文章编号:1007－6735(2024)03－0251－08　　DOI: 10.13255/j.cnki.jusst.20230827001

规避预处理的隐写载体选择

曹嘉明，　王子驰，　张新鹏
（上海大学 通信与信息工程学院，上海 200444）

摘要：在隐写术流程中，载体的选择在很大程度上影响着隐写系统的安全性。实验表明，经过预处理后的图像在用于隐写嵌入后会导致隐写安全性大幅降低。当给出较多备选图像时，可以选取多张图像用于进行隐写来提升隐写系统安全性。利用深度神经网络模型筛选出备选图像中已被预处理过的图像，根据深度神经网络输出赋予备选图像预处理失真，并结合传统的嵌入失真算法选择出最适合隐写的多幅图像进行隐写。与其他多载体隐写载体选择方案相比，所提出的载体选择方案在备选图像中含有预处理图像的情形下有着较好的表现，能够显著提升隐写系统安全性。

关键词：图像隐写；载体选择；深度神经网络；融合失真
中图分类号：TP 309　　**文献标志码：**A

Steganographic cover selection by circumvent preprocessing

CAO Jiaming,　WANG Zichi,　ZHANG Xinpeng
(*School of Communication & Information Engineering, Shanghai University, Shanghai 200444, China*)

Abstract: In the process of steganography, the choice of carrier greatly affects the security of steganography system. Experiments showed that the security of steganography would be greatly reduced when the preprocessed images were used for steganographic embedding. When a large number of alternative images were given, multiple images could be selected for steganography to improve the security of the steganography system. In this paper, the deep neural network model was used to screen out the images that had been preprocessed in the alternative images, and the alternative images were preprocessed according to the output of the deep neural network, and the most suitable images for steganography were selected by combining the traditional embedding distortion algorithm. Compared with other multi-vector steganographic carrier selection schemes, the proposed carrier selection scheme

收稿日期: 2023−08−27
基金项目: 国家自然科学基金资助项目(62376148, 62002214, U22B2047)；上海市教育发展基金会和上海市教育委员会“晨光计划”资助项目(22CGA46)
第一作者: 曹嘉明(2001−)，男，硕士研究生．研究方向：信息隐藏．E-mail：cjm_tongxin1122@shu.edu.cn
通信作者: 张新鹏(1975−)，男，教授．研究方向：人工智能安全．E-mail：xzhang@shu.edu.cn

引文格式: 曹嘉明，王子驰，张新鹏．规避预处理的隐写载体选择[J]．上海理工大学学报，2024，46(3)：251-258．DOI：10.13255/j.cnki.jusst.20230827001
Citation: CAO Jiaming, WANG Zichi, ZHANG Xinpeng. Steganographic cover selection by circumvent preprocessing[J]. Journal of University of Shanghai for Science and Technology, 2024, 46(3)：251-258.

had better performance in the case of preprocessed images in the alternative images, and could significantly improve the security of steganographic systems.

Keywords: *image steganography*; *cover selection*; *deep neural network*; *distortion fusion*

隐写术作为一种隐蔽通信手段，旨在将信息嵌入日常传播载体，如图像，而不影响载体的语义内容[1]。其核心目标在于将隐秘信息融入社交网络中进行传递。传统图像隐写方法通过微调图像像素值来实现，早期隐写技术中代价函数与像素位置无关。最低有效位编码(LSB)[2]和最低有效位匹配隐写方法(LSBM)[3]是比较经典的隐写技术。为保持像素分布的一致性，后续涌现了F5[4]，nsF5[5]，MB[6]，HPDM[7]等隐写技术。随着隐写术的发展，研究者发现不同嵌入位置导致的嵌入失真不同，因此，基于像素位置的代价函数计算成为新的研究方向。湿纸编码[8]、S-UNIWARD隐写方法[9]、HILL方法[10]等应运而生，这些方法都是定义新的代价函数，并且在隐写过程中尽量减小代价函数[11]。随着神经网络的不断发展，利用网络进行隐写的方法近年来也不断被提出。2019年，Yang等[12]提出的JS-GAN方法将对抗网络思想应用于JPEG图像；2020年，Tang等[13]提出的强化学习SPAR-RL方法弥补了生成式对抗网络中无法完美拟合真实情况下像素离散修改的缺陷，在安全性方面也有所提升；2021年, Tang等[14]提出的JEC-RL方法将强化学习应用于JPEG图像。

