High Secure Encryption and Masking Technique for 3D Point Cloud Models

Manikamma Malipatil, Dr.Shubhangi D C
Associate professor, Department of Computer Science and Engineering,
FETW,Sharnbasva University kalaburagi-585102 Karnataka, India
Professor, Department of Computer Science and Engineering,VTU,center for PG studies,
Kalaburagi-585105 Karnataka, India.

Abstract:
Robust reversible data masking (RRDM) mechanism for encrypted 3D point cloud model is a method that protect copyright information and privacy of data sharing in cloud environment. Generally, the organs, medical equipment, and building are built using 3D point cloud models. 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. This paper preset High Secure Encryption and Masking (HSEM) for 3D point cloud models. The HSEM first maps the vertex coordinates into bit-stream representation. Then, compute prediction errors for the vertices of the "embedded" set and perform encryption of bit-stream representation of 3D mesh model using robust homomorphic encryption (RHE). Using data hiding keys, several least significant bits (LSBs) are identified for masking information. Using encryption (i.e., private key) user can reconstruct the mesh using spatial correlation of 3D point cloud models. Experiment outcome shows the HSEM 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 point cloud models, Data masking, Homomorphic encryption, Reversible data hiding, Watermarking.

DOI: 10.24297/j.cims.2024.8.2

1. Introduction

With significant growth of 3D modelling and 3D printing technology, has resulted in increased generation of 3D point cloud models. The 3D point cloud models have been used in different range of applications such as 3D character scenes, 3D mechanic models, military geography 3D models, and medical 3D models [1]-[5]. Among these applications, the 3D point cloud model for 3D manufacturing and 3D printing provide wide significance and expensive because of huge investment and time-spent. Recently, the cloud computing environment has been adopted for designing and manufacturing of 3D mesh models [2]. Adoption of cloud environment offers significant cost reduction and faster modelling of 3D mesh models, but may induces copyright violations [19] as it can be easily copied and circulated in cloud environment [3], [4]. For providing

secure storage of 3D mesh models in cloud environment, the 3D mesh models are generally encrypted prior to uploading to cloud environment. Along with, copyright and authentication information are embedded into encrypted 3D point cloud model, generally employing reversible data masking (RDM) mechanism.

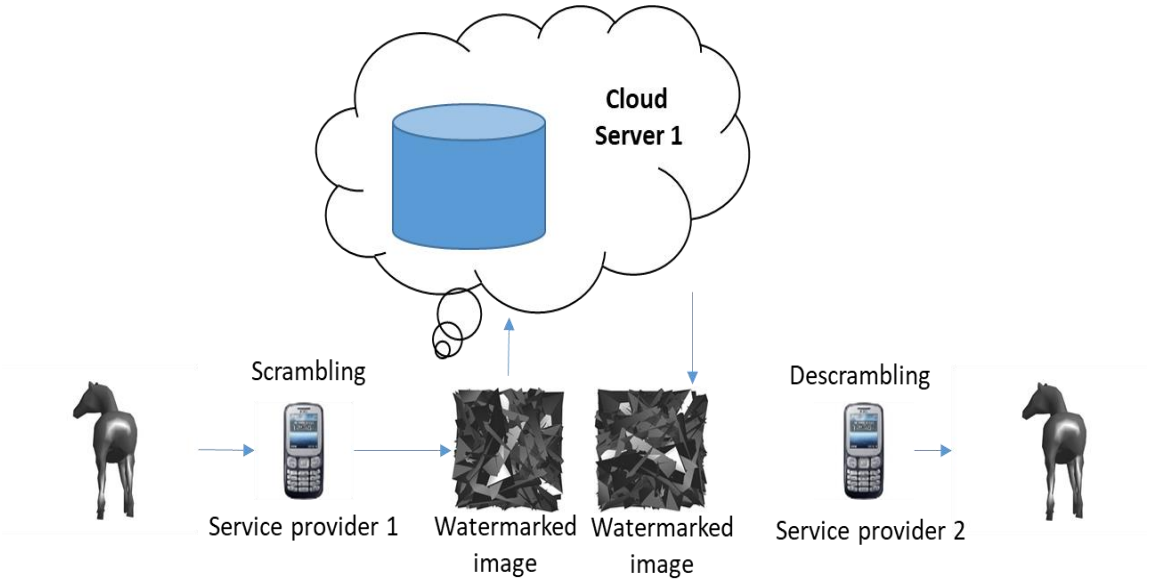


Fig. 1. General data masking architecture of 3D point cloud models.

A general application functionality for providing secure cloud storage is shown in Fig. 1. Here prior to uploading, the user scramble the 3D mesh model through encryption using service provider 1. Then, the cloud provider add masking information to the encrypted mesh models and store it in cloud environment. Then, user download the image from cloud environment through service provider 2 and decrypt and recover the original 3D point cloud mesh models.

