An Information Hiding Algorithm Based on Multi-carrier Fusion State Partitioning of 3D Models

Shuai Ren, Bo Li(✉), and Shengxia Liu

School of Information Engineering, Chang'an University, Xi'an, China
2022124144@chd.edu.cn

Abstract. Aiming at the shortcomings of existing single-vector 3D model information hiding algorithms in terms of capacity, robustness and invisibility, this paper proposes an information hiding algorithm based on multi-carrier fusion state partitioning of 3D models. Firstly, multiple three-dimensional vectors to be hidden are fused according to the radial distance between the center of each model and the inner tangential sphere, and then the inner tangential sphere of the fusion body is determined, and the fusion model is divided into inner and outer parts. Then, using the rectangular coordinate plane of space and the inner tangent sphere, the fused point cloud is divided into 16 point cloud model blocks, and the feature points in the subregion space are extracted. In the inner and outer regions of the inner tangent sphere, the two significant points with the lowest coordinate values of the three feature points are selected as the feature areas for hidden data embedding. The hidden data is scrambled by the knight parade method to obtain the corresponding binary coded sequence. Finally, the hidden data is embedded by matching and modifying the parity sequence of the two significant bits with the lowest coordinate values of the feature vertices. The simulation results show that the proposed algorithm has good robustness and invisibility.

Keywords: Information Hiding · 3D Models · Multi-carriers · 3D Fused State Models

1 Introduction

In recent years, there have been a lot of researches on information hiding algorithms based on 3D models, which can be divided into single vector information hiding and multi-vector information hiding from the perspective of embedded vectors.

Reference [1] proposes a differential shift scheme to hide secret bits in a reversible way; in reference [2], the boundary body is divided into a series of

This work has been supported by the National Natural Science Foundation of China (No. 62372062), and the Fundamental Research Funds for the Central Universities, CHD (No. 300102240208).

S. Goel and P. R. Nunes de Souza (Eds.): ICDF2C 2023, LNICST 570, pp. 162–175, 2024.
https://doi.org/10.1007/978-3-031-56580-9_10

blocks by using spatial subdivision technology and subdivision threshold, and the secret information is embedded into the encrypted vertices by combining the spatial coding method with embedded threshold; in reference [3], a set of wavelet coefficient vectors (WCV) is used to correlate a given grid representation with its lower and higher graphic resolution to improve the accuracy of steganographic analysis; reference [4] uses OSVETA to find the stable vertices of the 3D model and calculate the SDF value, vertex norm and vertex distribution rate of these vertices, which helps to improve the ability of the algorithm to resist the simplification attack; reference [5] uses 3d printing technology to realize information hiding methods, the data obtained confirm the possibility of identifying the embedded content of a solid-state object and reliable extraction of hidden information; in reference [2], Y. Tsai et al. proposed a separable and reversible data hiding algorithm based on spatial subdivision and encoding; reference [6] proposes an information hiding algorithm based on 3D model depth projection, which further improves security and robustness.

In this paper, multiple three-dimensional carriers to be hidden are fused based on the radial distance between the center of each model and the inner tangential sphere, and then the inner tangential sphere of the fusion body is determined, and the fusion model is divided into inner and outer parts. Then, using the rectangular coordinate plane of space and the inner tangent sphere, the fused point cloud is divided into 16 point cloud model blocks, and the feature points in the subregion space are extracted. In the inner and outer regions of the inner tangent sphere, the two significant points with the lowest coordinate values of the three feature points are selected as the feature areas for hidden data embedding. The hidden data is scrambled by the knight parade method to obtain the corresponding binary coded sequence. Finally, the hidden data is embedded by matching and modifying the parity sequence of the two significant bits with the lowest coordinate values of the feature vertices. It has been proved that the multi-vector fusion strategy proposed in this paper greatly increases the embedding capacity of the steganography algorithm, and the embedding region determined after the selection of feature points ensures a good embedding robustness.

