THE JOURNAL OF
DIGITAL FORENSICS,
SECURITY AND LAW

Journal of Digital Forensics,
Security and Law

Volume 17 Article 2

7-12-2022

Assessment of 3D mesh watermarking techniques

Neha Sharma
Delhi Technological University, nehashrm013@gmail.com

Jeebananda Panda
Delhi Technological University, jpanda@dce.ac.in

ASSESSMENT OF 3D MESH WATERMARKING TECHNIQUES

Neha Sharma, Jeebananda Panda
Delhi Technological University
Department of Electronics and Communication Engineering
New Delhi, Delhi 110042, India
nehashrm013@gmail.com
jpanda@dce.ac.in

ABSTRACT

With the increasing usage of three-dimensional meshes in Computer-Aided Design (CAD), medical imaging, and entertainment fields like virtual reality, etc., the authentication problems and awareness of intellectual property protection have risen over the last decade. Numerous watermarking schemes have been suggested to protect ownership and prevent the threat of data piracy. This paper begins with the potential difficulties that arose when dealing with three-dimension entities in comparison to two-dimensional entities and also lists possible algorithms suggested hitherto and their comprehensive analysis. Attacks, also play a crucial role in deciding on a watermarking algorithm so an attack based analysis is also presented to analyze the resilience of watermarking algorithms under several attacks. In the end, some evaluation measures and potential solutions are brooded over to design robust and oblivious watermarking schemes in the future.

Keywords: 3D Mesh, Watermarking, vertices, review

1. INTRODUCTION

Due to the advent of state-of-the-art technologies for storage, dissemination, and transmission of data (audio, video, images, etc.) over the last few decades, the threat of tampering, unauthorized duplication, and unrestrained propagation of data is on the rise. Intellectual property rights protection demands security, rightful ownership, and prohibition of unauthorized access to data. Digital watermarking seems a potential solution for this when compared to classical methods of data protection as former one secures data even after its transmission phase is over and accessibility to the data is procured (Borah & Borah, 2018).

The origin of the name “Watermark” dates back to the time when its existence was only seen on paper. In order to create a watermark, the width of the paper was modified when the paper was in wet condition and thus a shadowed or a lighter pattern was developed in the watermarked paper. Therefore, this process gets its name as a watermark. With the upsurge of digital content, this term came to be used with digital practices. The coinage of the term “Digital Watermark” was done by Andrew Tirkel and Charles Osborne in December 1992. Digital watermark shares a similar objective of physical watermark i.e. to verify the authenticity and integrity of the content as well as its ownership. But unlike a physical copy, a digital copy of data is identical to the original data so a digital watermark can only mark the data and cannot control its access. So it is a passive tool for content protection (Van Schyndel et al., 1994).

In digital watermarking, the embedding of some crucial information relating to either the owner or the content itself is done in such a way that its presence can't be avoided even after several manipulations of the digital media whether intentional or unintentional. The general watermarking system as shown in Figure 1 involves the host media which is to be watermarked undergoing an embedding process first. After being watermarked, media is distributed through channels wherein it bears all genuine and malicious attacks before reaching the final destination. At the receiver also, there has to be some mechanism to detect or retrieve the watermark to authenticate the content or verify ownership respectively (Potdar et al., 2005).

Similar to watermarking. there exist several other popular techniques like cryptography and steganography. Cryptography is usually involved in maintaining the secrecy of the information using a secret key and thus prohibits its reading by any illegitimate user. On the other hand, steganography makes use of cover media to hide information in such a way that it is hardly noticeable to the human eye. But both these techniques have no business in dealing with copyright issues and authentication of data; their prime concern is the protection of information content (Saini & Shrivastava, 2014).

We may classify digital watermarking into different categories based on the type of watermark, its robustness, application, host data and other features. The complete taxonomy of digital watermarking is shown in Table 1.

