

## 基于三维模型贴图与结构数据的信息隐藏算法

任帅<sup>1</sup>, 王震<sup>1</sup>, 苏东旭<sup>1</sup>, 张弢<sup>2</sup>, 慕德俊<sup>3</sup>

(1. 长安大学信息工程学院, 陕西 西安 710064; 2. 长安大学电子与控制工程学院, 陕西 西安 710064;  
3. 西北工业大学自动化学院, 陕西 西安 710072)

**摘要:** 针对三维模型信息隐藏无法有效抵抗联合攻击, 秘密信息极易被破坏而无法正确提取的问题, 提出一种基于三维模型贴图与结构数据的信息隐藏算法。首先, 在标准图片库中选取多幅原始 stl 三维模型载体的纹理贴图, 利用 db1 函数经过 2 次二维离散 Daubechies 变换将备份的隐秘消息以水印嵌入的思想隐藏其中; 其次, 以 stl 类型的三维模型为原始结构载体, 利用帧化采样的小波域三维模型信息隐藏算法, 将要隐藏的隐秘信息嵌入相应变换空间; 最后, 利用正交投影的纹理映射算法将二维贴图数据与三维 stl 数据矩阵相乘, 生成含密 obj 模型文件进行传输。算法利用三维模型的贴图与拓扑坐标空间双重嵌入隐秘信息, 有效增强了算法的顽健性。实验分析表明, 含密三维模型的不可见性、顽健性以及抗分析性均有提升, 可以实现不同类型载体冗余空间的备份隐藏嵌入, 为复杂环境下的信息安全传输提供一种可靠的技术手段。

**关键词:** 信息隐藏; 二维离散 Daubechies 小波变换; obj 模型; 抗分析性

**中图分类号:** TP309

**文献标识码:** A

**doi:** 10.11959/j.issn.1000-436x.2019108

## Information hiding algorithm based on mapping and structure data of 3D model

REN Shuai<sup>1</sup>, WANG Zhen<sup>1</sup>, SU Dongxu<sup>1</sup>, ZHANG Tao<sup>2</sup>, MU Dejun<sup>3</sup>

1. School of Information Engineering, Chang'an University, Xi'an 710064, China  
2. School of Electronic and Control Engineering, Chang'an University, Xi'an 710064, China  
3. College of Automation, Northwestern Polytechnical University, Xi'an 710072, China

**Abstract:** The existing 3D information hiding schemes are not robust enough against the joint attacks, as a result the secret information will be vulnerable and cannot be extracted correctly. In order to solve the above problem, an information hiding algorithm based on mapping and structure data of 3D models was proposed. First, several texture maps of the original 3D models in .stl format were picked from the standard model library, so the backup secret data after twice two-dimension discrete Daubechies transform can be embedded using db1 function just as the watermark. Secondly, the original 3D model in .stl format was operated by frame sampling in wavelet domain to obtain the coefficient in transform domain, thus the secret data was embedded into the corresponding transform coefficient. Finally, the .obj documents with the secret information were generated by multiplying the 2D texture map data and the 3D .stl data matrix based on orthogonal projection. Texture maps and coordinate space of 3D model were both used to embed the secret information repeatedly in order to enhance the robustness. The experiment analysis indicated that the imperceptibility, robustness and resistance against analysis are improved and information transmission safety in complex environment can be achieved based on the redundancy space of multi-type carriers.

**Key words:** information hiding, two-dimensional discrete Daubechies wavelet transform, obj model, resistance against analysis

收稿日期: 2018-10-08; 修回日期: 2019-03-28

通信作者: 王震, chang123an123@163.com

基金项目: 国家自然科学基金资助项目 (No.61702050); 大学生创新创业训练计划基金资助项目 (No.201810710052, No.201810710060, No.201810710215, No.201810710224)

**Foundations Items:** The National Natural Science Foundation of China (No.61702050), The National Training Program of Innovation and Entrepreneurship for Undergraduates (No.201810710052, No.201810710060, No.201810710215, No.201810710224)

## 1 引言

目前, 针对单载体信息隐藏已有许多成熟算法。空域方面最低有效位<sup>[1]</sup>替换算法是最普遍、实用的方法之一。如 Yuan 等<sup>[2]</sup>利用人眼对红、绿和蓝感知范围的差异特性, 基于二维图像位平面的特征和颜色分量值调整变换范围, 控制隐藏信息比特序列分布于载体内部区域。Zhou 等<sup>[3]</sup>基于彩色图像最低有效位 (LSB, least significant bit) 技术, 采用密码学理论提出了一种带密钥改进算法, 其应用形式是以数字签名与加密技术结合的身份认证呈现的, 一定程度上提高了信息数据的安全性。文献[4]以二维码为隐匿载体, 通过红绿蓝 (RGB) 颜色空间通道将含密消息嵌入其中, 保证算法较大容量的前提下实现了隐蔽通信。文献[5]利用数学插值思想, 基于直方图移位理论与 LSB 嵌入体系, 提出了通过可控调整最佳像素位置来提高图像质量的隐藏算法。上述空域算法实现简单, 并有效提高了信息的容量性与不可见性, 但仍有顽健性不强和嵌入长度易被统计检测方法分析出来这两方面的明显缺陷, 尤其无法抵抗较为典型的检测针对方法, 如 RS (regular and singular group) 方法、SPA (sample pair analysis) 方法、DIH (difference image histogram) 方法<sup>[6-8]</sup>等。在变换域算法中, 最为典型的是基于离散余弦变换 (DCT, discrete cosine transform) 和基于离散小波变换 (DWT, discrete wavelet transform) 的信息隐藏算法, 其具有较好的系统性能而受到广泛的应用。目前, 基于变换域的信息隐藏算法的研究主要集中在系数阈值和隐藏信息编码的研究上。

系数阈值是基于变换域算法的研究中最关键的问题, 文献[9]利用混合信息描述符 (HID, human interface device) 进行信息隐藏, 为本文算法提供了思路。Palak 等<sup>[10]</sup>结合 DCT、DWT、奇异值分解 (SVD, singular value decomposition) 及优化公钥数据加密标准方法 (RSA, rivest shamir adleman), 通过改进算法嵌入策略, 将秘密水印隐藏在公开载体中, 隐秘消息抗检测能力得到了增强。国内学者在基于图像载体的隐写领域也有一定突破。邵菲等<sup>[11]</sup>利用 Walsh 序列对隐藏的二值图像进行扩频调制, 使算法在低信噪比信道中具有较强的顽健性。文献[12]提出了一种以图像作为载体, 基于离散余弦变换和置乱融合模型的信息隐藏方法, 可以有效地实现图像信息的隐藏。目前, 基于变换域的信息隐藏算法在

顽健性方面具有较高的造诣, 但多数算法抗分析性不强, 且嵌入信息量也没有显著的提高。

多小波分析是由傅里叶变换发展而来的一门新兴的时频域分析方法。19 世纪 90 年代, Tjihuis<sup>[13]</sup>提出多元数傅里叶变换; 之后, 文献[14-15]提出了以多元数傅里叶变换为理论基础的彩色图像模型; 后期 Sangwine 等<sup>[16]</sup>提出了一种以多元数理论体系为支撑的彩色图像模型的边缘检测方法。21 世纪初, Moxey 等<sup>[17]</sup>对多元数自相关、多元数互相关以及多元数矢量相位相关的概念进行了阐述和分析, 阐明了代表图像间相对位移与旋转信息的多元数互相关概念。迄今为止, 多元数小波理论在信号解析、模式识别与机器学习、图像深度处理等领域被广泛应用, 但其重构器一般较为复杂, 计算量较大, 算法稳定性不足, 实用性较差。