For meeting above mentioned requirement, reversible data masking mechanisms have been employed for encrypted domain with possible solution. Initially, reversible data masking have been applied for encrypted multimedia data [20]. The objective of encryption is to scramble the information [6]-[10] and objective of reversible data masking mechanism is to distinctively embed information into multimedia data [11]-[13]. Initially, the reversible data masking for encrypted image [14] have been modelled in [15]-[16]. However, it cannot be directly applied for 3D point cloud models. Recently, some reversible data masking mechanisms for 3D mesh model have been presented [17]; however, it is not suitable for encrypted 3D point cloud model as there doesn't exist correlation among neighboring vertex coordinates. Thus, predicting neighboring coordinates becomes difficult. This issues led researcher to develop reversible data masking mechanism for 3D point cloud models. In [18] presented reversible data masking for encrypted 3D mesh model. Here they perform encryption of mesh through RC4 bit-stream encryption technique [18]. Then, by manipulating least significant bits they embed the information.

Embedding doesn't affect reconstruction quality [25]; however, the models are fragile to attacks and fails to protect their copyrights.

For overcoming research issues this paper present high secure encryption and masking (HSEM) technique for 3D point cloud models. Here we present a robust homomorphic encryption technique for performing encryption and decryption operation on 3D point cloud model. Then, this work employ data masking technique modelled in [18]. The data masking mechanism [27]-[29] first maps vertex coordinate in to integer representation, then perform bit-stream encryption using robust homomorphic encryption (i.e., using public key). Using data masking key, several least significant bits are masked into 3D mesh models. Presented error prediction mechanism to improve data masking accuracies [21]. Using data masking key, the receiver can recover content of mesh through spatial correlation that exist in 3D point cloud models and using decryption keys (i.e., private keys) high quality 3D mesh models can be reconstructed.

The HSEM technique can be adopted in applications of encrypted 3D mesh model is stored in cloud with preserved privacy. In comparison with images, the 3D point cloud models are extremely larger in size. Currently, the reversible data masking mechanism in non-separable in nature. However, the reversibility of encrypted 3D point cloud model offers cloud provider to manage mesh for masking information (in order to identify mesh owner identity and timestamp information etc.) without introducing any distortion to 3D mesh model or leaking any privacy information. Receiver can establish owner information and decrypt and recover high quality 3D mesh models. In this way, the cloud server can extract masked information without need for decrypting the meshes. Thus, enable cloud server to manage information to identify the mesh owner and timestamp for authenticating the integrity of encrypted 3D point cloud models [26].

The paper is arranged as follows. In section II, High secure encryption and masking technique for 3D point cloud models. In section III, the result achieved using HSEM and existing data masking technique is discussed. The research significance are concluded and future work for enhancing encryption and data masking model is presented in section IV.

