Indonesian Journal of Electrical Engineering and Computer Science
Vol. 24, No. 2, November 2021, pp. 957~964
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v24.i2.pp957-964

An efficient data masking method for encrypted 3D mesh model

Manikamma Malipatil[1], D. C. Shubhangi[2]
[1]Department of Computer Science and Engineering, Sharnbasva University, Kalaburagi, India
[2]Department of Computer Science and Engineering, Visvesvaraya Technological University, Kalaburagi, India

Article Info

Article history:

Received Feb 22, 2021
Revised Aug 31, 2021
Accepted Sep 8, 2021

Keywords:

3D mesh models
Chaotic sequence
Cryptography
Data masking
Watermarking method

ABSTRACT

The industrial 3D mesh model (3DMM) plays a significant part in engineering and computer aided designing field. Thus, protecting copyright of 3DMM is one of the major research problems that require significant attention. Further, the industries started outsourcing its 3DMM to cloud computing (CC) environment. For preserving privacy, the 3DMM are encrypted and stored on cloud computing environment. Thus, building efficient data masking of encrypted 3DMM is considered to be efficient solution for masking information of 3DMM. First, using the secret key, the original 3DMM is encrypted. Second without procuring any prior information of original 3DMM it is conceivable mask information on encrypted 3D mesh models. Third, the original 3DMM are reconstructed by extracting masked information. The existing masking methods are not efficient in providing high information masking capacity in reversible manner and are not robust. For overcoming research issues, this work models an efficient data masking (EDM) method that is reversible nature. Experiment outcome shows the EDM for 3DMM attain better performance in terms of peak signal-to-noise ratio (PSNR) and root mean squared error (RMSE) over existing data masking methods. Thus, the EDM model brings good tradeoffs between achieving high data masking capacity with good reconstruction quality of 3DMM.

Corresponding Author:

Manikamma Malipatil
Department of Computer Science and Engineering
Sharnbasva University
Vidya Nagar, Kalaburagi, Karnataka, India
Email: manikamma_malipatil@rediffmail.com

1. INTRODUCTION

In last decade, wide verity of tool has been employed for processing 3D mesh models (3DMM) with good result. Meshes are generally represented as a two dimensional surface sets defined within the three dimensional space. The 3DMM are widely used across various application right from gaming, biomedical to heritage, and 3D printing. 3D printing (3DP) technology has advanced toward the modern world. However, its significance was not broadly perceived until the beginning of 21st century. Nonetheless, it is presently quite evident that 3DP technology will affect numerous businesses. Number of research materials that has been published in news articles and the private segment stress the significance of 3DP in different segments. As quoted in [1], the 3DP market is expected to surpass 20 billion US dollars by 2020. Nonetheless, 3DP presents many copyright violation problems for computerized 3D mesh (3DM) models. Since, the 3D models can be printed directly and circulated physically or through web [2].

Provisioning security for multimedia data plays an important part in every areas, particularly in areas where strict security measure is required such as medical diagnosis, and military surveillance. With

advancement of cloud computing (CC), the development in data innovation has prompted genuine security issues where privacy, authenticity and trustworthiness are continuously compromised, by criminal and malicious operations such as replicating and vindictive utilization of data. The objective of cryptography design is for ensuring information privacies by completely or partly randomizing the data of 3D mesh models pictures [3]. For storing or communication of encrypted 3D mesh models, it is frequently important to investigate and process them without prior knowledge of source data and master key utilized for encrypting purpose [4]. As 3D mesh models is increasingly being utilized in wide range of applications. For example, virtual reality, medical diagnosis, 3D movies, and computer aided design (CAD), the need to secure the copyright and authenticity of 3D mesh models is turning out to be very important [5]. Watermarking method has turned out to be an effective method for protecting the copyright and authenticity of 3D mesh models [6].

