# Dual information hiding algorithm based on the regularity of 3D mesh model*

**REN Shuai[1], CHENG Huirong[1]**, and FAN Aoxiong[2]**

*1. School of Information Engineering, Chang'an University, Xi'an 710064, China*

*2. School of Science, Xi'an University of Architecture and Technology, Xi'an 710055, China*

(Received 18 March 2022; Revised 8 June 2022)



Aiming at the problems of low embedding capacity and inflexibility of embedded information in current three-dimensional (3D) model information hiding technology, a dual information hiding algorithm based on the mesh characteristics of 3D model is proposed. The algorithm adopts the strategy of double embedding. By analyzing the regularity of each region of the 3D model, the feature regions with higher regularity are extracted for embedding secret information. First, in these feature areas, the first secret information is embedded by changing the order of the face list of the object (OBJ) file of the 3D model. Secondly, filter the triangular meshes according to the regularity, calculate the angle between the plane normals of the two adjacent triangular meshes where the two vertices are adjacent, use the discrete cosine transform to process the angle sequence, and secret information is embedded in the transformation coefficients. The experimental analysis shows that the algorithm can significantly improve the embedding capacity and robustness, and it can effectively resist severe shear attack, geometric attack, and a certain degree of noise attack.

**Document code:** A **Article ID:** 1673-1905(2022)09-0559-7

**DOI** https://doi.org/10.1007/s11801-022-2035-4

With the development of Internet technology and the popularization of mobile devices, the phenomenon of illegal tampering and transmission of information has become more and more serious. In recent years, information hiding technology, as an important means of stealth communication, has become a hot spot in the field of information security and has been widely used. Information hiding technology refers to hiding secret information in the transmission carrier in the process of communication transmission, making it difficult for people to detect the existence of the secret information, thus effectively protecting the secret information and achieving the purpose of safe transmission.

Scholars have put forward various articles and achievements on information hiding. According to the embedding region of secret information, it can be divided into two algorithm types, spatial domain and transform domain[1]. Spatial domain algorithms embed secret information by modifying the geometry of a three-dimensional (3D) model. In 1997, OHBUCHI proposed the 3D model digital watermarking technology. Later, the triangle similarity quadruple (TSQ) algorithm and the tetrahedral volume ratio (TVR) algorithm based on the 3D mesh model were proposed[2]. Such algorithms can effectively resist geometric attacks, but cannot effectively resist mesh reconstruction and polygon simplification attacks. TSAI[3] used a spatial encoding method with an embedding threshold to embed secret messages into encrypted vertices. The algorithm has high secrecy, low computational complexity, and high embedding capacity. PENG et al[4] generalized two-dimensional (2D) region nesting to $n$-dimensional space. By placing original vertices and mapped vertices on a straight line to embed watermarks, the algorithm can significantly reduce distortion. The transform domain algorithm transforms the 3D model into the transform domain and modifies the transform coefficients to embed the secret information. HAMIDI et al[5] proposed a 3D mesh blind robust watermarking algorithm based on mesh saliency and wavelet transform. According to the mesh saliency of 3D semi-regular mesh, the wavelet coefficients were quantized and embedded in the watermark by quantization index modulation, which has a high imperceptibility. Al-SAADI et al[6] proposed 3D object vertex embedding based on the properties of discrete cosine transform in secret grayscale images three times, and the watermarking process is performed by using vertex coefficients and encrypted image pixels with high invisibility.

However, there are few researches on information hiding algorithms combining the spatial domain and the transform domain. This paper proposed a new dual information hiding algorithm based on the combination of the spatial domain and the transform domain. The comparison

* This work has been supported by the National Natural Science Foundation of China (No.61702050), and the Fundamental Research Funds for the Central Universities, CHD (No.300102240208).

** E-mail: chr@chd.edu.cn

of dual information hiding algorithms is shown in Tab.1. Through multiple embeddings in different regions, the shortcoming of insufficient capacity of single embedding is overcome. At the same time, according to the characteristics of the secret information, it is possible to choose whether to embed the same secret information twice. The flexibility of the algorithm is strong, which makes the algorithm achieve a better balance in terms of robustness, invisibility and capacity, and provides ideas for secure communication and copyright protection.

