Point Cloud Model Information Hiding Algorithm Based on Multi-scale Transformation and Composite Operator

Shuai Ren, Hao Gong(✉), Huirong Cheng, and Zejing Cheng

School of Information Engineering, Chang'an University, Xi'an, China
2022124045@chd.edu.cn

Abstract. In order to improve the security and robustness of the 3D model information hiding algorithm, this paper proposes a point cloud model information hiding algorithm based on multi-scale transformation and composite operator. Firstly, rasterizing the 3D point cloud model, and use the improved 3D Harris algorithm to extract the corner points of the rasterized model. Secondly, using SURF operator to screen robust feature points as embedding regions of secret information. Finally, the feature region is subjected to the multiscale transformation, and the secret information is hid by using a quantization-based method to embed it into the low-frequency coefficient matrix. The experimental results show that the algorithm can completely avoid affine transformation attacks and can achieve a Corr value of 0.729 in the face of a composite attack with 10% simplification, 0.5% noise and 10% shear. The algorithm's invisibility, capacity, and its robustness against multiple attacks are improved.

Keywords: Information hiding · 3D point cloud model · Feature extraction · NSCT transform

1 Introduction

With the popularization of mobile devices, information security has aroused people's great attention. Information hiding technology is an important means to ensure information security, which can improve information security by using specific algorithms to hide secret information in multimedia carriers. The carrier of information hiding in the early days was mainly images. With the rapid development of 3D technology, how to use 3D models as the carrier of information hiding has gradually become a research hotspot [1,2]. When designing an information hiding algorithm, two parts need to be clarified: the embedding

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. 146–161, 2024.
https://doi.org/10.1007/978-3-031-56580-9_9

domain of secret information and the embedding rules of secret information [3–5]. At present, most algorithms need to find features with good robustness to satisfy the strong robustness of the algorithm. Commonly used key point extraction algorithms based on point cloud models include 3D SIFT, 3D Harris algorithm, and key point extraction algorithms based on curvature limit threshold [6]. Among them, 3D Harris is an effective feature detection method. The Harris algorithm has better stability and can extract more accurate robust points. [7] Some studies have compared and analyzed the existing feature point detectors, among which the Harris operator is the most robust to topology changes and noise; the SURF operator is based on the SIFT operator, which improves the robustness and performance, and the extracted feature points by this operator have scale invariance [8,9]. Therefore, this paper selects the Harris operator and the SURF operator to extract the feature points of the point cloud model.

The above research has the following problems: (1) SURF and Harris operators are mainly aimed at feature extraction of images, so it need to be improved for 3D point cloud; (2) corner points are stable feature points, but the SURF algorithm is not sensitive to corner points; (3) the traditional SURF operator has the defect of high computational volume; and (4) the corner points extracted by Harris don't have scale invariance.

Therefore, this paper proposes to combine Harris with SURF operator. Firstly, using Harris operator with speed advantage to extract the corner points of the model. Then, using SURF operator to optimize the extraction to get the stable feature points as the embedding region. Finally, doing the multiscale transformation of the embedding region, and complete the information hiding in the transformation coefficients, so as to improve the robustness of the algorithm.

To sum up, our main contributions are:

- Improvement of Harris operator by introducing orthogonal convolutional gradient effectively reduces the effect of noise.
- Combination of Harris and SURF operator to extract strong robust points.
- The algorithm is equipped with affine invariance to resist affine transformation attack by doing NSCT transformation on the feature region.

2 Point Cloud Model Information Hiding Algorithm Based on Multi-scale Transformation and Composite Operator

The 3D point cloud model information hiding algorithm based on multi-scale transformation and composite operator mainly includes the following three stages. stage 1: embedding region extraction and optimization; stage 2: secret information embedding; and step 3: secret information extraction. As Fig. 1 shows the flowchart of the proposed algorithm. Firstly, the point cloud model is preprocessed to rasterize the point cloud, and the improved 3D Harris algorithm is used to extract the corner points of model, and the corner point cloud is converted into a depth image; then the depth image is subjected to SURF

feature extraction, and the robust feature points are found to be the embedding regions of the secret information. Secondly, the feature region is constructed into a matrix and its NSCT transform is performed to embed the secret information into the NSCT subbands with low frequency coefficients by using the quantization-based embedding method. Finally, at the receiver side, the secret information is extracted by inverse NSCT transform.