从目前研究进展来看, 各类载体固有特性的研究对预处理技术有着重要的意义, 数字图像依然是主要的一类载体, 而三维模型将是未来主要研究的一类非常规载体。文献[18]引入视频流思想, 将三维模型空间进行等高线分割, 利用帧化采样等特性进行零树小波系数变化完成信息隐藏。文献[19]对三维模型进行球型分割等预处理, 通过立体分区运算, 筛选出法线向量动态变化特征点, 使算法不可见性与抵抗常见随机加噪攻击的顽健性提高到新的水平。文献[20]提出以模型骨架点及内切球解析次数作为隐秘信息的修改特征度量方式, 提高了抵抗旋转攻击的能力。文献[21]针对三维模型信息隐藏无法有效抵抗联合攻击的问题, 提出一种新的基于特征点标注与聚类的隐藏算法。

当前, 几乎所有的信息隐藏算法与分存思想仅实现了单一载体的信息隐藏技术, 很少考虑以多个载体进行信息隐藏的嵌入方法, 已发表的与多载体信息隐藏相近的信息隐藏算法有基于多幅图像分存等类型。已有学者给出多载体信息隐藏的相关理论, 为了保证数字隐写的安全性, 在载体源的产生上应建立一些约束, 针对不同的载体信号, 考虑不同的方式, 设计不同的可逆数字隐写方案。文献[22]中用局部载体的自适应熵值来测量信息数据的稳定特征。在不改变图像原始质量展现细节的情况下提升了信息隐藏容量。文献[23-24]定义了相异载体模型的信息安全规则可达速率上界, 同时指出了隐写容量的上限边界。文献[25]从信息论角度给出隐藏容量的严格定义, 指出隐藏信息嵌入能量

与攻击噪声能量的约束共同决定信息隐写容量，且与顽健性和保真度相互制约形成一个三角关系，但此定义推算隐写容量时有所简化导致运算结果有一定误差。

Cogranne 等<sup>[26]</sup>和 Gao 等<sup>[27]</sup>提出批量隐写方案，给出了隐写安全模型的严格约束条件，但实际安全性无法保证。文献[28]针对常用信息隐藏方法隐藏容量有限而无法隐藏大文件的问题，提出一种利用多幅载体图像进行大文件嵌入的信息隐藏方法，以 Android Studio 平台对算法性能进行验证，一定程度上实现了多载体图像隐藏。文献[29]针对单一算法对同类型载体的隐写模式容易导致安全性的问题，提出了多类型算法协同隐写的嵌入方案，保证了算法的高安全性与良好的可行性。

相关学者结合多载体，打破常规做法，利用图像缩放算法实现了隐写<sup>[30]</sup>。文献[31]指出掩藏秘密信息存在性并非信息隐藏的必要条件，一定程度上解决了隐藏容量与顽健性间的矛盾。文献[32-33]分析了相异载体隐写算法研究的最新发展方向。文献[34]分析了隐写分析研究的进展和发展方向，指出了未来信息隐写领域面临的巨大挑战，详细展示了攻击者如何利用不同类型的数据隐藏机制漏洞进行隐秘信息的对抗攻击，即攻击者已经不局限于基于传统隐蔽通道，攻击以及有效信息检测攻防的手段层出不穷，因此提出有效的对策已迫在眉睫。

本文的核心贡献是综合利用二维图像数据与三维模型数据冗余空间，生成完整 obj 文件载体，多途径保护隐藏在不同类型载体中的隐秘信息，解决单一载体类型隐藏算法不能“备份”关键信息的缺点。仿真实验证明了本文所提的数字多载体数据信息隐藏方法性能稳定。

## 2 三维模型含密贴图生成

本文以上述成熟研究成果为基础，提出了利用 db1 小波函数进行二维离散 Daubechies 变换，将经 logistic 映射处理的隐秘图像隐藏到 obj 三维模型“表面贴图”的信息隐藏思想。备份隐秘信息隐藏过程具体介绍如下。

以基本茶壶体三维模型为例，选取 512 像素×512 像素的彩色 Lena 贴图、铁皮贴图、紫砂贴图以及剪纸贴图 4 幅贴图作为含密 obj 模型实验的纹理贴图。

1) 第一重隐秘信息嵌入步骤总结如下。

**Step1** 任选模型贴图库中的 4 幅贴图之一进行 2 次 db1 小波变换，得到其小波系数，并选出图像各变换区域中 LH<sub>2</sub> 的子带空间作为隐秘信息嵌入位置。各嵌入区域起始点记为(K<sub>1</sub>, K<sub>2</sub>)，选取 M×M 的系数矩阵。图 1 (a)~图 1 (d)分别为从 obj 模型文件中选取的 4 种贴图且用 2 次 db1 函数进行二维离散小波变换后的分解情况。

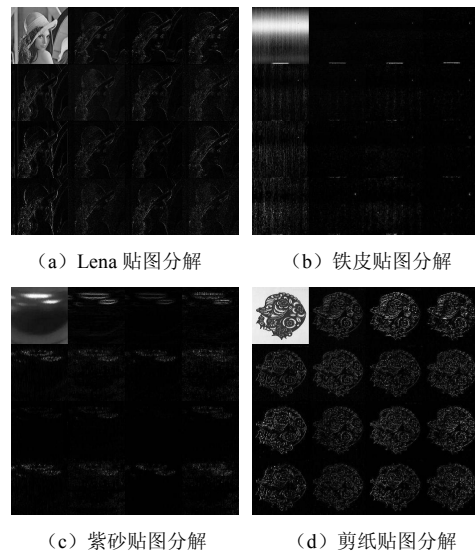


图 1 二次离散二维小波变换的一阶分解示意

**Step2** 选取 256 像素×256 像素的灰度 Scene 图像作为嵌入到贴图载体集中的第一重隐秘关键信息，将 CHD 校徽 (256 色位图) 灰度图像作为算法后文部分嵌入到 stl 模型的第二重非关键性迷惑信息。为与 obj 模型贴图的多元数小波变换空间契合，对其进行基于混沌的图像加密置乱，如式(1)所示。确定 logistic 映射的参数  $\mu$  和初始值  $g_k$ 。

$$g_{k+1} = \mu g_k (1 - g_k), \quad g_k \in (0,1) \quad (1)$$

隐藏信息按照参数  $g_k$  进行置乱，置乱后的比特序列记  $B_N^g$ ，用 logistic 映射生成混沌密码流，对密码流排序后生成置换地址集合，用这个地址集合对图像像素点进行重新排列，从而达到置乱的目的 (用 M 文件实现)。置乱加密情况图 2 所示。

**Step3** 将图 2(b)中经加密处理后 scene 信息进行时域变换，同时转换为  $M \times M$  二值矩阵，矩阵元素为 0 或 1。利用 TYC 提出的水印嵌入方案将 2 个大小一致的矩阵信息叠加融合，参数定义如下。D 为隐秘 scene 信息进行时域变换后得到的  $M \times M$  的矩阵，E 为矩阵 D 中含有的隐秘信息位置集合，H 为贴图载体经过 2 次二维离散 Daubechies 小波变换

后得到的系数矩阵 ( $M \times M$ ),  $I$  为模,  $F$  为矩阵  $H$  和矩阵  $E$  的交集, 参数  $\delta$  为矩阵  $D$  进行模运算后的值, 约束条件为  $\delta(i, j) = D(i, j) \bmod I$ . 隐秘信息融合规则如下。