**Tab.1 Comparison of dual information hiding algorithms**

| Algorithm | Embedded domain | Main idea | Purpose | Double embedding advantage |
|---|---|---|---|---|
| Layer 1 embedding algorithm | Spatial domain | The regularity of triangular meshes is calculated, triangular meshes with different regularity are classified, and information embedding is realized by modifying the face list of 3D model object (OBJ) file. | By embedding the secret information into the face list of the OBJ file, the invisibility of the carrier containing secret information is greatly improved. | By adopting the double embedding strategy, the capacity, robustness and invisibility of the secret information carrier can reach the maximum balance. At the same time, according to the characteristics of secret information, it is flexible to choose whether to embed the same secret information twice. |
| Layer 2 embedding algorithm | Transform domain | Select a triangle mesh that meets the regularity threshold, calculate the included angle between the plane normals of two vertices adjacent to the triangle mesh, and use discrete cosine transform (DCT) to process some sequences with larger included angles to realize information embedding. | DCT transform is used to embed the secret information into the included angle of the plane normal of the triangular mesh that meets the threshold, which significantly improves the capacity and robustness of the carriers containing secret information. | |

The first layer of secret information embedding process is shown in Fig.1.

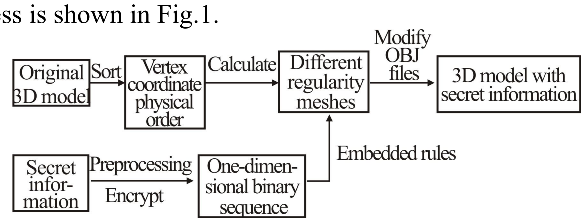



**Fig.1 The first information hiding flow chart**

The first layer of information hiding is to embed secret information into the spatial domain. The steps are described as follows.

**(1) Calculate the appropriate embedding region**

**Step 1**. Get the physical order of all vertices of the original 3D mesh model. Traverse all vertices and sort, and use a double-layer linked list structure to store the topology information of the 3D model. Specifically, traverse all triangular meshes $f_w$ and vertices $v_i$ of the 3D model according to the principle of "axis first, then vertices", and sort them according to the size of the vertex coordinates. The first layer stores the number $t$ of each triangle and vertex number $v$. The second layer stores each vertex number $v$ and the coordinate value $v_i$ of the vertex and the regularity $R$ of the triangle. After the above three steps, the topological structure of the 3D model is adjusted, the storage capacity is optimized, and the subsequent processing and calculation are facilitated.

**Step 2.** Calculate the regularity $R$ of each triangular mesh. The quality of the 3D model mesh is usually judged by the regularity $R$ of the triangle. The closer the triangular mesh ($R\to1$) is to a regular triangle, the higher the mesh quality.

The evaluation criteria for the regularity of a triangle mainly include the angle method, the side length method and the area method[7]. In this paper, the area method is selected for calculation. The calculation formula of the area method is

$$R=\frac{4\times\sqrt{3}\times S}{l_1^2+l_2^2+l_3^2}, \tag{1}$$

where $R$ is the regularity representing the quality of the triangular mesh, $l_1$, $l_2$, and $l_3$ are the lengths of the three sides of the triangle, and $S$ is the area of the triangle. $S$ can be obtained from Heron's equation as

$$S=\sqrt{(l'\times(l'-l_1)\times(l'-l_2)\times(l'-l_3))}, \tag{2}$$

$$l'=\frac{l_1+l_2+l_3}{3}. \tag{3}$$

At the same time $R\in(0, 1]$, it can be seen that the larger the value of regularity, the better the quality of the triangular mesh. When the mesh shape is a regular triangle, $R$=1. When the mesh shape is like a long and narrow triangle, its regularity $R\to0$. Judging whether a triangle is an elongated triangle is based on the regularity $R$ of the triangular mesh. The judgment range of an elongated triangle is $0< R\le h$, and $h$ is the discrimination threshold of the narrow triangle. In this paper, $h$ is set to 0.4, that is, the triangle with $R<0.4$ is narrow.

