ORIGINAL RESEARCH PAPER
Volume - 10 | Issue - 09 | September - 2021 | PRINT ISSN No. 2277 - 8179 | DOI : 10.36106/ijsr
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

ROBUST ENCRYPTION AND MASKING TECHNIQUE FOR 3D MESH MODELS

Computer Science

Manikamma Malipatil* Department of Computer Science and Engineering, FETW,Sharnbasva University kalaburagi-585102. Karnataka,India. *Corresponding Author

Dr.Shubhangi D C Professor,Department of Computer Science and Engineering,VTU,center for PG studies, Kalaburagi-585105 Karnataka,India.

ABSTRACT

the 3D mesh model can display real-world information in intuitive manner for varied applications such as medical equipment, organs, and architecture models. Nonetheless, a 3D point cloud model shared through internet can be manipulated easily by unlicensed users; thus for protecting and providing security for 3D point cloud models, robust reversible data masking mechanism using homomorphic encryption (HE) is needed. Thus, here a robust encryption and masking (REM) technique for encrypted 3D mesh models based on prediction error modellingis presented. In REM the vertex are encrypted employing homomorphic encryption. Thus, can mitigate wide range of attack and work seamlessly well for different kind of 3D mesh models and data formats well. Experiment are conducted using diverse set of 3D mesh models with different formats such obj and off.The REM technique achieves high masking capacity with reduced reconstruction error and high quality 3D mesh model reconstruction in comparison with other recent data masking methods.

KEYWORDS

3D mesh models, Cloud computing, Cryptography,Data hiding, Homomorphism, Watermarking method.

I. INTRODUCTION

With growth and adoption of cloud technology for storage and computing models have resulted in increased sharing of 3D mesh models. Providing effective data masking is the preliminary requirement of cloud-based 3D mesh models [1–4]. Nonetheless, cloud cannot perform data masking to original 3D mesh models during masking process. Thus, reversible data masking mechanism is needed [5].Along with, data masking/watermarking are vulnerable during transmission and they are expected to resist general attacks [6]. As a result, reversible data masking mechanism for encrypted mesh model have attracted researcher for different applications.

Generally, the data masking method are of two types such as fragile and robust data masking mechanism. The robust data masking mechanisms [7], [16]-[19] are used for safeguarding and attacks and fragile data masking method [8] are used for providing integrity during authentication process. In order to provide higher security level in field of medical domain and judicial authentication most of existing method have focused of fragile data masking method for encrypted mesh models.

Reversible data masking mechanism for encrypted mesh model is generally are of two types such as Reserving Room BeforeEncryption (RRBE) and Vacating Room After Encryption (VRAE). The architecture of RRBE and VARE model is shown in Fig. 1 and Fig. 2, respectively.

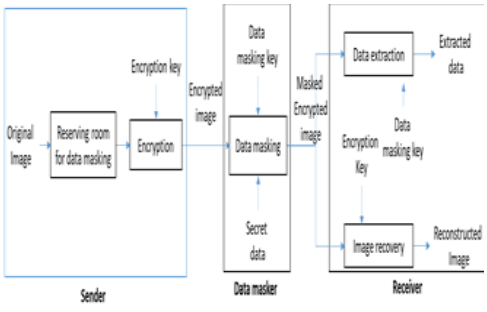


Fig. 1.The architecture of RRBE model.

The RRBE models reservesembedding room prior to perform encryption operation on the original multimedia content [9], [10]. With the expansion of reversible data masking mechanisms [11], the original imagecan be reconstructed efficiently after extraction of data masking information. The VRAE directly implementsdata masking by modifying the encrypted image [12] post completion of encryption. For example in [13] segmented the original image into blocks and encryption is done for each blocks, and then the histogram are computed in encrypted domain for optimizing masking information [13].