Recently, number of watermarking and steganography methods [7], are presented for securing 3D mesh models. The watermarking (WM) method techniques is composed of two classes such as frequency and spatial domain. In frequency domain [8]-[10], the WM data is embedded by changing its coefficients. In, spatial domain [11]-[15], the WM data is embedded by modifying geometry properties of 3D mesh models (3DMM). In [8], exhibited a WM method for 3DM model, and WM is embedded in wavelet coefficients (WC) considering diverse resolutions size. In [15] presented a security technique where WM is embed into to mesh model by modifying the ordinary vectors of the WC. In [15] determined the root mean square (RMS) curve of each vertex in its neighborhood region and separated the vertices into windows. For embedding WM data, the curve variance estimations of the vertices of every window were controlled. The existing WM techniques for 3DMM's have attained great exhibitions and has effectively tackled some problematic issues. In particular, methods of fragile watermarking based data masking (DM) in the cryptography system have been modelled for information improvement, verification, and authenticity in the cryptography system. For example, in CC environment the 3D mesh models are first encrypted without having any prior knowledge of source mesh data or the secret key utilized for carrying out encryption operation. It is then conceivable to mask a privacy information in the encoded picture. In decryption stage, the actual mesh models can be recovered efficiently and privacy information retrieved must be with good quality (i.e., with minimal or no error). Thus, there exists tradeoffs among reconstruction 3D mesh quality and masking capacity. For brining such tradeoffs various watermarking method are presented in literature. For extensive it is seen the existing model presented so far for masking data in 3D mesh models induces low masking capacity and reconstruction quality are very poor. Further, very limited work is carried out for masking information on encrypted 3D models. For overcoming research problems, this work present an improved data masking (i.e. watermarking algorithm) method for 3D mesh models. The model bring good tradeoffs between achieving higher masking capability with improved reconstruction quality.

The contribution of research work is as shown in:

- Presented efficient data masking method that brings good tradeoffs between embedding capacity and reconstruction quality.
- EDM method attain higher embedding capacity and higher quality recovery mesh and error-free extraction compared with the existing state-of-the-art data masking method [16].

The manuscript is organized in following structure. In section, the detailed survey of existing security method for image is described. In Section 3 the proposed efficient data masking method for securing 3D mesh models. The experiment outcome achieved is described in Section 4. The conclusion and future work is discussed in last section.

2. LITTERATURE SURVEY

This section present an extensive survey of various state-of-art existing data masking method for securing 3D mesh models. Both 3D meshes and 3D point cloud are fundamental portrayals of 3D models. As of late, a great deal of WM methods for 3DM models are being modelled. In [17], polygon mesh models are utilized across different places because of its superior versatilities and reliability. The perceptual abilities and also the visual knowledge of the watermarking model are frequently themed to falsification at each level, as the watermarking model frequently endure different levels of signal processing dealing out for the persistence of deformation, transmission, generalization and storage, perceptual abilities and also the visual practice of the 3DMM are frequently subjected to misrepresentation (i.e., distortion) at each level. Thus examining the perceptual accuracies and the visual knowledge of 3DMM has developed as one of the most difficult and challenging jobs for both the educational and industrial purpose. In [18], gives an easy as well as effectual security method, for data masking thru two standard 3D data masking methods [19]. The major factor is that at the time building efficient model the variances of [19].'s regularized histogram bins (HB) are projected to show Gaussian distribution (GD), in an established model there distribution must be bimodal. Further, they improved [20] WM methods thru data masking by modifying the histogram of the circular matches of the

vertices sets. Other than aiming on a continuous statistical properties as variance of the values in a HB, the WM alters a discrete statistical properties (i.e., the altitude of HB for attaining information hiding.

In dataset of 3D mesh models of off formats [21], proposed efficient WM method for three dimensional point cloud (PC) prototypes with the help of feature vertex sets to find the hidden/masked data. The vertex set with higher mean curvature are measured for obtaining feature vertex set that composed of masked data. Similarly, non-feature vertex set is utilized to form a coordinate framework (CF) in which the three dimensional PC prototype is categorized into bins that composed of having various longitudinal information. Every bit of the WM info is iteratively masked into a bin thru changing azimuth angles of feature vertex set within the bin. Non-feature vertex sets is utilized for masking the WM data, this allows the assembled CF for avoiding the effect of the masking of WM. The selection of masking location and redundant masking gives an ideal stability within noiselessness and robust nature of data masking method. Similarly, in [22] presented an efficient WM method for 3D PC models using vertex curvature for attaining and bringing good trade-offs among robustness and transparency. In [23], showed importance of building efficient 3DMM for safeguarding industrial products. They presented a flexible selection of masking location for data masking of 3DMM with minimal disturbance produced by the data masking method. In [24]-[26] presented an efficient error-free and divisible data masking method for encrypted image that is reversible in nature. However, these method cannot be applied for masking 3DMMs as they are designed only for masking 2D images.