2 3D Model Multi-carrier Fusion Method

This paper uses multiple 3D models $M_1, M_2, \cdots, M_n$ is used as a carrier of hidden data embedding to increase the data embedding capacity and improve the robustness of data embedding. Suppose the vertices in the 3D model are represented as $V\{V_1, V_2, \cdots, V_n\}$, m is the total number of all vertices in the three-dimensional model. This algorithm first uses formula (1) to determine the center of mass $O_h(x_{hc}, y_{hc}, z_{hc})$ of the three-dimensional model as the center point of the model. Then, the radial distance d_i from the center of mass of n three-dimensional models to a point on the surface of the inner tangent sphere is calculated by using formula (2). The center of mass of the three-dimensional model with the smallest radial distance is taken as the center point of the fusion

body, and the center point of the remaining $n-1$ three-dimensional models is fused according to the size of their center of mass and radial distance to obtain the fusion body of the three-dimensional point cloud model M_0.

$$\mathbf{x}_{hc} = \frac{1}{V_h}\sum_{i=1}^{V_h} x_i, y_{hc} = \frac{1}{V_h}\sum_{i=1}^{V_h} y_i, z_{hc} = \frac{1}{V_h}\sum_{i=1}^{V_h} z_i \tag{1}$$

$$d_i = \sqrt{(x_i - x_0)^2 + (y_i - y_0)^2 + (z_i - z_0)^2} \tag{2}$$

3 Multi-carrier Block and Feature Extraction

3.1 3D Model Compression and Partitioning

In this paper, the algorithm obtains the point cloud data of the fused state model M. Firstly, the PCA method [7] is used to normalize the fused state model, and then the vector similarity compression algorithm CVS [8–10] is used to perform the point cloud compression operation to obtain the three-dimensional point cloud fused state model $M_0{}'$ after compression.

After the above operation, the three-dimensional multi-carrier point cloud fusion model $M_0{}'$ eliminates the point set with insignificant structural features in its point cloud structure. Therefore, this algorithm directly combines the inner tangential sphere surface of the fusion state and the space rectangular coordinate plane to segment the fusion state model. Firstly, the inner tangential sphere of $M_0{}'$ is determined, through which the $M_0{}'$ is divided into two inner and outer regions, respectively denoted as $M_n{}'$ and $M_w{}'$. Then, in the space rectangular coordinate system, using the plane formed by axis x, y, z and origin o, the three-dimensional point cloud fusion state can be evenly divided into 8 parts around the coordinate axis. It is assumed that the inner and outer parts of the tangent ball in the $oxyz$ region are divided into $M_{1n}{}'$ and $M_{1w}{}'$, and the inner and outer parts of the tangent ball in the $o-xyz$ region are divided into $M_{2n}{}'$ and $M_{2w}{}'$. $ox-yz, o-x-yz, oxy-z, o-xy-z, ox-y-z, o-x-y-z$, and the inner and outer parts of the eight regions are represented as $M_{jn}{}'$ and $M_{jw}{}'$ respectively, and j represents the j-th coordinate axis region. According to the above segmentation method, M' has been divided into 16 sub-regions at this time,the specific block sorting results are shown in Table 1. Then, each subarea space is numbered accordingly. The rules for numbering subarea space are related to the coordinate axes of each subarea space and their positive and negative values. For example, the regional space numbered 1 and 2 is located in both the positive and negative directions of x axis and y axis and z axis, where the positive x axis is 1 and the negative x axis is 2. By analogy, the 16 subregions of the 3D model can be numbered successively, so that they have a certain order. Then the feature region is extracted and embedded into the hidden data twice in each of the 8 regions inside $M_n{}'$ and outside $M_w{}'$ of the $M_0{}'$ inner cutting sphere, which can improve the robustness of information hiding.

Table 1. Fusion state blocking

Axis area	Block number	Axis area	Block number
$oxyz$	${M_{1n}}'$	$oxy-z$	${M_{5n}}'$
	${M_{1w}}'$		${M_{5w}}'$
$o-xyz$	${M_{2n}}'$	$o-xy-z$	${M_{6n}}'$
	${M_{2w}}'$		${M_{6w}}'$
$ox-yz$	${M_{3n}}'$	$ox-y-z$	${M_{7n}}'$
	${M_{3w}}'$		${M_{7w}}'$
$o-x-yz$	${M_{4n}}'$	$o-x-y-z$	${M_{8n}}'$
	${M_{4w}}'$		${M_{8n}}'$

This algorithm fuses multiple three-dimensional model centers to improve the capacity of hidden data embedding in the process of information hiding, and then compresses the three-dimensional model fusion state to simplify the redundant point set in the three-dimensional point cloud fusion state model and reduce the computational complexity in the process of feature point extraction. Finally, the three-dimensional point cloud fusion state model is segmsegmed and the hidden data is doubly embedded. It can improve the robustness and anti-attack of the hidden data transmission process.