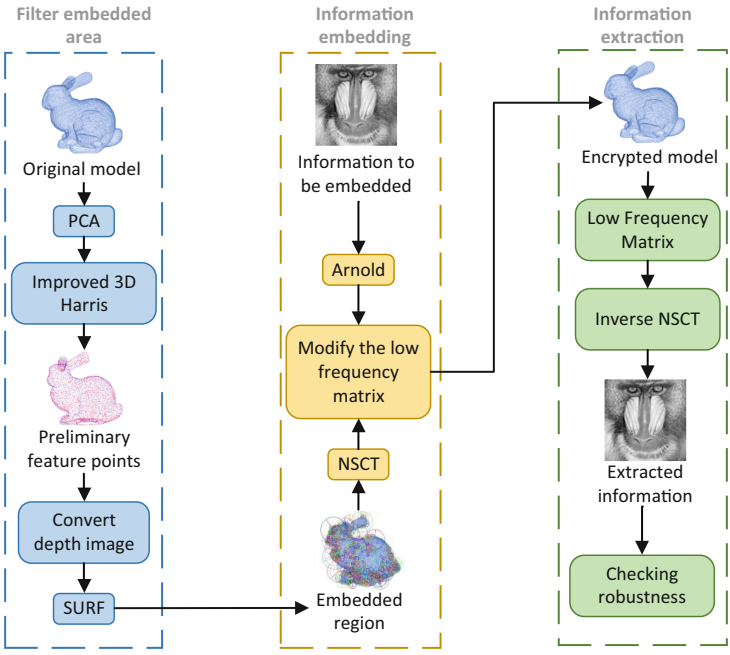


Fig. 1. Workflow for point cloud model information hiding algorithm based on multi-scale transformation and composite operator

2.1 Pre-processing

The experimental data is a raw point cloud without any spatial relationship and connectivity information, and it's not possible to directly use the 3D Harris corner point detection algorithm of the mesh model for the unstructured 3D point cloud. Therefore, the preprocessing operation of the point cloud model is essential for corner point detection.

The raw point cloud is preprocessed to generate a grid matrix that can hold the 3D point cloud. The point cloud is first rasterized by dividing the point cloud data into sets of points in a 3D grid structure of $N_x \times N_y \times N_z$ raster cells. Each raster cell contains some point cloud data inside. Then, Principal Component Analysis (PCA) is used to determine the optimal enclosing box for each raster cell [10], which in turn yields the spatial resolution of the grid cell as shown in Eq. 1. Figure 2 demonstrates the estimation of the point cloud data envelopment box using PCA method.

$$N_x = \frac{x_{max} - x_{min}}{\alpha}, N_y = \frac{y_{max} - y_{min}}{\alpha}, N_x = \frac{y_{max} - y_{min}}{\alpha} \tag{1}$$

where x_{max} and x_{min} denote the maximum and minimum coordinates in the x-axis direction in the raster, and the numerator refers to the average point spacing.

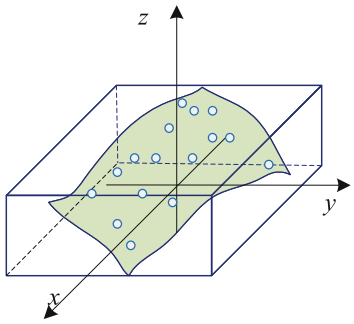


Fig. 2. Point cloud data wraparound box

2.2 Composite Operator Screening Embedding Region

The composite operator consists of the improved 3D Harris and SURF operators. The improved 3D Harris operator is responsible for extracting the corner points that are insensitive to rotation, noise effects and viewpoint transformations, and the SURF operator is responsible for extracting scale-invariant feature points on this basis. The final feature points obtained are the embedding regions.

Improved 3D Harris Operator. The Harris operator performs more stably in extracting corner points, but it is prone to produce pseudo-corner points due to the influence of noise factors, which reduces the extraction accuracy. For this reason, orthogonal convolutional gradients are introduced to the conventional Harris operator to effectively suppress the influence of noise and improve edge localization [11]. denotes a continuous function with first-order continuous partial derivatives, and the gradient within a raster cell for at a point can be expressed as Eq. 2 and Eq. 3.

$$\nabla f(x, y, z) = \frac{\partial f}{\partial x}\overrightarrow{i} + \frac{\partial f}{\partial y}\overrightarrow{j} + \frac{\partial f}{\partial z}\overrightarrow{k} \tag{2}$$

$$\nabla f(x, y, z) = I(x, y, z) = [I_x I_y I_z]^{\mathrm{T}} = \left[\frac{\partial f}{\partial x}\frac{\partial f}{\partial y}\frac{\partial f}{\partial z}\right]^{\mathrm{T}} \tag{3}$$

where $\overrightarrow{i}$, $\overrightarrow{j}$, $\overrightarrow{k}$ are the unit vectors in the x, y, z directions, respectively; I_x, I_y, I_z are the gradients of the points in the x, y, z directions, respectively. Since the

point cloud data points are disordered and discrete, the points in each raster cell are convolved with a $3 \times 3 \times 3$ convolution kernel, and the new value obtained from it is used as an approximation of the gradient.