隐写分析旨在检测图像是否经过隐写处理[15]。现代隐写分析借助有监督机器学习，从载体图像与含密图像中提取特征[16-17]，成对输入模型进而训练隐写分析模型参数。训练后得到的隐写分析模型可用于判别图像是否经过隐写。其中集成分类器[18]应用比较广泛，集成分类器训练多个弱分类器分别进行判别，在判别时合并多个弱分类器的结果进行最终判别。这种分析方式不仅提升了隐写分析的效率，也提高了隐写分析的精度。近年来，深度学习方法也在隐写分析方面取得重要进展[19-21]，深度学习方法主要是通过神经网络进行特征提取和特征分析以判断图像是否经过隐写。

Ker[22]在研究中证实，隐写的安全性与隐写过程中所使用图像数量的平方成正比。在备选图像充足时，选择多张合适图像进行隐写以提升隐写系统安全性的方式是可行的。由于隐写术倾向于将隐秘信息隐写在图像的复杂纹理处，所以在图像选择过程中倾向于选择复杂图像，如Kharrazi等[23]提出选择JPEG图像中可修改DCT特征较多者进行隐写。为抵御批量隐写分析，Wang等[24]使用与秘密图像集的最大均值差异(MMD)作为载体集的选择标准。Zhao等[25]则以直方图均衡度为度量，更倾向于使用直方图均衡度高的图像进行隐写嵌入。Wu等[26]将图像建模成高斯混合模型，通过计算Fisher信息矩阵来评估图像的隐写能力。还有团队通过块残差、块能量和块波动分析图像复杂度，优先选择复杂图像进行嵌入。文献[27]证实，随着嵌入信息增多，单张图像所受畸变的一阶导数单调递增，从而提出了一种多载体选择策略，确保各图像在嵌入后畸变的一阶导数相等，同时分配嵌入信息量。

为实现隐蔽的信息传递，隐写方案中的载体图像通常选自媒体传输的数字图像。然而，网络传输的图像可能经过预处理以增强内容，如使用维纳滤波对图像降噪或使用中值滤波降噪。预处理通常对图像复杂处的纹理进行平滑处理，而隐写则更倾向于更改图像的复杂纹理区域，因此预处理可能影响隐写安全性，之后我们也将利用实验验证这一观点。然而，传统方法往往仅考虑嵌入失真，忽略了预处理对隐写的影响。

本文提出一种综合考虑图像预处理失真与嵌入失真的载体选择方案，本方案可有效提升隐写系统的安全性。

1 预处理影响

本节主要通过实验探究使用经过预处理的图像进行隐写对于隐写系统安全性的影响。所使用的图像是从常用的BOSSbass ver. 1.01图像库[28]选择的，该图像库具有10 000张大小为512×512的灰度图。选取前500张图像进行测试，对选出的图像进行7种常用的预处理操作：腐蚀、直方图均衡、均值滤波、膨胀、锐化、维纳滤波、中值

滤波。

设置预处理后的图像嵌入率为 0.5 bpp，使用 HILL 方法嵌入隐秘信息于图像得到经过隐写的图像。提取图像的 SRM 特征[16]，并将提取所得 SRM 特征输入集成分类器[18]进行隐写分析。集成分类器进行判别，集成分类器判别的正确性P_{E}的计算公式为

$$P_{\mathrm{E}}=\min_{P_{\mathrm{FA}}}\frac{1}{2}(P_{\mathrm{FA}}+P_{\mathrm{MD}}(P_{\mathrm{FA}})) \tag{1}$$

式中：P_{FA}为虚报率；P_{MD}为漏报率。P_{E}一般取值在 0～0.5 之间，P_{E}越小说明隐写系统安全性越差。得到的结果如表 1 所示。从表 1 可以看出，经过中值滤波、腐蚀、膨胀等预处理的图像进行隐写后，隐写系统安全性为 0，锐化预处理的图像进行隐写后，隐写系统安全性是原本的 1/3，这也进一步证实，使用预处理的图像作为隐写载体，会使得隐写系统的安全性大大降低。

表 1　不同类型图像隐写安全性对比

Tab.1　Comparison of image steganography security in different types

图像类型	P_{E}
原始图像	0.2556
经均值滤波预处理(滤波器尺寸:3×3)	0.0016
经维纳滤波预处理(滤波器尺寸:3×3)	0.0086
经中值滤波预处理(滤波器尺寸:3×3)	0.0000
经腐蚀预处理(滤波器尺寸:3×3)	0.0000
经膨胀预处理(滤波器尺寸:3×3)	0.0000
经锐化预处理	0.0824
经直方图均衡预处理	0.0006