According to the topological order of the 3D model obtained in Step 1, the regularity of all triangular meshes is calculated according to the area method formula, and the results are stored in the corresponding position of the second-layer linked list.

**(2) Embedding of secret information**

**Step 1.** Preprocessing of secret information: According to the spread spectrum technology mentioned in Ref.[8], the secret information is binarized, and expand the original character secret information $b_i$ ($i$=1, 2, ..., $m$) into a one-dimensional binary bit sequence $I_i$ ($i$=1, 2, …, $m$), which is beneficial to the embedding of secret information. In order to improve the reliability performance, the binary sequence $I_i$ is scrambled, and a pseudo-random sequence is generated according to the key, thereby obtaining a one-dimensional binary bit sequence $w_i$ ($i$=1, 2, ..., $m$).

**Step 2.** Update the topology information of the 3D model. Adjust the triangular mesh with regularity $R$> 0.9 according to Eq.(3). The adjusted triangular mesh is a regular triangle ($R$=1). After adjustment, the data in the double-layer linked list is updated. Repeat the above steps until all mesh adjustments are complete.

**Step 3.** Embedding secret information. The length of the secret information is $m$, and the total length of embedding is $(m+1)\times p$, which is the total number of triangular meshes needed. $m$+1 represents the length of a single set of secret information, and $p$ represents the number of repeated embedding. Before the secret information is embedded, the regular triangle with $R$=1 is used as the starting flag bit, and then the embedding is started. According to the embedding rule, the secret information is embedded, and the idea of bubbling sorting is added when embedding information. By comparing the regularity $R$ of adjacent triangular meshes, the triangular mesh of the current position is determined. After embedding many times, the topological order of the remaining triangular meshes that did not participate in embedding remains unchanged. Finally, the face list of the 3D model OBJ file is modified according to the triangular mesh order, and the secret information is embedded. The embedding rule is shown as

$$R=\begin{cases} R=1 \rightarrow \text{Embed start tag} \\ R\le 0.4 \rightarrow w_i=0 \\ R>0.4 \rightarrow w_i=1 \end{cases}, \quad i\in[1, 2, 3, ..., m]. \quad (4)$$

**(3) Extraction of secret information**

The extraction process of secret information can be regarded as the inverse operation of the information hiding process. The first hidden information extraction is mainly divided into the following steps.

**Step 1.** Calculate the regularity $R$ of each triangular mesh of the carrier containing the secret information.

**Step 2**. Read the face list in the received carrier OBJ file containing secret information, and start extracting information according to Eq.(4) in combination with the regularity $R$ of the triangular mesh.

**Step 3.** After the extraction, a one-dimensional binary bit sequence $w_i$ is obtained. In order to ensure the accuracy of the secret information, multiple extraction methods can be used for comparison and verification.

**Step 4.** Utilize the key to carry out the decryption operation to the bit sequence, according to the bit sequence $I_i$ obtained after decryption, and utilize the spread spectrum technique[8] to recover and obtain the initial secret information $b_i$.

The second secret information embedding process is shown in Fig.2.

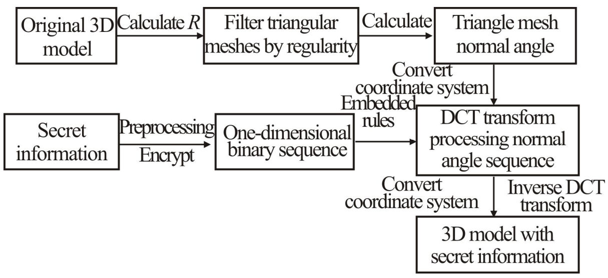



**Fig.2 The second information hiding flow chart**

The second of information hiding is to embed secret information into the frequency domain. The steps are described as follows.