Define the convolution kernel M in the x, y, z axis as Eq. 4, Eq. 5, Eq. 6.

$$M_x(x,y,z) = \left[\begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix} \begin{bmatrix} -2 & 0 & 2 \\ -4 & 0 & 4 \\ -2 & 0 & 2 \end{bmatrix} \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix} \right] \tag{4}$$

$$M_y(x,y,z) = \left[\begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix} \begin{bmatrix} 2 & 4 & 2 \\ 0 & 0 & 0 \\ -2 & -4 & -2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix} \right] \tag{5}$$

$$M_z(x,y,z) = \left[\begin{bmatrix} -1 & -2 & -1 \\ -2 & -4 & -2 \\ -1 & -2 & -1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 2 & 1 \end{bmatrix} \right] \tag{6}$$

The gradient is calculated as shown in Eq. 7 and Eq. 8.

$$I_i(x,y,z) = M_i(x,y,z) * P(x,y,z), i = x,y,z \tag{7}$$

$$I(x,y,z) = \sqrt{I_x^2 + I_y^2 + I_z^2} \tag{8}$$

where $*$ is the convolution symbol.

The main idea of the Harris operator is to use the autocorrelation matrix C to explore the localized values of spatial variations at a point $P(x,y,z)$, and to obtain the autocorrelation matrix C using Eq. 9.

$$C = \iiint_{V(x,y,z)} u(x,y,z) \begin{bmatrix} I_x^2 & I_{xy} & I_{xz} \\ I_{xy} & I_y^2 & I_{yz} \\ I_{xz} & I_{yz} & I_z^2 \end{bmatrix} dxdydz \tag{9}$$

where $I_{xy} = I_x \times I_y$ is the product of elements in the direction corresponding; $V(x,y,z)$ denotes the integral volume of the triple-integrated product function; $u(x,y,z)$ is the non-negative weighted window function that satisfies Eq. 10.

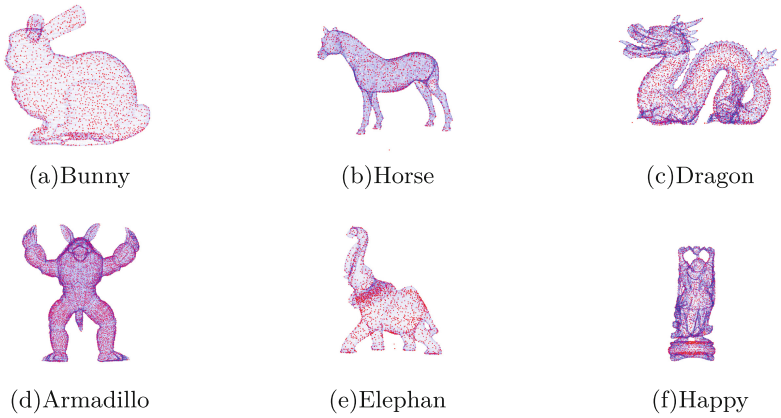
$$\iiint_{V(x,y,z)} u(x,y,z)dxdydz = 1 \tag{10}$$

The corner point response function $H(x,y,z)$ at the point $P(x,y,z)$ location in 3D space is calculated using Eq. (11).

$$H = det(C) - \zeta trac^2(C) \tag{11}$$

where ζ is the constant coefficient, experimentally determined ζ value between 0.03 and 0.06, in the subsequent experiment we take ζ as 0.04, $det(\cdot)$ is the determinant of the matrix, $trac(\cdot)$ is the trace of the matrix. In the spatial neighborhood centered on point P, determine whether the value of H is a local maximum value, and if the judgment is true, record the point, otherwise detect the next point.

In this paper, the improved Harris operator is used to extract corner points from six 3D point cloud models. As shown in Fig. 3, the algorithm extracts a large number of feature points for each model, where the red points represent the feature points.



(a)Bunny (b)Horse (c)Dragon

(d)Armadillo (e)Elephan (f)Happy

Fig. 3. Improved Harris feature point extraction results

SURF Operator. Harris extracted corner points don't have scale invariance, so the SURF with scale invariance is used to further optimize the extraction of feature points. By calculating the local depth values of the extracted point cloud at the corners, the 3D point cloud is projected onto the 2D plane to form a depth image, which is conducive for the SURF to detect the extreme points with scale invariance [12]. SURF is used to detect the extreme points in the depth image around the corner points. After constructing the scale space, the points that reach the maximum value of the Hessian matrix at all scales are identified as extreme points.The Hessian matrix is calculated as shown in Eq. 12.

$$H(L(x,y)) = \begin{bmatrix} \frac{\partial^2 L}{\partial x^2} & \frac{\partial^2 L}{\partial x \partial y} \\ \frac{\partial^2 L}{\partial x \partial y} & \frac{\partial^2 L}{\partial y^2} \end{bmatrix} \tag{12}$$

Before the construction of the Hessian matrix, it needs to be Gaussian filtered, but in order to improve the speed of the Hessian matrix determinant, a box filter approximation is used instead of the Gaussian filter. The Hessian matrix determinant is computed as shown in Eq. (13).

$$det(H) = D_{xx}D_{yy} - (0.9D_{xy})^2 \tag{13}$$

where D_{xx}, D_{xy}, D_{yy} are the convolution of the box filter with the integral image function , respectively.