2　载体选择方案

2.1　载体选择流程

本节提出了一种综合考虑图像预处理失真与嵌入失真的载体选择方案，载体选择流程图见图 1。将待选的n张图像$\{X_1,X_2,\cdots,X_n\}$输入神经网络，网络将输出 0～1 之间的一个数字，使用网络输出计算出图像的预处理失真$\{D_{\mathrm{Y1}},D_{\mathrm{Y2}},\cdots,D_{\mathrm{Y}n}\}$。使用传统方法计算$n$张图像的嵌入失真为$\{D_{\mathrm{E1}},D_{\mathrm{E2}},\cdots,D_{\mathrm{E}n}\}$，由于经过预处理的图像用于隐写会对隐写系统的安全性造成严重影响，所以本文所提出的排序方案会优先选择未经过预处理的图像用于隐写，为达到该目的，将融合失真时预处理失真权重设置得更大。假设n张图像中有α张图像未经过预处理，则这α张图像将会排在前α名，具体排名根据方案计算的融合失真确定；剩下的经过预处理的$(n-\alpha)$张图像根据计算所得融合失真排序在后面。最终排名为$\{D_{f(1)},D_{f(2)},\cdots,D_{f(n)}\}$，如果要选$k$张图像进行隐写，那么就选择排序前$k$张图像。也就是$\{D_{f(1)},D_{f(2)},\cdots,D_{f(k)}\}$这些特征对应的$\{X_{f(1)},\cdots,X_{f(k)}\}$图像进行隐写。

2.2　网络训练流程

a. 网络架构。

本方案参考 ResNet 架构[27]构建深度学习网络 ResNet06sig 作为流程图 1 中的神经网络，网络整体结构如图 2 所示。输入灰度图经过一个包含 64 个 7×7 卷积核，步长为 2，填充为 3 的卷积层后输入残差层。每个残差层包括两个残差卷积层(第一残差卷积层 rc1 和第二残差卷积层 rc2)，每个残差卷积层均包含 64 个大小为 3×3 的卷积核，步长为 1，填充为 1。输入信息依次经过两个残差卷积层 rc1 和 rc2，然后再经过批量归一化操作和一个 Relu 层后获得输出信息。数据 A1 经过第一残差层 r1 后，获得数据 A2，然后数据 A1 和数据 A2 相加得到数据 A3 作为残差层 r2 的输入信息，经过第二残差层 r2 后获得数据 A4，再将数据 A3 和数据 A4 相加得到数据 A5。网络最终经过 sigmoid 层输出 0～1 之间的一个数。

b. 数据集分配。

网络训练数据集使用的是 BOSSbass ver. 1.01 图像库[28]，共 10 000 张图像，前 5 000 张用于训练网络。对这 5 000 张图片分别进行腐蚀、直方图均衡、膨胀、锐化预处理后获得 4 份数据集，这 4 份数据集作为预处理图像数据集。为了数据平