**(1) Selection and calculation of feature regions**

**Step 1.** Calculate the normals of the triangular mesh faces. In order to improve the invisibility of the carrier, in the embedded area of this algorithm, select triangles with higher mesh quality, and set the threshold to [0.65, 0.95].

**Step 2.** Filter out all the triangular mesh surfaces that meet the threshold, and group all the triangular mesh surfaces containing $v_i$ into the set $H(v_i)$, and all the adjacent vertex of $v_i$ forms the set $L(v_i)=\{v_j|\ |v_iv_j|>0, j=1, 2, 3, …, n, i\neq j\}$.

**Step 3.** Calculate the angle between the normals of two adjacent triangular meshes on the edge of vertex $v_i$ and vertex $v_j$, and obtain the embedded area as

$$\varpi(v_i)=\sum\nolimits_{v_j\in L(v_i)}\frac{1}{\cos(u_{v_i}\bullet u_{v_j})}, \quad (5)$$

where $\frac{1}{\cos(u_{v_i}\bullet u_{v_j})}$ represents the angle between vertex $v_i$ and vertex $v_j$ adjacent to the triangular mesh normal, and the calculated $\varpi(v_i)$ is arranged in descending order.

**(2) Embedding of secret information**

**Step 1.** Coordinate system conversion. The center of the 3D model is translated to the origin of coordinates, and the 3D model is converted from the rectangular coordinate system to the spherical coordinate system according to

$$r_i=\sqrt{x_i^2+y_i^2+z_i^2},$$

$$\varphi_i=\arctan(\frac{y_i}{x_i}),$$

$$\theta_i=\arccos(\frac{z_i}{r_i}),$$

$$r_i\in[0,+\infty]; \quad \varphi_i\in[0,2\pi]; \quad \theta_i\in[0,\pi]. \quad (6)$$

**Step 2.** The length of the secret information is $l$, and the first $n\times p$ data of the $\varpi(v_i)$ sequence are taken out, and $p>l$, and each $p$ data is a group, and $n$ represents the number of times of repeated embedding. Here it is the same as the first embedding, and repeated embedment is adopted. Thus, the modulo length of each set of data forms a sequence $S=\{s_i, i=1, 2, 3, \ldots, n\times p\}$.

**Step 3.** The secret information is processed according to the first information hiding step to obtain a one-dimensional binary sequence $w_i$ ($i=1, 2, \ldots, k$), and $w_i$ is modified according to

$$w_i' = \begin{cases} -1, w_i = 0 \\ +1, w_i = 1 \end{cases}, \quad i = 0, 1, 2, ..., l. \tag{7}$$

Perform DCT[7] transformation on each value in the sequence $S$, the transformed coefficient sequence $G=\{g_i, i=1, 2, 3, \ldots, p\}$, the sequence selects $l$ transformation coefficients $g_i$, $g_2$, $g_3$, …, $g_i$, the secret information is embedded according to Eq.(8), and the rest of the transformation coefficients remain unchanged, where $\alpha$ represents the embedding strength factor, and $\alpha$ of the algorithm in this paper is 0.001.

$$g_i' = \begin{cases} g_i + \alpha, w_i = 1 \\ g_i - \alpha, w_i = -1 \end{cases}, \ i \in [1, l]. \tag{8}$$

**Step 4.** Perform inverse DCT transformation on $g_i$ to obtain a new modular length sequence $S'=\{s'_i, i=1, 2, 3, \ldots, n\times p\}$, and then convert the 3D model back to the Cartesian coordinate system according to Eq.(9). After completing the embedding of secret information, a 3D model containing secret information is obtained.

$$x_i = r \times \sin\theta \times \cos\varphi,$$
$$y_i = r \times \sin\theta \times \sin\varphi,$$
$$z_i = r \times \cos\theta. \tag{9}$$

**(3) Extraction of secret information**

**Step 1.** Calculate the regularity $R$ of the triangular meshes of the model to be extracted, filter the triangular meshes that meet the requirements according to the conditions, and calculate the normal $\Psi$ of the triangular meshes.

