软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2023,34(12):5773−5786 [doi: 10.13328/j.cnki.jos.006752]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于风格迁移纹理合成与识别的构造式信息隐藏*

秦 川, 董腾林, 姚 恒

(上海理工大学 光电信息与计算机工程学院, 上海 200093)

通信作者: 秦川, E-mail: qin@usst.edu.cn

摘 要: 传统的信息隐藏算法大都通过修改载体达到隐藏秘密信息的目的, 但不可避免地会在载体数据中留下修改痕迹, 故常难以抵抗隐写分析技术的检测, 为此无载体信息隐藏应运而生. 无载体信息隐藏并非不使用载体, 而是不对载体数据进行修改. 为了提高无载体信息隐藏算法的隐藏容量和鲁棒性, 提出了一种基于风格迁移纹理合成与识别的构造式信息隐藏算法. 该算法首先选取不同类别的自然图像和纹理图像分别建立内容图像库和纹理风格图像库, 并根据内容图像库中自然图像的类别构建二进制码的映射字典; 其次为了接收方能够从含密图像中提取出秘密信息, 需要构建带标签的纹理图像库, 并将其作为训练集输入到卷积神经网络中, 通过迭代训练获得纹理图像识别模型. 在秘密信息隐藏时, 根据秘密信息片段选择对应类别的自然图像, 并按照一定的顺序组合成含密拼接图像, 随后从纹理图像库中随机选择一张纹理图像, 通过风格迁移的方法将含密拼接图像转换成含密纹理图像, 从而完成秘密信息隐藏过程. 在信息提取过程中, 通过纹理图像识别模型可准确识别出含密纹理图像原本对应的图像类别, 再对照映射字典即可提取出秘密信息. 实验结果表明, 所提算法生成的含密纹理图像具有良好的视觉效果, 秘密信息隐藏容量较高, 且对 JPEG 压缩、高斯噪声等攻击具有较强的鲁棒性.

关键词: 构造式信息隐藏; 纹理图像; 隐藏容量; 鲁棒性; 图像风格迁移

中图法分类号: TP309

中文引用格式: 秦川, 董腾林, 姚恒. 基于风格迁移纹理合成与识别的构造式信息隐藏. 软件学报, 2023, 34(12): 5773–5786. http://www.jos.org.cn/1000-9825/6752.htm

英文引用格式: Qin C, Dong TL, Yao H. Constructive Data Hiding Based on Texture Synthesis and Recognition with Image Style Transfer. Ruan Jian Xue Bao/Journal of Software, 2023, 34(12): 5773–5786 (in Chinese). http://www.jos.org.cn/1000-9825/6752.htm

Constructive Data Hiding Based on Texture Synthesis and Recognition with Image Style Transfer

QIN Chuan, DONG Teng-Lin, YAO Heng

(School of Optical-electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China)

Abstract: Most traditional information hiding methods embed secret data by modifying cover data, which inevitably leaves traces of modification in cover data, and hence, it is difficult to resist the detection of the existing steganalysis algorithms. Consequently, the technique of coverless information hiding emerges, which hides secret data without modifying cover data. To improve the hiding capacity and robustness of coverless information hiding, this study proposes a constructive data hiding method based on texture synthesis and recognition with image style transfer. Firstly, natural images and texture images of different categories are used to construct the content image database and the textural style image database, respectively. A mapping dictionary of binary codes is established according to the categories of natural images in the content image database. Secondly, the labeled textural image database should be constructed and input into the convolutional neural network as a training dataset, and the texture image recognition model can be obtained by iterative training. In this way, the secret data can be extracted from stego images at the receiving end. During secret data hiding, natural images are selected from the content image database according to to-be-embedded secret data fragments, which are synthesized to form a stego mosaic image. Then, a texture image is randomly selected from the textural style image database, and the stego texture image can be generated by the

* 基金项目: 国家自然科学基金 (62172280, U20B2051, 62172281); 上海市科委高校能力建设项目 (20060502300)
收稿时间: 2021-05-31; 修改时间: 2021-10-08; 采用时间: 2022-07-25; jos 在线出版时间: 2022-10-27
CNKI 网络首发时间: 2023-02-08

selected texture image and the stego mosaic image with the strategy of style transfer to achieve secret data hiding. During secret data extraction, the obtained texture image recognition model can accurately identify the original categories of stego texture images corresponding to natural images, and secret data can be finally extracted by reference to the mapping dictionary. The experimental results demonstrate that the proposed method can achieve the stego texture image with a satisfactory visual effect and a high hiding capacity, and it illustrates strong robustness to attacks such as JPEG compression and Gaussian noise.

Key words: constructive data hiding; texture image; hiding capacity; robustness; image style transfer

信息隐藏技术是将秘密信息嵌入至公开的载体数据中, 进而完成信息的隐蔽传输[1], 常采用的载体为多媒体数据, 如文本[2]、视频[3]、音频[4]、图像[5]等. 数字图像由于在互联网中使用广泛, 因此是最常被使用的信息隐藏载体. 传统的图像信息隐藏方法通过各种手段对载体图像进行修改, 将秘密信息嵌入到载体图像中, 如基于空间域最低有效位 (least significant bit, LSB)[6]、基于 JPEG 压缩域[7]、基于变换域 DFT[8]、DWT[9]、DCT[10]等算法. 但信息的嵌入不可避免地会在载体图像中留下修改痕迹, 因此常难以抵抗隐写分析算法的检测. 为此, 无载体信息隐藏的概念应运而生. 无载体并不是指不需要载体, 与传统的信息隐藏相比, 它不再需要选择载体后再进行修改以嵌入秘密信息, 而是直接根据秘密信息来获取对应的含密载体, 或者以秘密信息为驱动来构造含密载体[11]. 相应地, 目前无载体信息隐藏主要可以分为两类: 基于载体选择的算法和基于载体构造的算法.

基于载体选择的信息隐藏算法大多是通过提取载体图像特征, 并与秘密信息建立一定的映射关系, 来完成信息隐藏. 文献 [12] 利用 BOW (bag-of-words) 模型提取图像的视觉关键词来表达秘密信息, 该算法不需要对载体图像进行修改, 但需要大量的图像构建码本, 且隐藏容量相对较小、鲁棒性弱. 为了提高无载体信息隐藏的鲁棒性, 文献 [13] 提出了一种基于图像 SIFT (scale-invariant feature transform) 特征和 BOF (bag-of-features) 模型的无载体信息隐藏算法, 该算法通过提取图像 SIFT 特征并与秘密信息构建相应的映射关系进行信息隐藏, 但该算法的隐藏容量相对较小. 为了进一步提高算法的鲁棒性和隐藏容量, 文献 [14] 提出了基于目标识别的算法, 通过构建秘密信息与物体类别的映射关系, 完成秘密信息隐藏, 并通过 Faster-RCNN 目标识别方法识别载体图像上的物体类别, 以提取出秘密信息. 该算法在一定程度上提高了信息隐藏算法的隐藏容量和鲁棒性, 但由于自然图像上通常包含不同类别的物体数量有限, 因此该算法难以隐藏大量的秘密信息.