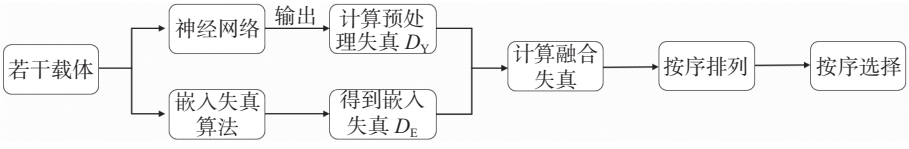


图 1　载体选择流程

Fig.1　Selection process of cover

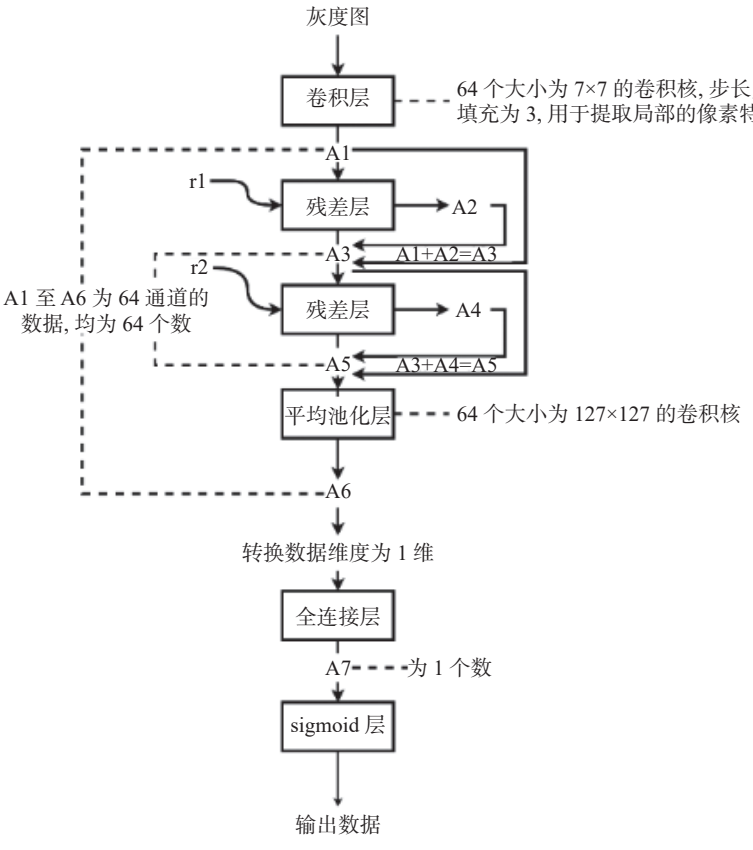


图 2 网络结构示意图

Fig.2 Diagram of network structure

衡，将前 5 000 张图片分别进行复制、旋转 90°、旋转 180°操作获得 3 份数据集，与原始 5 000 张图片的数据集作为未经预处理的图像数据集。8 份数据集一共 40 000 张图像，将每份数据集的前 80% 作为训练集、后 20% 中的 10% 作为测试集、剩下的 10% 作为验证集。将经过预处理的图像标签设置为 0，未经过预处理的图像标签设置为 1。使用训练集进行网络训练，每轮训练后使用测试集对模型精度进行测试，验证集用于对最终的模型进行精度测试。

c. 网络训练结果。

训练网络的过程中，每批次输入 32 张图像进行训练，初始学习率设置为 0.001。模型一共训练 40 轮，训练过程中设置动态学习率，每 4 轮学习率相同，下一个 4 轮学习率变为上 4 轮学习率的 0.7 倍，最后一轮学习率约为第一轮的 1/30，这使得模型更好地趋于最优点。使用二元交叉熵损失函数作为损失函数，利用 Adam 梯度下降算法优化模型参数。

在训练过程中，输出与标签之间差距小于等于 0.5，可认为网络输出准确。每次训练过后得到的模型在测试集上进行测试。选择在测试集表现最好的网络参数构成最终的网络，训练 40 轮后可以发现第 36 轮后所得参数最优秀，在验证集上准确度为 99.10%。

2.3 嵌入失真

使用常用的嵌入隐写算法如 S-UNIWARD 方法[9]、HILL 方法[10] 中的嵌入失真函数与最小化失真理论可以求得图像的嵌入失真，使用嵌入隐写算法中所定义的失真函数能够计算出每个像素被更改的代价。假设图像含有i个像素，可以表示为$X=\{x_1,x_2,\cdots,x_i\}$，通过失真函数计算出第i个像素加一减一的失真代价为ρ_i^+和ρ_i^-，则根据最小加性失真理论可以求得加密之后的理论最小加性失真D_{E}求解方法为

$$D_{\mathrm{E}}=\sum_{i=1}^{n}p_i^-\rho_i^-+p_i^+\rho_i^+ \tag{2}$$

其中，p_i可以通过ρ_i求得，方法如下：

$$p_i^+=\frac{e^{-\lambda\rho_i^+}}{1+e^{-\lambda\rho_i^+}+e^{-\lambda\rho_i^-}} \tag{3}$$

$$p_i^-=\frac{e^{-\lambda\rho_i^-}}{1+e^{-\lambda\rho_i^+}+e^{-\lambda\rho_i^-}} \tag{4}$$

p_i^-和p_i^+代表的是对第i个像素减一加一的概率，λ是与嵌入量m有关的一个参数，最终需要满足修改概率的三元信息熵等于m。已知ρ_i^+，ρ_i^-，m，可以通过式 (3)～(5) 计算出λ的值。

$$-\sum_{i=1}^{n}(p_i^+\log_2 p_i^+ + p_i^-\log_2 p_i^- + (1-p_i^- - p_i^+)\log_2(1-p_i^- - p_i^+)) = m \quad (5)$$

此时图像X的嵌入失真等于D_{E}。

2.4　失真融合与载体选择

由表 1 可以看出，使用预处理过后的图像用于隐写会损害隐写系统的安全性，所以方案优先选择未经预处理图像用于隐写，将预处理失真的优先级提高。为提升预处理失真优先级，本文赋予经过预处理的图像一个非常大的失真权重，使得预处理过后的图像总失真巨大，那么经过预处理的图像排序就会靠后，实际权重设置为10^{10}，预处理失真的计算公式为