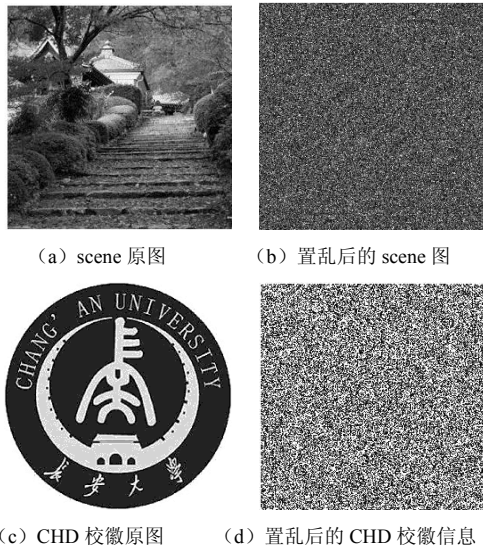


图 2 隐秘图像置乱加密情况

$D(i, j) = 1$ , 且  $H(i, j) \geq 0$ , 则  $F(i, j) = F(i, j) - \delta(i, j) + T_1$   
 $D(i, j) = 0$ , 且  $H(i, j) \geq 0$ , 则  $F(i, j) = F(i, j) - \delta(i, j) + T_2$   
 $D(i, j) = 1$ , 且  $H(i, j) < 0$ , 则  $F(i, j) = F(i, j) + \delta(i, j) - T_1$   
 $D(i, j) = 0$ , 且  $H(i, j) < 0$ , 则  $F(i, j) = F(i, j) + \delta(i, j) - T_2$

其中,  $T_1$ 、 $T_2$  为隐秘信息嵌入的阈值。安全性系数有  $M$ 、 $K_1$ 、 $K_2$ 、 $I$ 、 $T_1$ 、 $T_2$ 。

**Step4** 整理图像集矩阵  $F(i, j)$ , 第一重隐秘不可见水印嵌入完成。

2) 基于相异载体的信息隐藏算法的第一重隐秘信息提取过程如下。

**Step1** 得到含密三维模型文件后, 进行模型逆分解得到含密贴图载体, 进行 2 次二维离散 Daubechies 小波变换。

**Step2** 记  $Z$  为从二维离散 Daubechies 小波变换域抽取的  $M \times M$  的系数矩阵, 起始位置为  $(K_1, K_2)$ 。参数  $\theta$  为矩阵  $D$  进行模运算后的值, 约束条件为  $\theta(i, j) = Z(i, j) \bmod I$ , 对  $Z$  中的所有点  $(i, j)$  规则如下。

$$\begin{cases} G(i, j) = 1, & |\theta(i, j)| \geq \frac{T_1 + T_2}{2} \\ G(i, j) = 0, & |\theta(i, j)| < \frac{T_1 + T_2}{2} \end{cases}$$

此时得到  $M \times M$  的置乱矩阵  $G$ 。

**Step3** 依据隐藏信息置乱时的初始参数  $g_k$  与

$\mu$  值, 进行 logistic 反变换。重新按照置换地址集合对密码流解码排序后, 完成第一重隐秘图像像素点恢复过程, 隐秘 scene 提取工作结束, 即隐秘信息嵌入的逆过程。

三维模型含密贴图生成情况如图 3 所示。

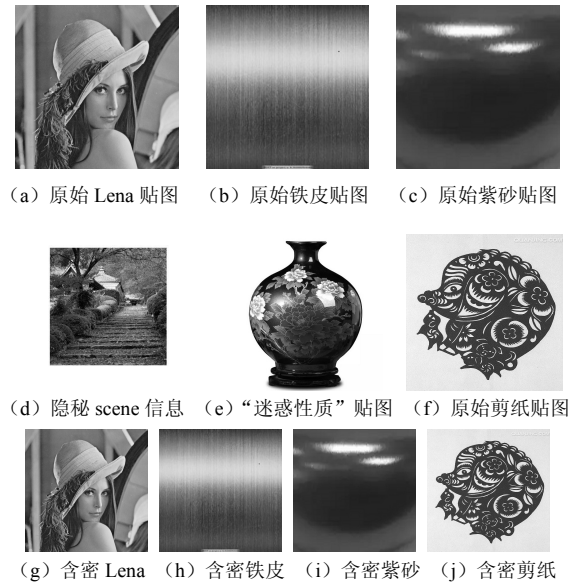


图 3 模型原始贴图与含密贴图情况

### 3 含密 stl 三维模型与完整含密 obj 模型文件生成过程

#### 3.1 Chinese flag 信息隐藏与含密 stl 模型生成过程

1) 第二重非关键性迷惑信息嵌入过程如下。

**Step1** 选取标准壶体 stl 模型为原始三维载体  $N$ , 以主成分分析法 (PCA, principal component analysis) 解析得到该模型重心坐标。该重心位置为新三维坐标系原点, 其他顶点坐标可从原始三维坐标系顶点整合得到, 将新三维模型记为  $N'$ , 使其可以抵抗一定程度的仿射变换 (旋转、平移和均匀缩放) 攻击。

**Step2** 将  $N'$  坐标系拓扑轮廓进行等高线分割, 选定  $X$  轴为操作轴, 从原点起沿  $X$  轴方向将  $N'$  的各坐标顶点取值, 即  $X = \{x_{ij}\}$ ,  $p \leq x_{ij} \leq P$ , 利用浮点系数  $p$ 、 $P$  可将  $[p, P]$  区间分为  $n$  份, 按取值方向依次记为  $i_0, i_1, \dots, i_{n-1}$ , 每份长度为  $h = P - p_n$ , 此时新模型  $N'$  中的  $X$  轴区间由  $n$  份区间序列构成。根据需要将参数  $n$  作为隐秘信息提取密钥的种子, 本文取  $K_0 = n^2$ 。

**Step3** 取某小份空间记为  $i_k$ , 采用视频帧思想构造顶点坐标帧数据序列。需要注意的是, 本文的顶点排序采用式(1)的混沌序列生成, 设置密钥加密

$K_1$ 。逐步完成模型顶点帧化数据的采样过程。最终将  $N'$  中的各顶点坐标变换为子区间序列中的广义灰度图序列。以该灰度图序列作为隐秘信息隐匿空间，利用文献[24]中的 Haar 小波分解算法，将经过小波变换后的广义灰度图零树结构中节点的小波系数作为隐匿载体，待传送第二重隐秘信息 CHD 校徽的隐藏过程由修改节点系数值完成，文章采用奇偶替换<sup>[35]</sup>思想进行信息嵌入。需要注意的是，一些零数小波结构的重要系数节点会可能对从三维模型操纵轴变换后的灰度图像细节产生影响，为遵守 HVS 特性，应提前设置零树小波阈值，记为  $S$ 。这样就可选择小波系数节点阈值内的区域作为隐秘信息嵌入的载体节点。

**Step4** 以隐秘信息的数据量  $T$  为参照，当  $X$  轴的小波变换灰度图空间的嵌入节点数据量  $Q > T$  时，信息隐藏过程完成。当  $Q < T$  时，可利用  $N'$  初始载体中的  $Y$  轴、 $Z$  轴，按照上述文献思想依次进行  $Y$  轴、 $Z$  轴帧化采样操作，整合构造  $Y$  轴、 $Z$  轴方向的广义灰度图  $Y = \{y_{ij}\}$ ， $Z = \{z_{ij}\}$ ，重复  $X$  操纵轴方向的 Haar 小波变换算法，完成较高容量的信息隐藏过程。含密 stl 三维模型生成情况如图 4 所示。