在基于载体构造的信息隐藏算法中, 由于纹理图像作为一种图像处理和计算机图形学应用中常见的图像类型在互联网上广泛存在且其视觉内容具有一定的规律性, 故构造生成含密的纹理图像是最具代表性的工作. 该类算法对应的应用协议为: 发送方首先基于秘密信息的驱动生成含密图像 (生成过程中的初始条件可为预定的生成图像的类型, 如纹理图像等), 再将生成的含密图像通过公用信道传输给接收方 (在传输过程中含密图像可能会遭受到攻击); 接收方收到含密图像后进行信息提取得到秘密信息; 设计的含密图像生成和信息提取算法需保证: 信息的隐藏容量尽可能的大, 提取出的信息要与隐藏的信息尽可能的相同, 且含密图像在视觉上要尽可能的自然, 三者分别对应隐藏容量、鲁棒性和隐蔽性这 3 个主要的性能指标. Ototi 等人[15]提出将秘密信息参与到纹理图像生成的过程中, 该方法从样本图像中选择若干彩色像素点, 使用 LBP 码来建立彩色点和一组二维数据之间的映射关系, 接着根据秘密信息预先确定若干位置的彩色点, 最后从样本图像中寻找合适内容生成大幅的含密纹理图像. 该方法能够隐藏的秘密信息相对较少, 且鲁棒性较弱. 与文献 [15] 基于含密纹理图像合成的算法不同, 文献 [16] 提出了一种基于模拟水影画 (又称湿拓画, marbling) 的信息隐藏算法. 该算法首先确定生成含密载体图像的大小, 并生成相应的空白图像; 然后将需要隐藏的秘密信息书写到生成的空白图像上, 为了使生成的纹理图像能够完全掩盖秘密信息, 需要在剩余的空白区域填充适合的背景图案, 最后再模拟水影画形变的方法, 生成能够隐藏秘密信息的纹理图像. 文献 [17] 首先构建不同的特征图形与二进制数据之间的映射关系, 在信息隐藏时, 根据二进制秘密信息选取不同的图形并确定该图形在含密载体上的位置, 然后通过添加背景元素并利用形变操作生成最终含密纹理图像. 该算法能够实现较大容量的信息隐藏, 但无法有效抵抗含密载体在传输过程中受到的外界攻击. 文献 [18] 提出了一种基于纹理特征分类的无载体信息隐藏算法. 该算法首先提取纹理图像 SIFT 特征, 然后通过监督式分类训练生成分类模型, 根据图像块分类和位置信息的不同与秘密信息构建映射字典, 并通过形变函数生成含密纹理图像, 虽然该算法在一定程度上提高了构造式信息隐藏算法的鲁棒性, 但生成的纹理图像与真实纹理图

像在视觉上相差较大, 容易引起攻击者的怀疑.

综上所述, 基于载体选择的无载体信息隐藏算法多存在隐藏容量小、需要构建大规模图像库等问题; 而基于载体构造的无载体信息隐藏算法多存在鲁棒性不理想的问题. 因此, 本文为了进一步提高无载体信息隐藏算法的隐藏容量及鲁棒性, 提出一种基于风格迁移 (image style transfer, IST) 纹理合成与识别的构造式信息隐藏算法, 可在提高隐藏容量和保证生成含密纹理图像视觉质量的同时, 仍具有较高的鲁棒性. 本文工作的主要创新点包括: 1) 通过建立映射关系将内容图像库中的图像拼接为含密载体, 提高了秘密信息的隐藏容量; 2) 基于 IST 模型和纹理风格图像库中的图像将含密拼接图像生成为含密纹理图像, 且具有良好的视觉效果, 减小了被攻击的风险; 3) 通过构建带标签的纹理图像样本库训练获得纹理图像识别模型, 并将其应用于秘密信息提取过程中, 有效提高算法的鲁棒性.

本文第 1 节分别介绍本文算法的整体框架、纹理图像的合成与识别过程、秘密信息隐藏及提取过程; 第 2 节为实验结果的分析与比较; 第 3 节为全文总结及将来的工作方向.

1 本文算法

本文提出的基于 IST 的无载体信息隐藏算法框架如图 1 所示, 主要由 3 部分组成, 分别为模型训练、信息隐藏和信息提取. 本文算法在发送方首先需构建内容图像库 Φ 和纹理风格图像库 Ψ, 内容图像库 Φ 中包含不同类别且图像尺寸一致的自然图像, 纹理风格图像库 Ψ 中包含不同风格的纹理图像. 在进行秘密信息隐藏时, 通过事先构建的内容图像库 Φ 中自然图像类别与秘密信息片段的映射关系, 从 Φ 中选择相应类别的自然图像; 再按照 Zig-Zag 顺序将这些不同类别的自然图像拼接成一张含密的拼接图像; 最后从纹理风格图像库 Ψ 中随机选择一张纹理图像, 利用 IST 方法对含密拼接图像进行处理, 生成具有复杂纹理且视觉自然的含密纹理图像, 从而完成秘密信息的隐藏过程.

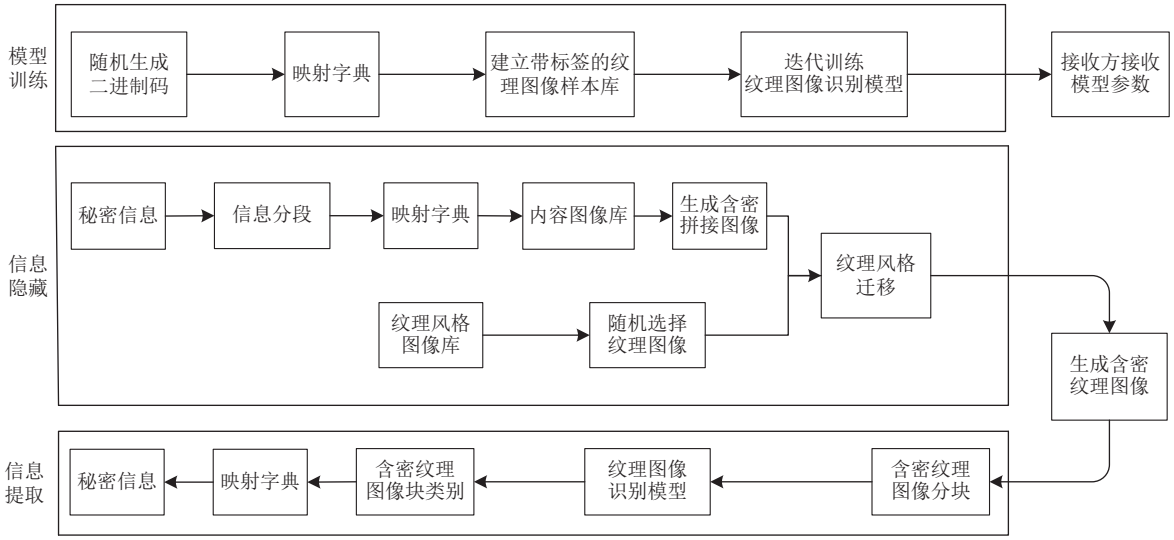


图 1 本文算法总体框架

为了能够从含密纹理图像中正确地提取秘密信息, 本文算法需要在发送方和接收方的隐蔽通信过程前训练得到纹理图像识别模型. 在训练纹理图像识别模型过程中, 首先需要构建带类别标签的纹理图像样本库; 然后将带类别标签的纹理图像样本库输入到待训练的纹理图像识别模型中, 通过多轮的迭代训练最后生成能够识别含密纹理图像类别的模型, 并将模型的相关参数发送给接收方. 本文算法的秘密信息提取过程, 即为纹理图像识别模型对含密纹理图像的识别过程. 当接收方接收到含密纹理图像后, 首先按照双方事先约定的分块大小对含密纹理图像进行分块操作; 然后将分块后的含密纹理图像块输入到训练好的纹理图像识别模型中, 从而得到每一个含密纹理图

像块对应的原始自然图像的类别, 最后根据映射字典即可获得从含密纹理图像中提取的秘密信息.

1.1 构建映射字典

本文所提出的构造式信息隐藏算法在进行秘密信息隐藏时, 需要根据秘密信息从内容图像库 Φ 中选取不同类别的自然图像生成含密的拼接图像, 因此需构建内容图像库 Φ 中图像类别与二进制码的映射关系字典. 设内容图像库 Φ 中有 λ 种不同类别的自然图像, 将 Φ 中自然图像的全部类别记为: $C=\{C_1, C_2, \ldots, C_\lambda\}$, 其中 C_i 表示 Φ 中自然图像的第 i 个类别. 因此内容图像库 Φ 中自然图像的每个类别 C_i 对应的二进制码的长度为: $K=\log_2\lambda$. 表 1 给出了一个映射关系字典的例子. 需要说明的是, 由于在信息隐藏和提取过程中都利用到该映射字典, 因此发送方和接收方需在隐蔽通信前共享该字典.