$$D_{\mathrm{Y}} = 10^{10}\times(1-L) \quad (6)$$

式中，L 代表深度网络输出结果。

融合后的总失真D的计算公式为

$$D = D_{\mathrm{Y}} + D_{\mathrm{E}} \quad (7)$$

式中，D_{E}代表图像的嵌入失真。

计算出所有备选图像总失真为$\{D_1, D_2, \cdots, D_n\}$后进行升序排列，设排序出的排序结果为$\{D_{f(1)}, D_{f(2)}, \cdots, D_{f(n)}\}$，其中$D_{f(1)}$对应的图像为$X_{f(1)}$，则最终输出的$k$张图像为$\{X_1, X_2, \cdots, X_k\}$。载体选择策略如下：输入，备选数据集$\{X_1, X_2, \cdots, X_n\}$，训练数据集$\{T_1, T_2, \cdots, T_r\}$，选择图像数量$k$；输出，选择的$k$张图像$\{X_{f(1)}, X_{f(2)}, \cdots, X_{f(k)}\}$。步骤：(a) 使用训练数据集$\{T_1, T_2, \cdots, T_r\}$训练 ResNet06sig 分类模型；(b) 将$\{X_1, X_2, \cdots, X_n\}$输入训练好的分类模型得到$L$，计算预处理失真$\{D_{\mathrm{Y1}}, D_{\mathrm{Y2}}, \cdots, D_{\mathrm{Yn}}\}$；(c) 根据式 (2) 计算$\{X_1, X_2, \cdots, X_n\}$的嵌入失真$\{D_{\mathrm{E1}}, D_{\mathrm{E2}}, \cdots, D_{\mathrm{En}}\}$；(d) 使用式 (7) 计算$\{X_1, X_2, \cdots, X_n\}$的总失真$\{D_1, D_2, \cdots, D_n\}$；(e) 将$\{D_1, D_2, \cdots, D_n\}$升序排列得到$\{D_{f(1)}, D_{f(2)}, \cdots, D_{f(n)}\}$；(f) 选择$\{D_{f(1)}, D_{f(2)}, \cdots, D_{f(k)}\}$对应的$\{X_1, X_2, \cdots, X_k\}$输出。

3　实验结果

3.1　备选数据集

实验过程中使用 BOSSbass ver. 1.01 图像库[28]的后 5 000 张图像作为备选图像集。其中 1 500 张不进行预处理，剩下的 3 500 张平均分为 7 组，分别进行腐蚀、直方图均衡、均值滤波、膨胀、锐化、维纳滤波、中值滤波预处理。将经过预处理的 3 500 张图像与 1 500 张原图合并作为备选图像集。

3.2　实验结果

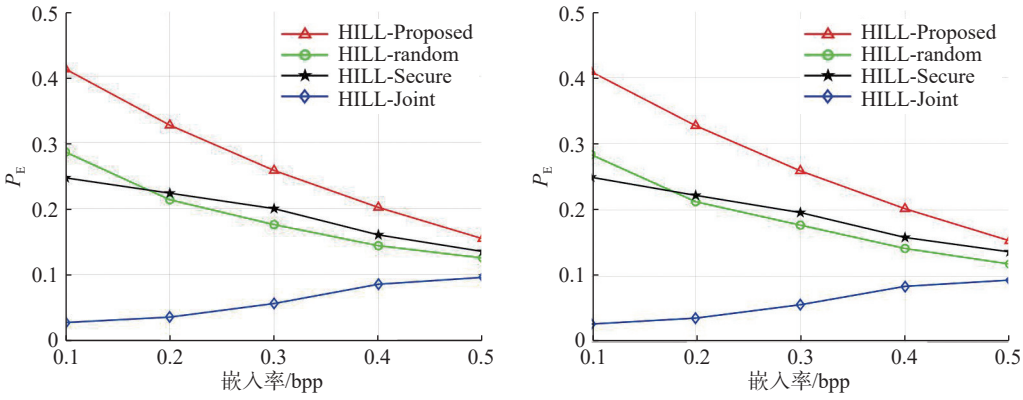
使用本文所述网络训练过程进行操作得到的网络在备选图像集上的准确度达到了 85.71%，由于训练过程中采用了 4 种预处理，而备选图像集含有 7 种预处理，说明本模型具有较好鲁棒性。

为了对比 4 种方法所选图像用于隐写的安全性，实验过程中使用 S-UNIWARD 隐写方法[9]或 HILL 隐写方法[10]进行隐写，嵌入率设置为 0.1，0.2，0.3，0.4，0.5 其中一个数值。隐写分析选用 SRM 特征[16]或者 maxSRM 特征[17]加上集成分类器的传统方法，集成分类器使用嵌入后的一半图像提取特征后进行训练。最后使用另外一半嵌入后的图像经过 10 次集成器模型判断，输出 10 次P_{E}的平均值用于度量所选图像用于隐写后的安全性，P_{E}越大说明载体选择方案安全性越高。

