Postprint: An Information Hiding Technique Based on Redundant Texture Mapping of 3D Models

Authors: Ren Shuai, Wang Zhen, Zhang Tao, Xu Zhenchao, He Yuan, Su Dongxu, Yunong Liu

Date: 2018-12-13T00:00:00+00:00

Abstract

To address the limitation of insufficient robustness in traditional 3D model information hiding techniques, this paper proposes an information hiding algorithm based on redundant texture mapping of 3D models. Firstly, the feasibility of applying patch textures under orthogonal projection texture mapping rules is verified. Secondly, a quaternion wavelet transform space incorporating surface color attributes is constructed, and the key information for transmission is selected and encrypted. Finally, after embedding the secret message into the robust space, a stego-obj model is generated, with texture maps and state information saved to MTL files, and the stego-model file is encrypted using RSA-based programming techniques. Simulation experiments demonstrate that, compared with 3D model watermarking and steganographic methods lacking surface texture attributes, the proposed algorithm exhibits strong anti-attack capabilities in special rendering environments.

Full Text

Preamble

Vol. 37 No. 2
Application Research of Computers (ChinaXiv Cooperative Journal)
Accepted Paper

An Information Hiding Technique Based on Redundant Texture Mapping of 3D Models

Ren Shuai[1], Wang Zhen[1], Zhang Tao[2]†, Xu Zhenchao[1], He Yuan[1], Su Dongxu[1], Liu Yunong[2]

([1]School of Information Engineering, [2]School of Electronic & Control Engineering, Chang' an University, Xi' an 710064, China)

Abstract: To address the limited robustness of traditional 3D model information hiding techniques, this paper proposes a novel information hiding algorithm based on redundant texture mapping of 3D models. First, the feasibility of applying orthogonal projection texture mapping rules for patch-level texturing is verified. Second, a quaternion wavelet transform space with surface color attributes is constructed, and the key information to be transmitted is selected and encrypted. Finally, the secret message is embedded into the robust transform space to generate a stego OBJ model, with texture and state information saved into an MTL file, and the secret-containing model file is encrypted using RSA programming techniques. Simulation experiments demonstrate that compared with 3D model watermarking and steganography methods without surface mapping properties, the proposed algorithm exhibits strong anti-attack capability in special rendering environments.

Keywords: information hiding; quaternion wavelet transform; secret obj model; MTL file

0 Introduction

Information hiding technology offers distinct advantages over conventional cryptography in practical applications. Traditional cryptographic techniques ensure that even if critical plaintext information is intercepted during transmission, attackers cannot easily decipher it. However, once the encryption method is cracked, adversaries can reconstruct the ciphertext into comprehensible documents, making the ciphertext itself susceptible to suspicion and decryption by malicious parties, which compromises security. Researchers in information hiding have leveraged the strengths of traditional cryptographic encryption while ensuring that hidden messages remain invisible to attackers even when information is intercepted. This approach deters indiscriminate attacks, as multimedia data is ubiquitous on the internet, rendering extreme attacks that aim to destroy all original data meaningless.

Three-dimensional model information hiding technology provides excellent imperceptibility and high capacity, making the enhancement of robustness a hot research topic in information security. Regarding capacity improvement and robustness strengthening, Reference [1] proposed a reversible information hiding method for 3D synthetic images based on a depth no-synthesis-error model, which combines prediction error expansion and histogram shifting algorithms to adaptively embed secret information by optimizing pixel selection and mapping ranges, thereby increasing embedding capacity while maintaining robustness. Reference [2] introduced a blind watermarking algorithm for 3D point cloud data based on distance mapping mechanisms, utilizing the parity of 3D coordinate values for information embedding to improve capacity and anti-attack

capability. Reference [3] presented an algorithm to increase secret information payload based on topological features of 3D meshes using Laplacian matrices while maintaining necessary robustness. Reference [4] balanced image and 3D model data characteristics, designing an energy-weighted approach combined with 3D model contour structures to classify and modify coordinate vertices for high-capacity embedding, enhancing steganographic robustness. Reference [5] avoided using model vertex arrangement order and topological structure as feature extraction indicators by introducing video streaming concepts and implementing a robust 3D hiding algorithm based on frame sampling in a wavelet domain hidden Markov model. Reference [6] strengthened resistance to geometric attacks in 3D model information hiding by employing principal component analysis and spherical coordinate transformation to construct embedding spaces, thereby enhancing robustness and capacity.

