JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 07, ISSUE 15, 2020

A WATER MARKING SCHEME TO PROTECT 3D MODELS

Meldie Apag and Desiderio Apag III
[1]Dean of College of Computer Studies,
Xavier University – Ateneo de Cagayan
Cagayan de Oro City,Philippines.

[2]Education Supervisor,
Commission on Higher Education, Philippines.

Corresponding Author's Email:[1]mapag@xu.edu.ph

Article History: Received xxxxx; Revised xxxx; Accepted xxxx

ABSTRACT: Three-dimensional (3D) models are used to imitate, represent, and resemble objects in a real world. But with its emergence, comes also issues relating to ownership claiming. There is an obvious need for multimedia data copyright protection and ownership claiming techniques and one seen technique is digital watermarking. Hence, this study demonstrated an invisibly-blind robust semi-public watermarking scheme to protect 3D models from data compression attack. The scheme used the Autodesk's 3DS Max software which generated a 3D polygonal mesh model.The watermarking was made on its mesh vertices where a 3-bit sequence was embedded through its binary file on the chunk of the file containing the vertices list and on its 0 bits. A software was designed for the process of embedding and extraction of the watermark. Data compression, as the form of attack on 3D models, was done in Autodesk's *maxzip* archiving system wherein the file size of a 3D model was narrowed down to a smaller file size for purposes of minimum storage and portability. The software then determined the presence of the watermark after decompression of the attacked watermarked file.Findings show that the watermarking scheme used in this study exhibited an imperceptible, detectable, and compression-resilient watermark for 3D polygonal mesh models.

KEYWORDS:*Digital Watermark, 3D, Data Compression*

1.0 INTRODUCTION

The past 20 years have seen pervasive digitization of multimedia data in the forms of photographs, paintings, speech, music, video and documents [1]. The amount of digital data distributed through international communication networks has also increased rapidly. Original digital products are easily copied, being tampered and transmitted back to the network [2-3]. Thus, there is an obvious need for multimedia data copyright protection and ownership claiming techniques and one seen technique is

ISSN- 2394-5125 VOL 07, ISSUE 15, 2020

digital watermarking.

Digital watermarking employs various techniques for embedding information into digital media such as text, spoken audio, music, images, animation, video or combinations of these formats. The information embedded can be used for media copyright protection, authentication, annotation, access control, data hiding, or for data and media manipulation. A watermark should be imperceptible by human perception or by software detection [4]. It should also be robust to stego media processing and potential attacks [5].

Most researches in watermarking had concentrated on cover media such as audio data, still images, fax data or video [6]. However, due to the nature of the data representing the cover media, these methods cannot be applied to three-dimensional (3D) graphical objects and models [7-8]. A 3D graphical object can be represented in various ways including polygonal meshes. A polygonal mesh or unstructured gridis a collection of vertices, edges and faces that defines the shape of a polyhedral object in 3D computer graphics and solid modeling.

3D models are usually used in entertainment and industry, particularly in human factors and ergonomics, information presentations and communications, display and control designs, human-computer interfaces, automation and human-machine integration, workstation and facility designs, systems / equipment and vehicle designs. These models are also used in health and safety, methods for research, testing and evaluation, product designs, packaging designs, games designs, web designs, architecture exhibition designs, film/entertainment industry among others.

Therefore, it is hereby investigated in this study on how to protect images, particularly three-dimensional (3D) polygonal mesh models against attacks that may be made on them. Three-dimensional images were given emphasis in this study since there is less concern given for the protection of these types of images due to its newness and complexity. Furthermore, to be able to protect these images from attacks, a watermarking scheme was investigated and thereby increased the possibility of tamper-free images.