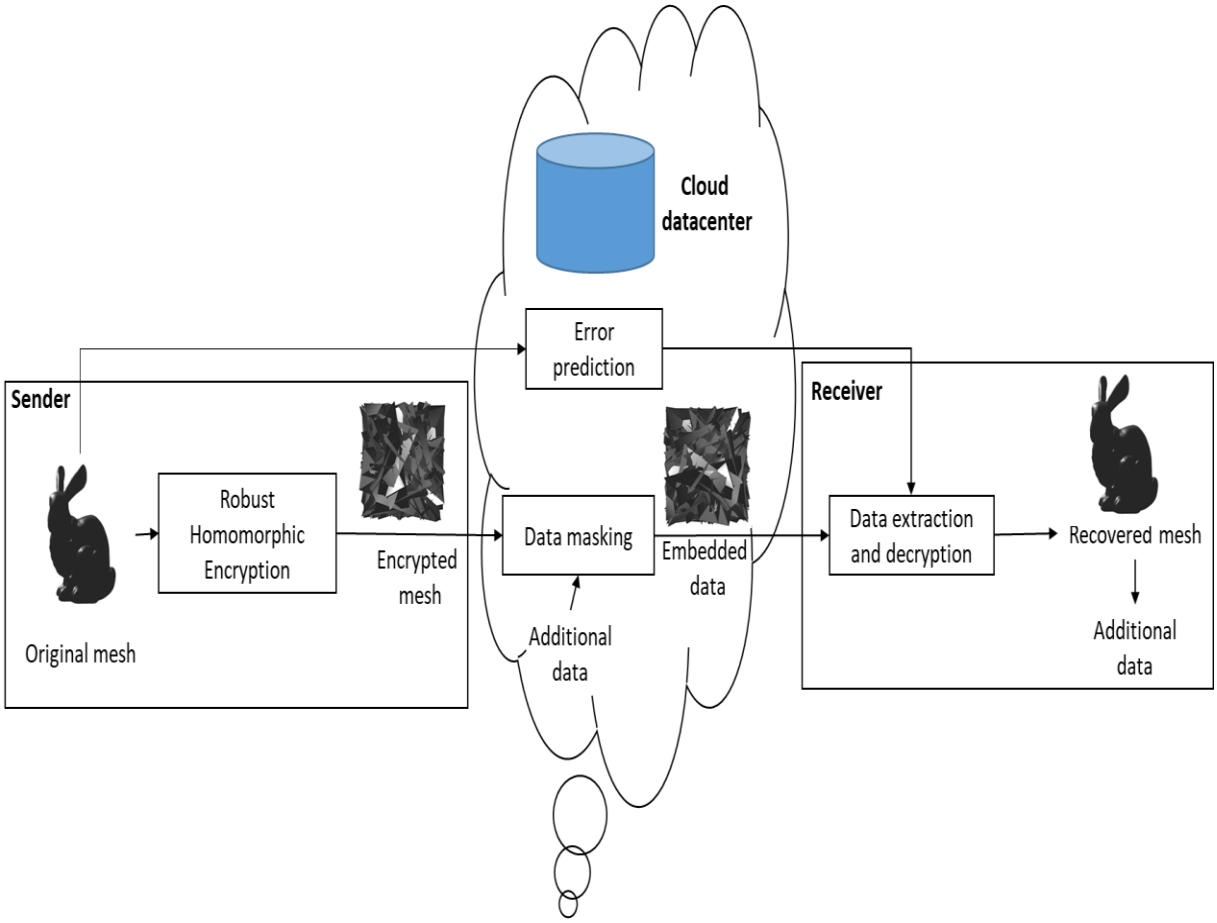


Fig. 2. Architecture of proposed efficient data masking method for 3D mesh model.

HIGH SECURE ENCRYPTION AND MASKING TECHNIQUE FOR 3D POINT CLOUD MODELS

This section presents High Secure Encryption and Masking (HSEM) Technique for 3D Point Cloud Models. First the system model HSE for 3D Point Cloud Models is presented. Then, 3D Point Cloud Models preprocessing technique prior to performing encryption and masking is presented. Third, encryption model for cipher generation is presented. Fourth, the process involved for performing data masking is presented. Finally, the reconstruction process for obtaining high quality 3D Point Cloud Models is presented.

a) Preprocessing 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. Generally, the vertex coordinates are defined as floating-point value; the values of the vertex coordinate varies significantly and are dependent on capturing device. The aforementioned characteristics makes encryption, masking, and mesh recovery a challenging task; thus, the coordinate values must be normalized.

The 3D point cloud model is made of triangle faces and spatial vertices. The vertices set is described as follows

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

where each vertex coordinates is composed of

$$W_j = \{a_j, b_j, c_j\}. \tag{2}$$

For easiness, the coordinates is represented as a matrix with dimension $M * N$, where $M = 3$ and N represent the column size. Generally, each vertex coordinate of an uncompressed 3D point cloud model is characterized with accuracies of 10^{-n}; from [24] it is seen that there are conditions where such high precision is not needed. Therefore, 64-bit floating value can be reduced to 16-bit floating value. The uncompressed vertex coordinates is defined as $d * 10^{-n}$, then the cumulated outcomes is defined by $\bar{\bar{c}} * 10^{-n}$, where $m \leq n$ and $\bar{d}$ is retained up to m weighted value of d behind the floating value. Finally, by dividing the quantization step 10^{-m} it is normalized as follows

$$\frac{\bar{d} * 10^{-m}}{10^{-m}} \tag{3}$$

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

$$\vec{W_j} = \lfloor W_j * 10^m \rfloor, \ \ j = 1, \dots, N \tag{4}$$

where $\vec{W_j}$ is defined as follows

$$\vec{W_j} = \{\bar{\bar{a}}_j, \bar{\bar{b}}_j, \bar{\bar{c}}_j\}. \tag{5}$$

Let every normalized vertex coordinates be in range of $0 - 2^e - 1$. Similar to [24], [31] in this work we consider $e \in [1,33]$. Therefore the encryption, decryption, data masking and information extraction is done using $\vec{W_j}$. Then, for generating processed meshes, here the integral coordinate of vertices $\vec{W_j'}$ are transformed inversely to obtain decimal coordinates $\vec{W_j}$

$$\vec{W_j} = \vec{W_j'} * 10^{-m}, \ \ j = 1, \dots, N \tag{6}$$

which can later be written to dedicated mesh formats and stored/shared in cloud computing environment.

b) Error prediction:

The source user traverses entire vertices in faces datas 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 faces datas 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.

c) Encryption of 3D mesh models:

Here we present a Robust Homomorphic Encryption (RHE) method for providing security to 3D point cloud model [29]. RHE is defined as the multiplication of two cipherdata of 3D point cloud models is identical with respect to sum of two respective plain 3D point cloud models. Using RHE we can use different parameter for performing encryption of same 3D point cloud models, but

still in can be decrypted for obtaining same plain 3D point cloud models. The RHE is composed of following phases such as key generation, encryption, decryption, and constraint for achieving robust encryption.