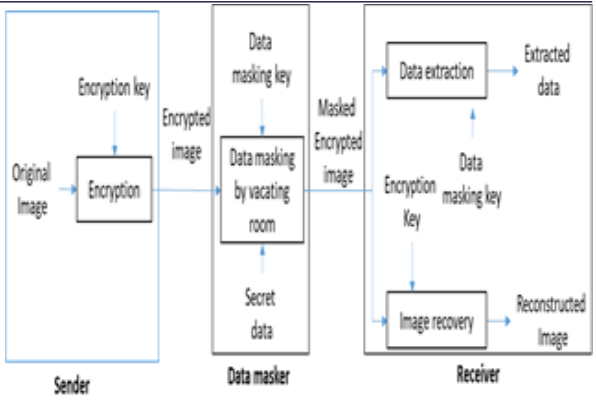


Fig. 2.The architecture of VARE model.

However, these models are used for multimedia data such as images; thus, will not be efficient (i.e., doesn't support) when applied for 3D models directlydue to structure variation among them. The generic reversible data masking architecture for 3D mesh model is shown in Fig. 3.

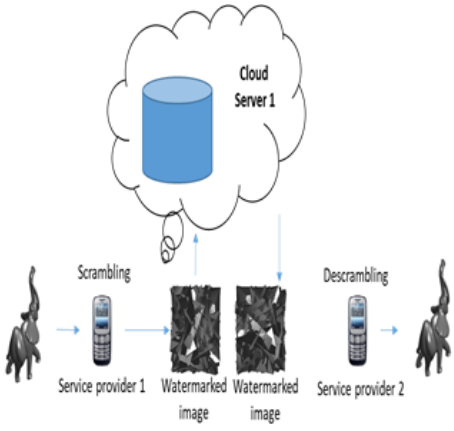


Fig. 3. Generic architecture of data masking methods for 3D mesh models.

In [14] segmented a 3D model into blocks, thendata masking is performed on each blocks by modulatingangle quantization [14]. Nonetheless, cannot provide reversible data masking mechanism. In [1] presented data masking method for encrypted mesh domain. The

data masking is done by reversing the least significant bits of the vertex coordinates by exploiting spatial correlation. In [2], presented data masking employing homomorphic encryption using VRAEmodel [2] as shown in Fig. 2.Nonetheless, those methods cannot protect their copyrights and are fragile to attacks. For overcoming aforementioned issues here we present robust encryption and data masking technique for 3D point cloud models. The REM technique achieves higher reconstruction quality with minimal error.

The paper is arranges as follows. In section, II robust encryption and data masking technique for 3D mesh models is presented. In section III, the outcome of REM over existing data masking method for 3D mesh model is discussed. Finally the research is conclude and future enhancement of data masking method are discussed.

II. ROBUST ENCRYPTION AND MASKING TECHNIQUE FOR 3D MESH MODELS

This section present robust encryption and masking technique for 3D mesh model. The architecture of proposed robust encryption and masking technique is shown in Fig. 4.

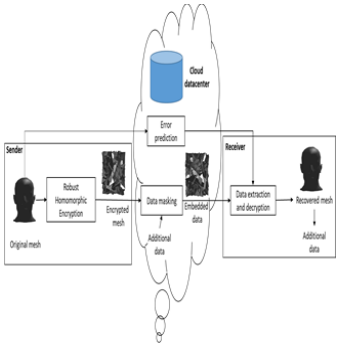


Fig. 4.Architecture of proposed robust encryption and masking technique for 3Dmesh model.

a) Preprocessing and error prediction of 3D point cloud models:

In preprocessing phase the mesh vertex coordinates are converted into integer representation for facilitating encryption and data masking in later stages.The 3D point cloud model is made of triangle faces and spatial vertices. The vertices set is described as follows

The vertices set is described as follows

$$W=\{W_1,W_2,\ldots,W_N\} \quad (1)$$

where each vertex coordinates is composed of

$$Wj=\{aj,bj,cj\}. \quad (2)$$

For every vertex W_j, the cumulated and normalization process is merged into following equation

$$Wj=\lfloor Wj*10^m \rfloor, \quad j=1,\ldots,N \quad (3)$$

where Wj is defined as follows

$$Wj=\{aj,bj,cj\}. \quad (4)$$

The encryption, decryption, data masking and information extraction is done using Wj

