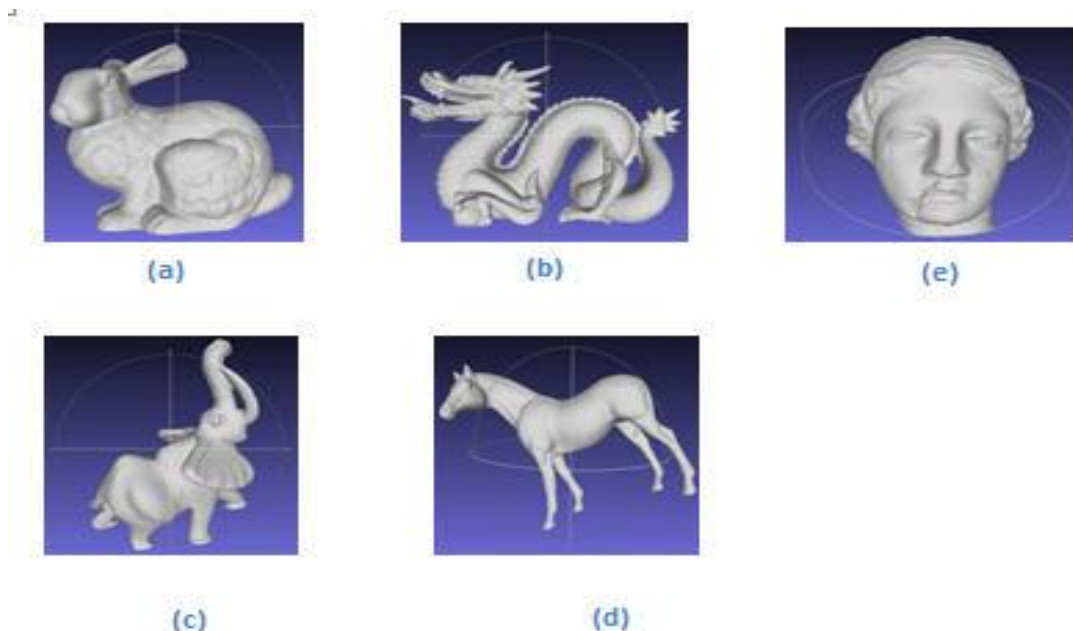**Figure 2: The similarity measurement.**

Figure 3: 3D models used for results evaluation; (a) bunny, (b) Dragon, (c) Elephant, (d) Horse, and (e) Venus.

Table (1) Characteristics of the used 3D models

Object	No. of vertices	No. of faces
Bunny	**34817**	**69630**
Venus	**100759**	**201514**
Horse	**112642**	**225280**
Dragon	**50000**	**100000**
Elephant	**24955**	**49918**

Results and Comparisons

This section demonstrates and evaluates the test results of the proposed watermarking scheme. The obtained results focused on three parameters of the watermarking scheme to test and measure imperceptibility, robustness, and performance. The results of imperceptibility and robustness are measured and evaluated according to the benchmark presented by (Wang, et al) [8].

The computation performance measured and evaluated individually, Its measures the visual distortion introduced by the watermark embedding process to the mesh model, and the error rate in the detected watermark compared to the original watermark. The optimum embedding strength selected by calculating PSNR between the original and extracted

The robustness of the proposed algorithm is measured at optimum embedding strength. The Similarity Measure test the extracted watermark bits showed on figure (6), the results shows the effect of geometry and connectivity attacks on watermark extracted bits. The extracted watermark does not affected by geometric attacks such as laplacian smoothing filter and having at least 70% typical extracted bits on connectivity watermark image at different attacks as shown in figure (5). The results are applied on Dragon model, which shows that the PSNR value is increasing as embedding strength increased for different attacks. The optimum embedding strength results occurs at value of k= 0.01. PSNR is measured at optimum embedding strength as shown in figure (7). The results show that the extracted watermark does not affected by geometric and connectivity attacks. The distortion, which occurred to the original cover mesh by the watermark embedding process clarify by the root mean square RMS and the MRMS. Figure (8) shows that distortion with a different embedding strength degree occurring the minimum distortion on the biggest embedding strength degree.