As of late, numerous strategies have been planned. The embedding are done before or after carrying out encryption operation. In decryption process, the 3D mesh models are reconstructed and embedded information can be handled simultaneously [26] or independently [26]-[28]. None of the existing method could bring good tradeoffs between attaining high masking capacity with good reconstruction 3D mesh models quality. In [17] has masking capacity of 0:5 bits per pixel (BPP) and reconstruction quality of 40 dB. The reconstruction quality is measure in terms of peak-signal-to-noise ratio. Also, [26] attain a masking capacity 0:1 BPP. Further, in existing DM method, the information is embed using least significant bit (LSB) substitution. Nonetheless, in cryptography system using these state-of-art method, it is hard to distinguish if a picture is composed of masked information or not. Since pixels value exhibits pseudo randomness. Further, in recent time wide research on data hiding (DH) for multimedia and 3D mesh models has been going on. The method presented so far has resulted in more ideal strategies theoretically. However, for 3D mesh models, the research activity is at very early stage. With increased usage of 3D mesh model based application has with increased capacity, 3D mesh model is significantly utilized and shared through web oriented application. Thus, has led researcher in building DM. From deep rooted survey it can be seen building efficient data masking method for 3D mesh model is challenging. Existing model suffers in providing tradeoffs between high embedding capacity and SNR. Further, due to the large ciphertext expansion and high computational complexity of existing security system. Thus, it not efficient in practice. Thus, this paper aims to improve the embedding ability and quality of the recovered mesh, and realizes error-free extraction of the data.

3. EFFICIENT DATA MASKING METHOD FOR ENCRYPTED 3D MESH MODELS

This work present an efficient watermarking method for 3D mesh model. The architecture of proposed efficient data masking method (EDM) method is shown in Figure 1. The architecture is composed of preprocessing phase, error identification prediction phase, encryption phase, data masking phase, data decryption and data reconstruction phase.

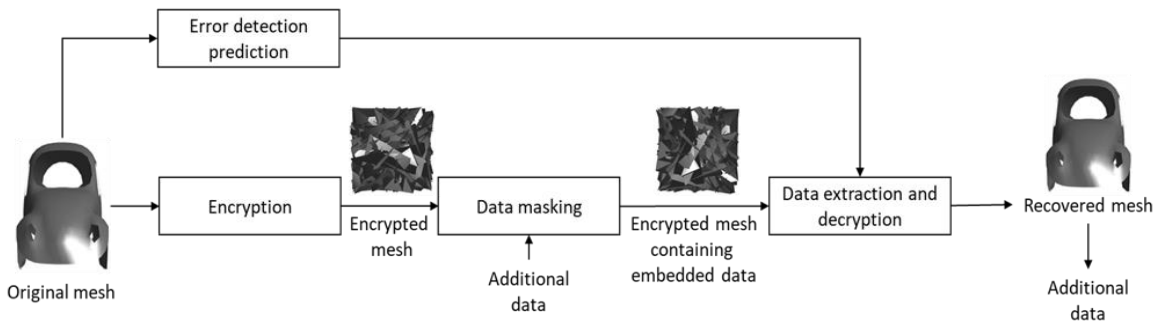


Figure 1. Architecture of proposed efficient data masking method for 3D mesh model

3.1. Preprocessing of 3D mesh models

Generally, the mesh file formats such as OFF represent an indexed data structure. The three dimensional i.e., triangle meshes is consist of two elements such as vertex data (VD) and face (connectivity) data (FD). VD is composed of coordinate position information of vertices. Further, VD may also have photometric information for example colors and generic vectors. The FD provides information of topology structure that depicts which vertices belongs to which triangles. Let $\{w_j\}_{j=0}^{O}$ depicts the set of vertices present during mesh traversing, where

$$w_j = (w_{j,a}, w_{j,b}, w_{j,c}) \quad (1)$$

and O is the vertices size. An important thing to be noted here is that every coordinates $w_{j,k} < 1, k \in \{a, b, c\}$. In general, the uncompressed (UC) form of mesh models (MM's) depicts vertex coordinate (VC) as a $32-$bit floating-point (FP) size. Further, the size of every VC's important parameter is 6. First, within an axis-aligned bounding box (BB) the positions are normalized. Second, uniformly the coordinates are quantized to l bits with certain accuracies. Thus, they can be described as integer form within 0 and$2^l - 1$. Empirically, $l \in [1, 33]$. For every coordinate $w_{j,k}$ of a vertex, it is normalized to $w''_{j,k}$ as described in (2).

