A Robust Watermarking Scheme for 3D Models Based on Encrypted Holographic Algorithm

Jenita Mary
A.Marinus Akash, R. Thanesh, S. Shathakathullah

Kings Engineering College Irrungatukottai, Chennai.
E-mail: marinus.akash3@yahoo.com

Abstract—We present a digital watermarking algorithm for 3D model which is based on encrypted holographic digital watermarking algorithm to protect the embedded watermark information (such as a specific identity of the copyright information, etc.) and to improve the security and robustness of the digital watermark information. Firstly, the watermark image is processed by the double random phase modulation to get the hologram watermark which makes a high security. Then in the embedding procedures, affine invariant preprocessing is used for 3D models. We calculate the distance of each vertex to center of gravity of the 3D model which is noted as r, and take it as the watermark embedding element to embed the watermark. The experimental results show that the algorithm had the good performance of the watermark robustness to attacks such as noise addition, model simplification, model cropping, and affine attacks. This algorithm can be widely used for digital copyright protection and other aspects of identity hidden.

Keywords—information optics; holographic algorithm; 3D model; digital watermarking; affine invariant; data confidentiality.

I. INTRODUCTION

With the development of science and technology, three-dimensional model has been used in many fields, such as medical industries, movies, video games, constructions and so on. With the growth of application areas, more and more digital products of three-dimensional model spread on the network. The copyright protection of three-dimensional model has become increasingly important. Study on the three-dimensional model for digital watermarking technology is becoming a new field of digital watermarking research [1].

Like the two-dimensional image watermarking, digital watermarking algorithm for three-dimensional model began from the spatial algorithm. In 1997, Ohbuchi published a paper about the three-dimensional model of digital watermarking [2] in the International Conference which is recognized as the first internationally published article on the three-dimensional model of digital watermarking technology. Research for the copyright protection of three-dimensional model began from that time and got much development in recent years. Among them, the early typical spatial algorithms are mainly Triangle Similarity Quadruple embedding, Tetrahedral Volume Ratio embedding, Mesh Density Pattern embedding [3] etc. However, because those algorithms are simple, they have not enough robustness to be applied to the actual copyright protection. In 2008, Liao put forward a spatial watermarking algorithm for three-dimensional model which is based on the ratio of the distance of focus intersection[4], but the algorithm can not handle mesh simplification and cropping attacks. In 2014, X.Feng proposed two different algorithms to embed watermark into the three-dimensional model [5], but the watermark information is not encrypted. Once the watermarking algorithm is cracked, the watermark information is not safe. In the same year, Wang put forward a digital watermarking algorithm for three-dimensional model which is based on the structural feature of the vertex distribution [6]: the algorithm has the drawbacks that the amount of data embedded is limited. Thereby, this paper applies encrypted holographic watermarking algorithm to the three-dimensional model to protect the watermark information (such as copyright information with specific identity) and improve the security, capacity of watermark embedding. We can get the original watermark information from the encrypted watermark only by the decrypt template and check the information of specific authentication. The proposed algorithm has high security and good robustness to common attacks.

The wave of light has a good ability of carrying information, thus the research of encryption and security which is based on optical information processing has got more and more attention. What's more, the optical holographic transform watermarking algorithm has been successfully applied to the copyright protection of two-dimensional image [7-8]. In our algorithm, the information of embedded watermark can be copyright information and maybe other types of watermark image, and the amount of embedded data is large. The extraction watermark is intuitive and easy to evaluate. We can get the highly similar watermark image even when the model is being attacked.

In our algorithm we choose the distance of barycentre to the vertex on the model as the embedded element noted as r and Hologram information generated from the Optical holographic encryption algorithm as the watermark information. The distance r is affine invariant, so it has good robustness. The Hologram information can be decrypted only by the secret key, so it has highly security.