3.2 3D Model Feature Point Extraction

In order to ensure the security of hidden data embedding, the algorithm in this paper adopts the point cloud feature point extraction algorithm based on multiple criteria to extract the feature points in the model [11,12] to determine the embedding area of hidden data.

This algorithm fuses multiple three-dimensional models. In view of the feature of a large number of boundary points or sharp points in the fused state model, the point cloud feature point extraction algorithm based on multiple criteria is used to extract the feature points, which can effectively avoid the drawback that sharp points or boundary points cannot be extracted in detail when extracting feature points using the traditional Angle between curvature and normal vector. It is also possible to extract more detailed features of flat surfaces.

The feature points of the 16 sub-regions are obtained, and the feature points in each region are sorted according to the normal direction of the feature points in each region space, and then the bit information of the hidden data is embedded successively according to the numbering order of the fused state region space.

4 The Process and Steps of Information Hiding

The flow chart of the information hiding algorithm based on multi-carrier fusion state partitioning is shown in Fig. 1 below, and its specific steps are as follows:

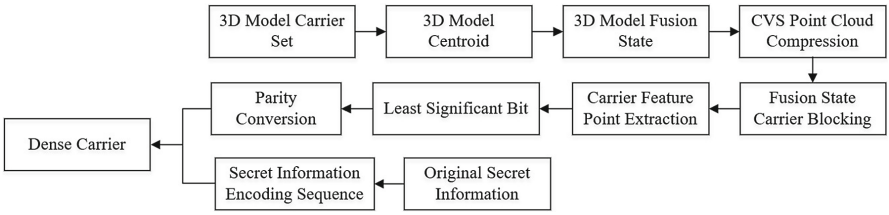


Fig. 1. Information Hiding Algorithm Flowchart.

Step 1: Model fusion.
Step 2: Fused state compression.
Step 3: Fusion state blocks.
Step 4: Feature point extraction.
Step 5: Select the embedding area. The lowest two significant bits among the three coordinate values of the vertices are selected according to the sequence of feature points in each of the 8 regions inside and outside the divided fusion state, and they are used as candidate bits for hidden data embedding, thus completing the double embedding of hidden data.
Step 6: Embed rules. The algorithm matches the parity sequence of the lowest two significant bits in the coordinate value of the vertex with the encoded sequence of the hidden data, and the matching rules are shown in Table 2.

Table 2. Secret information embedding rules.

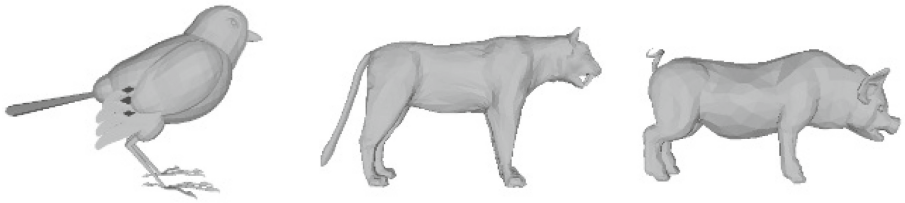
Parity of the lowest two significant bits	Match encoding sequence
Odd and Odd Numbers	11
Odd and Even Numbers	10
Even and Even Numbers	00
Even and Odd Numbers	01

Step 7: Embedding secret data. The secret data is transformed by knight parade, the encoded sequence of the secret data is obtained, and the secret data is embedded according to the matching rules in step 6.

5 Experimental Analysis and Comparison

In this paper, the algorithm in [13] (Distribution of Vertex Norms, DVN) and (Local Height and Mean Shift, LHMS) [14] are selected for experimental reference with the algorithm in this paper, and we conduct experimental comparisons from two aspects: algorithm invisibility and robustness. Besides the environment for completing the experiment of this algorithm is MatlabR2016a, MeshlabV2021

and PyCharm2020. The 3D model carrier set used in this article is selected from the Stanford University 3D model library. Figure 2 shows the original 3D model carrier selected for this experiment, the hidden data is lean picture.