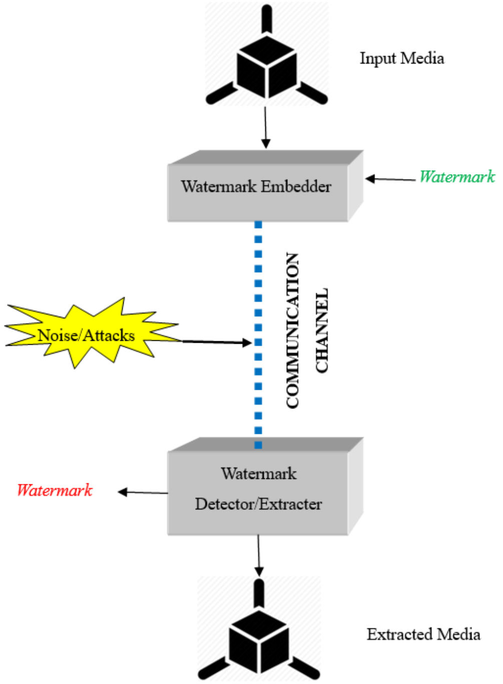

Figure 1. The digital watermarking system

On the basis of the type of watermark to be embedded, two categories are defined, the first is noise type, other is image type. In noise type, any pseudo, chaotic, random or Gaussian sequence can be embedded in the host media whereas, in image type watermark, any logo, stamp or binary image can be inserted in the media as a watermark.

Depending on the ability of the watermark to remain unaffected by modifications in the embedding media, three categories of watermark are defined, namely fragile, semi-fragile and robust. If watermarking is stubborn enough to withstand all modifications whether intentional or unintentional and still be recovered, then watermarking algorithm may be designated as a robust one. Usually, robust algorithms are used for copyright purposes so that it protects embedded copyright information to prevent its illegitimate usage. On the other hand, fragile techniques are used to detect even the slightest modification in the watermark to assess the amount

Table 1. Complete Taxonomy of Watermarking System

S.No	Basis	Categories
1	Type of watermark	Noise, Image
2	Robustness	Fragile, Semi-fragile, Robust
3	Domain of watermarking	Spatial, Spectral, Invariant
4	Imperceptibility	Visible, Invisible, Dual Watermark
5	Embedding Media	Image, Text, Audio, Video, 3D mesh
6	Extraction method	Blind, Semi-blind, non-blind
7	Application	Copyright, Tampering, Anti-counterfeit, Hidden annotation
8	Key usage	Asymmetric, Symmetric
9	Information	Informative, Non-informative

of tampering done. Some of the pioneering work such as R. Ohbuchi et al. (2004) realised that semi-fragile serves the characteristics of both, it is able to resist some degree of perturbations such as due to compression while still being fragile.

We may also choose the domain of embedding watermark such as spatial, spectral or invariant. If watermarking technique directly plays with the host media in the original domain, it is called spatial, and if frequency domain coefficients are altered, it is called spectral. Liu and Chen (2010) identified that it is desired to choose an invariant transform domain that provides robustness to withstand attacks..

We have seen logos of TV channels, stamps in the paper, etc which is conspicuous enough to assert ownership. Such overt labelling of channels, papers, or any other media comes under the category of visible watermarking. But at times, covert protection of ownership details is required without causing a perceptible change in the host media. This category of watermarking comes under an invisible one.

The extraction method of the watermark also varies as per the requirement of original data at the receiver's side. The non-blind technique requires original data for watermark retrieval and the process is much simple here while the blind technique forbids the usage of original data at the receiver's side which makes it complicated due to lack of prior information.

There are different applications of watermarking anti-counterfeiting, tampering, copyright and annotation hiding to name a few. Different applications demand different characteristics of the watermark, for instance, annotations used in confidential files need to be hidden from illegitimate users, therefore the watermark here should be invisible, imperceptible as well as robust to safeguard them.

Recipients of watermarked data are provided with a key to access the data. If this key is identical to the key used while embedding the watermark, such a technique is called symmetric watermarking. On the other hand, if both the keys are different, such a technique is called asymmetric watermarking. Watermark may contain some information indicating the ownership details or it may also be non-informative wherein the receiver's task is just to ascertain the presence or absence of a watermark(Saini & Shrivastava, 2014).

Watermark can be embedded in different types of data for instance text, audio, video 3D graphics etc. and thus is classified according to the domain of embedded media.

Of late, extensive usage of three-dimensional mesh in the medical, industrial, and entertainment industries can be observed that has propelled the need for its authentication check to curb the ill effects of its malicious usage. However, a relatively small body of literature exists for them when compared to their two-dimensional counterpart like images. This can be attributed to several potential challenges faced while designing algorithms for these models that are discussed as follows:

- There is a lack of unique arrangement for 3D mesh models, unlike images that are statically represented by rows and columns. This rearrangement leads to synchronization problems during the extraction phase.
- Number of vertices available in a 3D mesh is relatively less when compared to images where millions of pixels are available. So comparatively very less data is available for watermark insertion in the 3D mesh. Hence this poses another challenge in making watermarking distortion-free as well as robust under various attacks.
- Several distortion and distortion-less attacks also pose a threat to watermarked model by destroying the watermark. Similarity transforms, smoothing, noise addition, etc. are some of the distortion attacks which cause visual alteration of the model. Interestingly, some of the prominent works (Ai et al., 2009; J.-W. Cho et al., 2006) highlighted vertex reordering as one of the examples of a distortion-less attack that does not cause any perceptible change in the model.