The accuracies of prediction error outcomes play very important role in achieving very good data masking performance. Here we employ spatial correlation among adjacent vertices for error prediction value w j as follows

$$\bar{\bar{w}}_j = \frac{1}{O_j}\sum_{k=1}^{O_j} \bar{\bar{w}}_k', \quad k \in (1, O_j), \quad (5)$$

where $\bar{\bar{w}}_k'$ is neighboring to vertex $\bar{\bar{wj}}'$ and wj is the prediction outcome of vertex $\bar{\bar{wj}}'$, Oj represent neighboring vertices size of vertex $\bar{\bar{wj}}'$. The prediction error of $\bar{\bar{wj}}'$ is computed using following equation

$$\delta wj=\bar{\bar{wj}}'-\bar{\bar{wj}}, \quad (6)$$

where δw_j represent the prediction error of w j'. δw_j is a 3D vector with random direction. The modulus size $|\delta w_j|$ is generally small and are maximum E as there exist spatial correlation; thus, the range of $|\delta w_j|$ is set as follows

$$|\delta wj| \in [o,E] \quad (7)$$

b) Encryption of 3D mesh models:

The preprocessed vertices $\bar{\bar{W}}j$ are represented into bits form asd $_{j,k,0,}$d $_{j,k,1,}\ldots,_{dj,k,l,}$ where $1 \le j \le O$and $j \in \{x,y,z\}$ using following equation

$$d_{j,k,v}=\lfloor w_{j,k}'')2^v \rfloor \bmod 2, v=0,1,\ldots,l. \quad (8)$$

Using public key generated through of homomorphic encryption [2], the data owner then randomly chooses value s for encrypting vertex $\bar{\bar{W}}j$ with public key(O,h) for generating pseudo-random bits

$$d_j=E[d_{j,k,v},s_j]=k^{dj,k,v}s_j^O \bmod O^2, \ j \quad (9)$$

where d_j defines the cipherdata obtained from plain 3D point cloud models $\bar{\bar{W}}j$.

c) Data masking for encrypted 3D mesh models:

Here we first we 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. This work take a data masking key L_2 to encrypt the masked content. For every masked vertex in the masked set T_fin the encrypted integral mesh, if the added bit dto 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 nleast significant bits of the 3 coordinate sets fj,k,v to the opposite parameter as described below

$$f''_{j,k,v} = f_{j,k,v} \oplus d, \quad f_{j,k,v} \in T_f, k \in \{a,b,c\}, and\ v = 0,1,\ldots,n-1. \quad (10)$$

The other encrypted content are not modified.

d) Decryption and mesh reconstruction:

The receiver can perform decryption of 3D point cloud model using its private key β using homomorphic encryption. The process of decryption of 3D point cloud model is obtained using following equation

$$w_j'' = \mathcal{E}[\bar{d}_j] = \frac{\mathcal{M}\left((\bar{d}_j)^\beta \bmod O^2\right)}{\mathcal{M}(h^\beta \bmod O^2)} \bmod O. \quad (11)$$

The REM model is robust against noise with minimal error which shown experimentally shown in next section.

III. EXPERIMENT RESULT AND ANALYSIS

Here experiment is conducted for evaluating REM technique and existing Coyote Optimization Algorithm (COA) [17] and Feature localization vector (FLV)-based watermarking [15] method. The REM technique is implemented using Matlab 2018. The Mesh model used in this work for evaluating REM is downloaded from [20], [21].The signal-to-noise ratio (SNR) and root mean square error (RMSE) are metrics used for measuring the quality of reconstructed 3D point cloud model [15], [17].