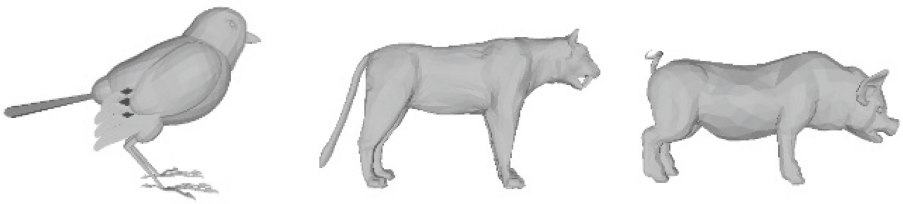


(a) Original carrier M_1 (b) Original carrier M_2 (c) Original carrier M_3

Fig. 2. Original 3D model carrier.

5.1 Invisibility

Experiments Based on HVS System. The algorithm combines multiple 3D models as a carrier for embedding secret information, improving the capacity and invisibility of the embedded data. As depicted in Fig. 3, after embedding the secret information, the dense fusion state model is split into individual carrier models, and it can be observed that there is no significant change in the appearance of the dense carrier model, satisfying the HVS human visual judgment characteristics. Thus, it can be concluded that the invisibility of our algorithm is better.



(a) Dense carrier $M_1{}'$ (b) Dense carrier $M_2{}'$ (c) Dense carrier $M_3{}'$

Fig. 3. Dense carrier model.

Signal to noise ratio (SNR) can measure the invisibility of algorithms by determining the degree of distortion changes between the original 3D model and the dense 3D model. The invisibility experiments of the algorithms in this paper

are selected to compare and analyse the DVN algorithm and the LHMS algorithm, calculate SNR value by formula (3), to determine the degree of distortion between the encrypted carrier and the original carrier after embedding different amounts of hidden data. The larger the SNR value of the algorithm, show that the better the invisibility of the algorithm, the smaller the SNR value, indicates that the worse the invisibility of the algorithm.

$$SNR=\frac{\sum_{i=1}^{V_m} x_i^2+y_i^2+z_i^2}{\sum_{i=1}^{V_m}\left(x_i{}'-x_i\right)^2+\left(y_i{}'-y_i\right)^2+\left(z_i{}'-z_i\right)^2} \tag{3}$$

where V_m is the number of vertices of the carrier, x_i, y_i, z_i are the coordinate values of the original 3D model vertices, $x_i{}'$, $y_i{}'$, $z_i{}'$ are the coordinate values of the corresponding vertices in the dense 3D model. As Fig. 4 shows the algorithm of this paper with DVN algorithm and LHMS algorithm at different levels of secret information embedding amount, changes in SNR indicator values.

In Fig. 4, when the embedding index $k < 15$, the SNR values of all three algorithms are greater than 50dB, the average SNR of this algorithm is 76.9, the average SNR values of DVN algorithm and LHMS algorithm are 71.67 and 72.6, respectively, can be obtained in the case that the embedding index $k < 15$ of the hidden data, the average SNR of the algorithm in this article is 7.29% and 5.92% higher than DVN algorithm and LHMS algorithm, respectively, the invisibility of the algorithm in this article is higher than that of DVN algorithm and LHMS algorithm. The three dashed lines t_1, t_2, and t_3 in the figure visually indicate that when the SNR value is 50 dB, the data embedding indices of this algorithm, DVN algorithm, and LHMS algorithm are 16.7, 15.3, and 15.65, respectively, the embedding capacity of the algorithm in this article is higher than that of the comparison algorithm.

5.2 Robustness

In this robustness analysis experiment, the dense carrier is subjected to different degrees of shear, simplification, non-uniform compression, rotation and noisy attacks respectively. The Correlation coefficient (Corr) between the hidden data extracted from the dense carrier after attack and the original hidden data is selected as the measurement index of the robustness performance of the algorithm. As shown in formula (4), the experimental results are analyzed and compared with DVN algorithm and LHMS algorithm.

$$Corr=\frac{\sum_{n=1}^{B}\left(B_n{}'-\bar{B}'\right)\left(B_n-\bar{B}\right)}{\sqrt{\sum_{n=1}^{B}\left(B_n{}'-\bar{B}'\right)^2\cdot\sum_{n=1}^{B}\left(B_n-\bar{B}\right)^2}} \tag{4}$$

where, $\bar{B}_n$ and $\bar{B}_n'$ respectively represent the mean value of the hidden data sequence B_n embedded in the carrier and the extracted hidden data sequence