$$w''_{j,k} = \lfloor w_{j,k} * 10^l \rfloor, k = a, b, c. \quad (2)$$

Thus, this work modelled 3D mesh models encryption, mesh data masking, mesh decryption and mesh data extraction using $w''_{j,k}$. For constructing managed meshes, the model transform the managed integral coordinates of vertices $\bar{\bar{w}}''_{j,k}$ to decimal coordinates $\bar{\bar{w}}_{j,k}$ in reversible manner $\bar{\bar{w}}_{j,k}$

$$\bar{\bar{w}}_{j,k} = \frac{\bar{\bar{w}}''_{j,k}}{10^l}, j = a, b, c. \quad (3)$$

The parameter l impacts the computation overhead of every stage of the building efficient watermarking method of encrypted mesh model. This stage is composed of mesh encryption, data masking, mesh decryption, data extraction, and mesh recovery. Along with, parameter l defines whether a 3D mesh models can be reconstructed in lossless nature to its actual mesh forms, and the threshold is represented l_{th}.

3.2. Error identification prediction

The source user traverses entire vertices in FD's of 3D mesh in an ascending order, and calculated masked set T_f and source set T_o according to topological information among vertices. Source traverses the initial vertex in the FD and add this vertex to T_f, establish its neighboring vertices and add them to T_o. The masked set T_f is used to mask additional data, and the source set T_o is utilized to recover/reconstruct the mesh without need of modifying the vertices during the entire procedure.

3.3. Encryption of 3D mesh models

This work considers preprocessed vertices, and signify the bits of an element of a vertex as $d_{j,k,0}, d_{j,k,1}, \ldots, d_{j,k,l}$, where $1 \leq j \leq O$ and $j \in \{x, y, z\}$. This infers that

$$d_{j,k,v} = \lfloor w''_{j,k}/2^v \rfloor \text{mod} 2, v = 0,1, \ldots, l. \quad (4)$$

The data owner then selects an encryption key L_1 using chaotic sequence for generating pseudo-random bits utilizing stream cipher (SC) function, and perform encryptions of the bitstream of the preprocessed 3D mesh models using (5).

$$f_{j,k,v} = d_{j,k,v} \oplus l_{j,k,v}, v = 0,1, \ldots, l \quad (5)$$

where $l_{j,k,v}$ depicts key stream bits, $d_{j,k,v}$ depicts constructed cipher data, and $\oplus$ represent exclusive OR (XOR). Thus, the encrypted integral 3D mesh models can be constructed using (6).

$$F_{j,k} = \sum_{v-1}^{l} f_{j,k,v} \cdot 2^v \quad (6)$$

where $F_{j,k}$depicts integral parameter of coordinate sets, $1 \leq j \leq O$ and $k \in \{a, b, c\}$. An important thing to be seen here is that the SC in (4) scrambles coordinate values. However, it does not scramble the location of coordinates.

3.4. Data masking of 3D mesh models

Possessing encrypted information of 3D mesh models, the data masker does not have any knowledge of the actual mesh data. Further, the masker can mask an additional data into the3D mesh by changing a certain portion of the encrypted mesh content. For masking the data into mesh model is selected based on following condition. Since a vertex is limited within numerous triangle sets, once if any modification is done to a vertex for masking data, the neighboring vertices must not be changed and is utilized to reconstruct the principal vertex by neighboring correlation at the end user. Thus, for data maskers, firstly they must segment the vertices into 2 sets namely the "masked" set and the "source" set. The "masked" set is utilized for masking message and the "source" set is utilized for reconstructing the neighboring "masked" message at the end user side. Data masking in masked set: This work takes a data masking key L_2 to encrypt the masked content. For every masked vertex (MV) in the masked set T_f in the encrypted integral mesh, if the added bit d to be masked is 0, no adjustment is required for 3 coordinate sets. Along with, if the added bit to be masked is 1, the model optimize the n least significant bits of the 3 coordinate sets $f_{j,k,v}$ to the opposite parameter as shown in (7).

$$f''_{j,k,v} = f_{j,k,v} \oplus d, f_{j,k,v} \in T_f, k \in \{a, b, c\}, and\ v = 0,1, \dots, n-1. \quad (7)$$