Key generation. First the model randomly select two large prime number x and y. Then, computed O using following equation

$$O = xy \tag{7}$$

and

$$\beta = L(x-1, y-1) \tag{8}$$

where L represent lowest common multiples (LCM). Then, randomly choose $h \in Z_{O^2}^*$ that satisfies constraint defined in following equation

$$G\left(M\left(h^{\beta} mod O^2\right), O\right) = 1, \tag{9}$$

where G defines greatest common deviser (GCD) among two inputs and $M(v)$ is obtained using following equation

$$M(v) = \frac{(v-1)}{O}. \tag{10}$$

The $A_{O^2}^*$ represent a number of A_{O^2} which is prime with O^2. The A_{O^2} is obtained through following equation

$$A_{O^2} = \{0,1,2,3, \ldots, O^2 - 1\}. \tag{11}$$

Lastly, the public key (O, h) and respective private key β is obtained.

Encryption. Randomly choose a value $s \in A_{O^2}^*$. The plain 3D point cloud models $n \in A_O$ is encrypted to obtain respective cipherdata d using following equation

$$d = E[n, s] = o^n * mod\ O^2, \tag{12}$$

where $E[*]$ defines the encryption process.

Decryption. The original plain 3D point cloud models n is obtained through following equation

$$n = D[d] = \frac{M\left(d^{\beta} mod\ O^2\right)}{M(h^{\beta} mod\ O^2)} mod\ O. \tag{13}$$

Properties/constraint for achieving robust encryption performance. This work considers the following properties/constraints for performing robust encryption and decryption operation. For any two plain 3D point cloud model $n_1, n_2 \in A_O$, estimate respective cipherdata d_1, d_2 with s_1, s_2 using Eq. (9), respectively. The condition $d_1 = d_2$ will be true provided if $n_1 = n_2$ and $s_1 = s_2$ are

true. For $\forall s_1, s_2 \in A_O^*$, two plain 3D point cloud models $n_1, n_2 \in A_O$ and respective cipherdata $E[n_1, s_1]$, $E[n_2, s_2] \in A_O^*$ satisfy following constraint

$$d_1 * d_2 = E[n_1, s_1] * E[n_2, s_2] = h^{n_1+n_2} * (s_1 * s_2)^O mod\ O^2, \tag{14}$$

$$E[d_1 * d_2] = D[E[n_1, s_1] * E[n_2, s_2] mod\ O^2] = n_1 + n_2 mod\ O. \tag{15}$$

Further, considering $n_1 - n_2$ of two numbers n_1, n_2 for performing encryption, the negative number i.e., $-, n_2$ must be stated as positive number i.e., $O - n_2$. Let $E[n_2]^{-1}$ represent the cipherdata of $O - n_2$, the cipherdata $E[n_2]^{-1}$ is computed using and modular multiplication inverse (MMI) Euclidean algorithm [30]. Thus, the resultant of $n_1 - n_2$ is as follows

$$E[n_1] * E[n_1]^{-1} mod\ O^2. \tag{16}$$

d) Encryption of 3D mesh models:

The preprocessed vertices $\vec{W}_j$ are represented into bits form as $d_{j,k,0}, d_{j,k,1}, \dots, d_{j,k,l}$, where $1 \leq j \leq O$ and $j \in \{x, y, z\}$ using following equation

$$d_{j,k,v} = \lfloor \frac{w''_{j,k}}{2^v} \rfloor mod 2, \qquad v = 0,1, \dots, l. \tag{17}$$

Using Eq. (10), the data owner then randomly chooses value s for encrypting vertex $\vec{W}_j$ with public key(O, h) for generating pseudo-random bits

$$d_j = E\left[d_{j,k,v}, s_j\right] = k^{d_{j,k,v}} {s_j}^O mod\ O^2, \ \ j \in \{a, b, c\} \tag{18}$$

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

The encrypted 3D point cloud models is reconstructed using following equation

$$F_{j,k} = \sum_{v-1}^{l} d_j \cdot 2^v \tag{19}$$

where $v = 1,2, \dots, l$, $F_{j,k}$defines integral parameter of coordinates, $1 \leq j \leq O$ and $k \in \{a, b, c\}$. Here only coordinates values are scrambled and coordinates location are kept unchanged.

e) 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 take 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 described below

$$f''_{j,k,v} = f_{j,k,v} \oplus d, \qquad f_{j,k,v} \in T_f, k \in \{a, b, c\}, and\ v = 0,1, \dots, n-1. \tag{20}$$

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

$$E = \frac{\|T_f\|}{\|T_f\| + \|T_o\|}. \tag{21}$$

As errors may arise, error correction codes (ECCs) is used and cause a dip in masking capacity. Prior to data masking, error correction codes is 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

$$E_q = \lfloor \|T_f\| \cdot \frac{l}{o} \rfloor. \tag{22}$$

Therefore, the real size of bits masked into the bitstream are described using following equation

$$E_f = \lfloor \|T_f\| \cdot \frac{l}{o} \rfloor \cdot \frac{o}{l}. \tag{23}$$

This work represent 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 $U = \left[U_1, U_2, U_{3,}, \dots, U_{E_f}\right]$

$$U = ECC(Q) \tag{24}$$

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

$$E_o = \frac{E_q}{\|T_f\| + \|T_o\|} \tag{25}$$

f) Decryption and data extraction method:

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

$$w''_j = E\left[\underline{d}_j\right] = \frac{M\left(\left(\underline{d}_j\right)^{\beta} mod\ O^2\right)}{M(h^{\beta} mod\ O^2)} mod\ O. \tag{26}$$

If the end user 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 exploit 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. Experiment are conducted to evaluate the proposed water marking method for 3D mesh model. Through experiment this work further shows that the proposed HSEM technique achieve high reconstruction quality with less error and masking efficiency.