The baseline evaluation results of the proposed scheme compared to another algorithms [8, 13] on Table (2). The results show that we provide much larger payload and RMS with a high redundancy of watermark embedding on the 3D models.

Also the proposed scheme provided embedding capacity (watermark payload) showed on Table (3) that varies according to the model size reach to 64*64 pixels a several times which gives the ability to hide a sizably large data.

Table (4) shows a comparison between the proposed algorithm and the previous algorithms [8, 9, 13] using Bit Error Rate (BER). The results evaluated at different attacks on Venus model. According to the results, the proposed algorithm is better than the others in geometry attacks (similarity transformation, smoothing with different iterations) and the connectivity attacks except the cropping and simplification.

Table (5) evaluates the robustness of the proposed scheme and some of non-blind 3D mesh watermarking schemes. The proposed method achieves maximum results in resisting smoothing attacks at iteration 5 compared with the pervious methods. Moreover, the results demonstrate that the proposed method is robust against cropping attacks except some of high degree of cropping because of the embedding of watermark was distributed randomly. Hence, when the cropping attack is applied, a part of the extracted watermark is lost within the cropped part of the watermarked object.

Figure 4: Original and watermarked dragon object before and after applying (a) Laplacian smoothing, (b) 10% cropping, (c) 30% cropping, (d) 50% cropping, € subdivision using midpoint scheme, (f) loop's subdivision and (g) simplification attacks.
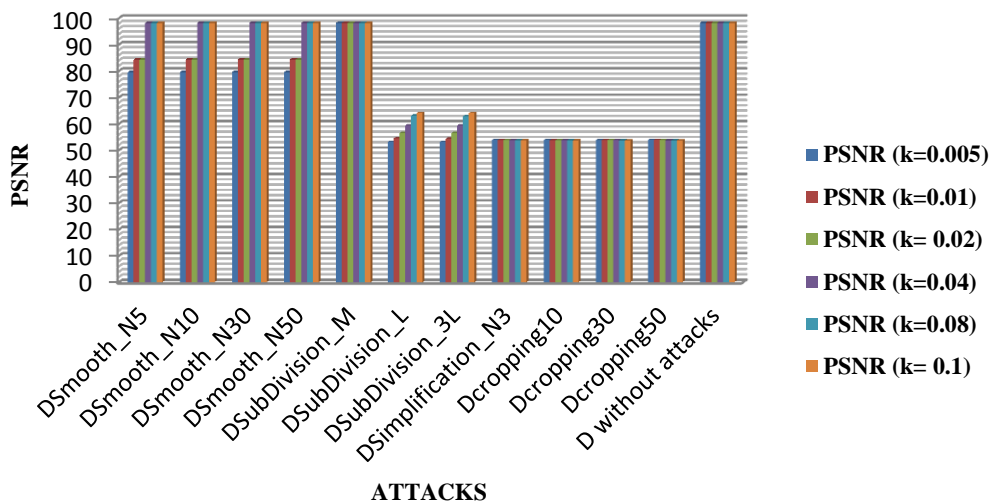