The precise localization of the extracted feature points. Since the points in the point cloud converted to depth image are discrete values, a second order

Taylor expansion of $D(x, y, z)$ is performed. The second-order Taylor expansion is used to $D(x, y, z)$, and the least squares method is used to fit the spatial function curve and derive the extreme value of the calculated curve, which is the feature point with high stability.

The improved composite Harris-SURF operator is an effective feature extraction method for 3D point cloud models, which is able to extract the feature points of the model uniformly and reasonably. The feature points with strong descriptive performance can be extracted even after affine transformation attack. The noise resistance of the algorithm is improved by suppressing the repeated response points and unstable edge response points. The algorithm quickly eliminates the unimportant points in the point cloud by Harris operator, which reduces the computational amount of feature point screening and improves the operation efficiency of the algorithm. On this basis, more robust feature points are optimally screened by SURF operator, and the number of extracted feature points can be flexibly selected by adjusting the threshold H according to the size of embedded secret information. The effect of the Hessian matrix threshold H on the performance of the algorithm is analyzed in the simulation experiments.

The proposed composite operator is utilized to extract features from3D point cloud models and the extraction results are shown in Fig. 4 (Colored circles are filtered feature points), and Table 1 counts the number of feature points extracted by the algorithm for the six models.

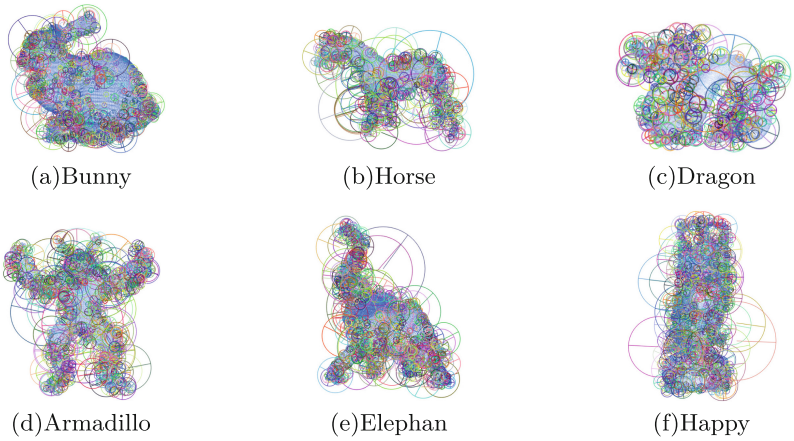


Fig. 4. Composite operator feature point extraction results (Color figure online)

Table 1. Statistics of feature point extraction results

Model	Bunny	horse	Dragon	Armadillo	Elephant	Happy
Vertex number	35947	48485	437645	172974	24955	543653
Eigenpoints	10784	14448	148799	53794	8110	173968

2.3 Embedding and Extraction of Secret Information

Embedding of Secret Information.

- Step1. Using Arnold disorder on the secret message to obtain a new message sequence $w(i,j)$.
- Step2. Filtering embedded regions using an improved composite Harris-SURF operator.
- Step3. NSCT Transformation with Secret Information Embedding. With the extracted feature points as the center, a $q \times q$ matrix Q is constructed as the object of secret information embedding. Perform NSCT transform on matrix Q to obtain its low frequency coefficient matrix R, and perform secret information embedding in matrix R. When the secret information $w(i,j)$ is 0, the coefficient matrix R is modified using Eq. (14).

$$R^{'} = \begin{cases} R(i,j) - \dfrac{s}{2}, & if mod(R(i,j),s) \geq \dfrac{s}{2} \\ R(i,j), & if mod(R(i,j),s) < \dfrac{s}{2} \end{cases} \tag{14}$$

  where $R^{'}$ is the matrix of low-frequency coefficients after embedding the secret information; s denotes the quantization step size, which is generally selected as 8. When the secret information $w(i,j)$ is 1, calculate $R^{'}$ by inverting the $if mod(R(i,j),s)$ in Eq. (14).
- Step4. The secret-containing model can be obtained by reconstructing the inverse NSCT transform of the data after embedding the secret information.