表 1 构建映射字典

类别C_i	二进制码 (K bits)
Bird	0 0 … 0
Bus	0 0 … 1
…	…
Plant	1 1 … 0
Airplane	1 1 … 1

1.2 纹理合成与识别

由图 1 所示的本文算法框架可以看到, 本文算法在进行秘密信息隐藏和秘密信息提取过程中需要进行纹理图像的构造以及含密纹理图像的识别, 下面将分别对本文算法中的基于风格迁移的纹理图像合成和纹理图像识别进行介绍.

1.2.1 基于风格迁移的纹理图像合成

卷积神经网络 (convolutional neural networks, CNN) 具有强大的图像特征提取能力, 浅层网络提取的卷积特征保留了原始图像中物体形状、位置、纹理、颜色等信息, 深层网络提取的卷积特征则仅保留原始图像中物体的大致形状和位置. 本文算法在秘密信息隐藏过程中, 利用基于 CNN 的 IST 技术来学习选定纹理图像的风格[19], 并把这种风格应用到含密拼接图像上, 从而生成纹理复杂且视觉效果良好的含密纹理图像.

基于风格迁移的纹理图像合成主要分为 3 个步骤: 图像内容表示、图像风格表示、IST. 设原始待合成的图像为 p, 需要学习的纹理风格图像为 a, 最终合成的纹理图像为 f. 在图像内容表示时, 为了原始图像 p 通过 IST 最终生成纹理图像 f, 首先需要让两张图像在图像内容上相互接近, 因此将原始图像 p 与生成的纹理图像 f 在内容上的差值定义为内容损失函数 L_c. 当内容损失函数 L_c 的值越趋近于 0 时, 代表原始图像 p 与生成的纹理图像 x 在图像内容上越相似, 反之二者在图像内容上越不相似. 具体地, 设 P^l、F^l 分别表示在卷积层的第 l 层提取原始图像 p 和期望生成的纹理图像 f 的卷积特征, 则原始图像 p 与期望生成的纹理图像 f 的内容损失函数 L_c 可表示为:

$$L_c(p,f,l)=\frac{1}{2}\sum_{ij}(P_{ij}^l-F_{ij}^l)^2 \tag{1}$$

其中, P_{ij}^l 表示原始图像 p 在卷积神经网络第 l 层中第 i 个卷积核的第 j 个位置的特征, F_{ij}^l 表示期望生成的纹理图像 f 在卷积神经网络第 l 层中第 i 个卷积核的第 j 个位置的特征.

在图像风格特征表示时, 可以利用卷积神经网络不同卷积核的之间的相互关系来表达, 且这种相互关系可基于 *Gram* 矩阵来表示:

$$\Lambda_{ij}^l=Gram(a)=\sum_k A_{ik}^l A_{jk}^l \tag{2}$$

$$\Gamma_{ij}^l=Gram(f)=\sum_k F_{ik}^l F_{jk}^l \tag{3}$$

其中, Λ_{ij}^l 和 Γ_{ij}^l 分别表示图像 a 和图像 f 各自在卷积神经网络第 l 层的特征图中第 i 个卷积核与第 j 个卷积核之间

的点积, 这样即可提取选定的纹理风格图像 a 以及期望生成的纹理图像 f 的风格特征. 为了使选定的纹理图像 a 的风格特征不断向期望生成的纹理图像 f 上进行迁移, 故将纹理风格图像 a 与期望生成的纹理图像 f 在卷积神经网络第 l 层的风格特征差值定义为风格损失函数 E_l:

$$E_l = \frac{1}{Q}\sum_{ij}(\Lambda_{ij}^l - \Gamma_{ij}^l)^2 \tag{4}$$

其中, Q 是归一化因子, 主要用于防止风格损失函数取值与内容损失函数取值相差过大. 同时, 通过提取不同卷积层的图像风格特征, 并计算图像在不同卷积层的风格损失函数 E_l 的加权平均值, 可得到选定的纹理图像 a 和期望生成的纹理图像 f 之间最终的风格损失函数 L_s:

$$L_s(a,f) = \sum_{l=0}^{N}\omega_l E_l \tag{5}$$

其中, ω_l 表示纹理风格图像 a 以及期望生成的纹理图像 f 在卷积神经网络第 l 层的风格损失函数 E_l 的权重系数, N 表示卷积神经网络的总层数.

当完成上述步骤后, 可得到原始图像 p 与期望生成的纹理图像 f 的内容损失函数 L_c 的值, 以及纹理风格图像 a 与期望生成的纹理图像 f 的风格损失函数 L_s 的值. 为了使得期望生成的纹理图像 f 既包含原始图像 p 的内容特征, 又包含纹理风格图像 a 的风格特征, 故最终的基于 IST 的纹理图像合成的损失函数 L_t 为:

$$L_t(p,a,f) = \alpha L_c(p,f) + \beta L_s(a,f) \tag{6}$$

其中, α, β 分别代表原始图像 p 的内容特征和纹理风格图像 a 的风格特征在期望生成的纹理图像 f 中所占的权重. 最终通过卷积神经网络的自我学习, 不断优化函数$\partial L_t/\partial x$, 从而生成最终的纹理图像 f.

1.2.2 含密纹理图像识别模型

本文算法中秘密信息隐藏的核心思想是发送方基于秘密信息生成含密纹理图像, 并将生成的含密纹理图像发送给接收方. 为了确保接收方能够从含密纹理图像中准确提取出秘密信息, 本文算法在发送方引入卷积神经网络对构建的带类别标签的纹理图像库进行训练和类别识别, 并在秘密通信前将训练得到的纹理图像识别模型相关参数共享给接收方. 纹理图像识别模型的训练过程如下: 首先根据随机生成的大量二进制信息片段和映射字典 (见第 1.1 节) 从内容图像库 Φ 中选择对应类别的自然图像 (该类别信息即为标签), 然后按照 Zig-Zag 的顺序将选择的自然图像拼接成一系列拼接图像, 并利用第 1.2.1 节中基于 IST 的纹理图像合成方法将拼接图像转换成视觉效果良好的纹理图像; 接下来对生成的纹理图像进行分块处理, 从而构建了含类别标签的纹理图像库, 最后将此纹理图像库作为纹理图像识别模型的训练集, 输入到纹理图像识别模型的卷积神经网络中, 通过迭代训练进而生成纹理图像识别模型, 具体的模型的训练流程如图 2 所示.

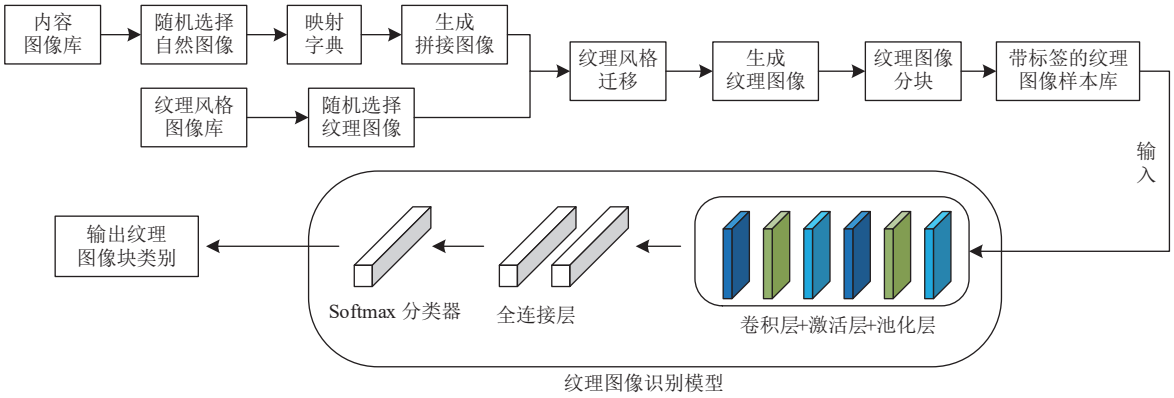


图 2 纹理图像识别模型训练流程图

该基于 CNN 的纹理图像识别模型可准确识别出含密纹理图像中各分块的类别, 模型的网络结构如图 2 中的虚线框所示. 模型一共分为 5 层: Layer 1 和 Layer 2 包括卷积层、激活层、以及池化层; Layer 3 和 Layer 4 是全连