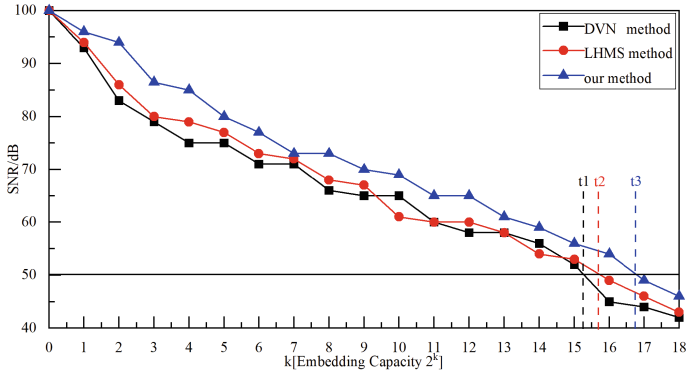


Fig. 4. Comparative analysis of algorithm SNR.

$B_n{}'$ in the dense carrier, and B is the total number of hidden data contained in the carrier.

The magnitude of the Corr correlation coefficient value can represent the similarity between the extracted secret data from the dense carrier and the original secret data, the larger the Corr, the more complete the extracted covert data, the smaller the Corr, the harder it is to recognize the extracted secret data. The Corr threshold is set to 0.5, when the Corr value exceeds 0.5, the extracted secret data can be accurately identified. Conversely, when the Corr value is less than or equal to 0.5, the extracted secret data cannot be recognized. Figure 5 illustrates the extraction of secret image information with different Corr values from the noisy dense carrier.

(a) Original Hidden Image (b) Corr=0.79 (c) Corr=0.5

Fig. 5. Extracting Hidden Images with Dense Carrier Noise.

Experimental Analysis of Shearing Attacks. In Fig. 6, it can be seen that when the shear rate of the dense carrier is less than 45%, which means that the Corr values of all three algorithms are higher than 0.5, the average Corr value of this algorithm is 0.748, the average Corr values of DVN algorithm and LHMS algorithm are 0.655 and 0.694, respectively, and the Corr value of our

algorithm has increased by 14.19% and 7.78% compared to the DVN algorithm and LHMS algorithm, respectively. The dashed lines a_1, a_2, and a_3 indicate that the maximum shear rates that DVN algorithm and LHMS algorithm can resist are 45% and 55%, respectively.

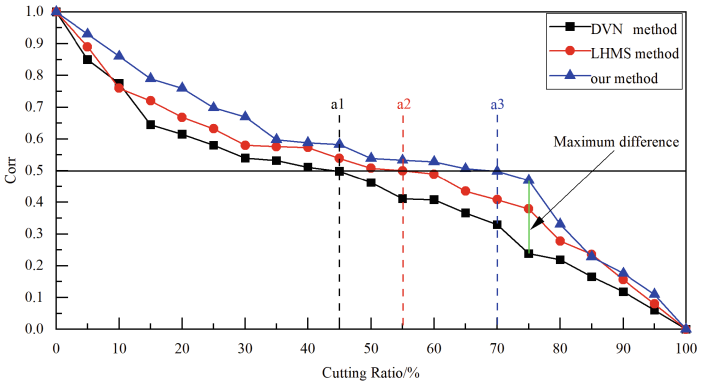


Fig. 6. Comparison of shear attack experimental results.

Experimental Analysis of Simplified Attacks. To simplify the process of covert transmission attacks on dense carriers, topological information such as vertices or triangular patches can be reduced, which destroys the dense carriers. The attacked 3D model will have a reduced number of vertices or triangular patches, while its basic shape will remain unchanged. In our algorithm, multiple 3D models are fused, and robust feature points are extracted from the fused state models to be used as embedding regions for secret data. To better resist simplified attacks, secret data is embedded twice inside and outside the tangent sphere in the fusion carrier. Figure 7 presents a comparison of the correlation coefficient Corr between the extracted secret data and the original secret data in the encrypted carrier when the algorithms in our paper, DVN, and LHMS are subjected to simplification attacks.