Extraction of Secret Information. Extracting secret information can be understood as the reverse process of information embedding. In the extraction of information, if a region extracts different information than most other regions, the secret information has the possibility of being tampered, which improves the security of the algorithm. The steps for extracting secret information are as follows:

- Step1. Filtering Embedding Region.
- Step2. Follow step 3 in Sect. 2.3.1 to construct a $q \times q$ matrix for the feature points for NSCT transformation and take its low-frequency coefficient matrix. Let the low-frequency coefficient matrix be R_n, and use Eq. (15) to extract the secret information for matrix R_n.

$$w_n(i,j) = \begin{cases} 0, if mod(R(i,j),s) < \dfrac{s}{2} \\ 1, if mod(R(i,j),s) \geq \dfrac{s}{2} \end{cases} \tag{15}$$

3 Experiments

The performance of the algorithm is related to the threshold H of the Hessian matrix. The higher the H, the smaller the embedding capacity and the stronger the robustness. The parameters are set in such a way that the algorithm has high robustness and capacity at the same time. In order to obtain stable

experimental results, six point cloud models are selected for experiments to test the performance of the proposed algorithm and to determine the optimal range of the Hessian matrix determinant threshold H.

Stage 1: Experiment on the relationship between threshold H and volumetricity. Threshold values ranging from 200 $\sim$ 1400 are selected to extract features for six point cloud models, and the average number of feature points for the six models is calculated. Figure 5 shows the variation in the number of average feature points extracted for the six models when different values of H are taken.

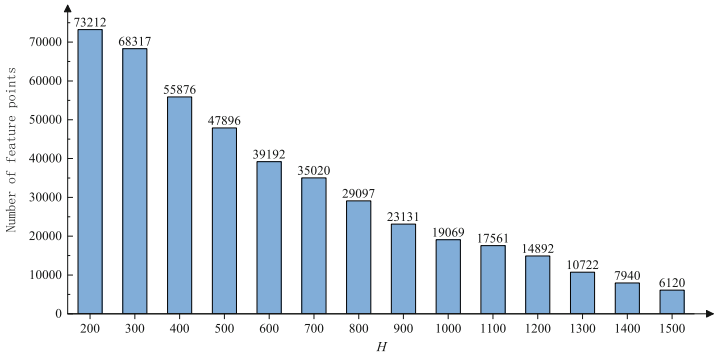


Fig. 5. Number of feature points extracted for different values of H

As can be seen in Fig. 5, the larger the threshold setting the smaller the number of feature points extracted. When the threshold is not specified, the number of extracted feature points averages 130,000 feature points, which can be embedded in approximately 220 bits.

Step 2: Experiment on the relationship between threshold H and robustness. The Corr index is used to measure the robustness, and Corr is the closeness between the extracted secret information and the original secret information. The larger the Corr, the closer it is, and the stronger the robustness. Figure 6 shows the change of Corr corresponding to different H.

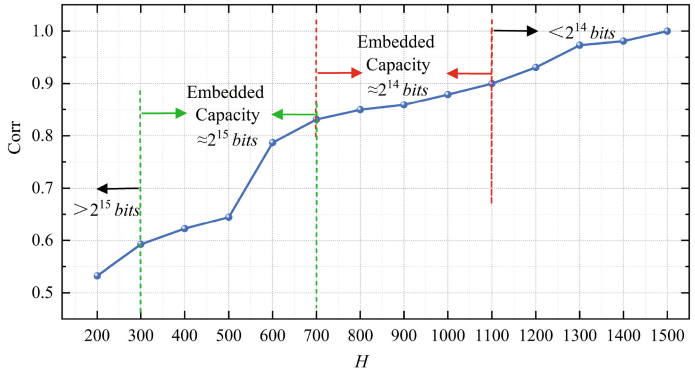


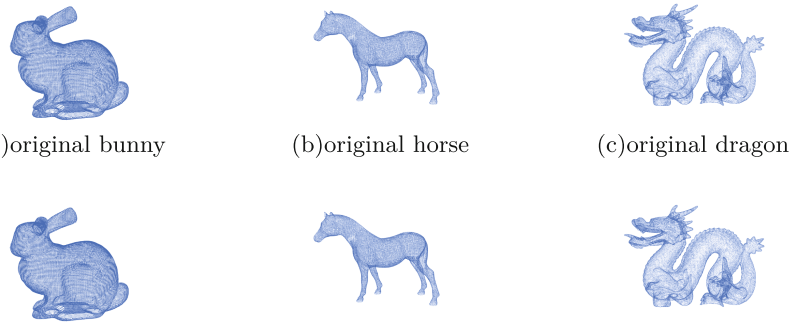
Fig. 6. Corr for different values of H

As can be seen from Fig. 6, the larger the H is set, the Corr gradually rises and the robustness of the algorithm increases. In this paper, the algorithm selects the threshold value within $700 \leq H \leq 1100$ to ensure that the algorithm has high embedding capacity and robustness at the same time.