The other encrypted content are not modified. An important thing to be noted n impacts the quality of decryption process of the 3D mesh models. Along with, impacts the mean precision of the data extraction. This work utilize bits per vertex (bpv) for measuring the masking rate E, which is equal to the size of masked bits separating the size of vertices, and;

$$E = \frac{\|T_f\|}{\|T_f\| + \|T_o\|} \quad (8)$$

As errors may arise, error correction codes (ECCs) is used and cause a dip in masking capacity. Prior to data masking, error correction codes are utilized for encoding the plain data bits. Considering that $[o, l]$ codes is utilized, a overall of E_q plain bits can be masked into the bitstream, where:

$$E_q = \lfloor \|T_f\| \cdot l/o \rfloor \quad (9)$$

Therefore, the real size of bits masked into the bitstream are described using (10).

$$E_f = \lfloor \|T_f\| \cdot l/o \rfloor \cdot o/l \quad (10)$$

This work represents E_f the masking capacity, and E_q the actual capacity that is the capacity of the plaintext bits. Then, the plaintext bits $Q = \left[Q_1, Q_2, Q_{3,}, \dots, Q_{E_q}\right]$ are coded into $U = \left[U_1, U_2, U_{3,}, \dots, U_{E_f}\right]$

$$U = ECC(Q) \quad (11)$$

where error correction codes denotes an error correction function. Several error correction codes algorithms can be utilized to guarantee accurate construction of the secret content. The actual masking rate E_o is the actual masking rate post completing error correction codes,

$$E_o = \frac{E_q}{\|T_f\| + \|T_o\|} \quad (12)$$

3.5. Decryption and data extraction method

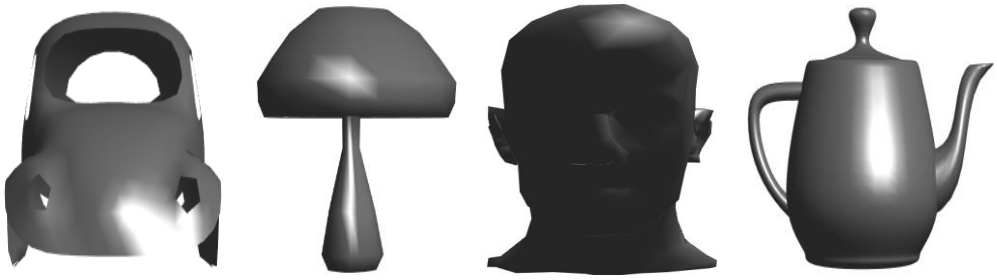
For an encrypted 3D mesh models composed of masked content, an end user first produces $l_{j,k,v}$ based on encryption key L_1, and computes the XOR of the obtained content and $l_{j,k,v}$ to perform decryption of 3D mesh models. If the end users possess the data masking key L_2, the end user will extract the masked bits and reconstruct the actual 3D mesh content from the decrypted meshes. This work exploits spatial correlation among adjacent coordinate sets for achieving good masking rate. Since the general 3D mesh models composed of series of flat triangles neighboring to each other around the examination point. Experiments are conducted to evaluate the proposed water marking method for 3D mesh model. Our model is robust against noise with minimal error which shown experimentally shown in next section.

4. RESULT AND DISCUSSION

The experiments are conducted on windows 10, 64-bit i-5 quad core processor with 12 GB RAM. The proposed watermarking model is implemented and executed using MATLAB R2018b. We download 3D mesh models with off format from [27], [28]. The additional data masked in the mesh is a randomly generated 0/1 sequence. The data masking process causes distortion to the original mesh models, which cannot be observed by the naked eye. Therefore, RMSE and signal-to-noise ratio (SNR) are used to measure the geometric distortion of the mesh model. The geometrical distortion of a mesh after introducing some random noise to the 3DMM's are estimated using signal-to-noise ratio (SNR) described in (13).

$$SNR = 10 * lg \frac{\sum_{j=1}^{O}\left[\left(w_{j,a}-\bar{\bar{w}}_a\right)^2+\left(w_{j,b}-\bar{\bar{w}}_b\right)^2+\left(w_{j,c}-\bar{\bar{w}}_c\right)^2\right]}{\sum_{j=1}^{O}\left[\left(h_{j,a}-\bar{\bar{w}}_a\right)^2+\left(h_{j,b}-\bar{\bar{w}}_b\right)^2+\left(h_{j,c}-\bar{\bar{w}}_c\right)^2\right]} \quad (13)$$