Although References [3–6] improved imperceptibility and capacity to some extent, they proved less effective against targeted complex geometric attacks and corresponding 3D model topological structure manipulations, exhibiting relatively weak robustness. This paper abandons the direct construction of robust spaces on 3D model surfaces and instead comprehensively utilizes the additional redundant texture mapping space of 3D models. By selecting an irreversible orthogonal projection texture mapping rule, attacks targeting surface feature extraction of 3D models do not affect the information transform space, thereby significantly enhancing algorithm robustness.

---

1 Algorithm Description

The proposed algorithm consists of four steps: (a) verifying the feasibility of model patch surface texturing based on 3D model vertices and overall topological structure, and utilizing redundant texture space of 3D data; (b) constructing a secret information hiding space using quaternion wavelet transform and encrypting key information to be hidden; (c) embedding critical secret messages into the previously constructed carrier space; and (d) preserving public and private keys through asymmetric encryption methods and encrypting the secret-containing OBJ file for transmission.

1.1 Redundant Data Characteristics of OBJ Model Files and Patch Texturing Methods

Three-dimensional models come in various formats such as STL and OBJ, depending on the types of surface attribute information they can carry. STL files cannot store texture coordinate information and offer limited redundant data options. In contrast, OBJ model files support surface texture rendering and can save rendered scene information as MAX files, where rendered 3D vertices, texture vertices, normal vertices, and patch information are typically stored in MTL files. Using the War horse.stl model as an example, this algorithm demon-

strates its data space redundancy characteristics, with the initial model effect shown in Figure 1 [Figure 1: see original paper].

Using Autodesk 3Ds Max 2016 as the experimental platform, the initial model was converted to architectural material according to built-in operation standards. A Wood texture map with rich texture information and no secret content was selected from the standard bitmap library as the original texture. To enhance attack resistance, a specific irreversible texture mapping algorithm—orthogonal projection texture mapping rules—was employed to project the original yellow texture information of the wood grain onto the surface of patches assigned with architectural material, with the redundancy effect shown in Figure 2 [Figure 2: see original paper].

In summary, OBJ files possess rich, extensive, and covert spatial characteristics suitable for embedding critical secret information. The overall hiding steps of the algorithm are illustrated in Figure 3 [Figure 3: see original paper].

1.2 Redundant Texture Space Construction and Key Information Encryption

Patch texture materials were selected from standard 3D model libraries, and a 500$\times$500 color Wood texture map with rich texture information was processed for redundant space. To enhance the robustness of the secret information embedding space, the regular transformation characteristics of quaternion wavelet transform, its resistance to geometric attacks, and shift invariance were combined. The quaternion wavelet transform was applied to the wood grain texture map. Note that the stability and reliability of the information hiding space depend on the decomposition and reconstruction structure of quaternion filters [9]. The decomposition framework adopted in this algorithm is specifically shown in Figure 4 [Figure 4: see original paper].

Here, X_j and X_{j+1} represent approximations of quaternion parameter values in the transformation direction from level j to $j+1$. All H_0 and G_0 in the framework are recorded as low-pass and high-pass decomposition filters of the quaternion wavelet transform. The reconstruction framework is similar to the decomposition framework, representing the inverse process of the former. Note that during inverse operations, the previous low-pass and high-pass decomposition filters must be replaced with low-pass and high-pass reconstruction filters.

From a mathematical perspective, after quaternion wavelet decomposition, the wood grain texture map can be expressed as a quaternion analytic signal. Let the texture map to be transformed be a 2D real signal as shown in Equation (1), with its quaternion analytic signal representing the Hilbert transforms of the Wood texture map along the x-axis, y-axis, and both x and y axes.

The analytic signal texture coefficients after quaternion wavelet transform can be converted into a coefficient matrix S, as specifically shown in Equation (2). Here, ξ represents local shift information of the image, ψ represents texture

features of the image, and each column in matrix S corresponds to a quaternion representation.

Figures 5(a)-(d) [Figure 5: see original paper] show the texture sub-images after transformation by the quaternion wavelet decomposition filter. At this point, the information hiding space construction for the redundant texture map is complete.

The Logistic mapping definition is proposed for the algorithm. Using a 256-pixel standard Chinese flag square image as experimental material for the secret key information, the algorithm leverages the unpredictable characteristics of chaos theory to randomly rearrange the pixels of the secret square image along nonlinear trajectories. The definition is given by Equation (4). When $3.5699 \leq \lambda \leq 4$ and $x \in [0, 1]$, the Chinese flag secret image enters a chaotic state. Figure 6 [Figure 6: see original paper] shows the experimental results when $\lambda = 0.32$ and $x = 4$.