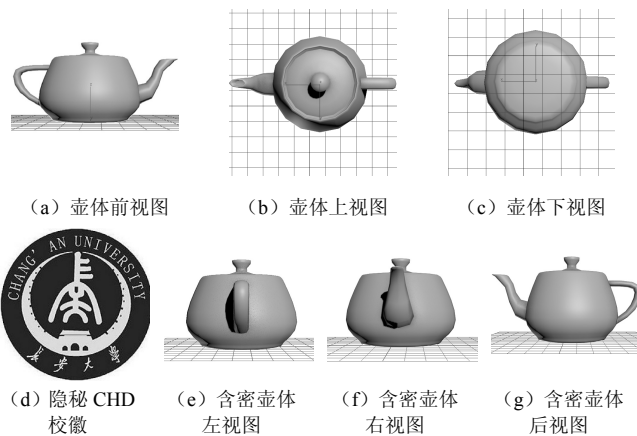


图 4 原始 stl 模型贴图与含密模型情况

2) 第二重非关键性迷惑信息提取过程如下。

**Step1** 接收得到含密三维模型文件后，进行模型逆分解得到含密 stl 三维模型。同理，分别经主元数学统计分析、解析模型重心坐标、归整原点坐标得到新三维坐标体系。

**Step2** 将新三维坐标体系中的模型拓补结构按照浮点参数  $p$ 、 $P$  以及密钥  $\sqrt{K_0}$  完成等高线分割操作，同样结合密钥  $K_1$  以 3.1 节信息嵌入过程中 Step3 的原理构造顶点坐标帧数据序列，逐步进行区间数据采

样，得到自区间序列的广义含密灰度图序列。

**Step3** 解析经 Haar 小波变换后的广义灰度图零树结构中节点的小波系数，进行频域系数值奇偶逆替换操作。需注意的是，当信息嵌入数据量满足  $Q < T$  时，以  $X$  轴方向完成 Step1、Step2 后，仍需按  $Y$  轴或  $Z$  轴方向进行循环操作；当  $Q > T$  时，只执行 Step1 与 Step2 即可完成第二重信息提取。

### 3.2 生成带有表面颜色属性的含密 obj 文件

根据三维载体模型区域不同，模型贴图可分为规则区域投影贴图与非规则区域投影贴图。不同 3D 模型具有不同的三维立体结构，可分为普通三维模型与复杂三维模型贴图<sup>[36]</sup>。对 3D 模型进行贴图，需要了解模型的构造方法与分类类型，之前三维模型研究大都是基于 Open GL 平台进行网格建模，但模型外观粗糙，可视化与美观性也较差。Autodesk 3ds Max 可根据客观对象快捷地构建可视性好的三维模型，本文正是基于 Autodesk 3ds Max 平台进行含密图像材质贴图工作。

本质上各三维模型建模平台的贴图映射规则相似，其核心思想都是先获取适当的 3D 模型与模型纹理贴图，然后运用投影方法在模型的表面对应区域附上对应的纹理信息，如纹理坐标关系等，以完成模型局部所有的纹理贴图。同时，为投影到模型的细节与边缘部分，相关学者利用几何与代数思想将模型中相邻三角面片与模型表面区域对应起来，使纹理贴图可以美观精细地自动匹配到 3D 模型的细节区域，具有更加真实的可视化效果。这类映射规则使 obj 模型具有对模型表面贴图进行一般操作而原贴图文件信息不受影响的特性，本文采用正交投影的纹理映射规则。

目前，二维图像含密载体数据已经隐藏完成，共选取了 5 幅贴图作为 obj 模型文件的图库。其中，含密贴图有 3 幅，分别为 Lena 含密贴图、含密铁皮贴图、含密紫砂贴图以及含密剪纸贴图；隐藏的秘密信息为 Scene 图像；注意第五张青花瓷贴图为代表图片库中迷惑攻击者的未隐藏信息的正常贴图。三维模型 stl 壶体含密载体数据也隐藏成功，隐藏的隐秘信息为 CHD 校徽图像。obj 模型文件的详细构成在后面进行详述。

为解决含密载体文件在传输过程中遭受高强度攻击后隐秘信息不能提取或没有备份信息可供提取的缺点，本文综合利用二维图像数据与三维模型数据隐藏空间，将多份备用的隐秘信息嵌入到图像数据后，再将不同的隐秘信息嵌入到 stl 三维模型中，最终生

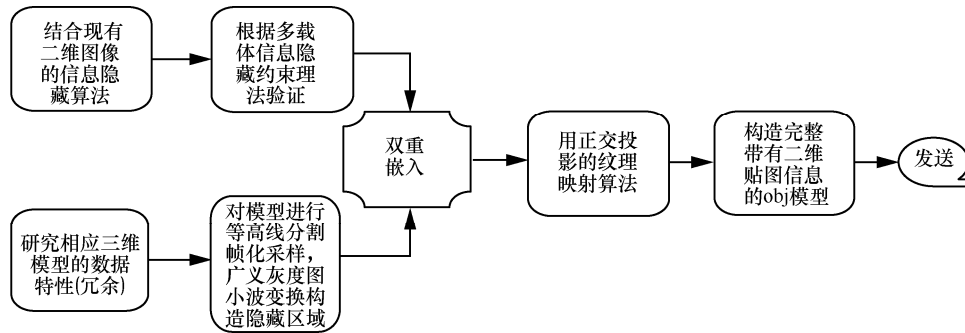


图 5 隐藏思路

成完整 obj 文件进行传输。详细隐藏思路如图 5 所示。

因 obj 模型文件支持贴图坐标与法线信息，因此载体文件包含标准图片库（能放置多幅图片）；同时，纹理与材质信息通常用配置文件（MTL, material library file）来存储。在该格式类型的三维模型文件中，常用一些关键字对模型的顶点进行分类，如  $v$  表示模型的几何体顶点，因此 obj 文件关键字  $v$  后面的三维坐标集合代表几何体顶点，此后相关意义不再赘述。 $v_i$  代表贴图坐标点， $v_n$  代表顶点法线， $f$  代表模型的组成元素面，该文件一般不需要文件头，但默认导出的 obj 模型文件以“#”作为文本注释信息代表符出现在文本开头。含密 obj 模型生成效果如图 6 所示。



图 6 带有贴图信息的 obj 模型立体效果

## 4 实验对此与分析评估

利用 Matlab、C++、Meshlab 和 3ds max 实现并验证本文算法。为证明本文算法的不可见性与顽健性，分别对 obj 含密文件进行深度攻击和浅度攻击（表层攻击）；最后运用灰度直方图频谱化的检测手段验证本文的算法的抗分析性。

### 4.1 不可见性实验分析

分别向图库中 4 幅载体贴图嵌入 4 份相同的 scene 隐秘信息后原贴图与含密贴图的不可见性感官表现效果见图 3，第 5 幅贴图，即图库中普通的青花瓷贴图，仅代表一类未隐藏任何隐秘信息并带有迷惑性质的载体贴图集。同理，原始 stl 壶体三维模型与隐藏隐秘 CHD 校徽信息的三维模型的直观感官差异见图 4。人眼观察可得，载体含密前后几乎没有差别，具有良好的不可见性。下面用客观指标衡量本文算法的不可见性。

信噪比<sup>[37]</sup>和 Hausdorff<sup>[38]</sup>距离是测量二维图形数与三维模型隐藏信息前后载体修改程度的简单有效的度量指标。实验结果如表 1 所示。

表 1 信噪比和 Hausdorff 距离

实验载体	信噪比/dB	Hausdorff 距离
Lena 贴图	36.24	0.003 075
铁皮贴图	33.62	0.003 149
紫砂贴图	38.49	0.002 987
剪纸贴图	29.51	0.003 832
壶体 stl 模型	25.72	0.004 294

实验结果表明，本文的隐藏算法对模型修改程度较小，且含密三维模型的不可见性与二维图像载体相比较差。实际产业化应用时可将关键或密级高的隐秘信息隐藏于 obj 文件的图像库中。

## 4.2 顽健性实验分析

### 4.2.1 深度攻击

分别对 4 幅含密贴图进行高斯噪声、高光平滑、灰度分割、均匀剪切、棋盘旋转及联合攻击，实验结果采用式(2)的归一化相关系数 NC 作为评估算法顽健性的标准。

$$NC = \frac{\sum_i^N w_i \hat{w}_i}{\sqrt{\sum_u^N w_u^2 \sum_u^N \hat{w}_u^2}} \quad (2)$$