where $\bar{\bar{w}}_a, \bar{\bar{w}}_b, \bar{\bar{w}}_c$ are the average of the mesh coordinates, $w_{j,a}, w_{j,b}, w_{j,c}$ are the original coordinates, $h_{j,a}, h_{j,b}, h_{j,c}$ are the modified mesh coordinates value, O is the number of vertices. Experiments are conducted for 3D mesh model shown in Figure 2. The outcome achieved by proposed high-capacity data masking method in terms of RMSE and SNR is shown in Table 1. Figure 3 shows the visual effects of encrypted, data masked and mesh recovery. The difference between the original and recovered meshes is not visible to the naked eye, which means we get a higher quality recovered mesh. Then in Table 2, comparative analysis of proposed and existing watermarking method [28] in terms of RMSE and SNR is shown. Table 2 and Figure 4 illustrate that the proposed EDM method attain better SNR performance than existing method. An average SNR performance improvement of 59.09% and 61.35% is attained by EDM over other existing methods respectively. Similarly, Table 2 and Figure 5 illustrate that the proposed EDM method get better RMSE performance than other existing method. An average RMSE reduction of 14.974% and21.462% is attained by EDM over other state of art techniques respectively.

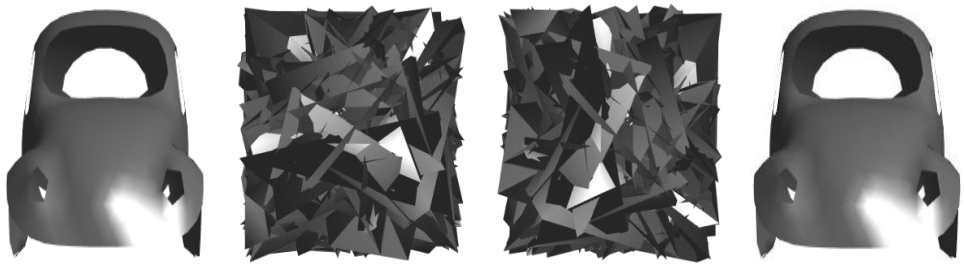


(a) (b) (c) (d)

Figure 2. 3D mesh model used for experiment analysis for (a) beetle, (b) mushroom, (c) mannequin and (d) teapot

Table 1. Performance attained by proposed EDM method

3D mesh models	SNR	RMSE
Beetle	158.089	51.1494
Mushroom	87.322	49.0566
Mannequin	92.4847	46.5753
Teapot	95.746	48.7671
Average	108.41	48.89



(a) (b) (c) (d)

Figure 3. The visual effects of different stages of each mesh: (a) actual mesh, (b) encrypted mesh, (c) marked encrypted mesh and (d) recovered mesh

Table 2. Performance attained by proposed EDM over existing data masking method

Method	SNR	RMSE
Feng *et al.*, [23]	41.9	62.25
Liu *et al.*, [5]	44.35	57.5
EDM	108.41	48.89

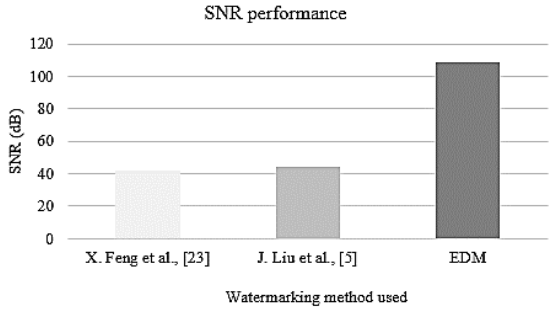


Figure 4. SNR performance of proposed efficient data masking method over existing data masking methods

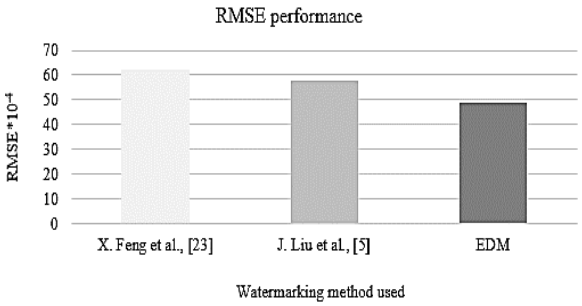


Figure 5. RMSE performance of proposed efficient data masking method over existing data masking methods