This paper gives a comprehensive review of the watermarking techniques proposed so far in the last two decades. The organization of the paper is as follows: Section 2 briefly introduces relevant preliminaries for three-dimensional mesh comprehension, Section 3 reviews the techniques proposed for 3D mesh watermarking categorized into different subsections based on insertion domain or type of algorithm used. Moreover, since resilience to attacks plays a vital role in designing a watermarking algorithm, Section 4 gives an attack-based analysis of them. Some evaluation measures to compare watermarking are discussed in Section 5 and lastly, section 6 concludes the review on a promising note.

2. PRELIMINARIES

The representation of 3D mesh usually takes the form of polygonal or triangular meshes in computer graphics or Computer-Aided Design(CAD). Several preliminaries are required to be constituted before venturing into the domain of 3D mesh watermarking. A 3D mesh is constituted by three different elements: vertices, edges, and faces. An example of a 3D mesh model is shown in Figure 2. Coordinates of vertices in a Cartesian plane provide geometrical information about the model while edges connecting vertices to form polygonal faces provide the connectivity details of a 3D mesh.

1-ring neighbourhood of a vertex v_i constitutes all the vertices that are adjacent to vertex v_i in a neighbourhood. The degree of vertex v_i is defined as the total number of vertices that are directly connected to it in a 1-ring neighbourhood. It is also referred to as the valence of a vertex. An example of vertices of valences 5 and 6 is shown in Figure 3. The valency of a vertex can be studied from the works by Borah and Borah (2018); El Zein et al. (2017); Ghali (2016); Soliman et al. (2013); Motwani and Harris Jr (2009) to get in-depth analysis of the 3D mesh attributes.

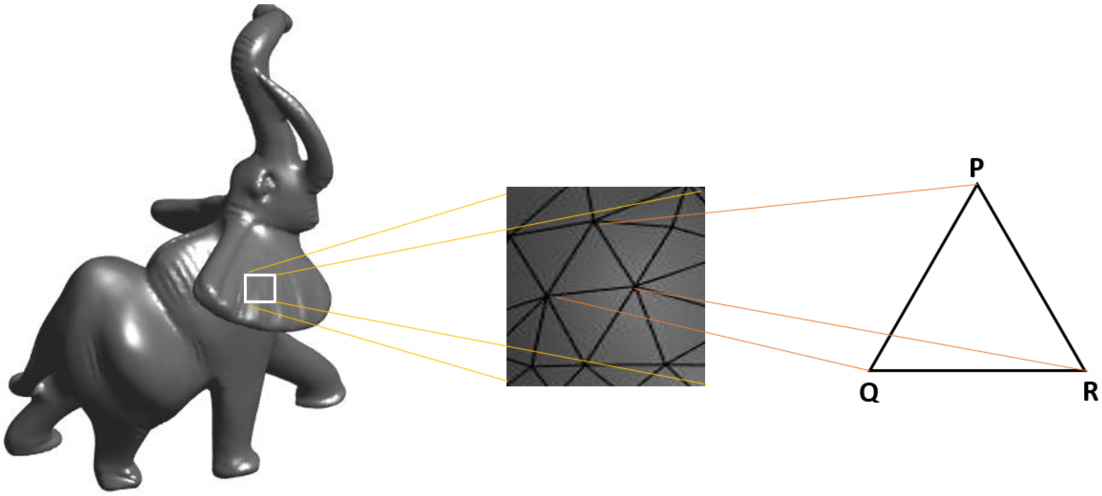

Figure 2. An example of a 3D mesh gives a closer look at the building blocks of mesh namely vertices, edges and faces. In a zoomed-in portion of the triangular mesh having vertices P, Q and R, the triangle PQR is one of the faces formed by joining edges PQ, QR and RP respectively.