其中， $w_i$  为原始信息比特数； $\hat{w}_i$  为提取的信息比特数； $T$  为判定隐秘信息存在与否的阈值， $NC \geq T$  时，表示存在秘密信息  $w$ ； $NC < T$  时，表示不存在秘密信息  $w$ 。根据文献[39]的实验方案，取  $T$  值为 0.5。

经各类深层次攻击后隐秘信息提取情况如图 7 所示，可以看到经过高斯噪声、高光平滑、灰度分割、均匀剪切、棋盘旋转以及联合攻击后，隐秘信息关键细节仍可被正确提取。同时，为具体分析各类攻击算法对水印提取的影响，采用式(3)中的错误信息比特提取率衡量含密载体水印的脆弱性标识影响程度。

$$BER = \frac{g'}{N} \quad (3)$$

其中， $g'$  为遭受不同种类攻击后提取的水印信息比特错误率， $N$  为含密贴图载体嵌入第一重隐秘水印信息的总信息位值。

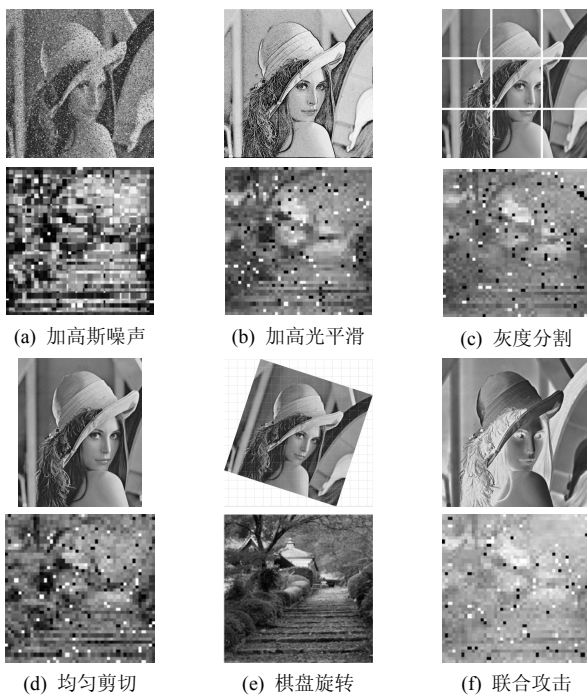


图 7 各类深层次攻击后隐秘信息提取情况

经各类深层次攻击后检测提到的 NC 值如表 2 所示。由表 2 可知，经过各种深层次攻击，提取信息的系数 NC 值仍大于最低阈值 0.5，尤其经历联合攻击后，4 种含密贴图系数值均在  $T$  值以上，贴图隐藏算法性能良好。

攻击参数	含密 Lena	含密铁皮	含密紫砂	含密剪纸
高斯噪声(3.5%)	0.736	0.792	0.724	0.689
高光平滑	0.692	0.721	0.645	0.592
灰度分割	0.615	0.611	0.627	0.619
均匀剪切	0.594	0.563	0.592	0.603
棋盘旋转	0.861	0.825	0.862	0.792
联合攻击	0.513	0.506	0.523	0.503

第一重秘密水印信息提取比特错误率比值如表 3 所示。依次遭受高斯噪声、高光平滑、灰度分割、均匀剪切、棋盘旋转以及联合攻击后，信息提取错误比特量与原始水印信息总信息量比值占比均小于 45%，即各类攻击算法对水印提取的影响程度较低。

攻击类型	含密 Lena	含密铁皮	含密紫砂	含密剪纸
高斯噪声(3.5%)	37.9%	35.7%	40.1%	39.9%
高光平滑	42.6%	37.2%	34.3%	29.1%
灰度分割	25.1%	28.2%	34.6%	40.1%
均匀剪切	31.4%	25.2%	18.1%	29.4%
棋盘旋转	29.1%	38.1%	42.4%	34.7%
联合攻击	40.3%	39.7%	37.2%	29.5%

衡量含密壶体 stl 三维模型的顽健性指标如式(4)的相关系数  $Corr$  所示。对其分别进行随机噪声、非均匀缩放、面片覆盖、角度旋转、面片剪切和顶点渲染攻击，其中将提取信息比特量记为序列  $\{s'_n\}$ ，将原始信息比特数记为  $d$  序列  $\{s_n\}$ 。攻击情况如图 8 所示。

$$Corr = \frac{\sum_{n=1}^{N-1} (s'_n - \bar{s}') (s_n - \bar{s})}{\sqrt{\sum_{n=1}^{N-1} (s'_n - \bar{s}')^2 \sum_{n=1}^{N-1} (s_n - \bar{s})^2}} \quad (4)$$

本文算法相关系数  $Corr$  指标如图 9 所示。可以看出不同攻击类型相同攻击强度下，三维模型隐藏算法性能相关度均在 60% 以上。其中对于角度旋转攻击，信息相关度达到 81.12% 以上，表明从含密 stl 模型提取的关键信息可以有效识别，顽健性较强。

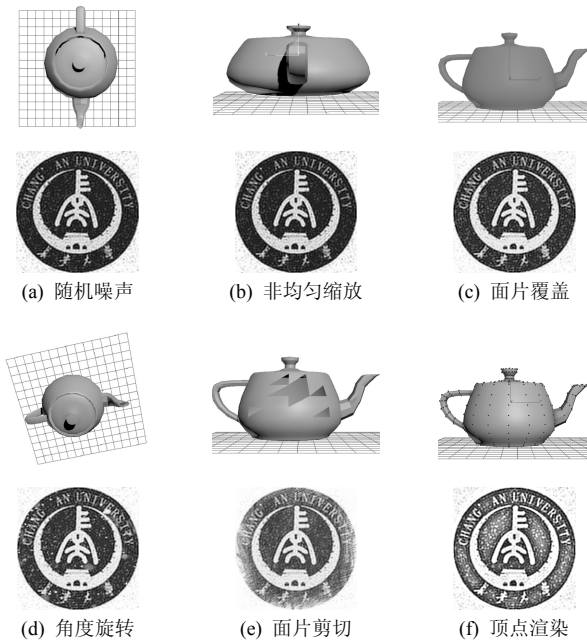


图 8 stl 模型受攻击及提取的隐秘信息情况

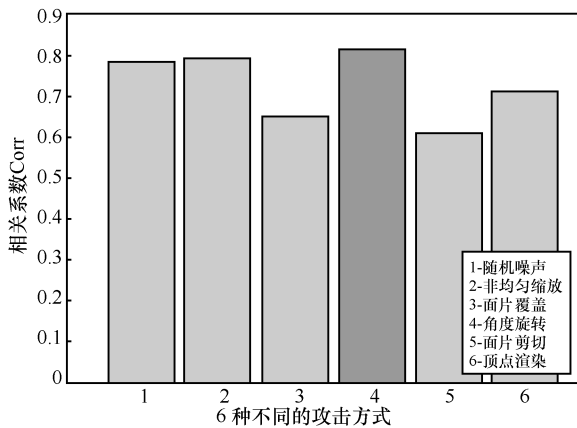


图 9 本文算法相关系数 Corr 指标

文献[19]算法相关系数 Corr 指标如图 10 所示, 利用相同的实验载体完成信息隐藏后进行指标提取。可以看出, 基于三维模型球型分割的隐藏算法性能大都在 55%以下, 仅对第四种角度旋转的抗攻击能力达到 71.2%以上。表明该算法抵抗攻击的类型单一, 顽健性有待加强。