1.3 Information Fusion Embedding and Secret-Containing Surface Texture Generation

(a) Considering the number of surface patches in the 3D model, the embedding capacity threshold, secret information fidelity, and robustness of critical secret image transmission were balanced. A 500-pixel Wood texture map color square image was selected as the redundant data carrier for the OBJ file. After quaternion wavelet transform as described in Section 1.1, a robust space for hiding was constructed.

(b) The scrambled branch parameters λ and initial value x from Equation (4) were recorded as secret keys K_1 and K_2, respectively, and then converted into a binary sequence δ.

(c) To ensure good imperceptibility of the algorithm and balance the practical application effects of the 3D model with surface texture attributes after adopting orthogonal projection texture mapping rules, the high-frequency components of coefficient matrix S from Equation (2) in Section 1.1 were selected, denoted as H.

(d) The binary secret sequence δ from step (b) was fused and embedded into the high-frequency coefficient portion from step (c), satisfying human visual imperceptibility. The high-frequency embedding formula is given by Equation (5), where H_i' is the high-frequency portion after binary sequence δ embedding, and μ is the information fusion embedding intensity factor. Adjusting μ controls the algorithm' s imperceptibility and robustness. Generally, larger μ values yield stronger robustness but poorer imperceptibility, while smaller μ values produce weaker robustness but better imperceptibility. In practical applications, appropriate values should be set based on specific scenarios.

(e) The secret-containing Wood texture map after Chinese flag sequence information fusion from step (d) was subjected to orthogonal projection texturing using the method described in Section 1.1. Since the selected texture projection algorithm is irreversible, it possesses strong anti-attack capability. After texturing, the secret-containing OBJ 3D model with surface color, brightness, and other attributes was constructed.

1.4 OBJ File Encryption and Transmission Processing

During the actual preparation stage for secret information channel transmission, both channel security and data integrity must be considered. Although OBJ files possess rich redundant data space that improves algorithm robustness and imperceptibility, the large amount of dispersed and heterogeneous fused redundant data also presents certain security risks. For information well-hidden in covert spaces, whether it can be safely and reliably delivered to recipients while maintaining data integrity is crucial.

This paper employs asymmetric encryption methods to ensure the security of dispersed texture files, MTL configuration files, OBJ model display files, and other components during transmission and reception. The typical asymmetric RSA encryption method was selected. Using specific OpenSSL platform commands, a 2$×$512-bit high-security key was generated. The key commands are as follows:

Command 1: `openssl genrsa -out private.key 1024`. This command generates a 2$×$512-bit decryption code for recipients to extract from subsequently transmitted files. This is the first private key instruction that secret model file recipients must extract.

Command 2: `openssl rsa -in private.key -pubout -out pub.key`. This command generates the public key instruction that must be sent by file recipients before senders transmit secret information, matching Command 1. This is the first public key instruction that secret message senders must possess.

Using the above public key instruction, senders encrypt the complete secret-containing obj file (including texture files, MTL files, and obj model status files) that have undergone chaotic scrambling, binary conversion, and information fusion from Section 1.2. The encrypted OBJ file is then transmitted along with secret keys K_1 and K_2 from Section 1.3 (the second password instruction). After receiving the file, recipients decrypt it using the first private key instruction to obtain the dispersed OBJ model files, perform inverse algorithm operations on the secret-containing texture map, and finally extract the critical Chinese flag secret image message using the second secret key instruction.

---

2 Simulation Experiments and Comparative Analysis

The advantages of employing information hiding technology are undeniable, yet attacks targeting this field continue to emerge. With the development of network and advanced data processing technologies, malicious actors typically tamper with data or perform non-severe destructive modifications before retransmission. Most existing information hiding techniques suffer severe damage to hidden critical information after such modification operations.

This paper focuses on testing the imperceptibility and robustness of the new algorithm. The experimental environment includes Autodesk 3Ds Max 2016, MATLAB, MeshLab, VC++, and OpenSSL. Experiments simulate the state of secret-containing OBJ files after being intercepted during transmission. After intercepting OBJ model files, attackers can display the file types shown in Figure 7 [Figure 7: see original paper].

Figure 7(a) shows the secret-containing texture file generated after information fusion embedding as described in Section 1.3. Figure 7(b) shows the backup Trojan model with architectural material, whose texture coordinate information is saved in the MTL1 file. Figure 7(c) shows the secret-containing Trojan model after orthogonal projection texturing. Upon obtaining these files, attackers first detect whether any suspicious messages are visible, simulating the imperceptibility after algorithmic embedding.

2.1 Imperceptibility Experiments

Based on human visual imperceptibility, observers are less sensitive to local detail changes or minor modifications. This paper actually hides the secret binary sequence in the high-frequency coefficients of the quaternion signal, with the processed secret Chinese flag ultimately fused into the texture edge shadows of the wood grain map.