3. LITERATURE REVIEW

Several past pieces of research on 3D mesh watermarking have been examined in this study. A specific searching standard utilized for a selection of peer-reviewed journals in this work is based on the following keywords: 3D mesh watermarking, digital watermarking, copyright protection, robust watermarking, etc. Prominent electronic research databases like Elsevier, Springer, IEEE, IET, etc. have been adopted in this survey.

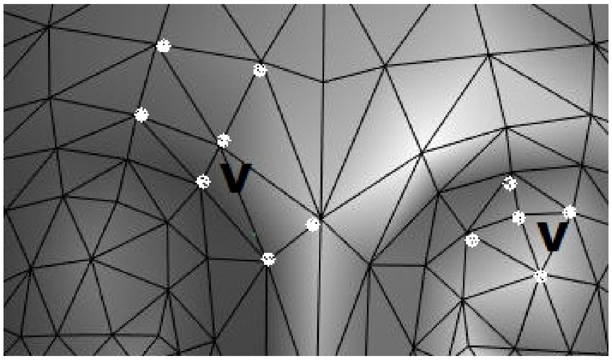

Figure 3. Example showing vertices of degree-6 and degree-5

3.1 Watermarking techniques based on geometrical transformations

Most of the initial watermarking techniques involved changing the coordinates of vertices of the 3D mesh model in accordance with the watermark directly. Such techniques generally come under the category of fragile watermarking. Yu et al. (2003) modified the length of vertices from the centre of gravity of the mesh to insert a watermark. Vertices are divided into groups and each group becomes a carrier of a 1-bit watermark as per the modified distance from the gravity centre. But this technique requires registration and re-sampling as a pre-processing step at the extraction site for robustness as this approach is not resilient to similarity transformations.

One of the most important entities of the 3D mesh model for watermark insertion is facets. R. Ohbuchi et al. (1998) proposed a blind watermarking approach using interesting characteristics of a facet in a 3D mesh-like Triangle Similarity Quadruple and tetrahedral volume ratio. The algorithm basically uses the ratio of the triangle's height and opposite edge length which is resilient to many transformations like rotation, scaling, and translation but not robust enough to other severe forms of attacks.

Such techniques employ modifications in the geometry of the model to insert a watermark which is simple to implement but their robustness quotient is on the lower side. Moreover, they also suffer from synchronization issues so even in absence of attacks watermark values seem perturbed.

3.2 Watermarking techniques based on direct spectral analysis

For other entities like image, audio, etc. it has been observed through spectral analysis that affecting low or middle-frequency coefficients does not distort the final visual output much. This characteristic has been exploited much in the case of image watermarking but in the case of 3D mesh, no such analysis has been made so far. So in such algorithms basic principle of watermarking revolves around modifying spectral coefficients. Different kinds of basis functions are utilized to analyze 3D mesh spectrally. In the laplacian basis function, a square dimension matrix of length equal to a number of vertices in a 3D mesh is made based on the connectivity order of the model. Suppose the number of vertices in a model is M then to determine M x 3 spectral coefficients, projections of the three coordinates vectors of all the vertices on M ordered and normalized eigenvectors of the Laplacian matrix are taken. . R. Ohbuchi et al. (2002) made use of this analysis to watermark 3D mesh by modifying low and middle-frequency coefficients. Cayre et al. (2003) improvised a step further by quantizing those frequency coefficients which will have little or no impact on the final watermarked model. However, the computation time in this work is directly in proportion with the mesh complexity due to the diagonalization of the NxN laplacian matrix. Moreover, the requirement of exact connectivity information for this algorithm to work makes it non-blind. Murotani and Sugihara (2003) used a lower dimension matrix to increase performance to computation time ratio.

3.3 Watermarking techniques based on Multi-Resolution analysis

The multi-resolution analysis serves as a perfect tool in order to strike the balance between the capacity of the available resources and the complexity order of the mesh. It gives a coarse (low frequencies) to fine (median and high frequencies) representation of the mesh from basic shape to intricate details at varying levels of resolution. This representation serves different purposes required for different applications, for instance, embedding in low resolution (low frequencies) provides robustness as well as imperceptibility whereas embedding in high-resolution details provides for high capacity.