5. CONCLUSION

Recently, data masking for 3D mesh models has attained wide attention across various research community. This is because of adoption of cloud computing (CC) platform for storing customer information. Thus, preserving privacy of customer information is a major research problem. Nonetheless, no prior work permit masking with high capacity in reversible nature. For addressing research problem, this paper presented an efficient 3DMM data masking method that is reversible in nature with a very high masking capacity and reconstruction quality. Our method highlights not only feasible and efficient reversible data masking in 3D meshes also a balance between capacity and distortion. Firstly, the sender maps vertex coordinates to integer values, and uses bitstream encryption algorithms to encrypt the 3D mesh. Then, the LSB of masked vertex coordinate is replaced by additional data. Since our method is separable, the recipient can use the DH key for extracting the information and use the encryption key to recover the original mesh separately. The performance of data masking method is measured in terms of PSNR and RMSE. Experiments outcome show that EDM method has higher embedding capacity and higher quality recovery mesh and error-free extraction compared with the existing state-of-the-art data masking method. Future work would consider development of 3D mesh watermarking algorithm for 3D mesh objects with improved key based security mechanism. The model will be designed considering using spatial correlation of the original mesh, recipient can perfectly predict the LSB of the masked vertex by the LSB of the adjacent vertices around the masked vertex. Then, evaluate proposed watermarking algorithm over existing watermarking algorithm for 3D mesh models in terms of embedding capacity, and computation overhead.

REFERENCES

[1] A. Zaleski, "Here's why 2016 could be 3D printing's breakout year," *Techical Report*, 2015.
[2] J. Hou, D. Kim, W. Ahn and H. Lee, "Copyright Protections of Digital Content in the Age of 3D Printer: Emerging Issues and Survey," in *IEEE Access*, vol. 6, pp. 44082-44093, 2018, doi: 10.1109/ACCESS.2018.2864331.
[3] W. Trappe and L. C. Washington, "Introduction to cryptography with coding theory," *Pearson Education India*, 2006.
[4] Z. Erkin *et al*, "Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing," *EURASIP Journal on Information Security*, vol. 2007, no. 17, pp. 1-20, 2007, doi: 10.1155/2007/78943.
[5] J. Liu, Y. Yang, D. Ma, Y. Wang and Z. Pan, "A Watermarking Method for 3D Models Based on Feature Vertex Localization," in *IEEE Access*, vol. 6, pp. 56122-56134, 2018, doi: 10.1109/ACCESS.2018.2872783.
[6] X. Rolland-Nevière, G. Doërr and P. Alliez, "Triangle Surface Mesh Watermarking Based on a Constrained Optimization Framework," in *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 9, pp. 1491-1501, Sept. 2014, doi: 10.1109/TIFS.2014.2336376.
[7] G. N. Pham, S.-H. Lee, O.-H. Kwon, and K.-R. Kwon, "A 3D printing model watermarking algorithm based on 3D slicing and feature points," *Electronics*, vol. 7, no. 2, p. 23, Feb. 2018, doi: 10.3390/electronics7020023.