The proposed algorithm is compared with the Zero-watermarking method (ZWM) [13] and the Dual information hiding (DIH) algorithm [5] for invisibility, robustness, and capacity experiments.

3.1 Invisibility

The evaluation of invisibility is categorized into subjective perception and objective calculation. Subjective perception refers to the inability to find secret information in the encrypted model through human vision. Figure 7 shows that the human eye can't distinguish between encrypted model and original model.



(a)original bunny (b)original horse (c)original dragon

(d)encrypted bunny (e)encrypted horse (f)encrypted dragon

Fig. 7. Invisibility experiment

Maximum Root Mean Square Error (MRMS) was used to objectively measure the invisibility. The experimental results are shown in Fig. 8, and it shows that proposed algorithm has a significant advantage within the embedding capacity of no more than 2^{15} bits and it's average MRMS value is reduced by 11.56% and 5.96% compared to the ZWM and DIH, respectively. This indicates that proposed algorithm invisibility is significantly improved.

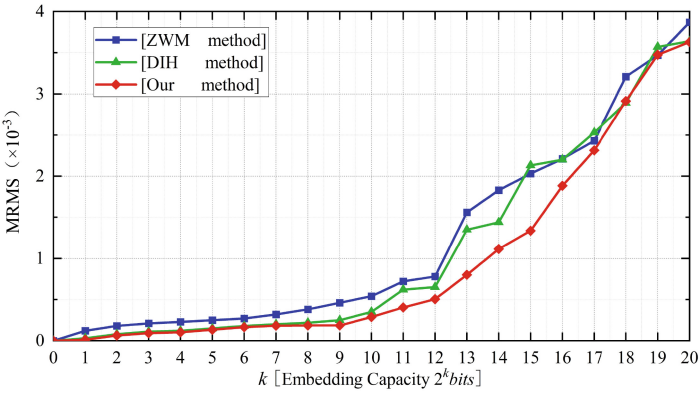


Fig. 8. Comparison of MRMS-based invisibility experiment results

3.2 Robustness

Robustness is the ability of the model to extract the secret information correctly even after an attack, and measuring robustness with Corr and error rate (BER).

Affine Transformation Attack Experiment. The embedding region is extracted by Harris operator with translation and rotation invariance and SURF operator with scale invariance; The secret information is embedded in the NSCT transform domain coefficients, so the embedding region has affine invariance. As shown in Fig. 9, the affine transformation attack experiment is carried out on the encrypted model, and the extracted secret information is consistent with the original secret information, and the correlation coefficient Corr = 1.

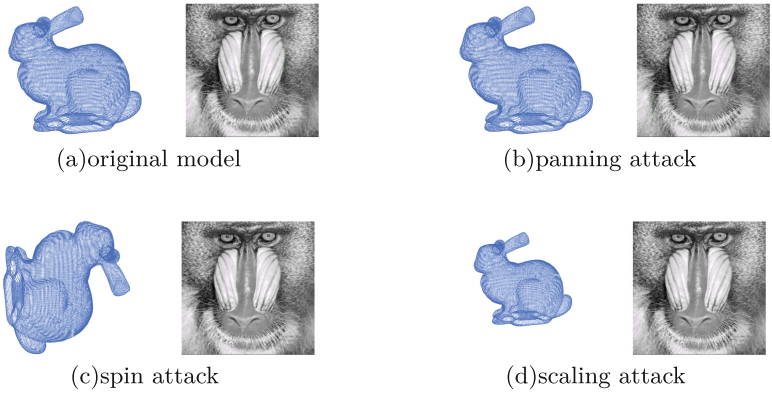


Fig. 9. Affine transformation attack

Noise Attack Experiment. When processing the noise attack on the dense-containing model, the added noise vectors will affect the information such as the curvature of the vertices. However, the proposed algorithm introduces orthogonal convolutional gradients before the Harris operator extracts the corner points, which effectively suppresses the noise effect. The Bunny model attacked by noise and the secret information extracted from it are shown in Fig. 10. For 0.1% noise amplitude, it is still possible to visually be able to recognize the extracted secret information, and for 0.5% noise intensity attack, the extracted secret information is visually compromised, and the subjective ability to perceive that there is an error rate in the extraction of the secret information.

(a) 0.1% noise (b) 0.5% noise

Fig. 10. Noise experiment

Figure 11 shows the BER values of the three algorithms for the Bunny model when attacked by 0%∼1% noise. The average value of BER of the proposed algorithm is reduced by 10.53% and 16.7% compared to ZWM and DIH respectively. Therefore, the proposed algorithm has a strong resistance to noise compared to the compared algorithms.