2. Result And Discussion

Here experiment is conducted for evaluating HSEM technique and existing Coyote Optimization Algorithm (COA) [29] and Feature localization vector (FLV)-based watermarking [27], [24] method. The HSEM technique is implemented using Matlab 2018. The Mesh model used in this work for evaluating HSEM is downloaded from [22], [23]. Experiment is conducted on I-5 quad-core Intel Processor with 8GB RAM. Similar to [27] in this work we embed $16 * 16$ bits of information into different 3D point cloud models for validating robustness of HSEM model. The data masking process induces certain noise into original 3D point cloud models, which cannot be observed through visible eye. The signal-to-noise ratio (SNR) and root mean square error (RMSE) are metrics used for measuring performance. The quality of reconstructed 3D point cloud model is measured using SNR metric as follows [27]

$$SNR = 10 * lg \frac{\sum_{j=1}^{o} \left[\left(w_{j,a} - \bar{w}_a\right)^2 + \left(w_{j,b} - \bar{w}_b\right)^2 + \left(w_{j,c} - \bar{w}_c\right)^2 \right]}{\sum_{j=1}^{o} \left[\left(h_{j,a} - \bar{w}_a\right)^2 + \left(h_{j,b} - \bar{w}_b\right)^2 + \left(h_{j,c} - \bar{w}_c\right)^2 \right]} \tag{27}$$

where $\bar{w}_a$, $\bar{w}_b, \bar{w}_c$ 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.

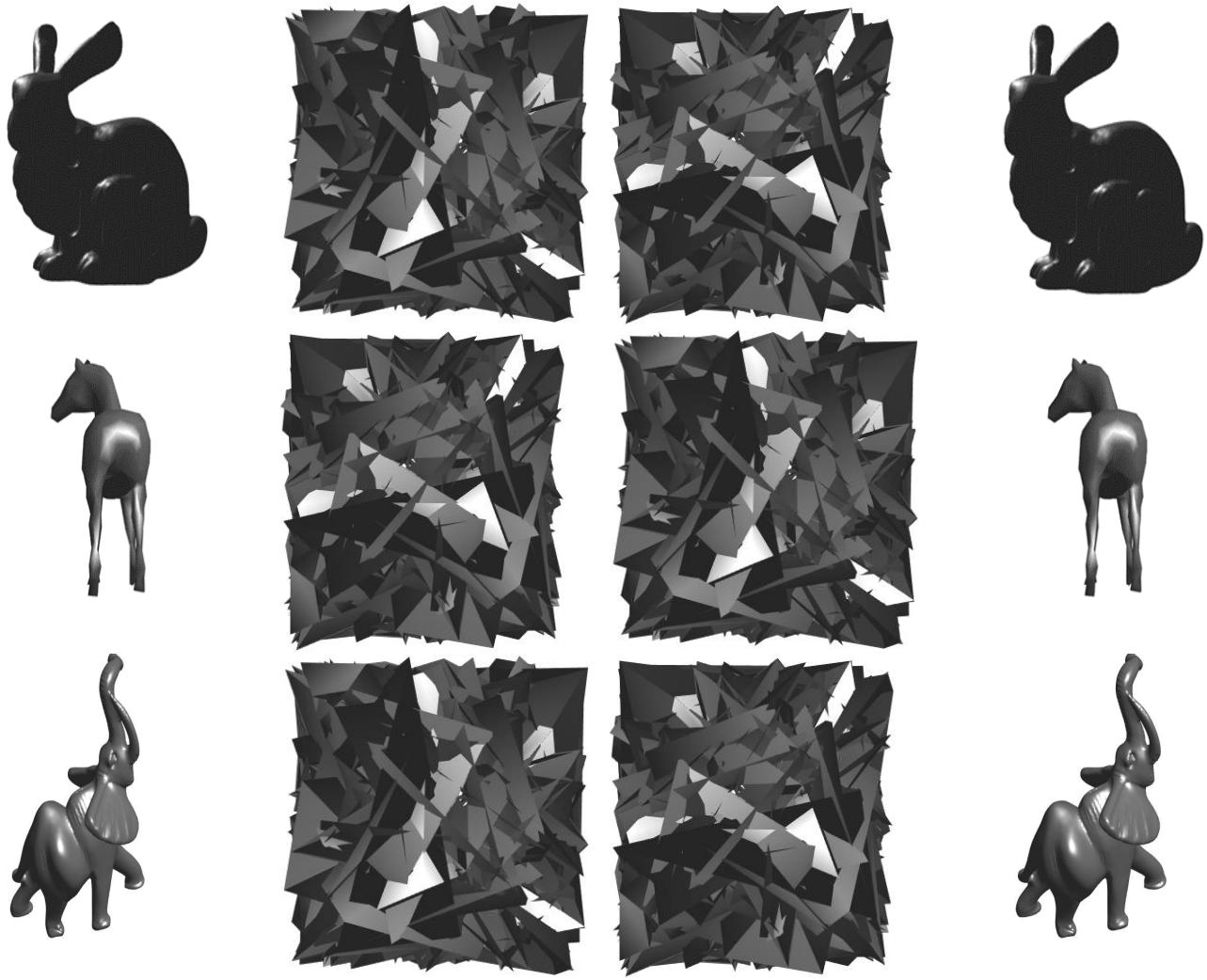
The total error in reconstructing 3D point cloud model is measured using RMSE metrics as follows [27]