Wavelets are generally used for such multiresolution analysis where watermark strings can be inserted in wavelet coefficients at different resolution levels. Under the assumption of statistical independence between wavelet coefficient norms and watermarking bits, Uccheddu et al. (2004) proposed an oblivious watermarking scheme using wavelet-based multiresolution analysis. W.-H. Cho et al. (2004); Jian-qiu et al. (2004) proposed a fragile watermarking technique using the same approach for authentication purposes. The later one made use of both spherical domain wavelet coefficients and coarsest representation to insert a watermark. To make the above approach robust and resilient to common mesh operations like rotation, translation, scaling, etc., and malicious attacks, several schemes were introduced. Yin et al. (2001) used Guskov's multiresolution signal processing method and a Burt-Adelson pyramid is built for mesh for watermark insertion. Praun et al. (1999) extended the spread spectrum approach by giving a solution for the dearth of natural parameterization for decomposition based on frequency.

Multiresolution techniques much in resonance with direct spectral analysis also lack sufficient robustness. Moreover, to ensure robustness, the requirement of registration and resampling at the extraction site by most of the techniques renders them non-blind or at least semi-blind.

3.4 Watermarking techniques based on Parameterization

Another interesting approach for watermarking meshes apart from direct spectral analysis and multi-resolution analysis is Parameterization. This approach facilitates the application of existing 2D algorithms on meshes by converting 3D mesh into 2D entities. A semi-blind method was proposed by L. Li et al. (2004) which modified harmonic coefficients of mesh as per the watermark after transforming the original mesh into a spherical parameterization domain.

3.5 Watermarking techniques based on Vertex norm distribution

J.-W. Cho et al. (2006) proposed a robust watermarking approach to insert a watermark in 3D mesh without comprising the imperceptibility requirement of the watermark by making use of statistical parameters of vertex norm distribution. In this technique, firstly Cartesian coordinates are transformed into spherical coordinates and only vertex norm values are considered for watermark while the other two spherical coordinates are kept intact so there is less visible distortion on the model. This method though robust but fails in the case of very small-sized models or CAD models which have too flat surfaces. Hu et al. (2009) used constrained optimization to minimize the least square difference between the original model and the watermarked one and proved to be better than Cho's method in resisting Gaussian noise. But this method has its own limitations as with the increasing size of the model, the computational complexity of quadratic programming problems also increases. Levenberg– Marquardt optimization method was also suggested Bors and Luo (2012) for reducing surface distortion to a minimum as well as preserving the original model. This method enhanced robustness against various common mesh operations. Methods like improved vertex grouping were suggested by works like S. Li et al. (2017) to ensure transparency while improving robustness.

3.6 Watermarking techniques based on the intelligent selection of watermark carriers

In the last few years, an intelligent watermark embedding technique has been prevalent that involves the selection of watermark carriers suitable for carrying watermark. Their suitability is assessed based on three crucial tenants of digital watermarking namely imperceptibility, capacity, and robustness of the watermarking process. The most common criteria employed for watermark selection in 3D models is their curvature. El Zein et al. (2017) made use of the Fuzzy C-means clustering technique to find vertices that will cause the least perceptible distortion to the 3D model after carrying watermark bits but the computational complexity of Fuzzy C-means slowed down the process. Soliman et al. (2013) employed another clustering technique namely Self Organising Maps(SOM) to select vertices after calculating the feature vector of the 1-ring neighbourhood of a vertex. Although this method results in better robustness but both the approaches discussed in this method were either non-blind or semi-blind causing additional payload in the watermark extraction process. S. Li et al. (2017) rejected marginal bins in the histogram of eigenvalues of the vertex by 10% and employed the rest of the bins as watermark carriers, however even this method could not improve robustness much in cases of flat-surfaced models like CAD models and small-sized models having fewer vertices. Sharma and Panda (2020) introduced a viable approach wherein computational overheads are reduced by employing histogram binning of feature vectors based on their surface inclination while not compromising the robustness of the watermarking technique as it involves statistical insertion in chosen watermark carriers.

4. ATTACK-BASED ANALYSIS

Attacks also form an inevitable factor when designing any watermarking technique. Without showing resilience to different types of attacks, watermarking algorithms may not be successful; therefore robustness towards these attacks becomes an important parameter for the evaluation of any watermarking technique.

4.1 Geometric Attacks

As the name itself suggests, these kinds of attacks reflect changes in the geometrical part of the model by perturbing the vertex's positions. Some common mesh operations like rotation, translation, and scaling together known as Similarity transformation fall into this category. Not just robust even fragile watermark is expected to withstand such operations. To make watermarking technique immune to these attacks, one of the suggested solutions in many papers reviewed above is to choose a space that is invariant to such changes in vertices positions. In fact, such space can be created by shifting the origin to the mesh's centre of gravity, uniform scaling bounded by a unit cube/sphere, and rotating towards principal axes of rotation; thus making it translation, scaling, and rotation invariant. Some of the features do change after watermark insertion but if some feature or characteristics of the embedding domain is known, successful extraction is possible but at the cost of making the algorithm more or less semi-blind.