In Fig. 7, the simplification rate of the dense fusion state is less than 34%, and the Corr values of all three algorithms are greater than 0.5. The average value of the Corr in our algorithm is 0.813, DVN algorithm and LHMS algorithm are 0.677 and 0.743, respectively. It can be concluded that when the shear rate is less than 34%, the Corr value of our proposed algorithm has increased by 20.08% and 9.42% compared to the DVN and LHMS. The distribution of dashed lines b_1, b_2, and b_3 in the figure shows that the algorithm in this paper simplifies by 60% with dense carriers, Corr equals 0.5, which indicates the extracted hidden images cannot be effectively recognized. Therefore, the maximum simplification rate that our algorithm can resist is 60%. Besides, when the Corr of DVN algorithm and LHMS algorithm is 0.5, the maximum simplification rates that it can withstand are 34.6% and 36.2%, respectively.

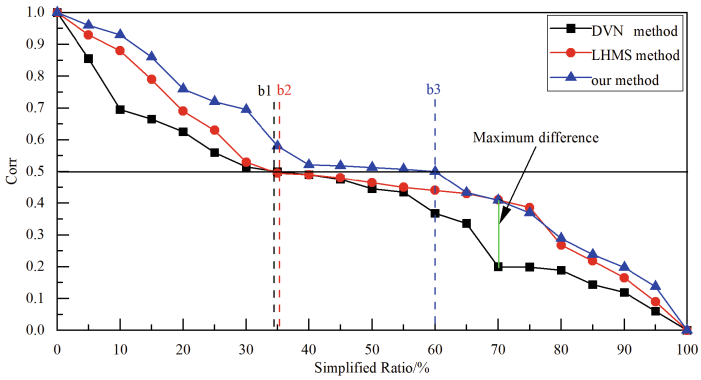


Fig. 7. Comparison of simplified attack experiment results.

Experimental Analysis of Non-uniform Compression Attacks. Non-uniform compression attacks can cause non-uniform damage to the topology structure of the model, leading to changes in the data information or position of 3D model vertices. When a dense carrier is subjected to such attacks, the encoding sequence of the secret data it contains will also be damaged to varying degrees. To address this issue, our algorithm uses a multi-carrier 3D point cloud fusion state model for data hiding, which offers a large embedding space and allows for the embedding of secret data in both inner and outer layers. This approach ensures the integrity of the secret data even when subjected to non-uniform compression attacks. Figure 8 shows the comparison of the Corr values between the extracted secret data and the original secret data in a dense carrier under varying degrees of non-uniform compression between our algorithm, DVN algorithm, and LHMS algorithm.

It can be seen from Fig. 8 that when the dense carrier is subjected to 70% non-uniform compression, the Corr value of our algorithm is 0.6, the Corr of DVN algorithm and LHMS algorithm are 0.38 and 0.43, respectively. The distribution of c_1, c_2, and c_3 in the figure indicates, when the Corr value is 0.5, the maximum non-uniform compression rate that the algorithm in this paper can resist is 74.2%, however, the maximum non-uniform compression rates that DVN algorithm and LHMS algorithm can resist are 62.2% and 66.8%, respectively. This means that the algorithm in this paper has a higher maximum non-uniform compression rate than the DVN and LHMS algorithm by 19.29% and 11.07%, respectively.

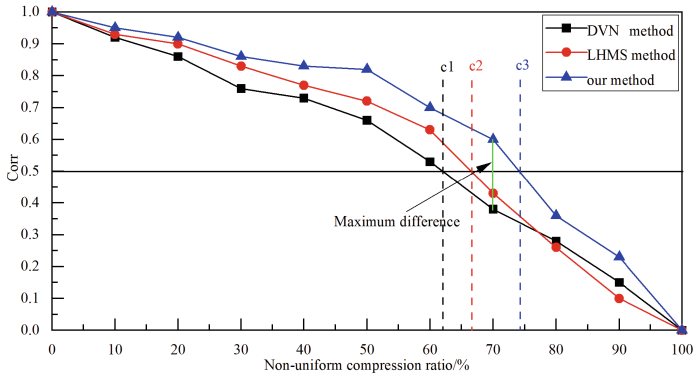


Fig. 8. Comparison of experimental results on non-uniform compression attacks.