$$RMSE = \sqrt{\sum_{j=1}^{O} \left(\underline{a}_j - a_j\right)^2 + \left(\underline{b}_j - c_j\right)^2 + \left(\underline{c}_j - c_j\right)^2} \tag{28}$$

where (a_j, b_j, c_j) and $(\underline{a}_j, b_j, \underline{c}_j)$ represent coordinates of vertices of original and final reconstructed 3D point cloud model, respectively.

a) Bunny **b) Elephant** **c) Horse**

Fig. 3. 3D point cloud model used for conducting experiments.



a) Actual 3D point cloud model | b) Encrypted 3D point cloud model | c) Masked 3D point cloud model | d) Recovered 3D point cloud model

Fig. 4. Outcome of 3D point cloud model considering different phases. a) Actual 3D point cloud model, b) Encrypted 3D point cloud model, c) Masked 3D point cloud model, and d) Decrypted and final recovered 3D point cloud model.

Table I: Performance attained by proposed HSEM method

3D mesh models	SNR	RMSE
Bunny	138.977292	50.15
Elephant	108.003248	50.251
Horse	137.830722	53.97
Average	**128.2704207**	**51.45**

Table II: Performance attained by proposed HSEM over existing data masking method

Method	SNR	RMSE
X. Feng et al., [24]	41.9	62.25

J. Liu et al., [27]	44.35	57.5
A. Hadid et al., cho [21]	97.75	177.0
A. Hadid et al., COA [21]	114.75	81.25
HSEM	128.27	51.45

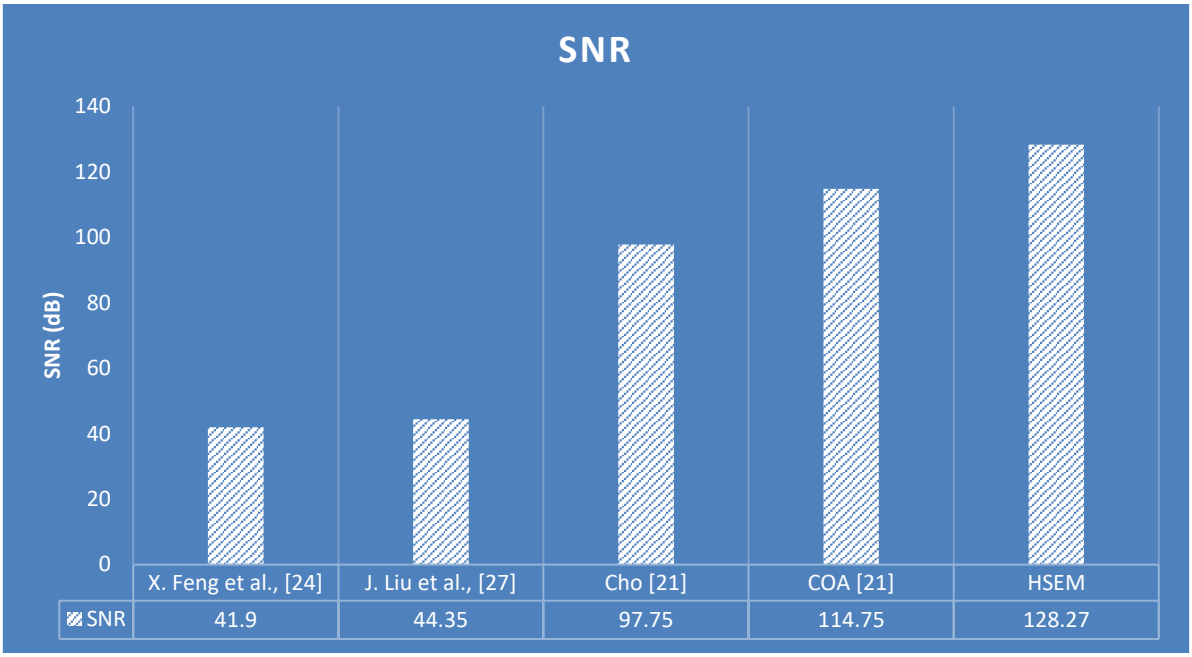


Fig. 4. SNR performance of HSEM and other standard data masking methods.

