文章编号:1674-2974(2019)12-0025-08 DOI:10.16339/j.cnki.hdxbzkb.2019.12.004

基于图像分类的无载体信息隐藏方法

吴建斌[1],康子阳[1†],刘逸雯[1],阎双奎[2],吴建平[3]
(1. 华中师范大学 物理科学与技术学院,湖北 武汉 430079;
2. 北京电子技术应用研究所,北京 100008;
3. 湖北幼儿高等师范专科学校,湖北 武汉 430223)

摘 要:为提高无载体信息隐藏的数据嵌入容量和通信效率,注意到半构造式无载体信息隐藏算法所具有的优势,在仔细分析几种社交平台的用户行为习惯后,提出了一种以社交平台的行为习惯为构造原则的半构造式无载体信息隐藏算法.该算法的具体思想通过构建小图标库中的图标与秘密消息的一一映射关系,将小图标按照一定的原则拼接,完成秘密消息的图像表达,通过传递拼接好的图片,实现秘密消息的传递.为了提高小图标的识别率和整个隐蔽通信系统的抗干扰能力,算法还引入了卷积神经网络对图标库中的图标进行训练和分类,同时在训练时特意引入经过多种攻击方式处理过的小图标作为干扰样本.实验和仿真结果表明,该隐藏方法具备良好的抗攻击能力,隐藏容量和通信效率得到了实质性的提高,可用于实际的隐蔽通信系统.

关键词:深度学习;图像分类;社交习惯;隐写;无载体信息隐藏
中图分类号:TP309.7 **文献标志码**:A

Coverless Information Hiding Algorithm Based on Image Classification

WU Jianbin[1], KANG Ziyang[1†], LIU Yiwen[1], GE Shuangkui[2], WU Jianping[3]
(1. School of Physics and Technology, Central China Normal University, Wuhan 430079, China;
2. Beijing Institute of Electronic Technology Application, Beijing 100008, China;
3. Hubei Preschool Teachers College, Wuhan 430223, China)

Abstract: In order to improve the data embedding capacity and the communication efficiency of coverless information hiding algorithm, addressing the advantages of semi-structured coverless information hiding algorithm, this paper introduces a semi-structured coverless information hiding algorithm based on the behavioral habits of social platforms. The specific idea of the algorithm is to build a one-to-one mapping relationship between icons and secret messages in a small icon library. According to certain principles, some small icons are montaged a picture, the secret information can be expressed by the splicing picture, and the transmission of secret messages is realized by delivering the spliced pictures. In order to improve the recognition rate of small icons and the anti-interference ability of the whole hidden communication system, convolutional neural network is also introduced to train and classify the icons in the icon library, and the interference samples are introduced as training samples set. The experimental re-

* **收稿日期**:2019-01-18
基金项目:国家自然科学基金资助项目(U1736121,U1536104),National Natural Science Foundation of China(U1736121,U1536104)
作者简介:吴建斌(1972—),男,湖北黄梅人,华中师范大学副教授,博士
† 通讯联系人,E-mail:ziyangkang666@163.com

sults show that the algorithm has good anti-attack ability and the hiding capacity can be improved, and therefore, the algorithm can be used in covert communication.

Key words: deep learning; image classification; behavioral habits; steganography; coverless information hiding

信息隐藏是将秘密信息隐藏于载体信号中,并在需要时将秘密信息提取出来,以实现隐蔽通信和版权保护等目的[1].由于数字图像冗余度大且使用广泛,常被作为信息隐藏载体.传统的嵌入式信息隐藏方法是通过对载体数据的修改,将秘密消息嵌入载体中,这必然会导致含密载体与原始载体间存在一定的差异,难以抵抗隐写分析检测[2].为提高隐蔽通信的安全性,无载体信息隐藏[3]受到了广泛关注."无载体"并不是指不需要载体,而是直接以秘密信息为驱动来"生成"或者"获取"含密载体.从本质上来说,基于图像的无载体信息隐藏是一种图像特征的编码方法.目前所见的无载体隐藏算法大多都存在数据嵌入容量不高的问题,离实用化还存在一定的距离.

为解决上述问题,本文提出了一种基于社交习惯的半构造式无载体信息隐藏算法[4],其思路是通过挖掘人们的社交行为习惯,以社交行为习惯为构造原则,设计不同的拼接模板,从图标库中选取图标,构造出一幅具有实际意义的图像并在社交平台中传输,达到隐蔽传输秘密消息的目的.其中,小图标库是在利用深度学习的方法对小图标进行训练、分类和识别的基础上所建立起来的.具体来讲,是利用卷积神经网络(Convolutional neural network,CNN)[5]提取图像特征并输入到该模型中进行训练,根据图像的高维特征对小图标进行识别和分类,考虑到传输过程中的图像可能会被攻击者攻击,用于训练的图像数据集应含有各种干扰样本.干扰样本来之于特殊处理过的图像数据,包含有干扰样本的训练集可以保证训练好的 CNN 网络能够在含密图像遭受攻击后也能对图标内容进行正确分类,确保算法的鲁棒性.