II. Related Knowledge

A. Affine Invariant of Three-dimensional Model

Mesh model can be expressed as (V_i, I), and the vertex is $V_i(V_x, V_y, V_z)$, I is the connection between vertices, i is a positive integer and satisfies $i \cdot N$, N is the total number of vertices. Firstly the mesh model can be pre-processing to make the watermark affine-invariant [5]. Steps are as follows:

1) Calculate the coordinate of barycentre of model, noted as $U(U_x, U_y, U_z)$. It is calculated as formula (1).

$$U(U_x, U_y, U_z) = \frac{1}{N} \sum_{i=1}^{N} V_i(V_{xi}, V_{yi}, V_{zi}) \quad (1)$$

2) Move the barycentre of the model to the coordinate origin. $U'(U_x', U_y', U_z')$ is the coordinate of the new barycentre which is shown in (2).

$$U'(U_x, U_y, U_z) = O(0,0,0) \quad (2)$$

3) Calculate the new coordinates of vertices after moving the barycentre, noted as $V_i'(V_{x'}, V_{y'}, V_{z'})$. The formula of computation is shown in (3).

$$V_i(V_{xi}, V_{yi}, V_{zi}) = V_i(V_{xi}, V_{yi}, V_{zi}) - U(U_x, U_y, U_z) \quad (3)$$

4) Principal Component Analysis (PCA)

Calculate the principal component of vertices on the model. Firstly compute the covariance matrix of the coordinates of vertices, noted as C. Then get the largest eigenvector corresponding to the largest eigenvalue of C, noted as G which is the principal component of vertices. The computational formulas are shown in (4), (5).

5) Convert the Euclidean coordinates $V_i'(V_x', V_y', V_z')$ into the Spherical coordinates $Q_i(r_i, \theta_i, \varphi_i)$

B. Encryption and Decryption of Holographic Watermark

In order to improve the security of the watermark, we process the watermark with double random phase modulation to generate a holographic watermark. Assume the image or data to be encrypted is the normalized f(x,y), and the size is $M \cdot N$. Provided (x,y) is the spatial coordinate, (α, β) is the coordinate of frequency domain, $\Phi(x,y)$ is the image of double random phase encryption, $b(\alpha, \beta)$ is two independent images with random white noise which are uniformly distributed in [0,1]. Then we can get:

$$\Phi(x, y) = \{f(x, y)\exp[j2\pi p(x, y)]\} * h(x, y)$$

The decrypted process is the reverse process of the encryption. The encrypted image takes the Fourier transform and then multiplies with $\exp[-j2\pi b(\alpha, \beta)]$, after that takes the inverse Fourier transform and multiplies with $\exp[-j2\pi p(x,y)]$, then we can get the original image f(x,y). Theories prove that $\Phi(x,y)$ is a white-noise image with mean zero.

III. Embedding Algorithms

The flow chart of watermark embedding algorithm is shown in Figure 1. The steps are as follows:

1) Process the three-dimensional model with an affine invariant;

2) Sort θ_i of vertices in ascending order, and store the corresponding r in the matrix D_j with size $n \cdot n$, then keep the location information of θ_i in a mark matrix. j is a positive integer and satisfies $j \cdot N$, the empty in the last matrix can be filled with zero; $(n \cdot n) \cdot 1$

3) Generate random matrix a and matrix b as double random phase modulation, which is key to encryption and decryption of holographic watermark;

4) The watermark image (such as copyright information) modulated by the random phase a takes Fourier transform, then the transformed image is modulated by the random phase b and takes inverse Fourier transform;

5) Coaxial holographic watermark H is then constructed by double random phase encryption;

6) Watermark matrix is expressed as

$$h_j \cdot D_j \cdot k \cdot H$$

where k indicates the weight of the hologram component. In this case, multiple watermarks are embedded which makes a higher robustness;

7) Three-dimensional Models is reconstructed by matrix h_j;

8) Spherical coordinates (r, θ, φ) is converted into Euclidean coordinates (x, y, z), and the formula of computation is shown in (11):

$$x = r + \sin O^* \cos O ,$$
$$y = r + \sin O * \cos O ,$$
$$z = r - \cos O$$

The hologram algorithm is used successfully in the 3D model watermarking.