图 3～图 6 是本文所做的隐写方案安全性对比实验，将本文提出的隐写载体选择方案与其他 3 种隐写载体选择方案进行对比。首先，采用不同的载体选择方案从备选图像集中选出指定数量的载体图像；之后，使用传统隐写方法对选出的载体图像进行图像隐写得到含密图像；最后，提取含密图像的特征，将提取的特征输入隐写分析器得到输出P_{E}。P_{E}能够间接体现出载体选择方案的安全性，P_{E}越大说明载体选择方案安全性越高。

其中，命名里的“Proposed”，“Joint”，“Secure”，“random”代表 4 种隐写载体选择方案，分别代表着本文所提出的方案、文献 [27] 中提出的方案、文献 [24] 中提出的方案、随机选择方案，“SUNI”与“HILL”指的是嵌入信息的方法，代表着使用 S-UNIWARD 方法[9]或 HILL 方法[10]进行隐写嵌入。

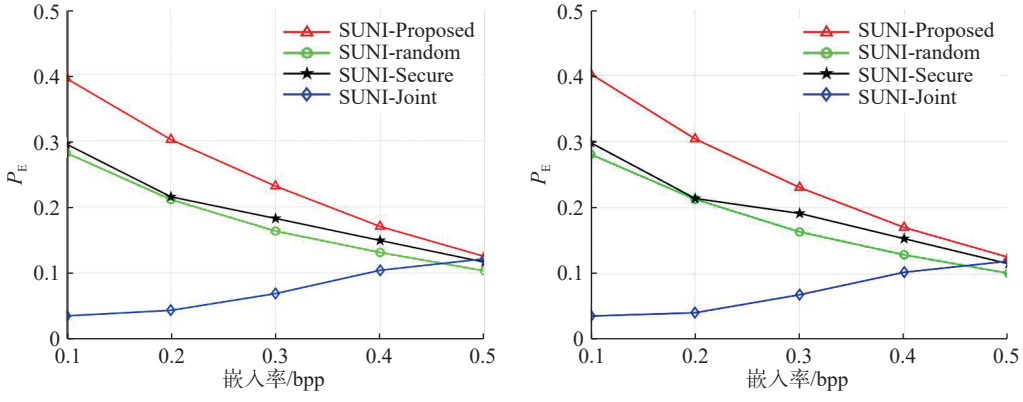
图 3 和图 4 是选择 500 张图像的情况下，更改隐写信息嵌入率的情况，可以看出，本文所提出的方法整体表现优于其他 3 种方法。除了文献 [27] 中所提出的方法，随着嵌入率的增加，其他 3 种方法的P_{E}逐渐降低，且本文所提出的方法受嵌入率影响较大。随着嵌入率提升，本文提出方



(a) SRM特征、固定图像数量、更改嵌入率　(b) maxSRM特征、固定图像数量、更改嵌入率

图 3　嵌入方法为 HILL 时，不同载体选择方案下隐写安全性对比

Fig.3　When the embedding scheme was HILL, steganographic security was compared under different cover selection schemes



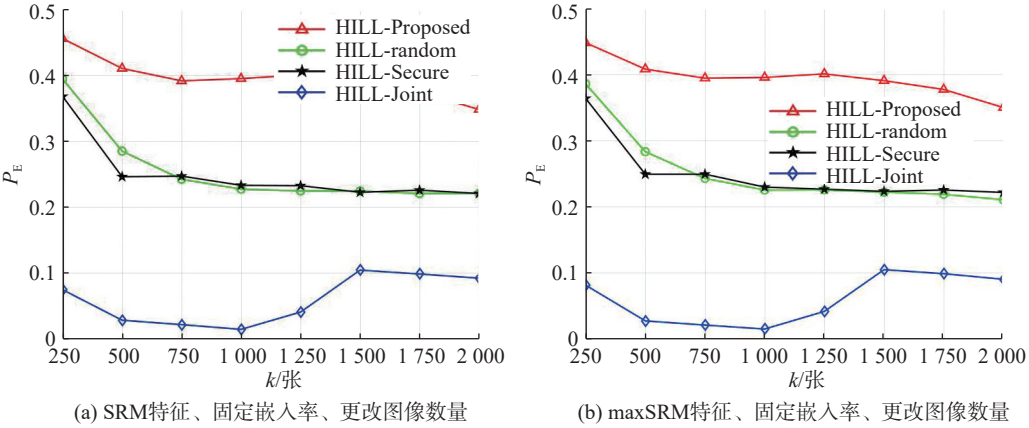
(a) SRM特征、固定图像数量、更改嵌入率　(b) maxSRM特征、固定图像数量、更改嵌入率

图 4　嵌入方法为 S-UNIWARD 时，不同载体选择方案下隐写安全性对比

Fig.4　When the embedding scheme was S-UNIWARD, steganographic security was compared under different cover selection schemes