1 利用 AlexNet 进行迁移学习

1.1 深度卷积神经网络 AlexNet 模型

卷积神经网络具有低网络模型复杂度,可减少权值数目等优点,被广泛用于深度学习.采用卷积神经网络进行深度学习,将图像直接输入网络,可以避免传统算法中的数据重建和复杂的特征提取过程,能提高算法的运行效率. Krizhevsky 等[6]提出的卷积神经网络 AlexNet 在图像分类和物体检测方面的性能优于传统方法,虽然 GoogleNet[7]和 VGG[8]的性能相比 AlexNet 网络性能更好,但其网络复杂,训练耗时.综合考虑训练及识别效率等因素,本文选用 AlexNet 网络进行图像识别与分类,其网络相对简单且易于训练,可通过修改神经网络中的某些参数提高网络性能.本文所采用的卷积神经网络 AlexNet 网络层次结构图如图 1 所示.

不计输入层,该模型共 8 大层,25 小层结构,前 5 层是卷积层,接着 3 层为全连接层[5],全连接的结果通过 Softmax 分类器[9]产生 1 000 个分类输出.在前 5 层中,每一层都包含有卷积子层[5],缩写为 Conv1 到 Conv5,每一个卷积操作后紧跟的是激活函数 reLu 处理.采用 reLu 激活函数[10]的作用是使学习周期大大缩短,提高运算速度和效率. Norm1 和 Norm2 表示归一化操作.最后是池化操作,相比平均池化,该神经网络采用的最大池化(max pooling)[11]可以让特征参数减少,使更多的纹理特征信息保留下来. Dropout[6]操作是在两个全连接层中,其作用是为了防止训练样本较少的时候模型过拟合,最后通过 Softmax 分类器产生多维分类输出.

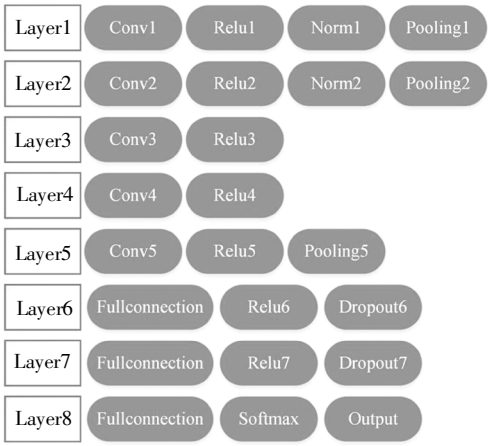

图 1 AlexNet 网络层次结构图

Fig.1 AlexNet network hierarchy chart

1.2 AlexNet 结构的修改

由于受时间和设备的计算能力所限,考虑到主要是做模型验证,因此本文在建立图标库时只选择了 32 种小图标. 为获得较好的分类性能，共享 AlexNet 的模型训练参数，达到迁移学习的目的[12],本文改造了部分网络结构:首先冻结 AlexNet 的前 7 大层,即前 23 小层,去掉 Layer8 并在后面加上自己的网络输出层. 本文在新的 Layer8 中先加一层输出为 64 的全连接层，然后接一层 relu 激活层精简特征参数,再接一层全连接层(Fullconnection)并接上一层 softmax 分类器和一层分类输出层（Output)共输出 32 个类别,改造后的网络结构如图 2 所示.

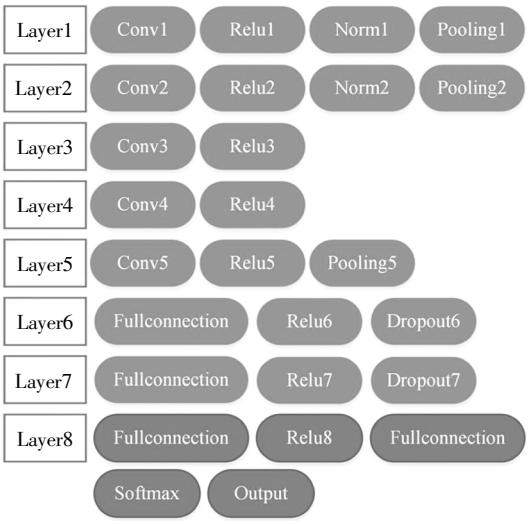

图 2　修改后的卷积神经网络层次结构图

Fig.2　Modified convolution neural network hierarchy

2　信息隐藏算法

由于受时间和具体计算设备的计算能力所限,为兼顾隐藏容量、误码率、鲁棒性以及拼接图像内容的合理性等要求,同时,本文旨在验证算法的可行性,因此,图标库只构建了 32 种小图标,每一个图标的类别标签对应一段 5 bit 的二进制序列.