接层; Layer 5 是输出层, 模型利用全连接层传送的图像卷积特征, 通过 Softmax 分类器, 完成图像识别任务, 获取图像对应的类别. 卷积层是本文设计的纹理图像识别模型中的重要部分, 通过对输入进行卷积运算, 分析并提取出图像的深度特征 $\Re$, 其数学表达式为:

$$\Re(W,b,x)=g(W\times x+b)=g\left(\sum_{v=1}^{V}\sum_{u=1}^{U}\sum_{m=1}^{M}w_{v,u,m}x_{i+v,j+u,m}+b\right) \tag{7}$$

其中, $\Re$ 表示经过卷积运算操作后输出的特征矩阵, W 为权重参数, b 为偏置项参数, x 为输入的图像特征矩阵, $g(\cdot)$ 为激活函数, U 和 V 为卷积核的尺寸大小, M 为输入特征的通道数, $w_{v,u,m}$ 表示第 m 个输入通道上第 v 行、第 u 列的卷积核的权重参数, $x_{i+v,j+u,m}$ 表示输入的特征矩阵上第 m 个通道上的第 $i+v$ 行、第 $j+u$ 列的元素. CNN 中常用的激活函数包括 ReLU、Sigmoid 及 tanh, 本文训练的纹理图像识别模型采用的激活函数为 ReLU, 如公式 (8) 所示:

$$g(x)=\begin{cases}0, & x<0\\ x, & x\geqslant 0\end{cases} \tag{8}$$

纹理图像识别模型中池化层的主要作用是对卷积层提取的深度特征进行降维处理, 减少神经网络的计算量. 池化层通过降低特征图的分辨率来获得具有空间不变性的特征[20]. 神经网络中的池化层常用的方法有最大池化、均值池化等. 本文设计的纹理图像识别模型中采用的是最大池化, 即计算池化窗口区域的最大值. 另外, 本文选择交叉熵函数作为纹理图像识别模型的损失函数, 如公式 (9) 所示:

$$H_{y'}(y)=-\sum_{i}^{T}y_i'\log(y_i) \tag{9}$$

其中, T 表示训练集中包含的图像类别数, y_i 表示纹理图像识别模型识别出当前纹理图像对应的类别, y_i'表示当前待识别纹理图像对应的真实类别, y 表示纹理图像识别模型识别得到的类别概率分布, y'表示训练集中纹理图像对应的真实类别, $H_{y'}(y)$ 可表示纹理图像识别模型的识别结果和真实结果之间的差别. 当 $H_{y'}(y)$ 值越小时, 表明模型的识别正确率越高, 反之越低. 本文设计的纹理图像识别模型在训练过程中的损失函数值 $H_{y'}(y)$ 随迭代次数的变化关系如图 3 所示. 通过对图 3 观察可知, 该模型的损失值 $H_{y'}(y)$ 随着迭代次数的增加, 逐渐趋近于 0, 因此本文设计的纹理图像识别模型可准确识别出含密纹理图像对应的类别.

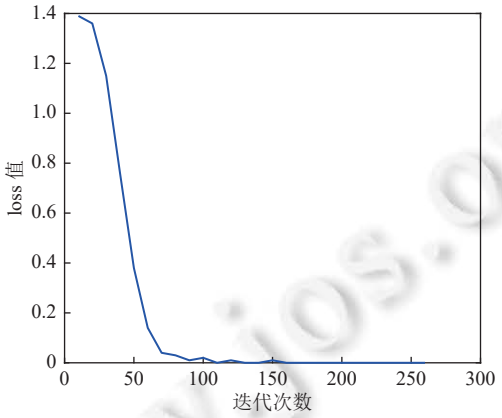


图 3 纹理图像识别模型的损失值变化趋势

1.3 信息隐藏

本文算法信息隐藏过程的主要步骤是首先根据秘密信息片段选取对应的一系列自然图像, 并将选取的自然图像按照 Zig-Zag 顺序组合成一幅拼接图像, 再通过基于 IST 的纹理合成方法获得风格迁移后的含密纹理图像, 流程如图 4 所示, 具体步骤如下.

步骤 1. 发送方首先将待隐藏的二进制秘密信息 S 以长度 K 为单位进行分段, 获得 n 个秘密信息片段 (为简单

起见, 假设 S 的长度为 K 的整数倍), 记为 $S=\{S_1, S_2, \ldots, S_n\}$, 其中 K 为内容图像库 Φ 中自然图像类别映射的二进制码长度 (见表 1).

步骤 2. 对每个长度为 K 的二进制信息片段 S_i, 通过映射字典查找对应的类别, 即可从内容图像库 Φ 中找到相应的自然图像; 通过将 Φ 中与各秘密信息段 S_i 对应选择的自然图像按照 Zig-Zag 顺序进行组合, 获得一幅含密拼接图像.

步骤 3. 在得到含密拼接图像后, 从纹理风格图像库 Ψ 中随机选择一幅纹理图像, 利用第 1.2.1 节中给出的基于风格迁移的纹理图像合成方法, 让含密拼接图像学习被选择的纹理图像的风格特征, 生成视觉效果良好的纹理图像, 最后将生成的含密纹理图像发送给接收方, 从而完成秘密信息的隐藏过程.

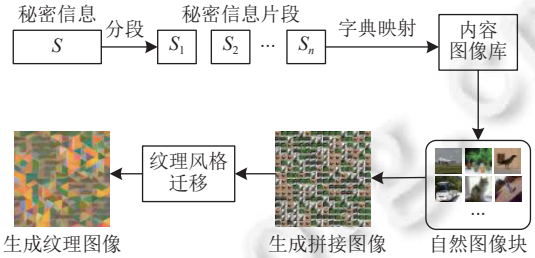


图 4 秘密信息的隐藏过程

1.4 信息提取

在进行秘密信息提取时, 接收方首先需要对接收到的含密纹理图像进行分块处理, 之后利用纹理图像识别模型识别出每个含密纹理图像块的类别. 因此接收方需要与发送方共享内容图像库 Φ 中自然图像的尺寸、内容图像库 Φ 中自然图像的类别 C 与二进制码的映射字典、训练完成的纹理图像识别模型的参数值. 信息提取过程如图 5 所示, 具体步骤如下.

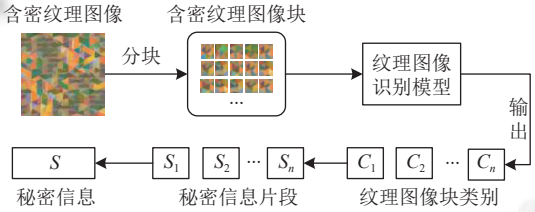


图 5 秘密信息的提取过程

步骤 1. 接收方收到含密纹理图像后, 首先根据内容图像库 Φ 中自然图像的尺寸对含密纹理图像进行分块处理, 得到 n 个含密纹理图像块.

步骤 2. 将 n 个含密纹理图像块按照 Zig-Zag 顺序依次输入到本文第 1.2.2 节给出的纹理图像识别模型中, 可获得 n 个含密纹理图像块对应的图像类别信息.