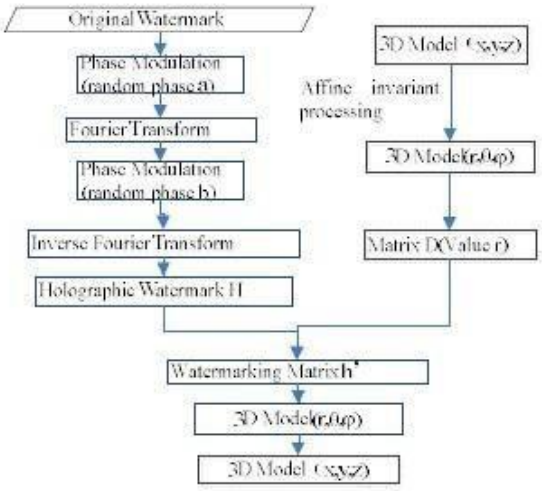


Fig. 1. The basic flowchart of watermark embedding

IV. Extraction Algorithms

The flow chart of watermark extraction algorithm is shown in Figure 2.The steps are as follows:

1) Relocate [9] and Resample operator [10];
2) Affine invariant processing of three-dimensional model;
3) Move the barycentre of the model to the coordinate origin and Euclidean coordinates (x, y, z) is converted into spherical coordinates (r, θ, φ);
4) Sort θ_i of vertices in ascending order, and find a matrix with size $n \cdot n$ according to the location of θ_i in mark matrix. If we cannot find the full matrix, then choose the matrix which is relatively integrate and the missing part can be filled with zeros. In this way, hologram watermarking matrix h' is reconstructed (With multiple watermarking embedded, the relatively integrity one is enough);
5) Coaxial holographic watermark H is then given as

$$H = \sum_{j} h'_j D_j / k$$

6) The holographic watermark H takes Fourier transform. And the transformed information is modulated by the random phase –b and takes inverse Fourier transform. Then it is modulated by the random phase -a. And we get the watermark image.

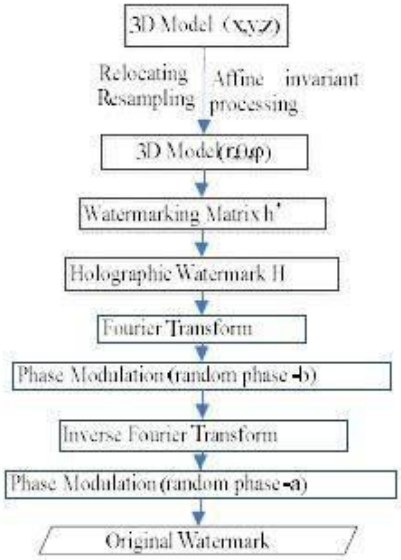


Fig. 2. The basic flowchart of watermark extraction

V. Quantitative Evaluation

There may be some differences between the extracted watermark and the embedded watermark information after processing or attacking to the model. Then we need to have a criterion to determine whether there is copyright watermark information, achieving the purpose of copyright authentication.

Calculate the correlation between the extracted watermark information and the original watermark information to determine whether the watermark exists. When the correlation is greater than the threshold value, it proves the existence of watermark. In this paper the threshold is 0.5 after experiments. The computational formula is shown in (13).

$$corr = \frac{\sum_{m}\sum_{n}(h' - \bar{h}')(h - \bar{h})}{\sqrt{\sum_{m}\sum_{n}(h' - \bar{h}')^2 \sum_{m}\sum_{n}(h - \bar{h})^2}}$$

In (13), h' is the extracted watermark information, h is the original watermark information, $\bar{h}$ is the mean of watermark information, m and n are the dimension of matrix D. The closer to 1 the value of corr is, the better the robustness of watermarking algorithm is.

A. Results and Discussions

To test the robustness and invisibility of the proposed algorithm, content images are embedded into two different models. One is Bunny, the other is Elephant. The dimension of the watermark image is $(64 \cdot 64)$, the strength of watermark embedding is 0.001.To prove the generality of the algorithm,

we choose different watermark images to embed into the Bunny model and the Elephant model.

In Figure 3, (a) is the original Bunny model, (b) is the watermark image '123', (c) is the embedded Bunny model, (d) is the extracted Holographic watermark image '123', (e) is the original Elephant model, (f) is the watermark image 'ABC', (g) is the embedded Elephant model,(h) is the extracted Holographic watermark image 'ABC'. Through the comparison between (a) and (c), (e) and (g), it proves the invisibility of the watermark. In the followed processing, experiments of noise, simplification, cropping, and rotation are performed.