[8] K. Wang, G. Lavoue, F. Denis and A. Baskurt, "Hierarchical Watermarking of Semiregular Meshes Based on Wavelet Transform," in *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 4, pp. 620-634, Dec. 2008, doi: 10.1109/TIFS.2008.2007229.
[9] J. Hou, D. Kim and H. Lee, "Blind 3D Mesh Watermarking for 3D Printed Model by Analyzing Layering Artifact," in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2712-2725, Nov. 2017, doi: 10.1109/TIFS.2017.2718482.
[10] M. Hamidi, M. E. Haziti, H. Cherifi and D. Aboutajdine, "A robust blind 3-D mesh watermarking based on wavelet transform for copyright protection," *2017 International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, 2017, pp. 1-6, doi: 10.1109/ATSIP.2017.8075525.
[11] J. Liu, Y. Wang, Y. Li, R. Liu, and J. Chen, "A robust and blind 3D watermarking algorithm using multiresolution adaptive parameterization of surface," *Neurocomputing*, vol. 237, pp. 304-315, May 2017, doi: 10.1016/j.neucom.2016.12.065.
[12] Y. Wang, J. Liu, Y. Yang, D. Ma, and R. Liu, "3D model watermarking algorithm robust to geometric attacks," *IET Image Processing*, vol. 11, no. 10, pp. 822-832, Nov. 2017, doi: 10.1049/iet-ipr.2016.0927.
[13] X. Feng, W. Zhang, and Y. Liu, "Double watermarks of 3D mesh model based on feature segmentation and redundancy information," *Multimedia Tools and Applications*, vol. 68, no. 3, pp. 497-515, Feb. 2014, doi: 10.1007/s11042-012-1039-7.
[14] S.-M. Mun, H.-U. Jang, D.-G. Kim, S. Choi and H.-K. Lee, "A robust 3D mesh watermarking scheme against cropping," *2015 International Conference on 3D Imaging (IC3D)*, 2015, pp. 1-6, doi: 10.1109/IC3D.2015.7391820.
[15] Y.-Z. Zhan, Y.-T. Li, X.-Y. Wang, and Y. Qian, "A blind watermarking algorithm for 3D mesh models based on vertex curvature," *Journal of Zhejiang University SCIENCE C*, vol. 15, no. 5, pp. 351-362, May 2014, doi: 10.1631/jzus.C1300306.
[16] X. Wu and W. Sun, "High-capacity reversible data hiding in encrypted images by prediction error," *Signal Processing*, vol. 104, pp. 387-400, 2014, doi: 10.1155/2020/6989452.
[17] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption," in *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 3, pp. 553-562, March 2013, doi: 10.1109/TIFS.2013.2248725.
[18] D. Xu and R. Wang, "Separable and error-free reversible data hiding in encrypted images," *Signal Processing*, vol. 123, pp. 9-21, 2016, doi: 10.1016/j.sigpro.2015.12.012.
[19] Y. Yang, R. Pintus, H. Rushmeier, and I. Ivrissimtzis, "A 3D Steganalytic Algorithm and Steganalysis-Resistant Watermarking," in *IEEE Transactions on Visualization and Computer Graphics*, vol. 23, no. 2, pp. 1002-1013, Feb. 2017, doi: 10.1109/TVCG.2016.2525771.
[20] L. Li, H. Li, W. Yuan, J. Lu, X. Feng, and C. -C. Chang, "A Watermarking Mechanism With High Capacity for Three-Dimensional Mesh Objects Using Integer Planning," in *IEEE MultiMedia*, vol. 25, no. 3, pp. 49-64, July-Sept. 2018, doi: 10.1109/MMUL.2018.112142343.
[21] Dataset of 3D mesh models of off formats, [Online]. Available at: http://shape.cs.princeton.edu/benchmark/index.cgi
[22] L. Jing, Y. Yajie, M. Douli, H. Wenjuan, and W. Yinghui, "A novel watermarking algorithm for three-dimensional point-cloud models based on vertex curvature". *International Journal of Distributed Sensor Networks*, vol. 15, no.1, p. 155014771982604, 2019, doi: 10.1177/1550147719826042.
[23] X. Feng, "A new watermarking algorithm for point model using angle quantization index modulation," in *Proceedings of the 2015 4th National Conference on Electrical, Electronics and Computer Engineering*, Xi'an, China, 2016, pp. 962-968.
[24] Y. Yu, F. Yang, H. Liu, and W. Zhang, "Perceptual Quality and Visual Experience Analysis for Polygon Mesh on Different Display Devices," in *IEEE Access*, vol. 6, pp. 42941-42949, 2018, doi: 10.1109/ACCESS.2018.2859254.
[25] J. Cho, R. Prost, and H. Jung, "An Oblivious Watermarking for 3-D Polygonal Meshes Using Distribution of Vertex Norms," in *IEEE Transactions on Signal Processing*, vol. 55, no. 1, pp. 142-155, Jan. 2007, doi: 10.1109/TSP.2006.882111.
[26] Xu, Dawen, Kai Chen, Rangding Wang, and Shubing Su, "Separable reversible data hiding in encrypted images based on two-dimensional histogram modification," *Security and Communication Networks*, vol. 2018, 2018, doi: 10.1155/2018/1734961.
[27] Shie, Shih-Chieh. "A Steganographic Scheme Implemented on BTCCompressed Image by Histogram Modification." in *Proceedings of the International Conference on Information and Knowledge Engineering (IKE)*, The Steering Committee of The World Congress in Computer Science, Computer Engineeriang and Applied Computing (WorldComp), 2017, pp. 135-136.
[28] Mo, Qun, Heng Yao, Fang Cao, Zheng Chang, and Chuan Qin, "Reversible Data Hiding in Encrypted Image Based on Block Classification Permutation," *Cmc-Computers Materials & Continua*, vol. 59, no. 1, pp. 119-133, 2019, doi: 10.32604/cmc.2019.05770.