Another solution suggested in the papers above was to use such ratios for instance between edge length and height of triangle of mesh which does not vary with watermark insertion or attacks as suggested by R. Ohbuchi et al. (1998) TSQ and TVR. Several signal processing attacks like random noise addition, smoothing, etc. also come under this category. Such operations can be dealt with nicely in spectral-domain with either direct frequency analysis pr multi-resolution analysis where it is found that low and medium frequency part is more resilient to such attacks and thus can be used for insertion of watermark as discussed in previous sections.

4.2 Connectivity Attacks

A common type of operation that comes under this category is cropping. Although it can be regarded as a geometric attack its consequences can be far worse as some part of the watermark string may be lost and become unrecoverable after an attack. A potential solution to this problem is a repetition of the watermark string in different patches of the mesh model so that the watermark string is recoverable even after the attack. Spatial techniques discussed before are less immune to these attacks due to geometric changes caused by cropping as well as loss of synchronization caused due to it. As far as spectral-domain-based techniques are considered whether direct frequency analysis based or multi-resolution analysis based, information about the vertices order or mesh connectivity or both are required at times, making these techniques also less immune to connectivity attacks.

Some other potential solutions in order to deal with connectivity attacks could be finding a domain for watermarking which is invariant to connectivity information as well as robust to connectivity attacks.

4.3 File format attacks

File attack includes the rearrangement of the vertices or faces in the mesh model. Format attack includes conversion of 3d model file type which may alter the structure of mesh and thus causing a change in the order of mesh vertices and faces. Watermarking schemes need to be synchronization independent to deal with such attacks. The process used for synchronization should not depend on the vertices and face order of the mesh.

5. EVALUATION PARAMETERS FOR ALGORITHM ASSESSMENT

A watermarked model must endure all attacks while preserving the model as well as the watermark. To show such a characteristic a watermarking scheme should possess robustness, imperceptibility as well as capacity which are often in contradiction with each other. For example, employing repetition of the watermark in different patches ensure robustness but decreases capacity. The visual quality of the watermark is also at risk if greater transformations are employed in the model to ensure robustness.

A benchmarking system is required for the evaluation of robust watermarking schemes to analyze the robustness of these schemes to different attacks and to assess their visual quality degradation after watermarking. Wang et al. (2010) provides a software tool for the same and also discusses parameters like MRMS (Maximum root mean square error) to measure the visual difference between the original model and the watermarked model. The endurance of the watermark inserted can be measured through correlation as shown by J.-W. Cho et al. (2006). Furthermore, the imperceptibility of the watermark can be evaluated through VSNR as in El Zein et al. (2017). An overall comparison of 3D watermarking techniques has been presented in Table 2.

Table 2. Comparative Analysis of 3D mesh watermarking techniques

Watermarking techniques based on	Techniques proposed in	Algorithm features	Attack-centric investigation		
			Geometric Attack	Connectivity Attack	File format Attack
Geometrical transformations	Yu et al. (2003) Ohbuchi et al. (2004)	Simple to implement Not robust enough, Also suffer synchronisation issues.	Invariant	Variant	Variant
Direct spectral analysis	Ohbuchi et al. (2002), Cayre et al. (2003) Murotani et al. (2003)	Robust and imperceptible Increased complexity and computation time.	Invariant	Variant	Variant
Multi-Resolution Analysis	Uccheddu et al. (2004) Cho et al. (2005) Jin et al.,2004) Yin et al. (2001) Praun et al. (1999)	Increased robustness and capacity. Requires resampling and registration	Invariant	Variant	Variant
Parameterization	Li et al. (2004)	Allows application of existing 2D algorithms on 3D mesh Semi-blind Approach.	Invariant	Semi-invariant	Variant
Vertex norm distribution	Cho et al. (2007), Bors et al. (2012)	Transparency as well as robustness increased. However, transparency is difficult to maintain in case of small sized models and complexity increases in case of large-sized models.	Invariant	Semi-invariant	Invariant
Intelligent watermark selection	Zein et al. (2016) Solimon et al. (2013) Li et al. (2017) Sharma et al. (2020)	Only selected carriers are chosen for watermarking thus causing minimum perceptible distortion in the model. Less prone to error in watermark extraction process as fewer vertices are involved.	Invariant	Mostly invariant	Invariant