2.0 THE WATERMARKING SCHEME

The watermarking scheme required an original 3D image in 3ds or max format which was then converted to a polygonal mesh model using Autodesk 3DS Max software as in Figure 1. The model was converted to its binary format using a software designed for this watermarking scheme and the vertices list of the model was obtained from its binary file based from the files' chunk for the vertices list. A 3-bit sequence was used as the watermark and was embedded in the chunk's vertices list. Data compression is the attack made to the watermarked model. Decompression of the attacked watermarked model and extraction of the watermark completed this watermarking

ISSN- 2394-5125 VOL 07, ISSUE 15, 2020

scheme.

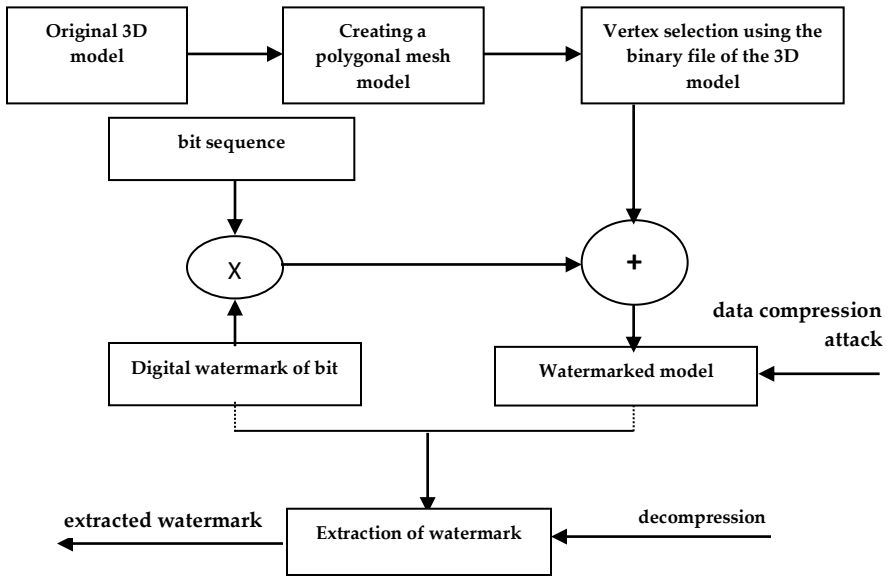


Figure 1: Compression-Resilient Watermarking Scheme

2.1 3D Polygonal Mesh Modeling

A smooth surfaced 3D model was generated using the software Autodesk 3DS Max and a polygonal mesh was then generated on the 3D model as in Figure 2. The generation of the polygonal mesh on a 3D model was made since the models available on the Internet and other medium are usually in its smooth surfaced 3D models used especially in 3D animations on films [9]. It is therefore necessary to convert these smooth surfaced models to polygonal mesh models to generate a binary file that will contain the vertices of the polygons of the model. Furthermore, from the polygonal mesh generated, vertex positions on each of the point in a polygon can be generated.