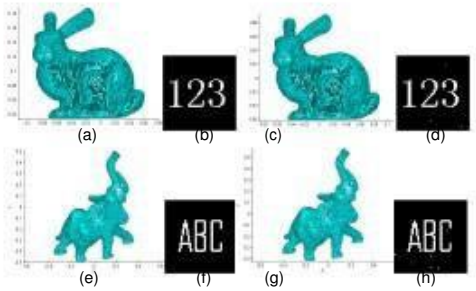


Fig. 3. (a)(e)Three-dimensional model(b)(f)Watermark image(c)(g)Three-dimensional watermark model(d)(h)Decrypted watermark image

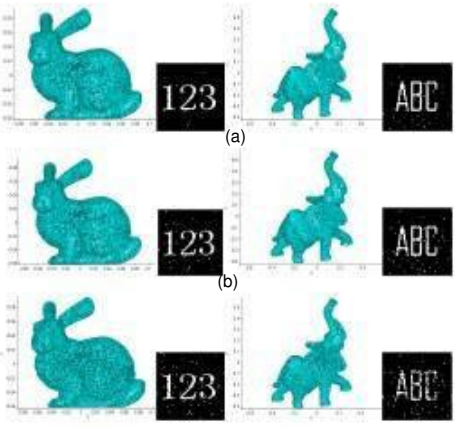
1) Noise Attacks

The experiments of noise attacks are adding the uniform noise into the vertices of the embedded model. The amplitude of noise equals to the results of the mean value of r multiply with the noise intensity L. In the experiment we choose different L to prove the good robustness of the algorithm to the noise. The results of experiments are shown in Table 1 and Figure 4.

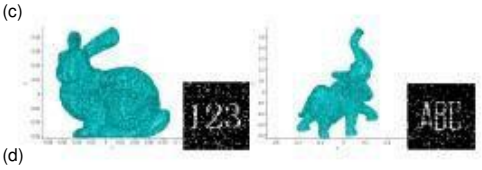
TABLE I. NOISE ATTACK EXPERIMENTAL RESULTS

Attack	(Bunny "123")	(Elephant "ABC")
Noise (L=0.1%)	0.9778	0.9490
Noise (L=0.3%)	0.9351	0.9099
Noise (L=0.5%)	0.8768	0.8802
Noise (L=1%)	0.7452	0.6068

(c)



(c)



(d)

Fig. 4. (a)Noise0.1%(b)Noise0.3%(c)Noise0.5%(d)Noise1%

2) Simplification Attacks

The experiments of simplification attacks are simplifying the vertices of the embedded model. The results of experiments are shown in Table 2 and Figure 5. The experiments prove the good robustness of the algorithm to the simplification.

TABLE II. SIMPLIFIE ATTACK EXPERIMENTAL RESULTS

Attack	(Bunny "123")	(Elephant "ABC")
Simplifie attack (10%)	0.9846	0.9762
Simplifie attack (20%)	0.8907	0.8093
Simplifie attack (30%)	0.7367	0.6909

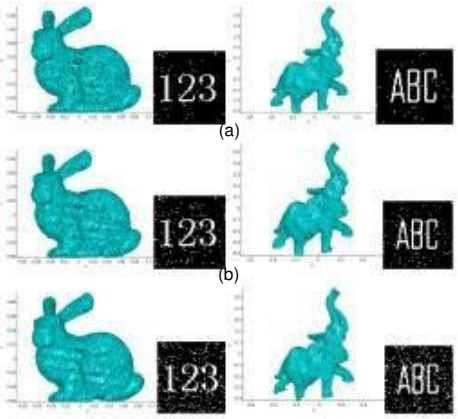


Fig. 5. (a)Simplified10%(b)Simplified20%(c)Simplified30%

3) Cropping Attacks

In our watermark procedure, multiple watermarks are embedded which means that the same watermark information is embedded into different locations in the three-dimensional models. With multiple watermarks, the algorithm achieves a robust manner against cropping of the geometry as long as relatively integral watermarking information is founded. Furthermore encrypted holographic algorithm has strong robustness against cropping, so the watermark procedure achieves good results against cropping. Random cropping attacks were tested on bunny model and elephant model. The cropping rates for bunny model were 30%, 86%, for elephant model were 40%, 60%. The experimental results are shown in Figure 6.

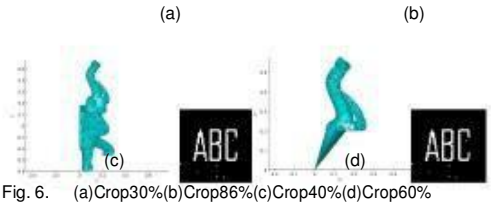


Fig. 6. (a)Crop30%(b)Crop86%(c)Crop40%(d)Crop60%

4) Affine Attacks

Affine attacks including rotation, translation and uniform scaling attacks are entirely undone by the registration process based on the principal component analysis (PCA).