Figure 5: The PSNR of extracted watermark for different embedding strengths with respect to applied different attacks
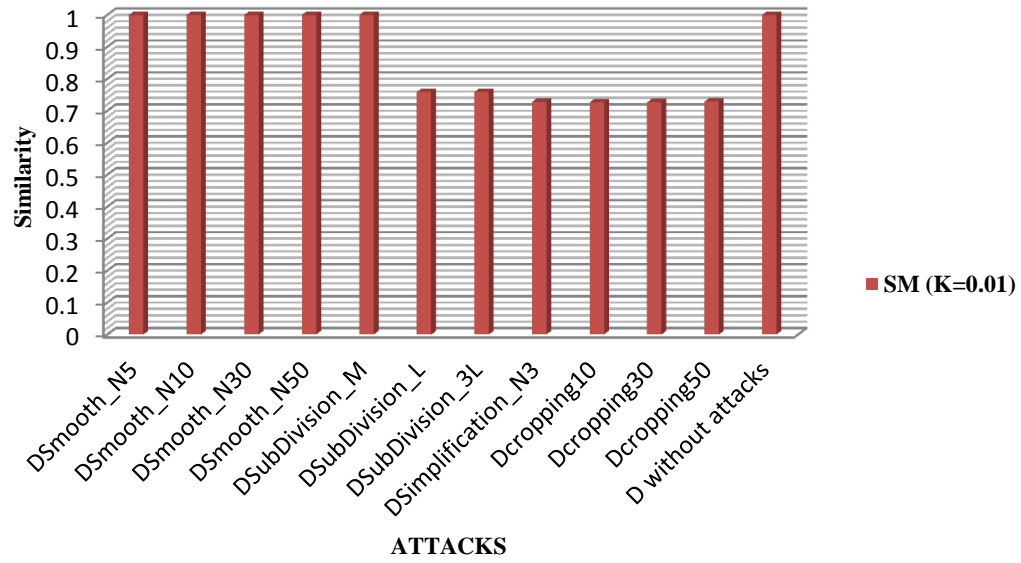
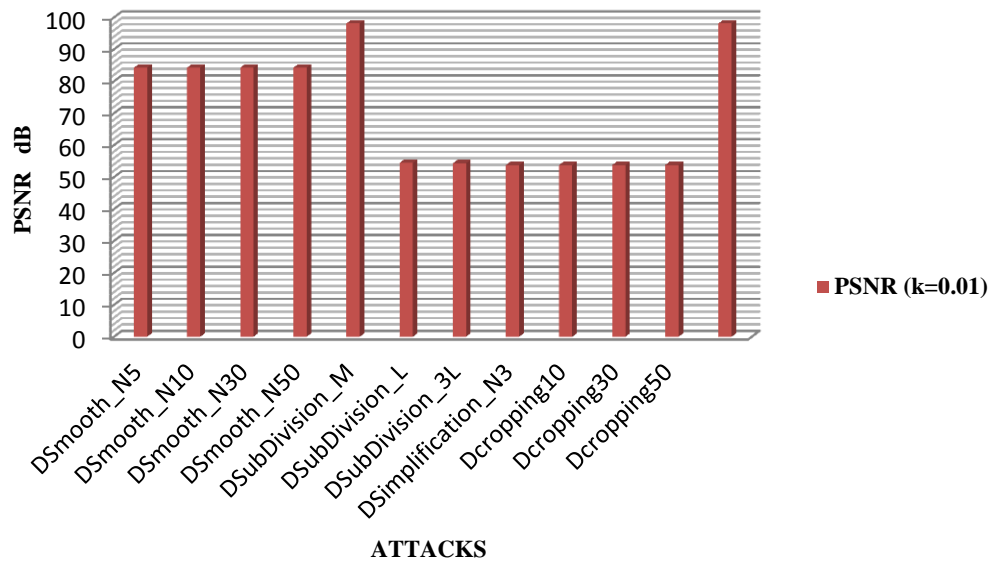**Figure 6: The Similarity Measure and the different attacks on an optimum embedding strength k=0.01**

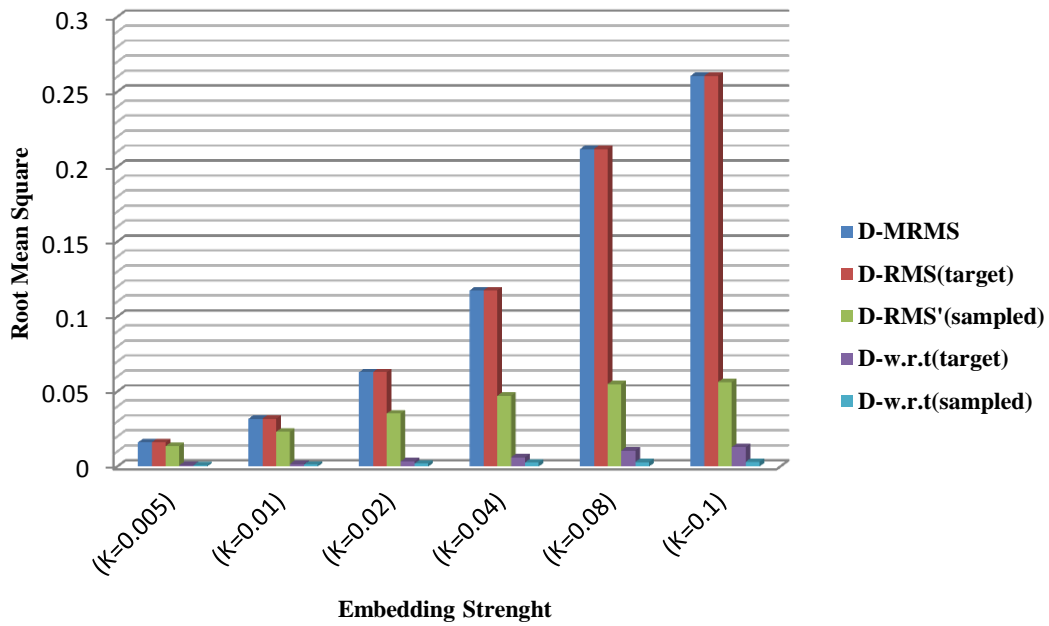**Figure 7: PSNR with different attacks at embedding strength k=0.01**