步骤 3. 根据获得的 n 个含密纹理图像块的类别信息, 通过查找双方共享的映射字典 (表 1) 即可获得对应的 n 个二进制秘密信息片段 $S_1, S_2, \ldots, S_n$.

步骤 4. 将 n 个二进制秘密信息片段 $S_1, S_2, \ldots, S_n$ 按顺序进行级联, 即可获得完整的秘密信息 S, 从而完成秘密信息的提取过程.

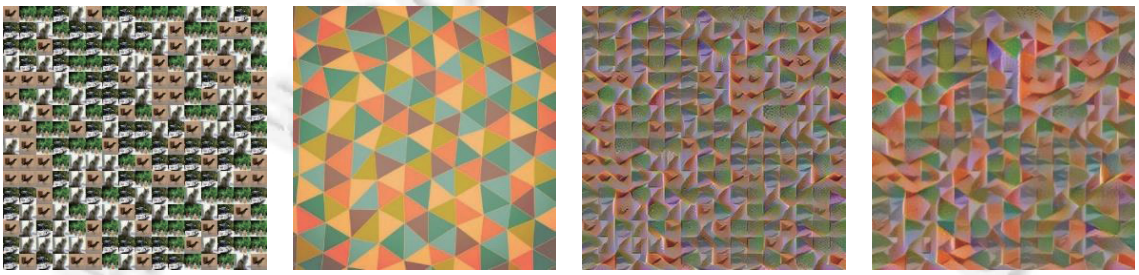
2 实验结果与比较

本文实验是在 Windows 10 操作系统、Python 3.6 编程语言以及深度学习框架 TensorFlow-GPU v1.10 环境下完成的. 实验中, 首先建立内容图像库 Φ 和纹理风格图像库 Ψ, 其中内容图像库 Φ 中包含 16 种不同类别的自然图像 (即 λ=16), 这样每个类别映射的二进制码的长度 K=4 bit, 另外图像的尺寸均为 32×32; 纹理风格图像库 Ψ 中包

含 8 种不同风格的纹理图像. 如果想要获取更大的隐藏容量和更多样的视觉效果, 可通过分别增加 Φ 和 Ψ 中的自然图像的类别数和纹理风格图像的类别数来实现. 经过大量实验后发现, 当内容损失权重 α 为风格损失权重 β 的 1/10 时, 生成的含密纹理图像可以较好地兼顾内容图像和风格图像的特征, 因此我们将公式 (5) 中的 IST 的内容损失权重 α 设为 50、风格损失权重 β 设为 500. 实验中为了训练纹理图像识别模型, 随机生成了 64 000 bit 的二进制数据, 再利用第 1.2 节中的合成方法生成了 16 000 张带类别标签的纹理图像块, 其中 11 200 张作为训练集, 另外 4 800 张作为测试集.

2.1 实验结果

为了验证本文算法的有效性, 在实验中随机生成了 1 024 bit 的二进制数据作为待隐藏的秘密信息, 并将其等分成 256 段, 即每段为 4 bit 二进制数据. 根据表 1 中的映射关系, 从内容图像库 Φ 中选择对应类别的自然图像. 将每段秘密信息对应选择的自然图像按 Zig-Zag 顺序排列获得含密拼接图像. 从纹理风格图像库 Ψ 中选择一张纹理图像, 调用基于 IST 纹理图像合成模型, 对含密拼接图像迭代处理后生成一张具有良好视觉效果的含密纹理图像, 完成秘密信息隐藏过程. 图 6 是用本文算法进行 1 024 bit 信息隐藏的实验结果. 图 6(a) 是根据 256 段 4 bit 秘密信息映射并排列组成的含密拼接图像, 尺寸为 512 × 512; 图 6(b) 是从纹理风格图像库 Ψ 中选取的纹理图像; 图 6(c)–图 6(h) 是对图 6(a) 按照图 6(b) 的纹理风格, 利用基于 IST 的纹理图像合成模型迭代训练 100–2000 轮后生成的含密纹理图像. 通过观察不同迭代训练次数生成的含密纹理图像可以发现, 当迭代训练次数小于 1 000 轮时, 生成的含密纹理图像和原始的纹理风格图像 (即图 6(b)) 视觉上相差较大; 当训练迭代次数大于 1 500 轮时, 生成的含密纹理图像具有较好的视觉效果. 因此为了获取理想的视觉效果, 实验中我们将最终迭代训练次数统一设置为 2 000 轮.



(a) 含密拼接图像 (b) 选择的纹理风格图像 (c) 含密纹理图像 (100 轮) (d) 含密纹理图像 (300 轮)

(e) 含密纹理图像 (500 轮) (f) 含密纹理图像 (1 000 轮) (g) 含密纹理图像 (1 500 轮) (h) 含密纹理图像 (2 000 轮)

图 6 含密纹理图像生成结果图示例 1

通过选取不同的纹理风格图像, 会生成不同视觉效果的含密纹理图像, 图 7 为选取另一张不同类型的纹理风格图像后生成含密纹理图像结果. 通过观察实验结果可以发现, 本文算法生成的含密纹理图像 (即图 6(h) 和图 7(h)) 分别与选择的纹理图像 (即图 6(b) 和图 7(b)) 的风格保持一致, 视觉效果较好; 同时也无法从图 6(h) 和图 7(h) 中看出图 6(a) 和图 7(a) 的图像内容, 故具有良好的安全性.

在进行秘密信息传输前, 接收方已获得了纹理图像识别模型的参数, 同时与发送方约定了内容图像库 Φ 中自然图像的尺寸 (即 32×32). 因此在接收方收到 512×512 的含密纹理图像后, 将含密纹理图像分割成 256 个含密纹

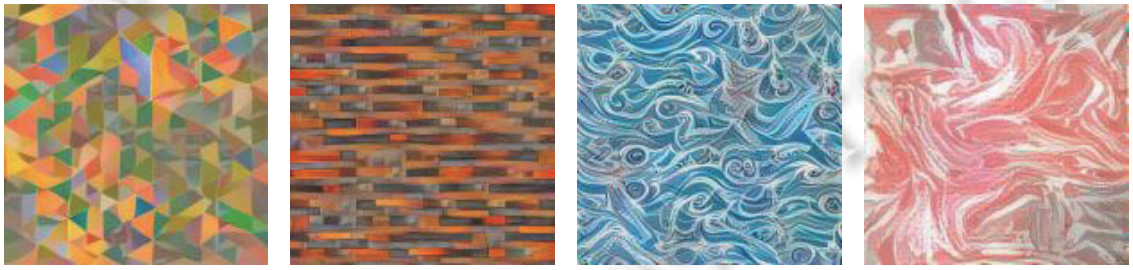
理图像块; 再通过调用纹理图像识别模型, 分别识别出这 256 个含密纹理图像块的类别, 根据映射字典获得 256 段秘密信息片段 S_i; 最后将这 256 段信息片段 S_i 级联得到完整的秘密信息 S. 由于本文实验中内容图像库 Φ 的每个类别的自然图像只有一张, 因此相同类别的自然图像对应的含密纹理图像块都极其相似, 而不同类别的自然图像生成的含密纹理图像块在视觉上差别较大, 从而使得纹理识别模型可正确识别出含密的纹理图像块的类别. 通过大量实验验证, 在含密纹理图像没有受到攻击的情况下, 本文算法秘密信息提取误码率为 0.

(a) 含密拼接图像 (b) 选择的纹理风格图像 (c) 含密纹理图像 (100 轮) (d) 含密纹理图像 (300 轮)

(e) 含密纹理图像 (500 轮) (f) 含密纹理图像 (1 000 轮) (g) 含密纹理图像 (1 500 轮) (h) 含密纹理图像 (2 000 轮)

图 7 含密纹理图像生成结果图示例 2

本文算法和文献 [18] 都是通过生成含密纹理图像来进行秘密信息隐藏的. 故为了进一步验证本文算法的性能, 我们在嵌入容量均为 1 024 bit 的条件下, 将本文算法与文献 [18] 生成的含密纹理图像进行比较, 见图 8.