文献[20]算法相关系数 Corr 指标如图 11 所示, 采用壶体 stl 三维模型作为实验载体。从统计的指标数据可看出采用内切球解析次数的三维模型隐藏算法性能相关度有 3 种在 53%以下, 即对非均匀缩放、按角度旋转和顶点渲染这 3 种攻击抵抗力较强, 顽健性良好, 其中, 角度旋转的抗攻击能力达到 81.26%以上, 表明该算法在抵抗旋转类型攻击的性能突出而稳定, 适合特定的操作应用领域。

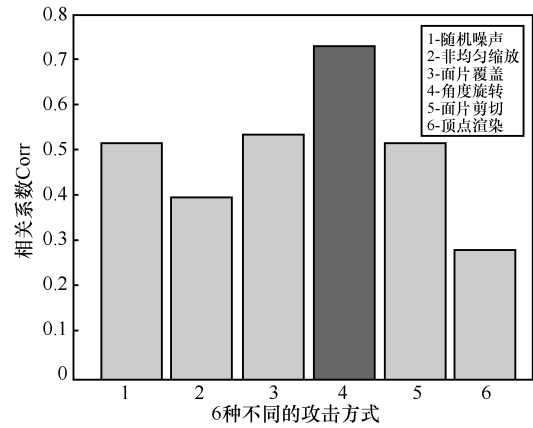


图 10 文献[19]算法相关系数 Corr 指标

### 4.2.2 浅度攻击 (表层攻击)

如图 5 所示, 本文将渲染构造好的含密模型以 obj 格式类型的形式导出, 选中材质导出项, 将模型的材质等信息保存在相应 MTL 配置文件内, 最后生成完整的 obj 三维含密模型进行传输。考虑到传输过程中破坏者会对含密模型进行浅度攻击, 并且模型应用可能会受到表层渲染, 本节仅以 Lena 含密贴图进行载体浅度攻击模拟实验。

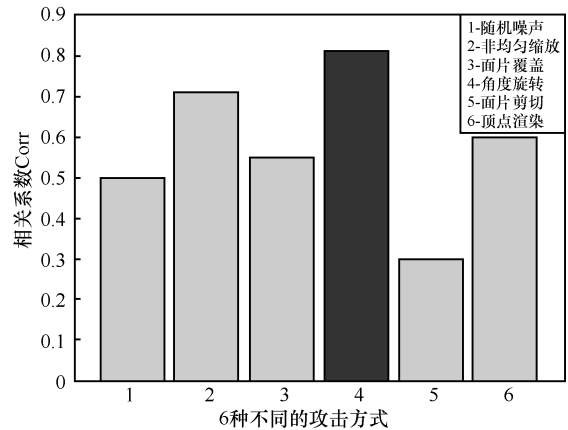


图 11 文献[20]算法相关系数 Corr 指标

表层攻击如图 12 所示。可以看出, 在完整含密 obj 文件进行相异载体不同隐秘信息隐藏处理后, 经历顶点绘制、面片覆盖、面片剪切、面片平滑、视角旋转和面片隐藏攻击后, 可供备份的隐秘 scene 信息几乎不被这类表层攻击影响到, 信息基本都可准确提取。

对 obj 模型载体分别进行上述 6 种攻击测试, 与文献[19]和文献[20]中信息隐藏算法做比较, 并着重对比前 3 种表层攻击中的特殊攻击, 顶点绘制攻击比较曲线如图 13 所示, 面片覆盖测算法性能如图 14 所示, 面片剪切攻击对此指标如图 15 所示。



图 12 表层攻击及提取的隐秘信息

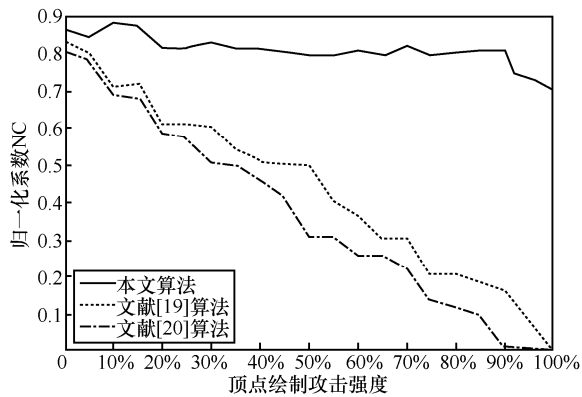


图 13 顶点绘制攻击算法性能比较曲线

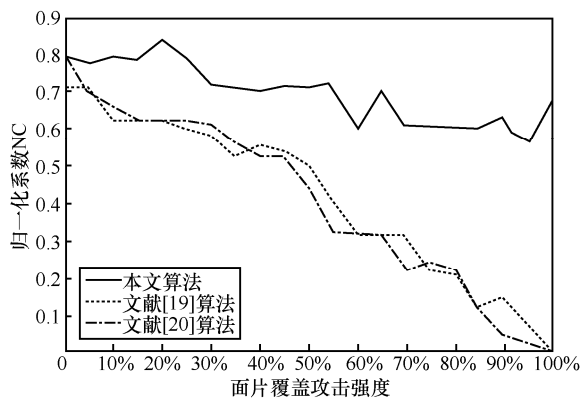


图 14 面片覆盖攻击算法性能比较曲线

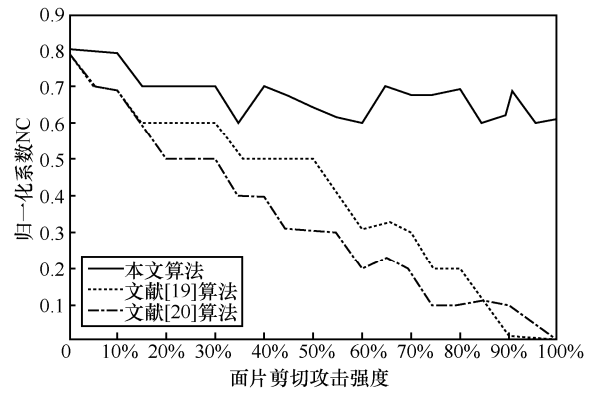


图 15 面片剪切攻击算法性能比较曲线

从图 13 曲线可看出在 obj 含密模型受到顶点绘制攻击后提取备份隐秘 scene 信息情况。经本文多载体算法与对照文献中三维模型球型分割算法以及内切球解析次数算法比较，随着顶点绘制密度增加，由于算法备份信息嵌入区域与模型表层攻击的顶点以及拓扑结构无关，多载体算法信息提取归一化系数保持在 0.8 以上，意味着备份信息经本文算法可以正常提取，算法顽健性与安全性得到极大增强。其他 2 种算法的隐秘信息在顶点绘制强度增强到 45% 及以上时，原始隐秘信息破坏严重，且攻击范围到 80% 时，用文献[19]算法和文献[20]算法已经无法提取有效的秘密信息，同时没有备份的关键信息可供提取，算法实用性与顽健性强度有限。

同理，从图 14 与图 15 中算法实验性能对比曲线可看出，随着面片覆盖范围与面片剪切程度增强到 43% 以上，对比文献中的 2 种算法的 NC 系数值已经低于秘密信息提取判定阈值 ( $NC < T = 0.5$ )，即提取有效可用的隐秘信息比较困难。对于表层攻击本文算法稳定性比文献[19]算法和文献[20]算法差，这是因为当表层攻击强度平均高于 40% 时，原始承载体 stl 模型的隐藏区域的隐秘 CHD 校徽信息已被破坏严重，关键信息提取严重依赖于 obj 文件标准图库中的贴图隐藏载体。但图片库中的多幅贴图的各种备份关键信息可缓解上述缺点。因此本文算法的整体抗攻击能力与实用性较强。