a) Beetle

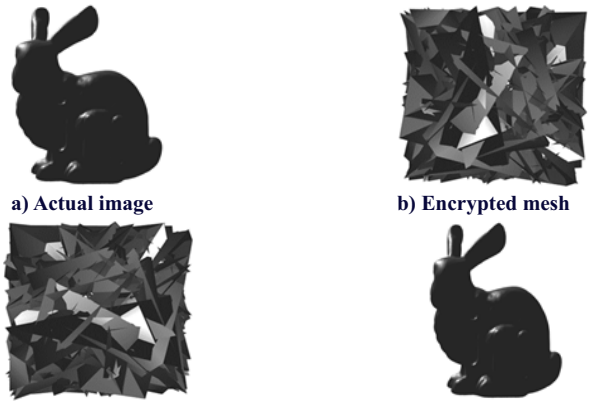
b) Bunny

c) Horse

d)Mannequin

e)Mushroom f)Teapot

Fig. 5.3D mesh model used for experiment analysis.



a) Actual image b) Encrypted mesh

c) Masked encrypted image d) Recovered mesh

Fig. 6. From left to right are the visual effects of different stages of each mesh: actual mesh, encrypted mesh, marked encrypted mesh, and recovered mesh.

Table 1: Performance attained by proposed REM method

3D mesh models	SNR	RMSE
Beetle	158.089	51.1494
Bunny	138.97	50.1475
Horse	137.83	53.9683
Mannequin	92.58	46.5753
Mushroom	87.96	48.89
Teapot	95.98	48.124
Average	**118.57**	**49.81**

Table 2: Performance attained by proposed REM over existing data masking method

Method	SNR	RMSE
J. Liu et al., [15]	44.35	57.5
COA [17]	114.75	81.25
REM	118.57	49.81

In this work experiment are conducted using 3D point cloud model described in Fig. 5. The outcome achieved for different phases for providing security to 3D point cloud model is shown in Fig. 6. The SNR and RMSE outcome attained by REM model is shown in Table I. In Table II comparative analysis of REM and other state-of-art data masking model is presented. In Fig. 7 graphical representation of SNR outcome of REM and other technique is presented. In Fig. 8 graphical representation of RMSE outcome of REM and other technique is presented. From experiment we can see that the proposed REM achieves higher reconstruction quality with less error. Thus, the REM model can be adopted for providing robust security environment such as for protecting medical data, diagnostic data etc.

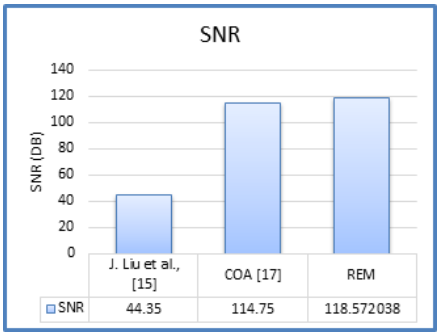


Fig. 7.SNR performance of proposed REM method over existing data masking methods.

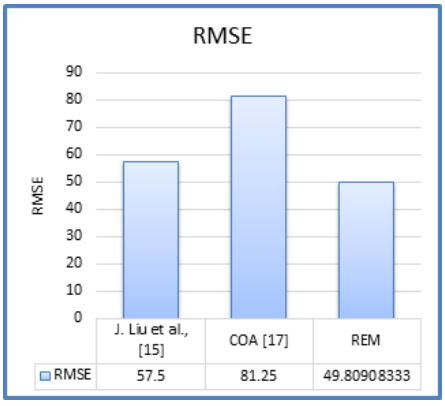


Fig. 8.RMSE performance of proposed REM method over existing data masking methods.

IV. CONCLUSION

In REM the mesh model represented in integer bit-stream for performing encryption using homomorphic encryption. Then, prediction error of the coordinates in the embedded sets are estimated using reference set. The REM is feasible and efficient and brings tradeoffs among capacity ad distortion. The receiver can use data masking key for reconstructing original 3D mesh models and private keys are used for reconstructing high quality 3D mesh model by exploiting spatial correlation of 3D point cloud models. Experiment outcome show REM achieves higher reconstruction quality with less error and maintain high level of embedding capacity in comparison with recent data masking methods.Future work would consider improving embedding capacity by effective selection of embedded sets.