(a) 本文算法生成的含密纹理图像

(b) 文献 [18] 生成的含密纹理图像

图 8 本文算法与文献 [18] 生成的含密纹理图像比较

图 8(a) 为本文算法利用不同风格的纹理图像生成的含密纹理图像, 图 8(b) 为文献 [18] 利用不同形变函数生成的含密纹理图像. 通过结果可以发现, 相比于文献 [18], 本文算法生成的含密纹理图像风格更加多元且视觉效果更加自然.

2.2 隐藏容量分析

由于本文算法是通过对内容图像库 Φ 中不同类别的自然图像组合生成含密拼接图像, 并利用纹理风格学习最终生成含密纹理图像, 因此本文算法的隐藏容量与内容图像库 Φ 中自然图像的类别数和尺寸、最终含密纹理图像的尺寸有关. 实际应用中可通过调节这些参数, 从而实现隐藏任意长度的秘密信息. 故本文算法的隐藏容量 η 可表示为:

$$\eta = \left(\frac{X_w \times X_h}{P_w \times P_h}\right)\log_2 \lambda \tag{10}$$

其中, λ 为内容图像库 Φ 中自然图像的类别数, P_w 和 P_h 分别是 Φ 中自然图像的宽和高, X_w 和 X_h 分别是最终生成的含密纹理图像的宽和高. 由公式 (10) 可知, 本文算法的隐藏容量 η 与内容图像库 Φ 中自然图像的类别数 λ、生成含密纹理图像的尺寸 $X_w \times X_h$ 成正比, 与 Φ 中自然图像尺寸 $P_w \times P_h$ 成反比.

为了分析本文算法的隐藏容量, 我们首先将本文算法与几种典型的同样基于载体构造的信息隐藏算法[16−18]进行比较, 实验结果如表 2 所示. 由于本文算法和文献 [16−18] 的隐藏容量都与生成的含密纹理图像的尺寸成正比, 故我们在进行比较时将生成的含密纹理图像尺寸统一设置为 800×800; 本文和文献 [16] 的隐藏方法都与内容图像库 Φ 中自然图像的尺寸成反比, 故我们将 Φ 中图像的尺寸统一设置为 32×32. 由表 2 可知, 本文算法在内容图像库中自然图像的类别数 λ=16 时的隐藏容量 H 为 2 500 bit, 大于文献 [16] 和文献 [18] 的隐藏容量. 文献 [17] 在稀疏比例为 0.03–1 时, 生成的含密纹理图像可以隐藏 800–3 750 bit 的秘密信息, 虽然其隐藏容量稍大于本文算法, 随着 Φ 中图像类别数 λ 的增加, 本文算法的隐藏容量可进一步提高.

另外, 我们还将本文算法与基于载体选择的信息隐藏算法[12−14,21]进行比较. 由于文献 [12,13,21] 是通过提取载体图像特征构建哈希来完成信息隐藏过程的, 其隐藏容量主要与构建的哈希函数的哈希值长度有关; 文献 [14] 基于含密载体图像中包含的不同类别的对象来完成信息隐藏过程, 因此其隐藏容量与对象库中的对象类别数以及含密载体图像中包含的对象数有关; 本文算法的隐藏容量与内容图像库中的图像类别数及生成含密纹理图像的尺寸相关. 因此为了公平起见, 在比较中我们将文献 [14] 对象库中的对象类别数、本文算法内容图像库中的图像类别数均设置为 λ, 且将文献 [14] 的含密载体图像中包含的对象数记为 γ. 不同算法的单张图像隐藏容量如表 3 所示, 由结果可以看出, 本文算法的隐藏容量远大于文献 [12,13,21]; 另外由于图像中包含的对象数 γ 一般相对有限, 而本文算法的含密载体图像与原始图像尺寸的比值 ($X_w X_h / P_w P_h$) 可以很大, 因此本文算法的隐藏容量性能也优于文献 [14].

表 2 与基于载体构造算法[16-18]的隐藏容量比较

方法	单张图像隐藏容量 (bit)
文献[16]	432
文献[17]	800–3750 (稀疏比: 0.03–1)
文献[18]	832
本文算法 (λ=4)	1 250
本文算法 (λ=16)	2 500

表 3 与基于载体选择算法[12-14, 21]的隐藏容量比较

方法	单张图像隐藏容量 (bit)
文献[12]	8
文献[13]	8
文献[14]	$\gamma \cdot \log_2 \lambda$
文献[21]	18
本文算法	$\log_2 \lambda \cdot X_w X_h / (P_w P_h)$

2.3 鲁棒性分析

在本文算法中, 发送方将生成的含密纹理图像通过公共信道传输给接收方的过程中, 可能会受到攻击, 从而对信息提取造成影响, 因此鲁棒性是衡量算法性能的一个重要指标. 为验证算法的鲁棒性, 我们在实验中采取了一系列图像攻击方式, 如表 4 所示. 通过采用表 4 中的不同参数下的处理对含密纹理图像进行攻击, 然后提取秘密信息

并计算信息提取的正确率 C_r:

$$C_r = (M_c/M_S)\times 100\% \tag{11}$$

其中, M_c 为提取正确的秘密信息长度, 即提取的秘密信息与原始秘密信息 S 对应位相同的比特数, $M_S=n\times K$ 为秘密信息的总长度. 也有一些无载体信息隐藏算法采用误码率 (bit error rate, BER) 衡量算法的鲁棒性, 即 BER=1−C_r.