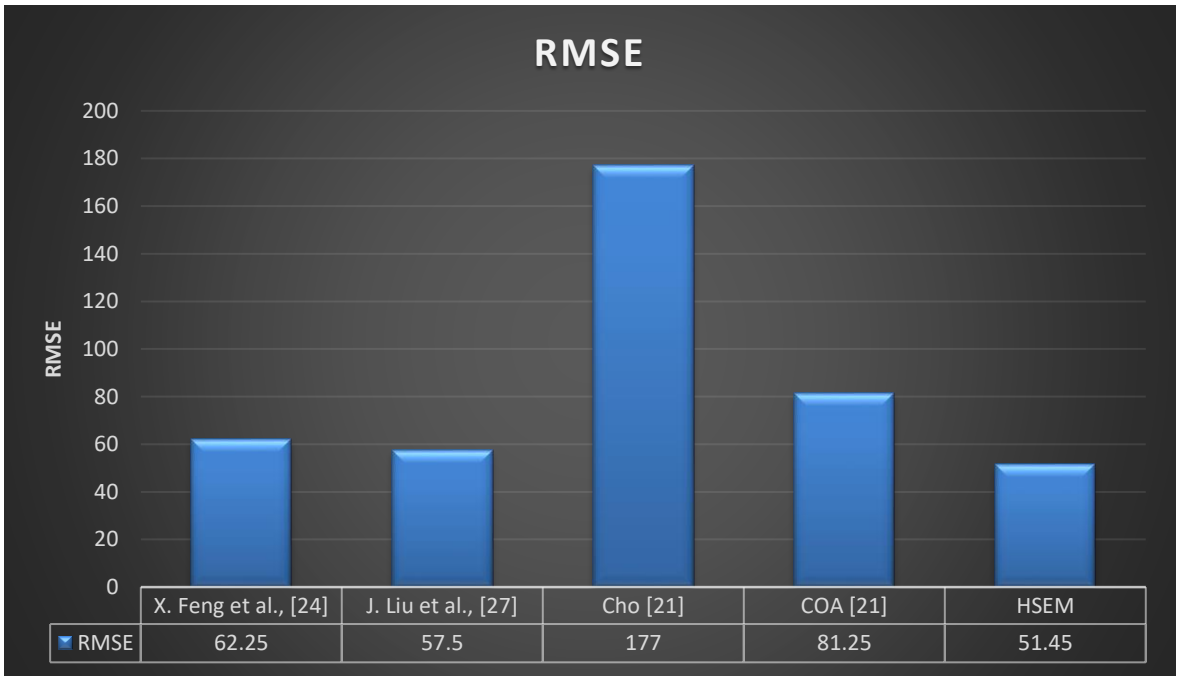


Fig. 5. RMSE performance of HSEM and other standard data masking methods.

In this work experiment are conducted using 3D point cloud model described in Fig. 3. The outcome achieved for different phases for providing security to 3D point cloud model is shown in

Fig. 4. The SNR and RMSE outcome attained by HSEM model is shown in Table I. In Table II comparative analysis of HSEM and other state-of-art data masking model is presented. In Fig. 5 graphical representation of SNR outcome of HSEM and other technique is presented. In Fig. 6 graphical representation of RMSE outcome of HSEM and other technique is presented. From experiment we can see that the proposed HSEM achieves higher reconstruction quality with less error. Thus, the HSEM model can be adopted for providing robust security environment such as for protecting medical data, diagnostic data etc.

3. Conclusion

The HSEM can protect copyright information and preserve privacy of 3D point cloud models; and are efficient for provisioning practical applications since the decrypted 3D mesh models possess less distortion in comparison with original 3D mesh models. Here the mesh are preprocessed and are encrypted using robust homomorphic encryption. Then, prediction error of the coordinates in the embedded sets are estimated using reference set. The HSEM 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 HSEM achieves higher reconstruction quality with less error and maintain high level of embedding capacity in comparison with recent data masking methods.

Future work would test the HSEM model considering diverse set of 3D point cloud models with different formats. Further, study how to enhance the similarities among directly decrypted 3D mesh models and the original 3D mesh models. Along with, improve embedding capacity by effective selection of embedded sets.