ISSN- 2394-5125 VOL 07, ISSUE 15, 2020

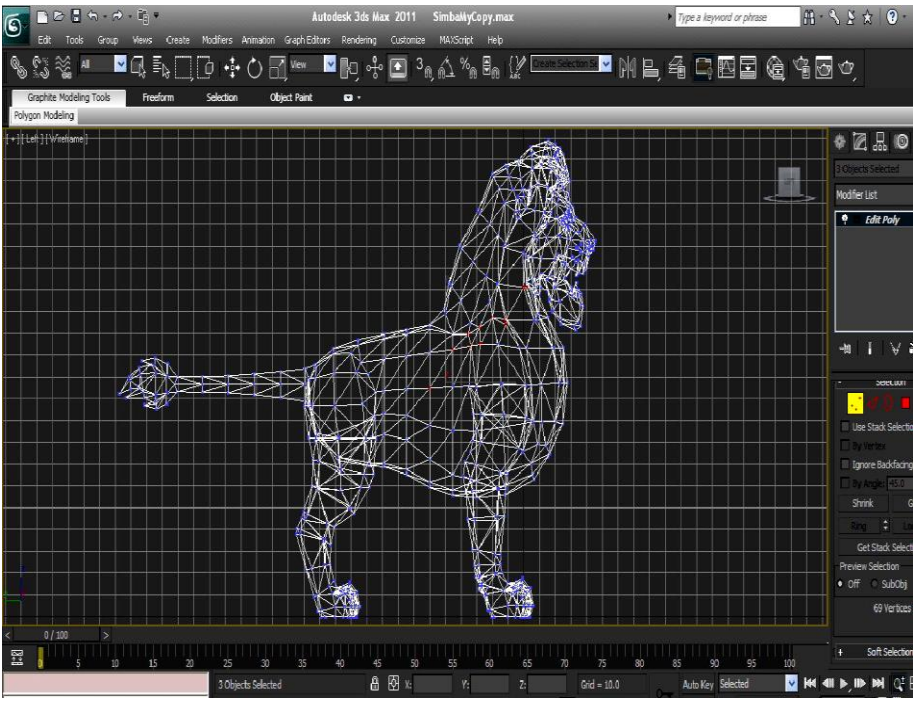


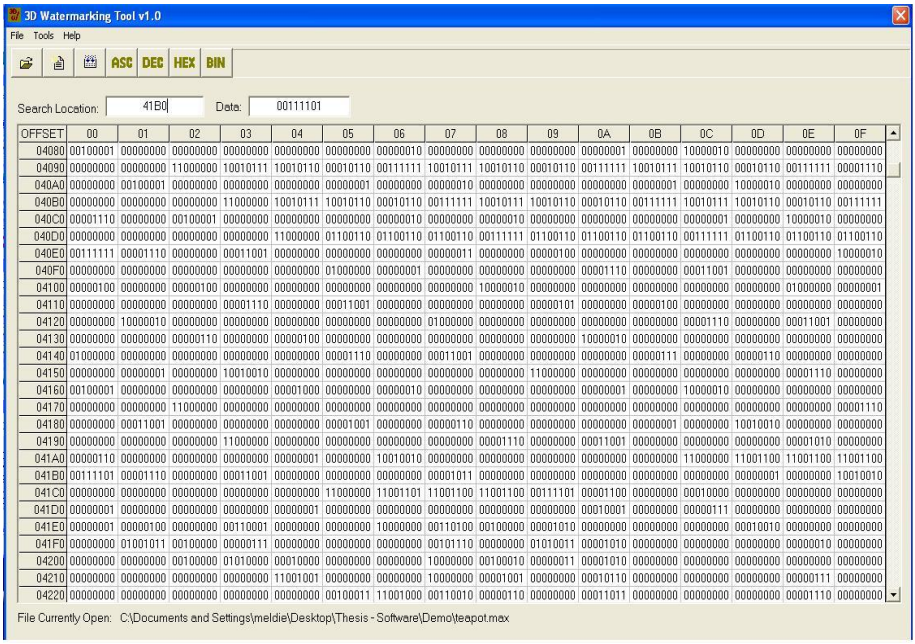
Figure 2: Generating a Polygonal Mesh Model with its Vertices

2.2 Embedding and Extraction of Watermark

Using the 3D model in its polygonal mesh with the vertices on each point in the polygons of the model, a software was designed to open the file of the 3D model in ASCII format, decimal format, hexadecimal format and binary format as in Figure 3. A 3ds or max file is a binary file based in chunks in which the address of 0x4110 contains the vertices list. It is then in this list that the embedding of the 3-bit sequencewas made on the binary sequence on the vertices list and produced a watermarked model.

Data compression on the watermarked model using the *maxzip*archiving system of the Autodesk 3DS Max was employed to test the resiliency of the watermarking scheme against this type of attack. After data compression and decompression, the software determined the presence of the bit sequence by again opening the file and locating the vertices list to extract the watermark.