法的P_E下降速率最快，在嵌入率为 0.5 的情况下，本文的载体选择方案安全性与其他 3 种方法的安全性相当。

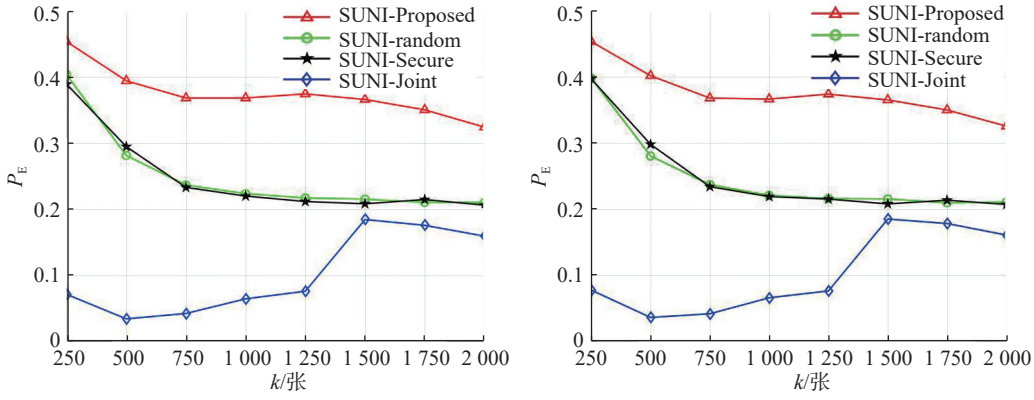
图 5 和图 6 是固定嵌入率为 0.1 的情况下，选择不同图像数量的情况，可以看出，绝大部分实验中，本文所提出的方法优于其他 3 种方法。随着嵌入图像增加，本文提出方法、文献 [24] 提出方法和随机选择策略的载体选择方案的P_E逐渐降低，其中本文所提出的载体选择方案的P_E下降速率最慢。被选图像中有 1 500 张未经过预处理的图



(a) SRM特征、固定嵌入率、更改图像数量　(b) maxSRM特征、固定嵌入率、更改图像数量

图 5　嵌入方法为 HILL 时，不同载体选择方案下隐写安全性对比

Fig.5　When the embedding scheme was HILL, steganographic security was compared under different cover selection schemes



(a) SRM特征、固定嵌入率、更改图像数量　　(b) maxSRM特征、固定嵌入率、更改图像数量

图 6　嵌入方法为 S-UNIWARD 时，不同载体选择方案下隐写安全性对比

Fig.6　When the embedding scheme was S-UNIWARD, steganographic security was compared under different cover selection schemes

像，当选择图像数量大于这个数量时，文献 [27] 的安全性也开始下降，本文所提出的载体选择方案的P_E下降速率增加一些，但整体安全性仍远高于其他 3 种方案。

4　总　结

关注到预处理过后的图像在经过隐写后会使得隐写系统安全性大大降低，于是提出一种将深度学习分类器与传统嵌入失真方法联合起来的规避预处理的多隐写载体选择方法。该方法采用融合预处理失真与嵌入失真的方式进行隐写载体选择。借鉴 ResNets 网络搭建并训练了一个神经网络用于判别图像是否经过预处理，并使用网络输出进行加权得到图像的预处理失真，与传统的嵌入失真融合进行载体隐写，可以有效规避经过预处理的图像，有效提升隐写系统安全性。还通过实验，与其他 3 种多载体隐写领域的载体选择方案进行比较，实验结果表明，本文所提出的隐写方法在备选图像集中含有预处理图像的情况下进行图像选择相比于其他方法在安全性上更具优势，并且更适合在选择更多数量的载体进行隐写且隐写信息嵌入率设置较低的情形，对于隐写系统的安全性更有保障，对于其他工作也有部分借鉴意义。

参考文献：

[1] FRIDRICH J. Steganography in digital media: principles, algorithms, and applications[M]. Cambridge: Cambridge University Press, 2009.

[2] MIELIKAINEN J. LSB matching revisited[J]. IEEE Signal Processing Letters, 2006, 13(5): 285−287,

[3] KER A D. Improved detection of LSB steganography in grayscale images[C]//Proceedings of the 6th International Workshop on Information Hiding. Toronto, Canada: Springer, 2004: 97–115.

[4] WESTFELD A. F5—a steganographic algorithm[C]//4th International Workshop on Information Hiding. Pittsburgh, PA, USA: Springer, 2001: 289–302.