References

1. Y. L. Moon, K. Sugamoto, A. Paoluzzi, A. Di Carlo, J. Kwak, D. S. Shin, D. O. Kim, D. H. Lee, and J. Kim, ``Standardizing 3D medical imaging,'' Computer, vol. 47, no. 4, pp. 76-79, Apr. 2014.
2. L. Zhang, Y. Luo, F. Tao, B. H. Li, L. Ren, X. Zhang, H. Guo, Y. Cheng, A. Hu, and Y. Liu, ``Cloud manufacturing: A new manufacturing paradigm,'' Enterprise Inf. Syst., vol. 8, no. 2, pp. 167-187, 2014.
3. B. Chen, J. Wan, A. Celesti, D. Li, H. Abbas, and Q. Zhang, ``Edge computing in IoT-based manufacturing,'' IEEE Commun. Mag., vol. 56, no. 9, pp. 103-109, Sep. 2018.
4. A. Galletta, L. Carnevale, A. Celesti, M. Fazio, and M. Villari, ``A cloud-based system for improving retention marketing loyalty programs in industry 4.0: A study on big data storage implications,'' IEEE Access, vol. 6, pp. 5485-5492, 2017.
5. H. Luo, T.-S. Pan, J.-S. Pan, S.-C. Chu, and B. Yang, ``Development of a three-dimensional multimode visual immersive system with applications in telepresence,'' IEEE Syst. J., vol. 11, no. 4, pp. 2818-2828, Dec. 2017.

6. L. Tawalbeh, M. Mowa, and W. Aljoby, ``Use of elliptic curve cryptography for multimedia encryption,'' IET Inf. Secur., vol. 7, no. 2, pp. 67-74, 2013.
7. J.-S. Pan, C.-Y. Lee, A. Sghaier, M. Zeghid, and J. Xie, ``Novel systolization of subquadratic space complexity multipliers based on toeplitz matrix Vector product approach,'' IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 27, no. 7, pp. 1614-1622, Jul. 2019.
8. T.-Y.Wu, C.-M. Chen, K.-H.Wang, C. Meng, and E. K.Wang, ``Aprovably secure certicateless public key encryption with keyword search,'' J. Chin. Inst. Eng., vol. 42, pp. 1-9, Jan. 2019.
9. C.-M. Chen, B. Xiang, Y. Liu, and K.-H. Wang, ``A secure authentication protocol for Internet of vehicles,'' IEEE Access, vol. 7, pp. 12047-12057, 2019.
10. B. Yan, Y. Xiang, and G. Hua, ``Improving the visual quality of size-invariant visual cryptography for grayscale images: An analysis-by-synthesis (AbS) approach,'' IEEE Trans. Image Process., vol. 28, no. 2, pp. 896-911, Feb. 2019.
11. Y.-Q. Shi, X. Li, X. Zhang, H.-T.Wu, and B. Ma, ``Reversible data hiding: Advances in the past two decades,'' IEEE Access, vol. 4, pp. 3210-3237, 2016.
12. S. Weng, Y. Shi, W. Hong, and Y. Yao, ``Dynamic improved pixel value ordering reversible data hiding,'' Inf. Sci., vol. 489, pp. 136-154, Jul. 2019.
13. S. Weng, Y. Chen, B. Ou, C.-C. Chang, and C. Zhang, ``Improved k-pass pixel value ordering based data hiding,'' IEEE Access, vol. 7, pp. 34570-34582, 2019.
14. L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, ``Reversible image watermarking using interpolation technique,'' IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187-193, Mar. 2010.
15. F. Huang, J. Huang, and Y.-Q. Shi, ``New framework for reversible data hiding in encrypted domain,'' IEEE Trans. Inf. Forensics Security, vol. 11, no. 12, pp. 2777-2789, Dec. 2016.
16. Q. Li, B. Yan, H. Li, and N. Chen, ``Separable reversible data hiding in encrypted images with improved security and capacity,'' Multimedia Tools Appl., vol. 77, no. 23, pp. 30749-30768, 2018.
17. Z.-M. Lu and Z. Li, ``High capacity reversible data hiding for 3D meshes in the PVQ domain,'' in Proc. Int. Workshop Digit. Watermarking. Berlin, Germany: Springer, 2007, pp. 233-243.
18. R. Jiang, H. Zhou, W. Zhang, and N. Yu, ``Reversible data hiding in encrypted three-dimensional mesh models,'' IEEE Trans. Multimedia, vol. 20, no. 1, pp. 55-67, Jan. 2018.
19. 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.
20. 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.
21. 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.
22. Dataset of 3D mesh models of .off formats. Available at: http://shape.cs.princeton.edu/benchmark/index.cgi, last access on: October 2019.

23. 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.
24. X. Feng, ``A new watermarking algorithm for point model using angle quantization index modulation,'' in Proc. NCEECE, Xi'an, China, 2016, pp. 962-968.
25. 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.
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 2018 (2018).
27. 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.
28. 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.
29. A. Hadid, Mourad & Soliman, Mona & Darwish, Ashraf & Hassanien, Aboul Ella. Watermarking 3D Printing Data Based on Coyote Optimization Algorithm. 10.1007/978-3-030-59338-4_29, 2021.
30. Donald, K. The Art of Computer Programming, 3rd ed.; Addison-Wesley: Massachusetts, USA, 1997; pp. 325-515.
31. 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.