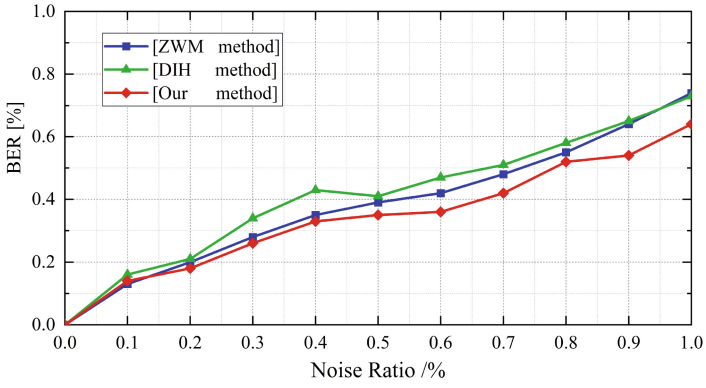


Fig. 11. Comparison of Noise Attack Experimental Results (BER)

Shear Attack Experiments. Shear attack experiments are done on the encryption model and the results are shown in Fig. 12. When the Bunny model is subjected to 5% shear attack, the extracted secret message can still be recognized; however, when it is subjected to 10% shear attack, according to Fig. 12(b), it can be seen that the extracted secret message is affected, and the performance of the proposed algorithm has begun to degrade. The shear attack is a direct cropping of the 3D model so that some vertices of the 3D model are lost. Since the proposed algorithm does not embed the secret information in different vertices repeatedly for many times, the complete secret information cannot be extracted when the model is subjected to a larger degree of shear attack. In the subsequent research of the algorithm, the algorithm needs to be further improved to cope with the shearing attack.

(a)Shear 5% (b)Shear 10%

Fig. 12. Shear Attack Experiments

Figure 13 shows that when the clipping rate is 30%, the BER values of the proposed algorithm, DIH and ZWM are 0.68, 0.75 and 0.8 respectively, and the proposed algorithm reduces the BER by 9.34% and 15% compared to the DIH and ZWM algorithms. Even after cropping 30% of the points, the proposed algorithm extracts more complete secret information compared to the comparison algorithms.

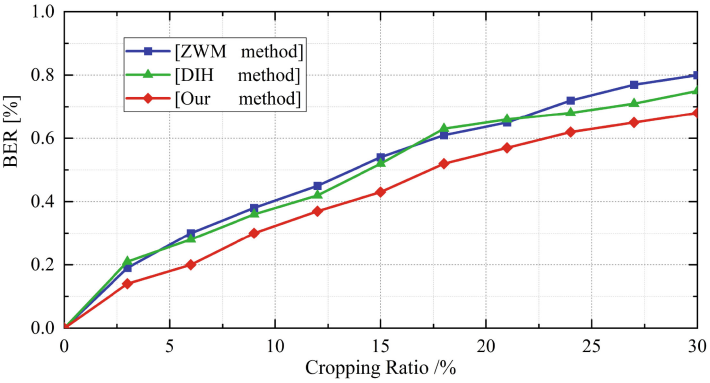


Fig. 13. Comparison of shear attack experimental results

Simplified Attack Experiments. Simplified attack experiments are done on the encryption model. Figure 14 shows that the proposed algorithm is able to extract the secret information more completely even with 5% and 15% simplification attacks. The simplification attack mainly targets the vertices that do not have important properties in the 3D point cloud model, and most of the unimportant vertices are lost in the secret-containing model after the simplification attack. The proposed algorithm accomplishes the secret information hiding in the vertices that really have the performance of surface shape description, so the encrypted model can extract the more complete secret information even if it suffers from the simplification attack.

(a)Simplified 5% (b)Simplified 15%

Fig. 14. Simplified Attack Experiments

As can be seen from Fig. 15, the BER value of the proposed algorithm is lower than the comparison algorithm when subjected to the same degree of simplification attack. When the simplification rate is 30%, the BER values of the proposed algorithm, ZWM and DIH are 0.73, 0.8 and 0.81, respectively, and the proposed algorithm reduces the BER values by 8.75% and 9.88% compared to ZWM and DIH, respectively, which indicates that the proposed algorithm is robust to simplification attacks.

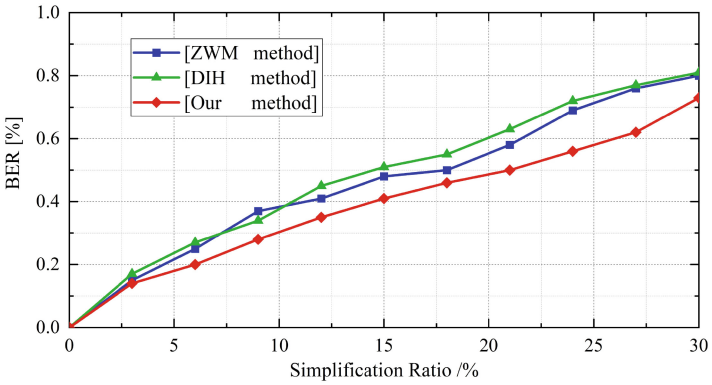


Fig. 15. Comparison of simplified attack experimental results

Compound Attack. In the actual transmission of the public channel, the model is attacked by multiple attacks at the same time. A compound attack experiment is carried out on the proposed algorithm. Table 2 shows some experimental data, where Sim, Noi and Dro represent 10% simplification, 0.5% noise and 10% cut, respectively. Under the attack of 10% simplification, 0.5% noise and 10% clipping, the average value of Corr is 0.729. Experimental results show that the proposed algorithm still has high robustness in the face of compound attacks.