ISSN- 2394-5125 VOL 07, ISSUE 15, 2020



3.0 RESULTS AND DISCUSSION

In the analysis of the watermarking scheme used in this study, this will identify if the watermark on the 3D model used here is perceptually invisible and the watermarking scheme is resilient to data compression attack.

3.1 Vertex Selection

Identifying the vertex to carry the watermarking information was done without altering the mesh topology. The selection of a vertex is at random and done on the vertices list of the chunk of the binary file of the 3D model. A vertex is selected as the watermark space since a vertex is a point in space of a 3D model. Overwriting this point in its bit values can avoid overwriting the significant bit values of the model [10].

A vertex is denoted by $\mathcal{V}i \, \epsilon \, \sigma$, where σ is the 3D graphical object, and its coordinates are defined by the vector $\mathcal{V}i$. The neighbor of a vertex as all the vertices from the same object that are connected to it by means of an edge is denoted as

$$\mathcal{N}(\mathcal{V}i) = \{\mathcal{V}j \,||\mathcal{V}j\mathcal{V}i| > \, 0, j = 1, \ldots, \mathcal{N}i\} \qquad (1)$$

where $|\mathcal{V}j\mathcal{V}i|$ represents the cardinal set between two neighboring vertices $\mathcal{V}i$ and $\mathcal{V}j$, while $\mathcal{N}i$ denotes the number of vertices from $\mathcal{N}(\mathcal{V}i)$. The vertex $\mathcal{V}i$ is not considered as a component of its own neighborhood. A vertex and its neighborhood are

ISSN- 2394-5125 VOL 07, ISSUE 15, 2020

considered as part of a set $\{\mathcal{V}i, \mathcal{N}(\mathcal{V}i)\}$.

3.2 Embedding the Watermark

The information to be embedded was represented as a sequence of bits generated according to a key. A 3-bit sequence is used as the watermark since it is easier to embed and debug in programming as well as to avoid overwriting bit values in the file that are significant thus avoiding corrupting the file. The watermarking technique in this study is a robust watermarking wherein the watermark must remain detectable after being attacked.

3.3 Extraction of the Watermark

The watermark detection stage using the software aimed to recover the information that has been embedded in the 3D model after a data compression attack. The extraction technique used in the watermarking method in this study is the invisible-blind semi-public strategy that does not require the original cover media for the detection of the watermark but the original watermark is necessary for comparing with the extracted watermark.

3.4 Testing the Watermarking Scheme

Various tests were conducted to determine the functionality of the watermarking scheme as shown in Table 1. These tests are: test for perceptual invisibility and test for resiliency against data compression attack.

Table1:List of Various Tests Conducted to Determine the Functionality of the Watermarking Scheme

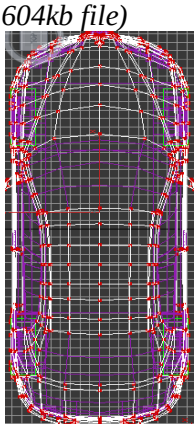
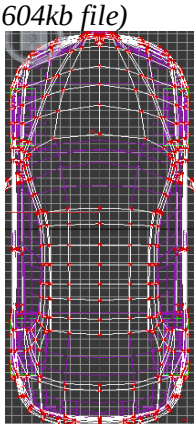
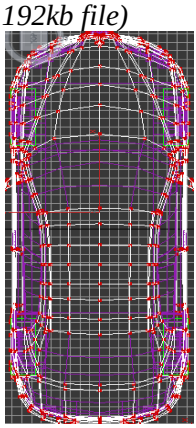
TEST	**Type of Test**	**Description**	**Input**	**Process**	**Expected Output**
SET 1	Test for Perceptual Invisibility	A set of tests to determine if the watermark on a 3D model is invisible or not	Original Shell/Boundary Model	Watermarking a 3-bit sequence on the binary file of the 3D model	Invisible or Imperceptible Watermark
SET 2	Test for Resiliency Against Data Compression Attack	A set of tests to detect the presence of the watermark	Compressed Watermarked Binary File of a 3D Model	Determine if the watermark is still present in the 3D	Extracted Watermark