**Step 2.** Calculate the angle $\varpi(v_i)$ between the plane normals $\Psi$ of the adjacent meshes on the sides of the two vertices, and arrange them in descending order.

**Step 3.** Set the sequence of the angle modulo length between the triangular mesh plane normals of the carrier model containing the secret information as $S^*=\{s_i^*, i=1, 2, 3, \ldots, p\}$, and perform a discrete cosine transform on $S^*$ , the coefficient sequence obtained after transformation is set to $G^*=\{g_i^*, i=1, 2, 3, \ldots, p\}$.

**Step 4.** Subtract the DCT coefficient sequence $G$ of the original 3D model and the DCT coefficient sequence $G^*$ of the carrier model with secret information respectively $\zeta_i=g_i^*-g_i$ to obtain the difference sequence $\zeta=\{\zeta_i, i=1, 2, 3, \ldots, l\}$. Perform extraction according to

$$w_i^* = \begin{cases} w_i^* = -1, \varsigma_i < 0 \\ w_i^* = +1, \varsigma_i \ge 0 \end{cases}, \quad i \in [1, l]. \tag{10}$$

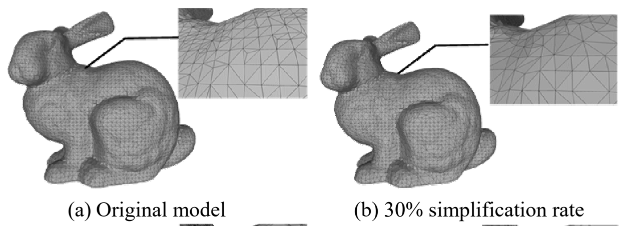
**Step 5.** The extracted $w_i^*$ is inversely mapped according to Eq.(7) to obtain $w_i$, and the key is used to decrypt the bit sequence $w_i$. According to the bit sequence $I_i$ obtained after decryption, the original secret information $b_i$ is recovered by the spread spectrum technique.

The experiments focus on testing the robustness of the algorithm. The simulation experiment was carried out under the Windows platform, using Autodesk 3DS Max 2016, MATLAB, VC++6.0, and using MeshLab software to check the model effect. Several groups of unified standard 3D test models provided by Stanford University were selected to obtain relatively stable experimental results, and at the same time, the performance of the information hiding algorithm in different structural models was tested. The secret information is randomly generated 1 000 bit binary bit data.

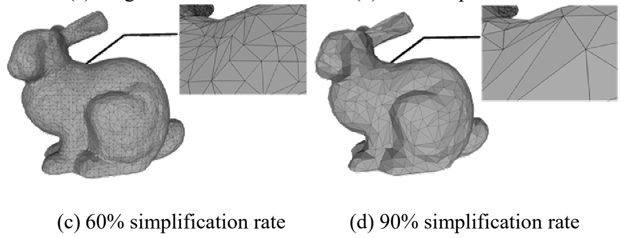
The general evaluation criterion used to evaluate the robustness of the algorithm is correction ($Corr$)[9]. The value of $Corr$ is between [−1,1]. When the $Corr$ is 1, it means that the received secret information is the same as the initial secret information. Conversely, the smaller the correlation coefficient, the weaker the robustness. In this paper, the threshold is set to 0.5. In addition, the objective indicator bit error rate ($BER$)[13], that is, the correct information extraction rate, is used to measure the robustness of the algorithm of the article. The value range of the $BER$ is [0, 1]. The higher the $BER$, the more errors in the extracted secret information and the weaker the robustness, and vice versa.

Since the algorithm preprocesses the 3D model to a geometrically invariant space[14] before embedding, and it has affine invariance, there will be no change after the geometrical attack. Therefore, the $Corr$=1 can resist geometric attacks such as rotation, translation, and uniform scaling, and can resist geometric transformation attacks.