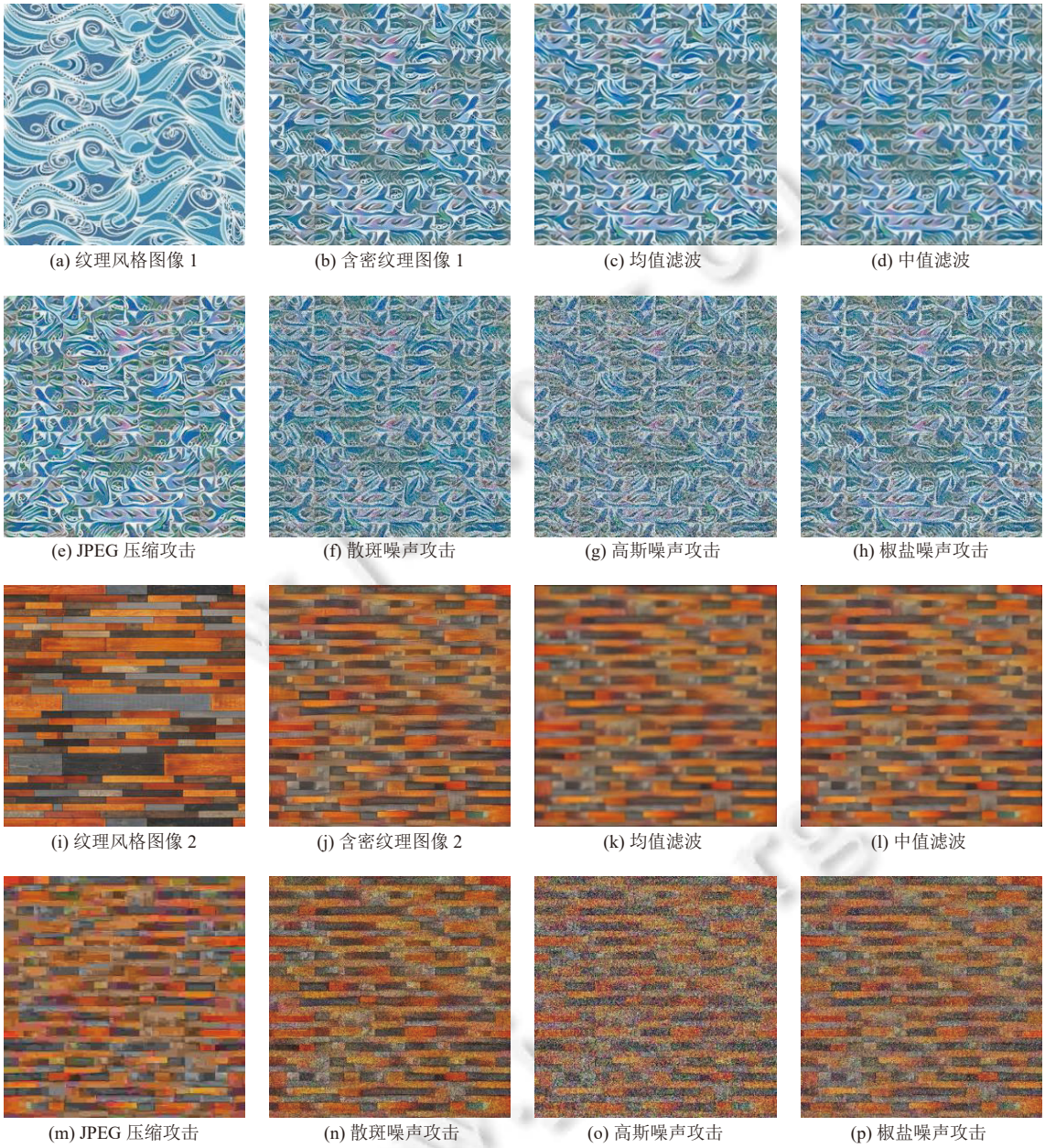
表 4 信息提取正确率实验结果与比较

攻击	参数名称	参数值	本文方法含密纹理图像1 (%)	本文方法含密纹理图像2 (%)	文献[21] (%)
中值滤波	模板大小	3×3	100	100	99.31
		5×5	100	100	95.84
		7×7	100	100	94.11
均值滤波	模板大小	3×3	100	100	96.53
		5×5	100	100	94.80
		7×7	100	100	94.63
JPEG压缩	质量因子	10	100	100	89.77
		30	100	100	96.80
		50	100	100	97.92
		70	100	100	98.27
		90	100	100	99.48
散斑噪声	噪声方差	0.01	100	100	90.00
		0.05	100	100	88.30
		0.1	100	100	83.80
高斯噪声	噪声方差	0.001	100	100	93.41
		0.005	100	100	89.25
		0.01	99.43	99.78	86.32
		0.1	71.84	71.78	83.19
椒盐噪声	噪声方差	0.001	100	100	99.31
		0.005	100	99.73	97.75
		0.01	100	99.73	94.69
		0.1	99.87	99.73	90.99

图 9 为含密纹理图像受到攻击后的结果, 其中图 9(a) 和图 9(i) 为两张纹理风格图像, 图 9(b) 和图 9(j) 分别为对应的含密纹理图像 (隐藏容量为 1 024 bit), 图 9(c)–图 9(h) 和图 9(k)–图 9(p) 分别为图 9(b) 和图 9(j) 受到中值滤波 (模板大小为 7×7)、均值滤波 (模板大小为 7×7)、JPEG 压缩 (质量因子为 50)、散斑噪声 (均值为 0, 方差为 0.01)、高斯噪声 (均值为 0, 方差为 0.01)、椒盐噪声 (均值为 0, 方差为 0.01) 攻击后的结果. 对攻击后的含密纹理图像提取信息并利用公式 (11) 计算正确率, 结果如表 4 所示. 本文算法生成的不同风格的含密纹理图像, 对中值滤波、均值滤波、JPEG 压缩、散斑噪声、椒盐噪声攻击具有良好的鲁棒性, 信息提取正确率均在 99.5% 以上; 对高斯噪声攻击的鲁棒性稍差, 信息提取的正确率随着高斯噪声的方差的增加而下降. 当高斯噪声方差小于 0.005 时, 信息提取正确率为 100%; 当高斯噪声方差大于 0.005 且小于 0.01 时, 信息提取正确率大于 99%; 当高斯噪声方差大于 0.01 且小于 0.1 时, 通过计算可知, 受到攻击后含密图像的 PSNR 值骤降, 即图像内容信息被破坏严重, 由于本文算法不能完全抵抗含密图像内容损失严重的攻击, 因此提取秘密信息的正确率受到影响, 但仍高于 70%. 总而言之, 本文算法生成的不同风格的含密纹理图像在抵抗高斯噪声、椒盐噪声、均值滤波等攻击时, 均具有良好的鲁棒性.

为了进一步验证本文算法的鲁棒性, 我们还与文献 [21] 进行了比较, 如表 4 所示. 文献 [21] 首先通过 LDA 算法将原始图像库进行了分类处理, 再构造鲁棒哈希函数的映射关系从而完成秘密信息的隐藏. 由表 4 可以看出, 对于中值滤波、均值滤波、JPEG 压缩、散斑噪声攻击, 文献 [21] 的信息提取正确率随攻击的强度变化而变化, 而本文算法的信息提取正确率保持在 100%. 当高斯噪声方差小于 0.01 时, 本文算法的信息提取正确率明显高于文献 [21]; 当高斯噪声方差大于 0.01 时, 本文算法和文献 [21] 的信息提取正确率均随噪声方差变大而下降; 当高斯

噪声攻击方差为 0.1 时, 本文算法的信息提取正确率低于文献 [21]. 在含密图像受到椒盐噪声攻击时, 本文算法即使在噪声方差较大的情况下, 信息提取的正确率仍高于文献 [21]. 通过上述分析可知, 本文算法的鲁棒性总体优于文献 [21].



(a) 纹理风格图像 1 (b) 含密纹理图像 1 (c) 均值滤波 (d) 中值滤波

(e) JPEG 压缩攻击 (f) 散斑噪声攻击 (g) 高斯噪声攻击 (h) 椒盐噪声攻击

(i) 纹理风格图像 2 (j) 含密纹理图像 2 (k) 均值滤波 (l) 中值滤波

(m) JPEG 压缩攻击 (n) 散斑噪声攻击 (o) 高斯噪声攻击 (p) 椒盐噪声攻击

图 9 针对含密纹理图像的攻击结果图

2.4 安全性分析

本文提出的构造式信息隐藏算法在进行秘密信息隐藏时, 首先将秘密信息通过映射字典映射成一张由若干自然图像组成的拼接图像, 并通过风格迁移模型将其生成为一张视觉效果良好的纹理图像, 相比于传统的基于载体修改的信息隐藏算法, 本文算法能够更加隐蔽地进行秘密信息的通信. 另一方面, 在发送方隐藏秘密信息时, 首先

需要将内容图像库 Φ 中自然图像的全部类别 C 映射成对应的二进制码, 接收方在提取秘密信息时同样需要通过该映射字典获得秘密信息. 举例说明, 如内容图像库 Φ 中有 16 种不同类别的自然图像, 因此自然图像种类与二进制码的映射关系存在 16! ($\approx 2\times10^{13}$) 种排列的可能性, 故攻击者很难在不知道映射关系的前提下进行暴力破解. 此外, 接收方提取秘密信息时需通过调用纹理图像识别模型来识别各含密纹理图像块的类别, 而该模型的相关参数是发送方完成模型训练后并在双方秘密信息通信前, 利用密钥共享协议或安全信道传输给接收方, 故攻击者在不知道纹理图像识别模型参数的情况下也无法正确提取信息. 因此, 从含密纹理图像的视觉效果和秘密信息隐藏/提取的过程两个方面来分析, 本文算法均具有较高的安全性.