		after data compression attack		model after data compression attack	

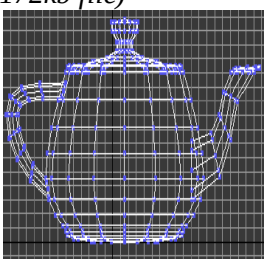
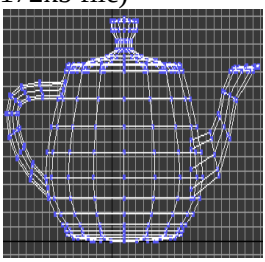
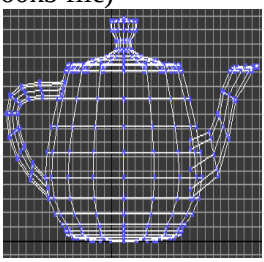
Test for Perceptual Invisibility

To test for perceptual invisibility, various tests are conducted in the form of testing two types of 3D models: the complex 3D models which are made of thousands of vertices, such as a car model with 1,231 number of vertices and the standard primitive models which are made of hundreds of vertices such as a teapot model with 530 number of vertices as shown in Table 2.

Table2:Test for Perceptual Invisibility of Watermark

Original Shell/Boundary Models	**TEST # 1**	**TEST # 2**
	Watermarked Model	**Attacked Model**
Complex 3D Model: *Car (1231 vertices, 604kb file)* 	*Car (1231 vertices, 604kb file)* 	*Car (1231 vertices, 192kb file)* 
RESULTS:	The car model and 9 other complex 3D models showed: • No distortion on the modelsafter watermarking • 0% visibility of the watermark	The car model and 9 other complex 3D models showed: • No distortion on the models after an attack • 0% visibility of the watermark after an

ISSN- 2394-5125 VOL 07, ISSUE 15, 2020

		attack
Standard Primitive Model: *Teapot (530 vertices, 172kb file)* 	Teapot (530 vertices, 172kb file) 	Teapot (530 vertices, 60kb file) 
RESULTS:	The teapot model and 9 other standard primitive 3D models showed: • No distortion on the models after watermarking • 0% visibility of the watermark	The teapot model and 9 other standard primitive 3D models showed: • No distortion on the models after an attack • 0% visibility of the watermark after an attack

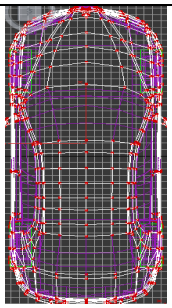
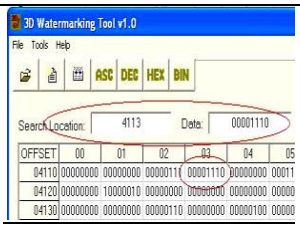
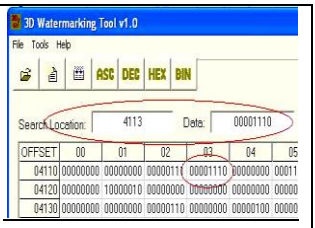
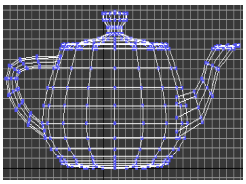
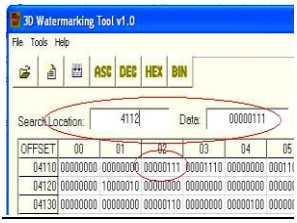
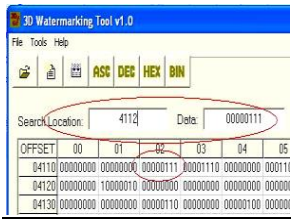
Test for Resiliency Against Data Compression Attack

Another set of tests for determining the presence of the embedded 3-bit sequence on the watermarked model after a compression attack was madeas shown in Table 3.Decompression was applied and using the attacked model on its corresponding binary file, detection of the watermark using the software developed in this study followed.