We tested affine robustness against rotation as an example. As expected, our approach achieves good results shown in Figure 7.

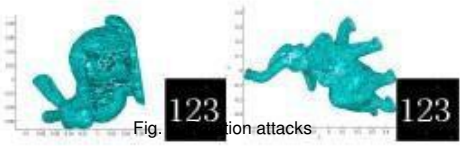


Fig. tion attacks

B. Comparative Experiments

For the common attacks (such as noise attacks, simplification attacks, cropping attacks and affine attacks), reference [5] was compared with our experimental results. The comparative experimental results are shown in Table 3.

TABLE.III COMPARATIVE EXPERIMENTAL RESULTS

Attack	our algorithm(corr)	reference 5 (corr)
Noise (L=0.1%)	0.9778	0.9483
Noise (L=0.2%)	0.9351	0.8254
Noise (L=0.5%)	0.7452	0.6805
Noise (L=1%)	0.5452	/
Simplification (10%)	0.9846	/
Cropping (30%)	1	1
Cropping (60%)	1	/
Cropping (86%)	1	/
Affine	1	1

VI. CONCLUSION

In this paper we have presented a new robust watermarking for 3D model. This new method is based on encrypted holographic algorithm, using double random phase modulation to make the embedding watermark information more secure. The results clearly show that the presented watermarking procedure can tag objects with watermarks in a robust way. It is invisible and the cropping attacks can be successfully handled. Also the algorithm guarantees the good performance of the watermark robustness to attacks such as noise addition, model simplification and affine attacks.

Even though our approach already delivers good results, some future improvements are conceivable. This algorithm is relatively complex. Furthermore, the experimental results are impacted on the parameters of watermark strength, but we haven't known a good parameter estimation method. However a study with the parameter remains as a problem to be addressed in the future.

ACKNOWLEDGMENT

This work is supported in part by a grant from the Funding Scheme for Training Young teachers in Shanghai Colleges in 2013(No. slg14039), Innovation Program of Shanghai Municipal Education Commission (No.13ZZ111), the bidding project of Shanghai research institute of publishing and media (No.SAYB1408) funded by the National Higher Vocational and Technical Colleges construction project of the Shanghai Publishing and Printing College.

REFERENCES

[1] Min H, Yin X, Liangfeng X, Feng X, “A geometry property based adaptive watermarking Scheme for 3D models,”Journal of Computer-Aided Design & Computer Graphics, vol.20, pp. 390-402, 2008

[2] Ohbuchi R, Masuda H, Aono M, “Watermarking three dimensional polygonal model through geometric and topological modifications,” IEEE Journal on Selected Areas in Communications, vol.16, pp. 551-560, 1998

[3] Xiaoqing F, Wenyu Z, Yanan L, “Double watermarks of 3D mesh model based on feature segmentation and redundancy information,” Multimed Tools Appl, vol.68, pp.497–515, 2014

[4] Xinyu W, Yongzhao Z, “A watermarking scheme for three-dimensional models by constructing vertex distribution characteristics,” Journal of computer-Aided Design &Computer Graphics, vol.2, pp.272-279, 2014

Liujie S, Songlin Z, “Digital watermarking of encrypted in-line holography,” 0ptics and Precision Engineering, vol.15, pp.428-431,2007

[5] Liujie S, Songlin Z, “Anti-fake technique by double random phase encrypted holographic mark,”A CT A OPT ICA SINICA, vol.27, pp.31-34, 2007

[6] Tsai Y Y, “An adaptive steganographic algorithm for 3D polygonal models using vertex decimation,” Multimed Tools Appl, vol.69, pp.859–876, 2014

[7] Molaei A M, Ebrahimnezhad H, Sedaaghi M H, “A blind fragile watermarking method for 3D models based on geometric properties of triangles,” 3D Res, vol.4, pp.1-9, 2013

[8] Toshiyuki U T O, Takemura Y, Kamitani H, Kenji Ohue, “A correlation-based watermarking technique of 3D meshes via cyclic signal processing,” IEICE Trans. Information and Systems, vol.95, pp.1272–1279, 2012