The mesh simplification attack experiment is carried out on the 3D information carrier containing secret information. The Bunny models with simplification rates of 30%, 60% and 90% are shown in Fig.3. And the experimental results are shown in Fig.4.



(a) Original model (b) 30% simplification rate



(c) 60% simplification rate (d) 90% simplification rate

**Fig.3 Mesh simplification attack on Bunny model**

The algorithm adopts the method of double embedding in the spatial domain of the carrier model and frequency domain, and each embedding is multiple embeddings. The simplification attack changes the vertex positions of the 3D model and the topological connection of the patches, which leads to the change of the storage order in the model file. It can be seen from the experimental results that when the simplification rate exceeds 40%, the deformation of the carrier leads to a significant increase in *BER*, and the correct rate of extracting secret information is greatly reduced. Therefore, the mesh simplification attack has a greater impact on the algorithm.

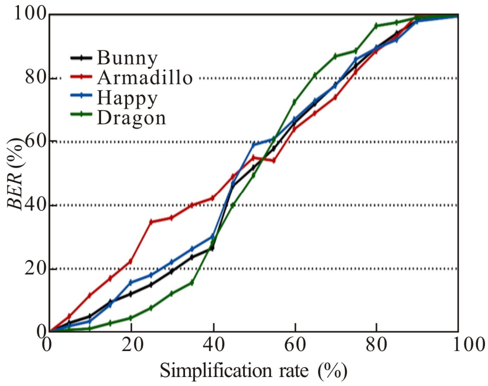



**Fig.4 *BER* results of mesh simplification attack**

Noise attack[15] experiments are carried out on 3D carriers containing secret information, and uniform random noise is added to the vertices of the model. The experimental results of noise attack of Bunny and Armadillo models are compared in Fig.5 and Fig.6.

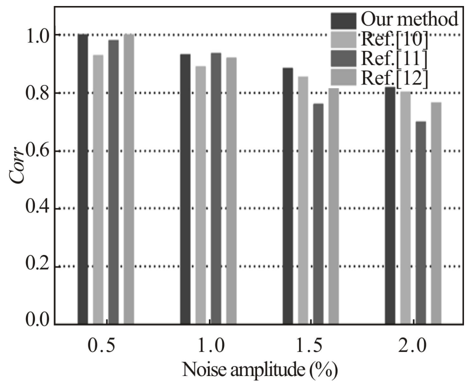



**Fig.5 Correction results comparison of noise attack**

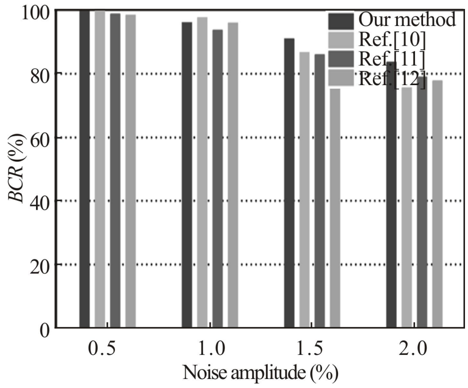



**Fig.6 *BCR* results comparison of noise attack**

It can be seen from Fig.5 and Fig.6 that as the noise amplitude gradually increases, the impact on the model is greater. When the noise amplitude is 2%, the visual effect of the carrier has been seriously affected. However, the first algorithm in this paper is for the face list embedding of the OBJ file of the 3D model. The noise attack will not change the storage order of the triangular mesh faces, so it can maintain a high accuracy rate after extraction. At the same time, Fig.6 shows that the *BCR* value of the algorithm in this paper is also higher than that of the comparison algorithm, so the algorithm in this paper can reflect relatively strong robust performance when dealing with noise attacks.

Joint attack experiments are carried out on 3D carriers containing secret information. Tab.2 gives the results of eight joint attack experiments on the model, where Cut, Noi, and Sim represent 25% shear, 1% noise amplitude, and 20% simplification, respectively. Fig.7 shows the experimental results based on the Dragon model under joint attack.