Table 3:Test for Resiliency Against Data Compression Attack

Original Shell/Boundary Models	**TEST #1** **Watermarked Model**	**TEST #2** **Watermark-Extracted Model After Data Compression Attack**
Complex 3D Model: *Car (1231 vertices, 604kb file)*	Using the software, a 3-bit sequence was watermarked on address 4113 of the car model.	Using the software, the 3-bit sequence was extracted on address 4113 of the car model.

ISSN- 2394-5125 VOL 07, ISSUE 15, 2020

		
RESULTS:	The car model and 9 other complex 3D models showed: • 100% watermarked	The car model and 9 other complex 3D models showed: • 100% extracted watermark
Standard Primitive Model: *Teapot (530 vertices, 172kb file)* 	Using the software, a 3-bit sequence was watermarked on address 4112 of the teapot model. 	Using the software, a 3-bit sequence was watermarked on address 4112 of the teapot model. 
RESULTS:	The teapot model and 9 other standard primitive 3D models showed: • 100% watermarked	The teapot model and 9 other standard primitive 3D models showed: • 100% extracted watermark

The test for the resiliency of the watermarking scheme against data compression attack were conducted in the form of testing two types of 3D models: the complex 3D models which are made of thousands of vertices, such as a car model with 1,231 number of vertices and the standard primitive models which are made of hundreds of vertices such as a teapot model with 530 number of vertices.

3.5 Evaluation of the Watermarking Scheme

ISSN- 2394-5125 VOL 07, ISSUE 15, 2020

Watermarks are usually assessed based on the watermarking scheme's effectiveness and strength [11]. The effectiveness of a watermarking scheme can be determined by a demonstration of the invisibly-blind robust semi-public characteristics of the scheme. In an invisibly-blind watermarking scheme, a watermark should remain imperceptible by human perception and cannot be easily detected by ordinary viewing but can be extracted by software detection. A robust watermarking scheme should contain a watermark that will remain detectable after being attacked. And a semi-public watermarking scheme should have, at the extraction stage, the presence of the watermark after decompression of the 3D models' file and it does not need the original file in the watermark extraction but the original watermark is necessary for comparing with the extracted watermark.

A watermarking scheme's strength can be determined by the algorithm used in the scheme and the watermark's power to protect 3D models using the bit sequence.

Table 4:Evaluation of the Watermarking Scheme

EFFECTIVENESS		**STRENGTH**	
Criteria	*Evaluation*	*Criteria*	*Evaluation*
Invisibly-Blind Watermarking Scheme	The results of the tests for perceptual invisibility demonstrated a watermark that remained imperceptible by human perception and cannot be easily detected by ordinary viewing but can be extracted by software detection.	Scheme	The results of the various tests conducted showed that the watermarking scheme's algorithm exhibited watermark invisibility and resiliency against data compression attack.
Robust Watermarking Scheme	The results of the tests for resiliency against data compression attack showed that the watermarking scheme used here is robust wherein the watermark remained detectable after being attacked.	Bit Sequence	The 3-bit sequence used as the watermark in the algorithm of the watermarking scheme was sufficient in exhibiting an invisible and resilient watermark.
Semi-Public	The results of the tests for resiliency		

ISSN- 2394-5125 VOL 07, ISSUE 15, 2020

Watermarking Scheme	against data compression attack showed that the watermarking scheme used here is semi-public wherein in the extraction stage the original file is not necessary but the watermark was used to compare it with the extracted watermark.		
CONCLUSION	Effectiveness: 100%	CONCLUSION	Strength: 100%

4.0 CONCLUSION

This study was able to develop and demonstrate an invisible-blind robust semi-public watermarking scheme for 3D models in its polygonal mesh. The watermark on the testing models used remained imperceptible by human perception but can be detected and extracted only by the software. Furthermore, after data compression and decompression of the watermarked file of the 3D models, the watermark remained detectable and can be extracted from the file thereby being resilient to data compression attack. Therefore, the watermarking scheme developed in this study is an effective tool in upholding the property rights of the owners of these media thus protecting the authenticity and credibility of the media information such as the 3D models.