Table 2. Compound attack experiment results

Experiment	Model with Secret Information				Corr
	Bunny	Dragon	Amadillo	Happy	
Experiment 1	Sim	Noi			0.7851
Experiment 2		Sim	Noi		0.7742
Experiment 3	Noi			Sim	0.7517
Experiment 4		Noi	Dro		0.7489
Experiment 5	Dro			Noi	0.7487
Experiment 6	Sim	Noi	Dro		0.7287

3.3 Capacity Analysis

The number of facets and vertices of each model varies, and the embedding ability cannot be evaluated only by the total embedding amount, so the maximum embedding rate index is used to evaluate the embedding ability. Table 3 shows that the proposed algorithm improves the maximum embedding rate by 14.2% on average over the DIH algorithm.

Table 3. Capacity analysis experiment

Model	Vertices	Grid	Embedded rate	
			DIH	Our
Bunny	35947	69451	0.799	0.901
Armadillo	172974	345944	0.807	0.933
Happy	543652	1087716	0.875	0.960

4 Conclusions

In this paper, a plaintext domain information hiding algorithm based on multi-scale transform and composite operator is proposed. The algorithm utilizes the improved Harris-SURF operator to extract features from the point cloud model,

which can efficiently extract robust feature points; then the embedding region is transformed to the NSCT domain, and the quantization-based embedding method is used to embed the secret information into the low-frequency coefficient matrix to realize the hiding of secret information. The threshold value can be adjusted in the practical application so that the capacity and robustness of the algorithm can reach an optimal balance. The experimental results show that the invisibility and robustness of the proposed algorithm are better than the current more advanced algorithms.

References

1. Ohbuchi, R., Masuda, H., Aono, M.: Watermarking three-dimensional polygonal models. In: Proceedings of the fifth ACM International Conference on Multimedia (1997)
2. Ohbuchi, R., Masuda, H., Aono, M.: Watermarking three-dimensional polygonal models through geometric and topological modifications. IEEE J. Select. Areas Commun. 551–560 (1998)
3. Hamidi, M., Chetouani, A., El Haziti, M., El Hassouni, M., Cherifi, H.: Blind robust 3D mesh watermarking based on mesh saliency and wavelet transform for copyright protection. Information **10**(2), 67 (2019)
4. Nam, S.H., et al.: NSCT-based robust and perceptual watermarking for DIBR 3D images. IEEE Access. **8**, 93760–93781 (2020)
5. Shuai, R., Huirong, C., Aoxiong, F.: Dual information hiding algorithm based on the regularity of 3D mesh model. Optoelectron. Lett. **18**(9), 559–565 (2022)
6. Boyer, E., et al.: SHREC 2011: robust feature detection and description benchmark. arXiv preprint arXiv:1102.4258 (2011)
7. Hartkens, T., Rohr, K., Stiehl, H.S.: Evaluation of 3D operators for the detection of anatomical point landmarks in MR and CT images. Comput. Vis. Image Underst. **86**(2), 118–136 (2002)
8. Xi, W., Shi, Z., Li, D.: Comparisons of feature extraction algorithm based on unmanned aerial vehicle image. Open Phys. **15**(1), 472–478 (2017)
9. Kovač, I., Marák, P.: Finger vein recognition: utilization of adaptive Gabor filters in the enhancement stage combined with sift/surf-based feature extraction. Signal Image Video Process. **17**(3), 635–641 (2023)
10. Zhang, F., Zhang, C., Yang, H., Zhao, L.: Point cloud denoising with principal component analysis and a novel bilateral filter. Traitement du Signal (2019)
11. Phan, A.T.T., Huynh, T.N.: Pavement crack extraction method from mobile laser scanning point cloud. In: Advances in Civil Engineering (2022)
12. Roveri, R., Rahmann, L., Oztireli, C., Gross, M.: A network architecture for point cloud classification via automatic depth images generation. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (2018)
13. Liu, G., Wang, Q., Wu, L., Pan, R., Wan, B., Tian, Y.: Zero-watermarking method for resisting rotation attacks in 3D models. Neurocomputing **421**, 39–50 (2021)