### 4.3 抗分析性实验分析

常见的抗分析方法包括抗 RS 检测或抗  $\chi^2$  检测，抗灰度图分析等算法<sup>[40]</sup>。本文将隐藏有备份 Scene 信息的初始含密 Lena 图的灰度图作为抗检测分析的实验样本，以文献[11-12]的图像隐藏算法作为对比组。初始含密 Lena 图像灰度图参数与各算法指标如图 16(a) ~ 图 16(d) 所示。

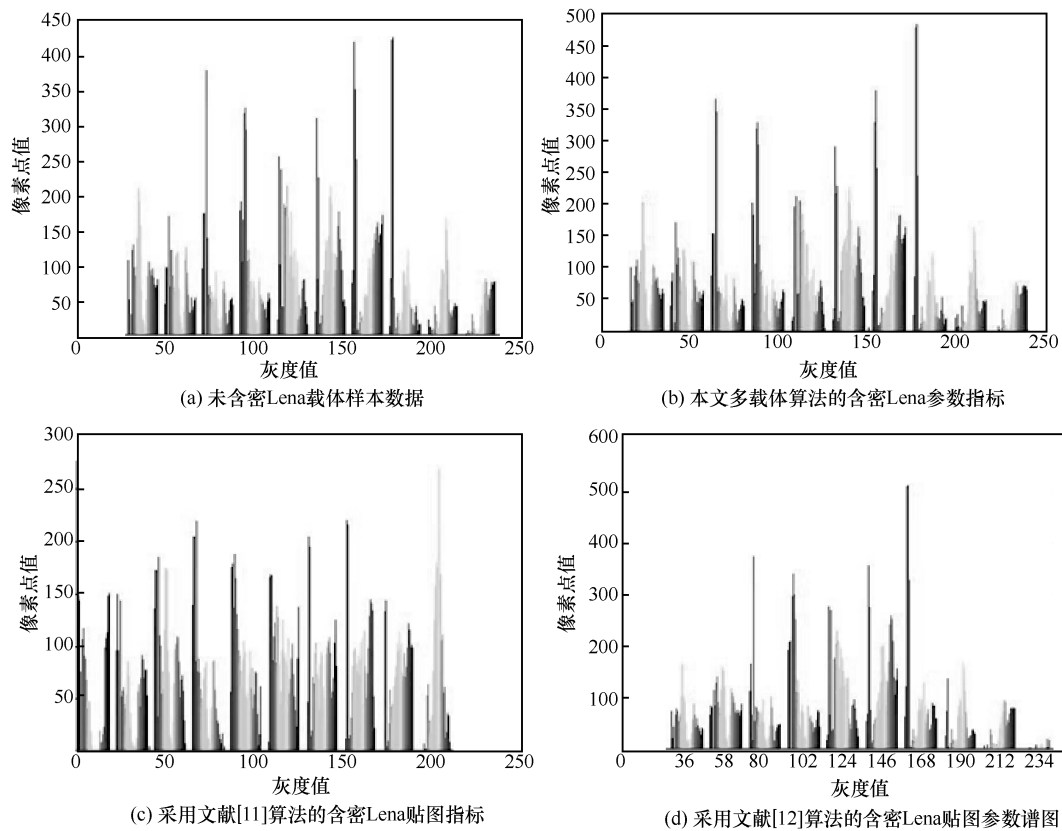


图 16 未含密贴图数据与各算法含密贴图数据

从图 16 各对象系谱数据对比可得, 运用本文相异多载体算法嵌入进行信息隐藏, 信息嵌入前后的系谱数据只有细微的差别, 抗分析性良好; 运用文献[11]算法和文献[12]算法, 信息嵌入前后具有较大差异, 抗分析性能有待加强。

## 5 结束语

为提高隐秘信息传输后抵抗攻击的能力, 增强信息隐藏技术实用性并缩短信息隐藏产品产业化投入周期。本文基于二维离散小波变换算法与 stl 模型帧化以及广义灰度图方法, 通过选取不受 obj 模型正交投影影响的理贴图图库作为备份关键信息隐藏的嵌入载体群。综合利用二维图像载体库与三维模型数据冗余空间, 保证了算法的不可见性与顽健性, 满足三维模型可视化与信息隐藏技术的性能要求。仿真实验证明, 算法适用于对顽健性要求较高的场景应用环境。算法稳定性与安全性严重依赖 obj 文件的贴图图库集, 但可通过批量隐写的手段将多种待备份的隐秘信息嵌入丰富的图片载体群中, 同时根据应用需求可选取待嵌入隐秘信息的类型与备份信息数量。故在后续研究中, 将着重建

立该类算法批量隐写方案与信息容量性评估。

## 参考文献:

- [1] 王静, 郁梅, 蒋刚毅, 等. 基于单深度帧内模式的 3D-HEVC 深度视频信息隐藏算法[J]. 光电子·激光, 2017(8):893-901.  
WANG J, YU M, JIANG G Y, et al. An information hiding algorithm of depth video in 3D-HEVC based on single depth intra mode[J]. Journal of Optoelectronics•Laser, 2017(8):893-901.
- [2] YUAN Z Q, GUAN Z J, FENG H. An improved information hiding algorithm based on image[C]// IEEE International Conference on Software Engineering Research. IEEE, 2017.
- [3] ZHOU X, GONG W, FU W L, et al. An improved method for LSB based color image steganography combined with cryptography[C]// IEEE/ACIS International Conference on Computer & Information Science. IEEE/ACIS, 2016.
- [4] LIU X S, ZHANG J X. Large-capacity LSB information hiding scheme based on two-dimensional code[C]//The 7th International Conference on Electronics Information and Emergency Communication. IEEE, 2017.
- [5] TSAI Y Y, HUANG Y H, LIN R J, et al. An adjustable interpolation-based data hiding algorithm based on LSB substitution and histogram shifting[J]. International Journal of Digital Crime & Forensics, 2016, 8(2):48-61.
- [6] KER A D. Improved detection of LSB steganography in grayscale images[C]//International Conference on Information Hiding. 2004: 97-115.