Figure 8: Root Mean Square and embedding strength for watermarked dragon model

Table 2: Baseline evaluation results

Model	payload				RMS		
	Wang's	Lamia's	Proposed scheme		Wang's	Lamia's	Proposed Scheme
			Watermark size	No. of redundant watermark			
Bunny	67	144	4096	25	0.0017	0.0053	0.000863
Horse	46	64	4096	82	0.0010	0.0014	0.000534
Dragon	49	256	4096	36	0.0018	0.0057	0.000740
Venus	75	256	4096	73	0.0023	0.0027	0.000940
Average values	59.25	180	4096	54	0.0015	0.0041	0.000760

Table 3: Information embedding capacity

Scheme	*Wang's*	Lamia's	*Proposed Scheme*
Payload/RMS	$34.8 * 10^3$	$4.7 * 10^3$	$5.3 * 10^6$

Table 4 : Robustness compression between 4 scheme

Attacks	Chos's BER	Wang's BER	Lamiaa's BER	Proposed Scheme BER
Similarity Transformation	0.0	0.0	0.0	0.0
Smoothing N = 5	0.01	0.0	0.013	0.0004
Smoothing N = 10	0.23	0.01	0.015	0.0004
Smoothing N = 30	0.38	0.07	0.02	0.0004
Smoothing N = 50	0.45	0.14	0.02	0.0004
Geometry attacks average	0.214	0.044	0.014	0.00032
Subdivision Midpoint	0.04	0.0	0.02	0.0
Subdivision Root 3	0.14	0.0	0.04	0.1426
Subdivision Loop	0.16	0.0	0.045	0.1426
Simplification	0.01	0.0	0.02	0.27
Cropping 10%	0.5	0.51	0.012	0.27
Cropping 30%	0.53	0.49	0.014	0.27
Cropping 50%	0.51	0.49	0.013	0.27
Connectivity attacks average	0.27	0.21	0.047	0.19

Table 5: Comparing the robustness performance with literature schemes.

Model	Proposed scheme				Clustering vertices's scheme[16]				Soliman's scheme[15]			
	Smooth (itr.5)	Crop 10%	Crop 50%	Crop 70%	Smooth (itr.5)	Crop 10%	Crop 50%	Crop 70%	Smooth (itr.5)	Crop 10%	Crop 50%	Crop 70%
Bunny	1	0.726	0.724	0.0207	0.940	0.994	0.790	0.789	0.968	0.851	0.660	0.527
Venus	1	0.727	0.726	0.0252	0.947	0.975	0.959	0.613	0.910	0.686	0.016	0.016
Dragon	1	0.723	0.714	0.0102	0.929	0.891	0.806	0.739	0.910	0.700	0.353	0.173

Conclusion

This paper proposed a new non-blind robust three-dimensional watermarking scheme based on spatial domain. The proposed scheme provides high performance. Moreover, the complexity of the proposed scheme is lower than the most common known techniques. The proposed scheme's objectives are to increase the robustness of the watermark against various attacks while maintaining the visual quality of the 3D models, and to enhance the overall performance of the watermarking scheme. The watermarking scheme was tested against several attacks and achieved enhancement in robustness compared to other schemes. Experimental results show that the watermarking scheme is robust against translation, rotation, uniform scaling noise, simplification, cropping, quantization, smoothing, subdivision and their combined attacks. The future work is to propose a method measuring the influences of attacks on 3D model and then continue to improve the robustness of watermarking scheme against various attacks.