Comparison of Experimental Results of Rotation Attacks. The paper's algorithm utilizes fusion of multiple 3D point cloud models to create a multi-carrier fusion state point cloud model, from which feature points are selected for secret data embedding. The point cloud models have rotation invariance, so the fusion state model is not impacted by rotation attacks. This means that if the dense point cloud fusion state model is subjected to the rotation attacks, the encoding sequence of the secret data can still be fully extracted from it. The experimental analysis of rotation attacks in this paper compares and analyzes the results of the presented algorithm with LHMS algorithm. Table 3 presents the correlation coefficient Corr values of the extracted secret data for both algorithms when subjected to different degrees of rotation attacks.

From Table 3, it can be seen that our algorithm in this paper is not affected by rotation attacks from any angle, the secret data extracted from its dense carrier is relatively complete. When the carrier with dense fusion state is subjected to a 30° rotation attack, the Corr value of our algorithm has increased by 15.74% compared to the comparison algorithm, and when the dense carrier is subjected to a 45° rotation attack, the Corr value of our algorithm has increased by 56.49% compared to the comparison algorithm.

Experimental Analysis of Noise Attacks. Noise attack destroys the integrity of the encoded sequence of secret data contained in a dense carrier by adding noise interference, and it will not have a significant impact on the basic shape and topology of the model, during the information hiding process, we select the feature regions with high robustness in the model as the embedding regions for secret data, it can effectively resist a certain level of noise attacks. Figure 9 shows the comparison of the correlation coefficient Corr value between the extracted secret data and the original secret data when our algorithm, DVN algorithm, and LHMS algorithm are subjected to varying degrees of noise attacks.

Table 3. Comparison of experimental results of rotation attacks.

Rotation angle around the x-axis	LHMS algorithm	Our algorithm
10°	0.959	1
30°	0.864	1
45°	0.639	1

In Fig. 9, when the noise attack is 0.5%, the Corr difference between our algorithm and DVN algorithm and LHMS algorithm has reached the maximum, the Corr of this algorithm is 0.66, the Corr values of DVN algorithm and LHMS algorithm are 0.457 and 0.543, respectively, the Corr of our algorithm is improved by 44.42% and 21.54% compared to DVN and LHMS algorithms. From the distribution of dashed lines d_1, d_2, and d_3 in the figure, it can be seen that this algorithm is vulnerable to 0.7% noise attack, Corr value is 0.5, it unable to recognize extracted hidden images. Therefore, the maximum level of noise attack that our algorithm can resist is 0.7%, but the DVN algorithm and LHMS algorithm are no longer able to recognize and extract images when subjected to noise attacks of 0.48% and 0.6%, respectively.

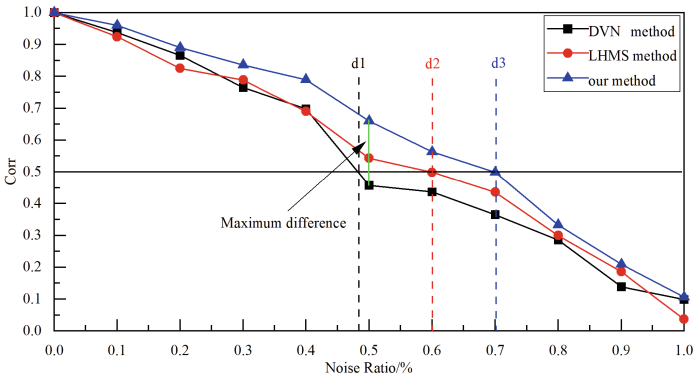


Fig. 9. Comparison of Noise Attack Experimental Results.

6 Conclusion

In this paper, an information hiding algorithm based on three-dimensional model multi-vector fusion state partitioning is proposed. Firstly, multiple three-dimensional vectors to be hidden are fused according to the radial distance between the center of each model and the inner tangential sphere, and then the inner tangential sphere of the fusion body is determined, and the fusion model is divided into inner and outer parts. Then, the fusion state point cloud is

divided into 16 point cloud model blocks by using the spatial rectangular coordinate plane combined with the inner tangent sphere, and the feature points in the subregion space are extracted. The two significant bits with the lowest coordinate values of the three feature points are selected respectively in the inner and outer regions of the inner tangent sphere, and the encoded sequence of the hidden data is embedded in the feature points of the fusion carrier. The experimental results show that the proposed algorithm has good invisibility and robustness when the three-dimensional model fusion is used as the hidden carrier.