Considering the worst-case scenario where attackers possess profound professional expertise, even when using professional image display software and the Autodesk 3Ds Max 2016 3D model platform to detect detailed edges of secret-containing models, there is almost no difference between the carrier data before and after embedding, making visual distinction nearly impossible, especially since no original data carrier samples are available in the intercepted files.

Algorithm transparency comparison experiments are shown in Figure 8 [Figure 8: see original paper]. The subjective visual comparison experiments above satisfy human eye imperceptibility. The algorithm also employs objective metrics to express transparency, using the Metro tool to detect the Hausdorff distance of the War horse model after embedding the secret Chinese flag message. The total binary amount of the scrambled Chinese flag secret message is 217.4279 bits, while its Hausdorff distance is only 0.005162.

Considering carrier material types, algorithm processing procedures, and secret feature extraction, recent literature [10, 11] was selected as reference for algo-

rithm transparency comparison. Figure 9 [Figure 9: see original paper] shows detailed statistics using the objective Hausdorff distance metric. The horizontal axis represents the amount of embedded key information data, and the vertical axis represents the Hausdorff distance parameter. When data embedding intensity interval $k \in [11, 23]$, this algorithm' s distance metric is significantly smaller than the Hausdorff distances in References [10, 11], thus offering better imperceptibility. When $k \geq 24$, meaning when the total amount of fused secret key information exceeds 224 bits, noticeable changes detectable by human eyes occur at detail edges between the original and secret-containing texture maps. Therefore, this algorithm is suitable for carrier space transformations based on heterogeneous carrier types with dispersed redundant data.

2.2 Robustness Experiments

Experiments simulate the ability of the algorithm to resist attacks after special attacks and tampering on intercepted secret-containing OBJ files during transmission. The relatively obvious secret-containing Trojan model was sequentially subjected to 俯视旋转 (top view rotation), patch extrusion, patch clipping, and 3D vertex blue painting attacks using the mainstream professional 3D model processing platform Autodesk 3Ds Max 2016. As shown in Figures 10(a)-(d), simulation experiments demonstrate that after these four information tampering attacks and rendering, the secret flag information can still be effectively extracted and recognized. Additionally, noise attacks and wireframe rendering attacks after patch removal were applied to the Trojan model on the MeshLab platform without surface texture attributes. As shown in Figures 10(e)-(f), even when the Trojan model' s surface and topological structure have been tampered with and transformed, the secret flag information can still be normally extracted with high recognizability, essentially due to the irreversible orthogonal projection texture mapping algorithm used in this paper.

Similarly, for subjective visual identification of 3D model anti-attack capability, subsequent experimental sections employ the objective metric BCR (Bit Correct Rate) shown in Equation (6) to measure algorithm robustness.

Here, the numerator δ' represents the binary secret information sequence that can still be correctly extracted after various types and degrees of attacks, and the denominator Θ represents the total information bit value of the secret information embedded in the wood grain texture carrier.

The secret-containing OBJ model with surface texture attributes was subjected to complex attacks including translation/rotation, patch cropping, vertex blue painting, and topological wireframe rendering as shown in Table 1 . The correct message sequence extraction ratio of this algorithm is higher than 60% for all attacks, exceeding the minimum BCR threshold of 10.08%, and overall outperforming the algorithm performance in References [10, 11].

As triangular patches are important components of 3D models, research and experiments on specific attacks targeting their structure are particularly impor-

tant. The algorithm focuses on comparing information extraction performance under quantitative patch extrusion attacks in the 3D model information hiding field. Using the same literature for comparison, statistical results are shown in Figure 11 [Figure 11: see original paper]. After simulation attacks of different intensities, this algorithm demonstrates good stability, with secret information extraction rates exceeding 65% and strong robustness with minimal impact from the attack environment.

In the Autodesk 3Ds Max 2016 experimental attack platform, patch clipping rendering was selected while controlling patch clipping attacks, with statistical results shown in Figure 12 [Figure 12: see original paper]. When the OBJ model patch clipping area ratio reaches 40%, this algorithm's BCR extraction rate is as high as 80.07%, showing good secret information recovery capability compared with other algorithms in the field. Finally, when patch clipping intensity is increased to 80% in the simulation attack platform, the correct message sequence can still be extracted at a high rate, attributed to quaternion transform [13] and heterogeneous carrier feature image fusion principles.