References

1- R. Ohbuchi, H. Masuda and M. Aono, "Watermarking Three- Dimensional Polygonal Models Through Geometric and Topological Modifications,"IEEE Journal on Selected Areas in Communications, Vol. 16, Issue 4, pp. 551 -560, May 1998.

2- R. Ohbuchi, H. Masuda and M. Aono, "A Shape-preserving Data Embedding Algorithm for NURBS Curves and Surfaces," IEEE Computer Graphics International Proceedings, pp. 180 -187, 1999.

3- O. Benedens, "Affine Invariant Watermarks for 3D Polygonal and NURBS Based Models," Springer, Information Security, Third International Workshop,ISW 2000, vol. 1975, pp. 15-29, Australia, December 2000.

4- O. Benedens, "Geometry-based Watermarking of 3D Models," IEEE Computer Graphics and Applications, Vol. 19, pp. 46-55, Jan.-Feb 1999

5- O. Benedens, "Two High Capacity Methods for Embedding Public Watermarks into 3D Polygonal Models," Proceedings of the Multimedia and Security-Workshop at ACM Multimedia 99, pp. 95 - 99, Orlando, Florida, 1999.

6- K. Wang, G. Lavoue, F. Denis, and A. Baskurt, 'A Comprehensive Survey on Three- Dimensional Mesh Watermarking', IEEE Transactions on Multimedia, vol. 10, no. 8, pp. 1513–1527, 2008.

7- Zhang Diming, Yao Li "A Non-Blind Watermarking on 3D Model in Spatial Domain "2010 International Conference on Computer Application and System Modeling (ICCASM 2010).

8- K. Wang, G. Lavoué, F. Denis, A. Baskurt, and X. He, 'A Benchmark for 3D Mesh Watermarking', 2010 Shape Modeling International Conference, pp. 231 - 235. 2010.

9- Cho, Jae-Won, Rmy Prost, and Ho-Youl Jung. "An oblivious watermarking for 3-D polygonal meshes using distribution of vertex norms." IEEE Transactions on Signal Processing 55.1 (2007): 142-155.

10- R. Hu, P. Rondao-Alface, and B. Macq, "Constrained optimisation of 3D polygonal mesh watermarking by quadratic programming," in Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on, 2009, pp. 1501-1504.

11- Motwani, Mukesh, et al. "Adaptive fuzzy watermarking for 3D models." Conference on Computational Intelligence and Multimedia Applications, 2007. International Conference on. Vol. 4. IEEE, 2007.

12- Feng, Xiaoqing, Wenyu Zhang, and Yanan Liu. "Double watermarks of 3D mesh model based on feature segmentation and redundancy information." Multimedia tools and applications 68.3 (2014): 497-515.

13- Lamiaa Basyoni "Enhanced Watermarking Scheme for 3D Mesh" ICIT 2015 The 7th International Conference on Information Technology, pp. 612-619, 2015.

14- Lavoué, Guillaume, and MassimilianoCorsini. "A comparison of perceptually-based metrics for objective evaluation of geometry processing." IEEE Transactions on Multimedia 12.7 (2010): 636-649.

15- Soliman, Mona M., Aboul Ella Hassanien, and Hoda M. Onsi. "A Blind Robust 3D-Watermarking Scheme Based on Progressive Mesh and Self Organization Maps." Advances in Security of Information and Communication Networks.Springer, Berlin, Heidelberg, 2013. 131-142.

16- El Zein, Ola M., Lamiaa M. El Bakrawy, and Neveen I. Ghali. "A NON-BLIND ROBUST WATERMARKING APPROACH FOR 3D MESH MODELS." Journal of Theoretical and Applied Information Technology 83.3 (2016): 353.