[5] FRIDRICH J, PEVNÝ T, KODOVSKÝ J. Statistically undetectable jpeg steganography: dead ends challenges, and opportunities[C]//Proceedings of the 9th Workshop on Multimedia & Security. Dallas: ACM, 2007: 3–14.

[6] SALLEE P. Model-based steganography[C]//Second International Workshop on Digital Watermarking. Seoul, Korea: Springer, 2004: 154–167.

[7] EGGERS J J, BAEUML R, GIROD B. Communications approach to image steganography[C]//Proceedings of SPIE 4675, Security and watermarking of Multimedia Contents IV. San Jose: SPIE, 2002: 26–37.

[8] FRIDRICH J, GOLJAN M, LISONEK P, et al. Writing on wet paper[J]. IEEE Transactions on Signal Processing, 2005, 53(10): 3923−3935.

[9] HOLUB V, FRIDRICH J, DENEMARK T. Universal distortion function for steganography in an arbitrary domain[J]. EURASIP Journal on Information Security, 2014, 2014: 1.

[10] LI B, WANG M, HUANG J W, et al. A new cost function for spatial image steganography[C]//2014 IEEE International Conference on Image Processing (ICIP). Paris: IEEE, 2014: 4206–4210.

[11] FILLER T, JUDAS J, FRIDRICH J. Minimizing additive distortion in steganography using syndrome-trellis codes[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 920−935.

[12] YANG J H, RUAN D Y, KANG X G, et al. Towards automatic embedding cost learning for JPEG steganography[C]//Proceedings of ACM Workshop on Information Hiding and Multimedia Security. Paris: ACM, 2019: 37–46.

[13] TANG W X, LI B, BARNI M, et al. An automatic cost learning framework for image steganography using deep reinforcement learning[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 952−967.

[14] TANG W X, LI B, BARNI M, et al. Improving cost learning for JPEG steganography by exploiting jpeg domain knowledge[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 32(6): 4081−4095.

[15] 王朔中, 张新鹏, 张卫明. 以数字图像为载体的隐写分析研究进展 [J]. 计算机学报, 2009, 32(7): 1247−1263.

[16] FRIDRICH J, KODOVSKY J. Rich models for steganalysis of digital images[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(3): 868−882.

[17] DENEMARK T, SEDIGHI V, HOLUB V, et al. Selection-channel-aware rich model for steganalysis of digital images[C]//2014 IEEE International Workshop on Information Forensics and Security (WIFS). Atlanta: IEEE, 2014: 48–53.

[18] KODOVSKY J, FRIDRICH J, HOLUB V. Ensemble classifiers for steganalysis of digital media[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 432−444.

[19] QIAN Y L, DONG J, WANG W, et al. Deep learning for steganalysis via convolutional neural networks[C]//Proceedings of SPIE 9409, Media Watermarking, Security, and Forensics 2015. San Francisco: SPIE, 2015: 94090J.

[20] XU G S, WU H Z, SHI Y Q. Structural design of convolutional neural networks for steganalysis[J]. IEEE Signal Processing Letters, 2016, 23(5): 708−712.

[21] HUANG J W, NI J Q, WAN L H, et al. A customized convolutional neural network with low model complexity for JPEG steganalysis[C]//Proceedings of the ACM Workshop on Information Hiding and Multimedia Security. Paris: ACM, 2019: 198–203.

[22] KER A D. Perturbation hiding and the batch steganography problem[C]//10th International Workshop on Information Hiding. Sana Barbara, CA, USA: Springer, 2008: 45–59.

[23] KHARRAZI M, SENCAR H T, MEMON N. Cover selection for steganographic embedding[C]//2006 International Conference on Image Processing. Atlanta: IEEE, 2006: 117–120.

[24] WANG Z C, ZHANG X P. Secure cover selection for steganography[J]. IEEE Access, 2019, 7: 57857−57867.

[25] ZHAO Z Z, GUAN Q X, ZHAO X F, et al. Universal embedding strategy for batch adaptive steganography in both spatial and JPEG domain[J]. Multimedia Tools and Applications, 2018, 77(11): 14093−14113.

[26] WU S T, LIU Y, ZHONG S H, et al. What makes the stego image undetectable?[C]//Proceedings of the 7th International Conference on Internet Multimedia Computing and Service. Zhangjiajie: ACM, 2015: 47.

[27] WANG Z C, ZHANG X P, YIN Z X. Joint cover-selection and payload-allocation by steganographic distortion optimization[J]. IEEE Signal Processing Letters, 2018, 25(10): 1530−1534.

[28] BAS P, FILLER T, PEVNÝ T. “Break our steganographic system”: the ins and outs of organizing BOSS[C]//13th International Conference on Information Hiding. Prague, Czech Republic: Springer, 2011: 59–70.

（编辑：黄 娟）