3 结 论

本文提出了一种新的构造式无载体信息隐藏算法, 与当前已有的无载体信息隐藏算法不同, 本文算法通过 IST 模型学习生成含密纹理图像来实现秘密信息的隐藏, 并基于纹理图像识别模型来实现秘密信息的提取. 算法首先将二进制数据片段与自然图像块类别建立映射关系, 从内容图像库中选择一系列与待隐藏的秘密信息片段对应类别的自然图像块来生成含密拼接图像, 再通过对选定的纹理图像进行风格迁移学习, 将含密拼接图像转换成一张视觉效果良好的含密纹理图像, 接收方可通过训练好的纹理识别模型准确识别含密纹理图像分块的类别从而提取秘密信息. 大量实验结果表明, 与已报道的代表性算法相比, 本文提出的算法具有较大的隐藏容量和良好的鲁棒性, 在一定程度上解决了无载体信息隐藏算法隐藏容量与鲁棒性无法很好兼顾的问题.

References:

[1] Shen CX, Zhang HG, Feng DG, Cao ZF, Huang JW. A survey of information security. Science China, 2007, 37(2): 129–150 (in Chinese with English abstract). [doi: 10.3969/j.issn.1674-7259.2007.02.001]

[2] Khosravi B, Khosravi B, Khosravi B, Nazarkardeh K. A new method for pdf steganography in justified texts. Journal of Information Security and Applications, 2019, 45: 61–70. [doi: 10.1016/j.jisa.2019.01.003]

[3] Yang YY, Li ZH, Xie WC, Zhang ZZ. High capacity and multilevel information hiding algorithm based on pu partition modes for HEVC videos. Multimedia Tools and Applications, 2019, 78(7): 8423–8446. [doi: 10.1007/s11042-018-6859-7]

[4] Soliman NF, Khalil MI, Algarni AD, Ismail S, Marzouk R, El-Shafai W. Efficient HEVC steganography approach based on audio compression and encryption in QFFT domain for secure multimedia communication. Multimedia Tools and Applications, 2021, 80(3): 4789–4823. [doi: 10.1007/s11042-020-09881-8]

[5] Chen JF, Fu ZJ, Zhang WM, Cheng X, Sun XM. Review of image steganalysis based on deep learning. Ruan Jian Xue Bao/Journal of Software, 2021, 32(2): 551–578 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6135.htm [doi: 10.13328/j.cnki.jos.006135]

[6] Yang CH, Weng CY, Wang SJ, Sun HM. Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Trans. on Information Forensics and Security, 2008, 3(3): 488–497. [doi: 10.1109/TIFS.2008.926097]

[7] Song XF, Liu FL, Zhang ZG, Yang CF, Luo XY, Chen LJ. 2D Gabor filters-based steganalysis of content-adaptive JPEG steganography. Multimedia Tools and Applications, 2017, 76(24): 26391–26419. [doi: 10.1007/s11042-016-4157-9]

[8] Chen WY. Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques. Applied Mathematics and Computation, 2008, 196(1): 40–54. [doi: 10.1016/j.amc.2007.05.063]

[9] Thanki R, Borra S. A color image steganography in hybrid FRT-DWT domain. Journal of Information Security and Applications, 2018, 40: 92–102. [doi: 10.1016/j.jisa.2018.03.004]

[10] Huang FJ, Huang JW, Shi YQ. New channel selection rule for JPEG steganography. IEEE Trans. on Information Forensics and Security, 2012, 7(4): 1181–1191. [doi: 10.1109/TIFS.2012.2198213]

[11] Zhou ZL, Sun HY, Harit R, Chen XY, Sun XM. Coverless image steganography without embedding. In: Proc. of the 1st Int'l Conf. on Cloud Computing and Security. Nanjing: Springer, 2015. 123–132. [doi: 10.1007/978-3-319-27051-7_11]

[12] Zhou ZL, Cao Y, Sun XM. Coverless information hiding based on bag-of-words model of image. Journal of Applied Sciences, 2016, 34(5): 527–536 (in Chinese with English abstract). [doi: 10.3969/j.issn.0255-8297.2016.05.005]

[13] Yuan CS, Xia ZH, Sun XM. Coverless image steganography based on SIFT and BOF. Journal of Internet Technology, 2017, 18(2): 435–442. [doi: 10.6138/JIT.2017.18.2.20160624c]

[14] Zhou ZL, Cao Y, Wang MM, Fan EM, Wu QMJ. Faster-RCNN based robust coverless information hiding system in cloud environment. IEEE Access, 2019, 7: 179891–179897. [doi: 10.1109/ACCESS.2019.2955990]

[15] Otori H, Kuriyama S. Texture synthesis for mobile data communications. IEEE Computer Graphics and Applications, 2009, 29(6): 74–81. [doi: 10.1109/MCG.2009.127]

[16] Xu JY, Mao XY, Jin XG, Jaffer A, Lu SF, Li L, Toyoura M. Hidden message in a deformation-based texture. The Visual Computer, 2015, 31(12): 1653–1669. [doi: 10.1007/s00371-014-1045-z]

[17] Pan L, Qian ZX, Zhang XP. Steganography by constructing texture images. Journal of Applied Sciences, 2016, 34(5): 625–632 (in Chinese with English abstract). [doi: 10.3969/j.issn.0255-8297.2016.05.015]

[18] Si GW, Qin C, Yao H, Han YF, Zhang ZC. Robust coverless data hiding based on texture classification and synthesis. Journal of Applied Sciences, 2020, 38(3): 441–454 (in Chinese with English abstract). [doi: 10.3969/j.issn.0255-8297.2020.03.010]

[19] Gatys LA, Ecker AS, Bethge M. Image style transfer using convolutional neural networks. In: Proc. of the 2016 IEEE Conf. on Computer Vision and Pattern Recognition. Las Vegas: IEEE, 2016. 2414–2423. [doi: 10.1109/CVPR.2016.265]

[20] Gu JX, Wang ZH, Kuen J, Ma LY, Shahroudy A, Shuai B, Liu T, Wang XX, Wang G, Cai JF, Chen T. Recent advances in convolutional neural networks. Pattern Recognition, 2018, 77: 354–377. [doi: 10.1016/j.patcog.2017.10.013]

[21] Zhang X, Peng F, Long M. Robust coverless image steganography based on DCT and LDA topic classification. IEEE Trans. on Multimedia, 2018, 20(12): 3223–3238. [doi: 10.1109/TMM.2018.2838334]

附中文参考文献:

[1] 沈昌祥, 张焕国, 冯登国, 曹珍富, 黄继武. 信息安全综述. 中国科学 E辑:信息科学, 2007, 37(2): 129–150. [doi: 10.3969/j.issn.1674-7259.2007.02.001]

[5] 陈君夫, 付章杰, 张卫明, 程旭, 孙星明. 基于深度学习的图像隐写分析综述. 软件学报, 2021, 32(2): 551–578. http://www.jos.org.cn/1000-9825/6135.htm [doi: 10.13328/j.cnki.jos.006135]

[12] 周志立, 曹燚, 孙星明. 基于图像Bag-of-Words模型的无载体信息隐藏. 应用科学学报, 2016, 34(5): 527–536. [doi: 10.3969/j.issn.0255-8297.2016.05.005]

[17] 潘琳, 钱振兴, 张新鹏. 基于构造纹理图像的数字隐写. 应用科学学报, 2016, 34(5): 625–632. [doi: 10.3969/j.issn.0255-8297.2016.05.015]

[18] 司广文, 秦川, 姚恒, 韩彦芳, 张志超. 基于纹理特征分类与合成的鲁棒无载体信息隐藏. 应用科学学报, 2020, 38(3): 441–454. [doi: 10.3969/j.issn.0255-8297.2020.03.010]

秦川(1980－), 男, 博士, 教授, 博士生导师, CCF 高级会员, 主要研究领域为多媒体信息安全, AI 安全, 数字图像处理.

姚恒(1982－), 男, 博士, 副教授, CCF 专业会员, 主要研究领域为数字图像取证, 多媒体信息隐藏, 模式识别.

董腾林(1994－), 男, 硕士, 主要研究领域为多媒体信息隐藏.