Vertex blue painting attacks were conducted on the War horse.stl model, with different intensity painting rearrangement experiments performed on model vertices. Comparison results are shown in Figure 13 [Figure 13: see original paper]. When model vertex painting rearrangement approaches 80%, the information extracted by this algorithm can still be effectively recognized, with BCR ratios exceeding 60%, indicating that the OBJ model algorithm in this paper also possesses strong anti-attack capability against specific types of 3D vertex attacks.

In summary, the experimental statistical results demonstrate that this algorithm is suitable for information hiding in heterogeneous dispersed data carriers, i.e., multi-carrier low-density secret file hiding, while exhibiting strong robustness against attacks targeting 3D model data composition and topological structure characteristics, such as quantitative patch extrusion, regional patch clipping, and 3D vertex color painting. Finally, the algorithm' s good imperceptibility enables wide application of this hiding technology in special environments.

---

3 Conclusion

In summary, this paper proposes an information hiding method based on the redundant texture data characteristics of OBJ models, comprehensively utilizing quaternion wavelet transform, chaotic mapping algorithms, and RSA asymmetric encryption. Secret messages are hidden in texture space, with texture carriers only appearing on 3D model patch surfaces. This approach satisfies the performance requirements of information hiding technology while enabling surface color attribute visualization of 3D models. Simulation experiments show that the algorithm is suitable for application scenarios with high robustness requirements. However, the secret information embedding capacity [14] may vary with the functionality and timeliness of Autodesk 3Ds Max 2016 and MeshLab

platforms, and the embeddable information capacity is limited by the texture carrier space [15] while maintaining algorithm robustness. Therefore, future research should focus on establishing an evaluation system for algorithm capacity while attempting information hiding algorithms for multiple texture carrier groups.

References

[1] Ou Bo, Shi Xianglian. Reversible data hiding for three-dimensional image based on depth no-synthesis-error model [J]. Information Network Security, 2018(5): 24-31.

[2] Wang Gang, Ren Na, Zhu Changqing, et al. The digital watermarking algorithm for 3D models of oblique photography [J]. Journal of Geo-Information Science, 2018, 20(6): 738-743.

[3] Li Shiqun, Li Guiqing, Xian Chuhua. Eigenvector-based watermarking for 3D Mesh models [J]. Journal Of Graphics, 2017, 38(2): 155-161.

[4] Lei Jingxiang. Design and research of Information Steganography Algorithm Based on energy weight [D]. Xi' an: Chang' an University, 2016: 39-48.

[5] Qi Ke, Zhang Dafang, Xie Dongqing. Steganography for three-dimensional model based on frame transform and HMM model in wavelet domain [J]. Journal of Computer-Aided Design & Computer Graphics, 2010, 22(8): 1406-1411.

[6] Ren Shuai, Zhang Tao, Yang Tao, et al. Information hiding algorithm based on spherical segmentation of three-dimensional model[J]. Journal of Computer Application, 2017, 37(9): 2576-2580.

[7] Soulard R, Carré P. Quaternionic wavelets for texture classification [J]. Pattern Recognition Letters, 2011, 32(13): 1669-1678.

[8] Bahri M, Ashino R. Relationship between quaternion linear canonical and quaternion fourier transforms [C]//Proc of International Conference on Wavelet Analysis and Pattern Recognition. Piscataway, NJ: IEEE Press, 2014: 116-121.

[9] Yin Ming. Research on quaternion wavelet transformation theory and its application in image processing[D]. Hefei: HeFei University of Technology, 2012.

[10] Wang Xinyu, Zhan Yongzhao. A watermarking scheme for three-dimensional models by constructing vertex distribution characteristics [J]. Journal of Computer-Aided Design & Computer Graphics, 2014, 26(2): 272-279.

[11] Yang Biao, Lyu Mengqi, Wang Yimin, et al. Structure complexity based multi-layer steganography for 3D model[J]. Electronic Measurement Technology, 2016, 39(12): 164-167.

[12] Carlson N A, Porter J R. On the cardinality of Hausdorff spaces and H-closed spaces [J]. Topology & Its Applications, 2013, 160(1).

[13] Khoubani S, Hassan M M, Sheikhhosseini M. Quaternion wavelet frame rate up-conversion [C]//Proc of the 24th National and 2nd International Iranian Conference on Biomedical Engineering. Piscataway, NJ: IEEE Press, 2017: 1-5.

[14] Han Jialing. Research on digital image information hiding algorithms based on hiding capacity [D]. Changchun: Jilin University, 2015: 34-42.

[15] Chai Pengfei, Luo Xiaoqing, Zhang Zhancheng. Image fusion using quaternion wavelet transform and multiple features [J]. IEEE Access, 2017, (99): 1.

Note: Figure translations are in progress. See original paper for figures.