According to Tab.2, when the algorithm simultaneously deals with 25% shear, 1% noise amplitude and 20% simplified attacks, the mean of *Corr* and *BCR* are 0.516 and 46.50%, respectively. It can be seen from Fig.7 that when the algorithm resists the general joint attack of 25% shear, 20% simplification and 1.3% noise amplitude, the *BCR* can keep above 80%. When dealing with a high-intensity combined attack of 36% shear, 40% simplification and 2% noise amplitude, the *BCR* can also reach 52.50%. In summary, the proposed algorithm has strong robust performance and can resist high-strength combined attacks.

Using the method proposed in this paper, the models are respectively subjected to capacity experiments, and the capacity of embedding can be determined according to the number of embedding multiples. Tab.3 shows the maximum embedding capacity for embedding secret data in different 3D models. Tab.4 compares the computational complexity of the proposed method with existing algorithms.

Ref.[10] can achieve a high embedding capacity of up to 131 072 bits by embedding secret information and eigenvectors into the DCT transform domain coefficients, but it needs to associate the secret image with the feature vector, and the high computational complexity limits its algorithm efficiency. Ref.[11] encapsulates the original secret information into a carrier image, performs sparsity analysis on the components, and selects the most suitable embedding position. The complex mechanism can handle high-capacity secret information, but is sensitive to the selection of relevant parameters. In addition, the algorithm cannot effectively resist simplification attacks. Ref.[12] embeds secret information by changing the histogram of the radial coordinates of the vertices. The algorithm is simple and effective, but its capacity is low. The proposed algorithm embeds secret information in the spatial domain by changing the order of the face list and changing the coefficients in the transform domain, and the algorithm has low computational complexity. Experimental results demonstrate that the proposed algorithm not only outperforms other existing methods in terms of capacity, but also maintains satisfactory robustness. Furthermore, the complexity of the embedding and extraction process is lower than other existing information hiding schemes.

**Tab.2 Experimental results of joint attack**

| Experiment number | | 3D model with secret information | | *Corr* | *BER* |
|---|---|---|---|---|---|
| | | Bunny | Dragon | | |
| Experiment 1 | Type of attack | Cut, Noi | / | 0.845 | 7.64% |
| Experiment 2 | | / | Cut, Sim | 0.796 | 13.37% |
| Experiment 3 | | / | Noi, Sim | 0.683 | 19.82% |
| Experiment 4 | | Cut, Noi, Sim | / | 0.536 | 41.66% |
| Experiment 5 | | Cut, Sim | / | 0.736 | 20.28% |
| Experiment 6 | | / | Cut, Noi, Sim | 0.495 | 51.35% |
| Experiment 7 | | / | Cut, Noi | 0.827 | 11.80% |
| Experiment 8 | | Noi, Sim | / | 0.652 | 33.33% |

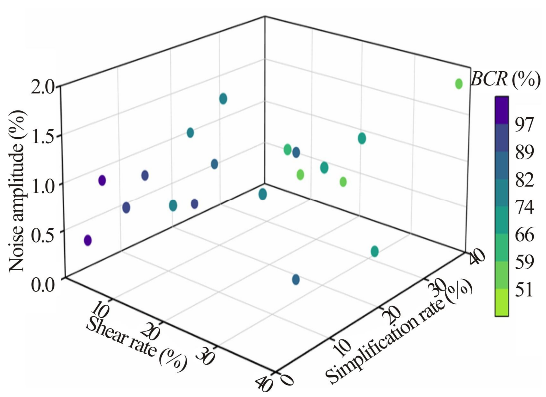



**Fig.7 Experimental results of joint attack**

**Tab.3 Embedding capacity of different models**

| Model | Number of triangular meshes | Number of available triangular meshes | Embedded capacity (bit) |
|---|---|---|---|
| Bunny | 69 451 | 27 780 | 41 670 |
| Armadillo | 345 944 | 138 377 | 207 565.5 |
| Happy | 1 087 716 | 435 086 | 652 629 |
| Dragon | 871 414 | 348 565 | 522 847.5 |