REFERENCES

[1] E.E. Abdallah, A.F. Otoom, A.E. Abdallah, M. Bsoul and S. Awwad, "AHybrid Secure Watermarking Scheme Using Nonnegative Matrix Factorization and FastWalsh-Hadamard Transform",*Journal of Applied Security Research*,2019 doi: 10.1080/19361610.2019.1624100.

[2] M.R. Ashourian, J. Enteshari and Jeon (2004).*Digital Watermarking of Three-Dimensional Polygonal Mesh Models in the Spherical Coordinate System* [Online].
http://www.csdl.computer.org/dl/proceedings/cgi/2004/2171/00/21710590.pdf.

[3] M. Ashourian (2011).*A New Mixed Spatial Domain Watermarking of Three-Dimensional Triangle Mesh*, Association of Computing Machinery Inc. [Online]. http://portal.acm.org/ft_gateway.cfm?id=1174473&type =pdf.

[4] A.G. Bors, "Watermarking Mesh-Based Representatives of 3D Objects Using Local Moments", Proceedings of the IEEE Transactions on Image Processing,2006 Vol. 15 No 3, http://ieeexplore.ieee.org/iel5/ 10206/4782049/04770149.pdf?arnumber=4770149.

[5] C.M. Chou and B.C. Tseng, "Technologies for 3D Model Watermarking: A Survey", *IJCSNS International Journal of Computer Science and Network Security*,2017 Vol. 7 No 2, http://citeseerx.ist.psu.edu/viewdoc/ download?doi=10.1.1.105.5917&rep=rep1&type=pdf.

[6] N.V. Dharwadkar and B.B. Amberkes, "An Efficient Non-blind Watermarking Scheme for Color Images Using Discrete Wavelet Transformation", *International Journal of Computer Applications*2010 Vol. 2 No 3, http://www.ijcaonline.org/volume2/number3/ pxc387897.pdf.

[7] T.H.N. Le, K.H. Nguyen and H.B. Le (2010).*Literature Survey on Image Watermarking Tools, Watermarking Attacks and Benchmarking Tools*, IEEE Computer Society [Online].http://doi.ieeecomputersociety.org/ 10.1109/ MMEDIA.2010.37.

[8] G. Louizis, A. Tefas and I. Pitas (2004). *Copyright Protection of 3D Images Using Watermarks of Specific Spatial Structure*, Department of Informatics, Aristotle University of Thessaloniki [Online]. http://etdncku.lib. ncku.edu.tw/ETD-db/ETD-search-c/view_etd? URN=etd-0616103-090647.

[9] A.G. Perez and O. Corcho (2002).*Ontology Languages for the Semantic Web*, IEEE Intelligent Systems [Online]. http://oa.upm.es/2646/1/JCR01.pdf.

[10] J. Liu, Y. Yang, D. Ma, and Y. Wang, "A Watermarking Method for 3D Models Based on Feature Vertex Localization", IEEE Access 2018 Vol. 6 pp. 56122-56134.

[11] Z.N. Al-Qudsy, S.H. Shaker and N.S. Abdulrazzque, "Robust Blind Digital 3D Model Watermarking Algorithm Using Mean Curvature", International Conference on New Trends in Information and Communication Technology Applications 2018, CCIS Vol 938 pp. 110-125.

[12] K.M. Mabrouk, N.A. Semary and H. Abdul-Kader, "Fragile

ISSN- 2394-5125 VOL 07, ISSUE 15, 2020

Watermarking Techniques for 3D Model Authentication: Review",
International Conference on Advanced Machine Learning
Technologies and Applications 2019, AISC Vol. 921 pp. 669-679.