6. DISCUSSIONS AND POTENTIAL SOLUTIONS

6.1 Capacity, Robustness and Imperceptibility Trade-off

If a watermarking algorithm is designed to be robust under various attacks, then it is observed that the quality of watermarked mesh usually degrades. This visual degradation mortification of the model after watermarking decreases the imperceptibility of the model. Similarly, one of the methods to increase the robustness of the watermark is redundant insertion so that even after several malicious attacks whether intended or not, a significant portion of watermarking bits are preserved. However, such a redundant insertion deteriorates the capacity of the model to carry a watermark as presented in significant works by Sharma and Panda (2020); Wang et al. (2010). The potential solution as suggested by contemporary literature lies in finding an insertion domain or a feature or shape descriptor in the 3D mesh which is invariant to common mesh operations and attacks. The embedding feature or domain is required to be chosen intelligently to ensure the imperceptibility of the watermarked mesh.

6.2 Computational Complexity and Execution Time Trade-off

Although non-blind watermarking methods have proven to be more robust than their blind counterparts, the requirement of the original model at the extraction site leads to an excessive payload. Hence the future research proposals are inclined towards a blind framework of watermarking to avoid the expenses and hassle of sending the original model along with the watermarked model. However, the blind watermarking retrieval process is more complex than the non-blind or semi-blind methods due to the absence of the original model (Praun et al., 1999). Some of the relevant works such as by J.-W. Cho et al. (2006), assessed that blind approaches cannot simply rely on comparison with the original mesh to retrieve the watermark rather they require some other information be its the length of the watermark, location of the watermark, etc. which serves as the key for watermark extraction purposes. These approaches require better comprehension of the mesh model characteristics therefore the need for algorithms of complex nature comes into play. The higher the complexity, the higher is the correlation between the true watermark and extracted watermark. Nonetheless, higher complexity also leads to an increase in execution time which is not a desirable characteristic of watermarking process. A potential solution lies in reaching a compromise between the fast execution time of the algorithm and the high correlation between the original and extracted watermark such that optimum efficiency is gained in the watermarking process.

7. CONCLUSION

This paper discusses some of the breakthrough research contributions in the 3D mesh watermarking domain in the last two decades. However, owing to many difficulties in constructing an algorithm for watermark insertion in a 3D model as discussed in this paper, the research in this area can still be considered in its infancy stage. Several issues are hampering the utilization of watermarking in 3d mesh at full scale. There is still uncertainty regarding what possible fusion of a variety of attacks, a model may have to undergo in myriad instances. Finding a feasible approach to tackle them without compromising the watermark and the model, pose a big challenge. Future directions of research could focus on studying hybrid attacks rather than individual attacks and their solutions. Furthermore, there is huge research scope in discovering a new insertion domain, transform domain or a novel approach that will facilitate the optimum requirement of robustness, imperceptibility, and capacity concurrently.

REFERENCES

Ai, Q., Liu, Q., Zhou, Z., Yang, L., & Xie, S. (2009). A new digital watermarking scheme for 3d triangular mesh models. *Signal Processing*, *89*(11), 2159–2170.

Borah, S., & Borah, B. (2018). Watermarking techniques for three dimensional (3d) mesh authentication in spatial domain. *3D Research*, *9*(3), 1–22.

Bors, A. G., & Luo, M. (2012). Optimized 3d watermarking for minimal surface distortion. *IEEE Transactions on Image Processing*, *22*(5), 1822–1835.

Cayre, F., Rondao-Alface, P., Schmitt, F., Macq, B., & Maıtre, H. (2003). Application of spectral decomposition to compression and watermarking of 3d triangle mesh geometry. *Signal Processing: Image Communication*, *18*(4), 309–319.

Cho, J.-W., Prost, R., & Jung, H.-Y. (2006). An oblivious watermarking for 3-d polygonal meshes using distribution of vertex norms. *IEEE Transactions on Signal Processing*, *55*(1), 142–155.

Cho, W.-H., Lee, M.-E., Lim, H., & Park, S.-Y. (2004). Watermarking technique for authentication of 3-d polygonal meshes. In *International workshop on digital watermarking* (pp. 259–270).