- [7] DUMITRESCU S, WU X, WANG Z. Detection of LSB steganography via sample pair analysis[C]// Revised Papers From the International Workshop on Information Hiding. 2002:355-372.
- [8] FARID H. Detecting hidden messages using higher-order statistical models[C]//International Conference on Image Processing. IEEE, 2002.
- [9] SINGH V P, MALHOTRA S, SRIVASTAVA R. Combining hybrid information descriptors and DCT for improved CBIR performance[C]// International Conference on Control. IEEE, 2017.
- [10] PATEL P, PATEL Y. Secure and authentic DCT image steganography through DWT - SVD based digital watermarking with RSA encryption[C]//The 15th International Conference on Communication Systems & Network Technologies. IEEE, 2015.
- [11] 邵菲, 花俊. 基于 Walsh 序列扩频的图像信息隐藏[J]. 国外电子测量技术, 2009, 28(8):32-34.  
SHAO F, HUA J. Image information hiding based on Walsh sequence spread spectrum[J]. Foreign Electronic Measurement Technology, 2009, 28(8):32-34.
- [12] 陈胜, 王兴众. 基于离散余弦变换和置乱融合模型的图像信息隐藏方法研究[J]. 舰船电子工程, 2017(12):64-67.  
CHEN S, WANG X Z. Research on image information hiding method based on DCT and scrambling fusion model[J]. Ship Electronic Engineering, 2017(12):64-67.
- [13] TIJHUIS A G. Stability analysis of the marching-on-in-time method for one- and two-dimensional transient electromagnetic scattering problems[J]. Colloquium topics in applied numerical analysis, 1984(2):363-386.
- [14] SWELDENS W. The lifting scheme: a custom-design construction of biorthogonal wavelets[J]. Applied & Computational Harmonic Analysis, 1996, 3(2):186-200.
- [15] SANGWINE S J. Fourier transforms of colour images using quaternion or hypercomplex, numbers[J]. Electronics Letters, 1996, 32(21):1979-1980.
- [16] SANGWINE S J. Colour image edge detector based on quaternion convolution[J]. Electronics Letters, 2002, 34(10):969-971.
- [17] MOXEY C E, ELL T A, SANGWINE S J. Hypercomplex operators and vector correlation[C]// Signal Processing Conference, IEEE, 2002:1-4.
- [18] 慕科, 张大方, 谢冬青. 基于帧化采样和小波 HMM 的三维模型信息隐藏[J]. 计算机辅助设计与图形学学报, 2010, 22(8):1406-1411.  
QI K, ZHANG D F, XIE D Q. 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.
- [19] 任帅, 张弢, 杨涛, 等. 基于三维模型球型分割的信息隐藏算法[J]. 计算机应用, 2017, 37(9):2576-2580.  
REN S, ZHANG T, YANG T, et al. Information hiding algorithm based on spherical segmentation of three-dimensional model [J]. Journal of computer application, 2017, 37(9): 2576-2580.
- [20] 张弢, 慕德俊, 任帅, 等. 利用内切球解析的三维模型信息隐藏算法[J]. 西安电子科技大学学报, 2014, 41(2):185-190.  
ZHANG T, MU D J, REN S, et al. Information hiding scheme for 3D models based on skeleton and inscribed sphere analysis[J]. Journal of Xidian University, 2014, 41(2):185-190.
- [21] 任帅, 张弢, 徐振超, 等. 特征点标注与聚类的三维模型信息隐藏算法[J]. 计算机应用, 2018, 38(4):1017-1022.  
REN S, ZHANG T, XU Z C, et al. Information hiding algorithm for 3D models based on feature point labeling and clustering[J]. Journal of Computer Applications, 2018, 38(4):1017-1022.
- [22] PUTEAUX P, PUECH W. Reversible data hiding in encrypted images based on adaptive local entropy analysis[C]// The 17th International Conference on Image Processing Theory. IEEE, 2018.
- [23] ZHOU W, ZHANG W, YU N. A new rule for cost reassignment in adaptive steganography[J]. IEEE Transactions on Information Forensics and Security, 2017:1-1.
- [24] CHANDRAMOULI R, MEMON N D. Steganography capacity: a steganalysis perspective[J]. Security & Watermarking of Multimedia Contents V, 2003, 5020.
- [25] JOSEPH P, VISHNUKUMAR S. A study on steganographic techniques[C]//Global Conference on Communication Technologies (GCCT). IEEE, 2015:206-210.
- [26] COGRANNE R, SEDIGHI V, FRIDRICH J. Practical strategies for content-adaptive batch steganography and pooled steganalysis[C]// IEEE International Conference on Acoustics. 2017.
- [27] GAO Z Z, TANG G M, DAI J M. Research on payload adaptive batch steganography[J]. Application Research of Computers, 2013, 30(9):2780-2783.
- [28] 杨焯, 孙容海, 施林甫, 等. 面向大文件的多载体图像信息隐藏方法[J]. 信息技术, 2018(5):60-62.  
YANG Y, SUN R H, SHI L F, et al. Multiple cover images based information hiding method for large file[J]. Information Technology, 2018(5):60-62.
- [29] 黄福鸿. 数字图像多算法协同隐写方案研究与设计[D]. 北京: 北京邮电大学, 2018.  
HUANG H F. Research on scheme of multiple digital image algorithms cooperate for steganography[D]. Beijing: Beijing University of Posts and Telecommunications, 2018.
- [30] 林代茂, 胡岚, 郭云彪, 等. 广义信息隐藏技术的机理与模型[J]. 北京邮电大学学报, 2005, 28(1):1-5.  
LIN D M, HU L, GUO Y B, et al. The mechanism and model of generalized information hiding technology[J]. Journal of Beijing University of Posts and Telecommunications, 2005, 28(1):1-5.
- [31] KER A D. The square root law requires a linear key[C]// The 11th ACM Workshop on Multimedia and Security. 2009: 85-92.
- [32] PEVNY T, FRIDRICH J. Merging Markov and DCT features for multi-class jpeg steganalysis[C]// Security, Steganography and Watermarking of Multimedia Contents IX. International Society for Optics and Photonics, 2007:650503.
- [33] 梁小萍, 何军辉, 李健乾, 等. 隐写分析——原理、现状与展望[J]. 中山大学学报(自然科学版), 2004, 43(6):93-96.  
LIANG X P, HE J H, LI J K, et al. Steganalysis——principle, actuality and prospect [J]. ACTA Scientiarum Naturalium Universitatis Sunyatseni, 2004, 43(6):93-96.
- [34] 胡自权. 博弈论在信息隐藏中的生存能力研究[D]. 成都: 电子科技大学, 2013. 6-8.  
HU Z Q. Research on survivability of hidden information using game theory[D]. Chengdu: University of Electronic Science and Technology of China, 2013. 6-8.
- [35] 姚辉灿. 基于图像的信息掩密技术[D]. 西安: 西北工业大学, 2004: 16-22.  
YAO X H. Image-based information masking technology[D]. Xi'an:

Northwestern Polytechnical University, 2004: 16-22.

[36] 熊秋波. 不规则区域纹理提取与 3D 模型贴图[D]. 长沙: 中南林业科技大学, 2010: 20-29.

XIONG Q B. The irregular regional texture extraction and 3d model mapping[D]. Changsha: Central South University of Forestry and Technology,2010: 20-29.

[37] 王新宇, 詹永照. 构造顶点分布特征的三维模型数字水印算法[J]. 计算机辅助设计与图形学学报, 2014, 26(2):272-279.

WANG X Y, ZHAN Y Z. A watermarking scheme for three-dimensional models by constructing vertex distribution on characteristics [J]. Journal of Computer-Aided Design & Computer Graphics, 2014, 26(2):272-279.

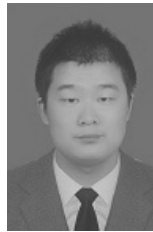
[38] CARLSON N A, PORTER J R. On the cardinality of hausdorff spaces and h-closed spaces[J]. Topology & Its Applications, 2013, 160(1): 137-142.

[39] 张弢, 柳雨农, 邢亚林,等. 基于直方图移位的 AMBTC 域无损信息隐藏[J]. 计算机应用研究, 2019(6):1-8.

ZHANG T, LIU Y N, XING Y L, REN S, et al. Lossless information hiding in ambtc domain based on histogram shift [J]. Application Research of Computers, 2019 (6):1-8.

[40] 姜艳梅. 抗 RS 检测的无损信息隐藏算法研究[D]. 天津: 天津大学, 2007: 38-51.

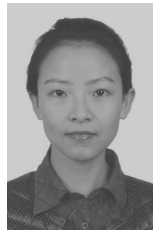
JIANG Y M. Research on lossless information hiding resisting rs detection[D]. Tianjin :Tianjin University, 2007: 38-51.



王震 (1993- ), 男, 山西运城人, 长安大学硕士生, 主要研究方向为信息隐藏技术。

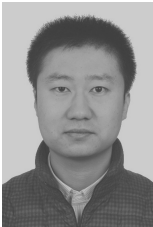


苏东旭 (1995- ), 男, 河南许昌人, 长安大学硕士生, 主要研究方向为多媒体数据检索及认证。



张弢 (1984- ), 女, 山西吕梁人, 博士, 长安大学副教授, 主要研究方向为多载体信息隐藏技术。

[作者简介]



任帅 (1982- ), 男, 山西太原人, 博士, 长安大学副教授, 主要研究方向为信息隐藏技术。



慕德俊 (1963- ), 男, 山东荣成人, 博士, 西北工业大学教授, 主要研究方向为网络与信息安全。