REFERENCES

[1] Jiang, R.Q.; Zhou, H.; Zhang, W.M. Reversible Data Hiding in Encrypted Three-Dimensional Mesh Models. IEEE Trans. Multimed. 2018, 20, 55–67.
[2] Shah, M.; Zhang, W.M.; Hu, H.G. Homomorphic Encryption-Based Reversible Data Hiding for 3D Mesh Models. Arab. J. Sci. Eng. 2018, 43, 8145–8157.
[3] Wu, H.T.; Cheung, Y.M.; Tang, S.H. A high-capacity reversible data hiding method for homomorphic encrypted images. J. Vis. Commun. Image Represent. 2019, 62, 87–96.
[4] Xiang, S.J.; Luo, X.R. Reversible Data Hiding in Homomorphic Encrypted Domain by Mirroring Ciphertext Group. IEEE Trans. Circuits Syst. Video Technol. 2018, 28, 3099–3110.
[5] Liu, J.; Wang, Y.; Li, Y. A robust and blind 3D watermarking algorithm using multiresolution adaptive parameterization of surface. Neurocomputing 2017, 237, 304–315.
[6] Amini, M.; Ahmad, M.; Swamy, M. A Robust multibit multiplicative watermark decoder using vectorbased hidden markov model in wavelet domain. IEEE Trans. Circuits Syst. Video Technol. 2016, 1, 402–413.
[7] M. Malipatil and D. C. Shubhangi, "An Efficient 3D Watermarking algorithm for 3D Mesh Models," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2020, pp. 1-5, doi: 10.1109/I-SMAC49090.2020.9243381.
[8] Wu, Q.L.; Wu, M. Adaptive and blind audio watermarking algorithm based on chaotic encryption in hybrid domain. Symmetry 2018, 10, 284–295.
[9] Zhang, W.; Ma, K.; Yu, N. Reversibility improved data hiding in encrypted images. Signal Process. 2014, 94,118–127.
[10] Shiu, C.-W.; Chen, Y.C.; Hong, W. Encrypted image-based reversible data hiding with public keycryptography from difference expansion. Signal Process. Image Commun. 2015, 39, 226–233.
[11] Wu, H.T.; Cheung, Y.-M. Reversible watermarking by modulation and security enhancement. IEEE Trans. Instrum. Meas. 2010, 59, 221–228.
[12] Zhang, X.; Qian, Z.; Feng, G. Efficient reversible data hiding in encrypted images. J. Vis. Commun. Image Represent. 2015, 25, 322–328.
[13] Xiang, S.J.; Yang, L. Robust and reversible image watermarking algorithm in homomorphic encrypted domain. Ruan Jian Xue Bao/J. Softw. 2018, 29, 957–972.
[14] Feng, X. A new watermarking algorithm for point model using angle quantization index modulation. In Proceeding of the National Conference on Electrical Electronics and Computer Engineering, Xi'an, China, 12-13, December, 2015; pp. 962–968.
[15] 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.
[16] 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.
[17] A. Hadid, Mourad & Soliman, Mona & Darwish, Ashraf & Hassanien, Aboul Ellasdezrt. Watermarking 3D Printing Data Based on Coyote Optimization Algorithm 10.1007/978-3-030-59338-4_29, 2021.
[18] 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 59, no. 1 (2019): 119-133.
[19] Yuan, Wenqiang & Li, Hangkai & Li, Li & Feng, Xiaoqing & Lu, Jianfeng & Chang, Chin-Chen. A Watermarking Mechanism with High Capacity for 3D Mesh Objects using Integer Planning. IEEE MultiMedia. PP. 1-1. 10.1109/MMUL.2018.112142343, 2018.
[20] Dataset of 3D mesh models of .off formats. Available at: http://shape.cs. princeton. edu/benchmark/index.cgi, last access on: October 2019.
[21] Liu, Jing & Yang, Yajie & Ma, Douli & He, Wenjuan & Wang, Yinghui. A novel watermarking algorithm for three-dimensional point-cloud models based on vertex curvature. International Journal of Distributed Sensor Networks. 15. 155014771982604. 10.1177/1550147719826042, 2019.