El Zein, O. M., El Bakrawy, L. M., & Ghali, N. I. (2017). A robust 3d mesh watermarking algorithm utilizing fuzzy c-means clustering. *Future Computing and Informatics Journal*, *2*(2), 148–156.

Ghali, N. I. (2016). A non-blind robust watermarking approach for 3d mesh models.

Hu, R., Rondao-Alface, P., & Macq, B. (2009). Constrained optimisation of 3d polygonal mesh watermarking by quadratic programming. In *2009 ieee international conference on acoustics, speech and signal processing* (pp. 1501–1504).

Jian-qiu, J., Min-ya, D., Hu-jun, B., & Qun-sheng, P. (2004). Watermarking on 3d mesh based on spherical wavelet transform. *Journal of Zhejiang University-Science A*, *5*(3), 251–258.

Li, L., Zhang, D., Pan, Z., Shi, J., Zhou, K., & Ye, K. (2004). Watermarking 3d mesh by spherical parameterization. *Computers & Graphics*, *28*(6), 981–989.

Li, S., Ni, R., & Zhao, Y. (2017). A 3d mesh watermarking based on improved vertex grouping and piecewise mapping function. *J Inf Hiding Multimedia Signal Process January*, *8*(1), 97e108.

Liu, C.-C., & Chen, J.-Y. (2010). A watermarking scheme for 3d models using haar discrete wavelet transform. In *2010 international symposium on computer, communication, control and automation (3ca)* (Vol. 1, pp. 244–247).

Motwani, R. C., & Harris Jr, F. C. (2009). Robust 3d watermarking using vertex smoothness measure. In *Ipcv* (pp. 287–293).

Murotani, K., & Sugihara, K. (2003). Watermarking 3d polygonal meshes using the singular spectrum analysis. In *Mathematics of surfaces* (pp. 85–98). Springer.

Ohbuchi, R., Masuda, H., & Aono, M.

(1998). Watermarking three-dimensional polygonal models through geometric and topological modifications. *IEEE Journal on selected areas in communications*, *16*(4), 551–560.

Ohbuchi, . R., Mukaiyama, . A., & Takahashi, . S. (2002). A frequency-domain approach to watermarking 3d shapes. In *Computer graphics forum* (Vol. 21, pp. 373–382).

Ohbuchi, R., Mukaiyama, A., & Takahashi, S. (2004). Watermarking a 3d shape model defined as a point set. In *2004 international conference on cyberworlds* (pp. 392–399).

Potdar, V. M., Han, S., & Chang, E. (2005). A survey of digital image watermarking techniques. In *Indin'05. 2005 3rd ieee international conference on industrial informatics, 2005.* (pp. 709–716).

Praun, E., Hoppe, H., & Finkelstein, A. (1999). Robust mesh watermarking. In *Proceedings of the 26th annual conference on computer graphics and interactive techniques* (pp. 49–56).

Saini, L. K., & Shrivastava, V. (2014). A survey of digital watermarking techniques and its applications. *arXiv preprint arXiv:1407.4735*.

Sharma, N., & Panda, J. (2020). Statistical watermarking approach for 3d mesh using local curvature estimation. *IET Information Security*, *14*(6), 745–753.

Soliman, M. M., Hassanien, A. E., & Onsi, H. M. (2013). Robust watermarking approach for 3d triangular mesh using self organization map. In *2013 8th international conference on computer engineering & systems (icces)* (pp. 99–104).

Uccheddu, F., Corsini, M., & Barni, M. (2004). Wavelet-based blind watermarking of 3d models. In *Proceedings of the 2004 workshop on multimedia and security* (pp. 143–154).

Van Schyndel, R. G., Tirkel, A. Z., & Osborne, C. F. (1994). A digital watermark. In *Proceedings of 1st international conference on image processing* (Vol. 2, pp. 86–90).

Wang, K., Lavoué, G., Denis, F., Baskurt, A., & He, X. (2010). A benchmark for 3d mesh watermarking. In *2010 shape modeling international conference* (pp. 231–235).

Yin, K., Pan, Z., Shi, J., & Zhang, D. (2001). Robust mesh watermarking based on multiresolution processing. *Computers & graphics*, *25*(3), 409–420.

Yu, Z., Ip, H. H., & Kwok, L. (2003). A robust watermarking scheme for 3d triangular mesh models. *Pattern recognition*, *36*(11), 2603–2614.