**Tab.4 Computational complexity of different algorithms**

| Algorithm | Ref.[10] | Ref.[11] | Ref.[12] | Proposed |
|---|---|---|---|---|
| Embedding method | Transform domain | Spatial domain | Transform domain | Double embedding |
| Computational complexity | High | High | Low | Low |
| Embedding capacity | High | High | Low | High |

For the dual information hiding algorithm based on the mesh characteristics of the 3D model proposed in this paper, the secret information is double embedded in space domain and frequency domain, and does not interfere with each other during the embedding process. At the same time, dual embedding ensures a better balance of robustness, capacity and invisibility. The experimental results show that after the secret information is embedded by the algorithm, it has good invisibility, and can resist attacks on 3D models, such as geometric attacks, shear attacks and noise attacks. The carrier has good performance.

## Statements and Declarations

The authors declare that there are no conflicts of interest related to this article.

## References

[1] LI Z, BORS A G. Steganalysis of meshes based on 3D wavelet multiresolution analysis[J]. Information sciences, 2020, 522：164-179.

[2] OHBUEHI R, MASUDA H, AONO M. Watermarking three-dimensional polygonal models though geometric and topological modifications[J]. IEEE journal on selected areas in communications, 1998, 16(4)：551-560.

[3] TSAI Y Y. Separable reversible data hiding for encrypted three-dimensional models based on spatial subdivision and space encoding[J]. IEEE transactions on multimedia, 2021, 23：2286-2296.

[4] PENG F, LONG B, LONG M. A general region nesting based semi-fragile reversible watermarking for authenticating 3D mesh models[J]. IEEE transactions on circuits and systems for video technology, 2021, 31(11)：4538-4553.

[5] HAMIDI M, CHETOUANI A, HAZITI M E, et al. Blind

robust 3D mesh watermarking based on mesh saliency and wavelet transform for copyright protection[J]. Information-an international interdisciplinary journal, 2019, 10(2)：67.

[6] Al-SAADI H S, GHAREEB A, ELHADAD A. A blind watermarking model of the 3D object and the polygonal mesh objects for securing copyright[J]. Computational intelligence and neuroscience, 2021, 2021：1392903.

[7] CAO Z H, HUANG C B, ZHENG H. Feature preserving mesh simplification based on hybrid collapse[J]. Optics and precision engineering, 2019, 27(4)：971-983. (in Chinese)

[8] ZHANG F, ZHANG H, ZHANG P, et al. Optical domain despreading method of optical time-domain reflectometer using spread spectrum technology[J]. Optical engineering, 2021, 60(5)：055103.

[9] SHARMA N, PANDA J. Statistical watermarking approach for 3D mesh using local curvature estimation[J]. IET information security, 2020, 14(6)：745-753.

[10] REN S, WANG M, FAN A X, et al. Zero-high-resolution information hiding algorithm for 3D mesh model[J]. Computer science, 2020, 47(7)：328-334. (in Chinese)

[11] LI L, LI H, YUAN W, et al. A watermarking mechanism with high capacity for three-dimensional mesh objects using integer planning[J]. IEEE multimedia, 2018, 25(3)：49-64.

[12] YANG Y, PINTUS R, RUSHMEIER H, et al. A 3D steganalytic algorithm and steganalysis-resistant watermarking[J]. IEEE transactions on visualization & computer graphics, 2017, 23(2)：1002-1013.

[13] NARENDRA M, VALARMATHI M L, ANBARASI L J. Watermarking techniques for three-dimensional (3D) mesh models：a survey[J]. Multimedia systems, 2022, 28(2)：623-641.

[14] REN S, WANG Z, SU D X, et al. Information hiding algorithm based on mapping and structure data of 3D model[J]. Journal on communications, 2019, 40(5)：211-222. (in Chinese)

[15] REN S, SHI L, WANG B B, et al. Multi-carrier information hiding algorithm based on three-dimensional model's concave-convex structure characteristics[J]. Telecommunications science, 2022, 38(02)：59-70. (in Chinese)