References

1. Girdhar, A., Kumar, V.: A reversible and affine invariant 3D data hiding technique based on difference shifting and logistic map. J. Ambient Intell. Human. Comput. **10**, 4947–4961 (2019)
2. Tsai, Y.: Separable reversible data hiding for encrypted three-dimensional models based on spatial subdivision and space encoding. IEEE Trans. Multimed. **23**, 2286–2296 (2021)
3. Li, Z., Bors, A.: Steganalysis of meshes based on 3D wavelet multiresolution analysis. Inf. Sci. **522**, 164–179 (2020)
4. Wang, X., Zhan, Y.: A zero-watermarking scheme for three-dimensional mesh models based on multi-features. Multimed. Tools Appl. **78**, 27001–27028 (2019)
5. Kuznetsov, A., Stefanovych, O., Gorbenko, Y., Smirnov, O., Krasnobaev, V., Kuznetsova, K.: Information hiding using 3D-printing technology. In: 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), vol. 2, pp. 701–706 (2019)
6. Dan, Z., Lei, X., Ren, S., Liu, S., Feng, Q.: Information hiding algorithm based on depth projection of 3D model. In: 2021 2nd International Conference On Electronics, Communications and Information Technology (CECIT), pp. 681–686 (2021)
7. Kalivas, A., Tefas, A., Pitas, I.: Watermarking of 3D models using principal component analysis. In: 2003 IEEE International Conference on Acoustics, Speech, and Signal Processing, 2003. Proceedings. (ICASSP 2003), vol. 5, pp. V–676 (2003)
8. Zhang, X., Niu, B., Zhang, J.: Recoverable 3D point cloud compression algorithm based on vector similarity. J. Front. Comput. Sci. Technol. **14**, 657–668 (2020)
9. Bazazian, D., Casas, J., Ruiz-Hidalgo, J.: Fast and robust edge extraction in unorganized point clouds. In: 2015 International Conference On Digital Image Computing: Techniques And Applications (DICTA), pp. 1–8 (2015)
10. Han, H., Han, X., Sun, F., Huang, C.: Point cloud simplification with preserved edge based on normal vector. Optik - Int. J. Light Electr. Optics **126**, 2157–2162 (2015)
11. Wang, Q., Huang, R., Yan, X., Cheng, T.: Feature point extraction of scattered point cloud based on multiple criterions. Appl. Res. Comput. **36**, 1585–1588 (2019)
12. Gautam, S., Agrawal, V.: Feature curve extraction from data points. In: IOP Conference Series: Materials Science and Engineering, vol. 1136, p. 012004 (2021)
13. Cho, J., Prost, R., Jung, H.: An oblivious watermarking for 3-D polygonal meshes using distribution of vertex norms. IEEE Trans. Signal Process. **55**, 142–155 (2007)
14. Ren, S., Zhao, X., Zhang, T., Shi, F., Mu, D.: Information hiding scheme for 3D models based on local height and mean shift clustering analysis. Comput. Sci. **44**, 187–191 (2017)

15. Zhou, H., Chen, K., Zhang, W., Yao, Y., Yu, N.: Distortion design for secure adaptive 3-D mesh steganography. IEEE Trans. Multimed. **21**, 1384–1398 (2019)
16. Zhang, C., Li, H., Lu, H., Su, P.: Research on information encryption and hiding technology of 3D point cloud data model. In: Proceedings - 2020 International Conference on Computer Science and Management Technology, ICCSMT 2020, pp. 54–58 (2020)
17. Zhang, Q., Wen, T., Song, X.: Multilevel reversible data hiding based on difference histogram for 3D point cloud models. In: 2019 6th International Conference on Information Science and Control Engineering (ICISCE), pp. 380–384 (2019)
18. Zeng, Y., Lou, Z.: The new PCA for dynamic and non-gaussian processes. In: 2020 Chinese Automation Congress (CAC), pp. 935–938 (2020)
19. Lou, Z., Shen, D., Wang, Y.: Two-step principal component analysis for dynamic processes monitoring. Canadian J. Chem. Eng. **96**, 160–170 (2018)
20. Qian, Z., Zhou, H., Zhang, W., Zhang, X.: Robust steganography using texture synthesis. In: Advances in Intelligent Information Hiding and Multimedia Signal Processing, pp. 25–33 (2017)