2.1　题目规则的设计

为了避免被第三方怀疑,在社交网络上传播的含密载体应当符合人们的社交习惯. 为此,利用数据挖掘的方法,对社交平台上的各种数据进行挖掘并进行数据分析以寻求使用较为广泛的大众行为习惯，按照这种行为习惯设计图片的拼接原则和思考题的题目规则. 以将图片处理成一些有趣味性的智力题目为例,目前设计了 5 种规则拼接生成含密载体图像，如:“算价格”,“分类别”,“编故事”,“找最长”和“找相同”.

2.2　隐藏算法

隐藏秘密信息的流程示意图如图 3 所示，其具体的实现步骤如下:

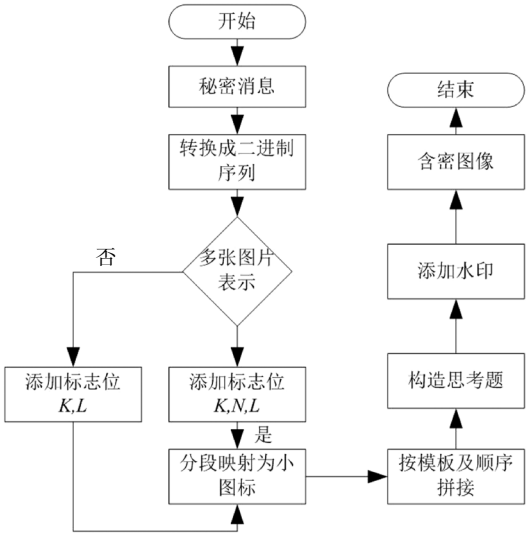

图 3　秘密信息隐藏流程图

Fig.3　Flow chart of secret information hiding

步骤 1　输入一段秘密信息 S(信息内容可以是中文汉字,英文单词,二进制或者是十进制数,也可以选择生成一段 80 bit 长度的随机二进制序列,输入类型 K 用 2 bit 二进制数表示)，将待隐藏的信息转换为二进制序列 E,根据 O 的长度判断需要 X 张图片将秘密隐藏完全表达. 将 X 分为若干段，每段计算其长度 L 作为标志位一,每张图像的顺序序号 N 作为标志位二,接着选择相应的输入类型 K 作为标志位三，这样最多可构成一个 13 bit 的二进制序列作为标志位.

步骤 2　将标志位加在含密序列 E 的前端,得到最终的含密二进制序列 C. 对 C 进行分段,每 5 位为一段,每一段根据二进制序列与自建图像库中 32 种物体标签的映射关系进行查询，映射为相应的类别标签并获得相应的物体图像,按从左至右、从上往下的顺序将这些子图像拼接起来.

步骤 3　拼接图像的大小根据 E 的长度 L 相应有 2×2、3×3、4×4、5×5、6×6 共 5 种模板. 在每个模板能表达的位数区间内，不足区间上限的补随机数至区间上限值.

步骤 4　对图片内容的题目描述类型目前设计了 5 种:“算价格”,“分类别”,“编故事”,“找最长”和“找相同”,其中“找相同”只有拼接图片为 6×6 形式的时候才可能出现,因为图像数据库中一共只有 32

种不同的类别，而 6×6 的拼接图片中 36 张图片必然有相同的类别. 可以自行指定 4 种题目类型之一，也可以设置为随机选择.

步骤 5 为了确认发送的题目图片是发送方发出的含密图片，也为了防止被攻击者篡改，主要是防止被攻击者交换题目中各子图位置甚至替换图中的子图，需要设计一种独特的、不易被改变能检测的水印. 本文采用的水印为一个根据题目图片的各拼接子图的信息熵和权值加权计算出的特征值.

$$E = \sum_{n=1}^{m} \frac{n^2}{n^2-1} M_n \tag{1}$$

式中：M 为每一子图的信息熵；m 为小图标的个数；n 为小图标自上而下、由左向右的顺序序号.

Shannon 提出的信息熵用于图像领域可以表征图像的纹理复杂度和灰度的密度分布特性. 对一整幅 256 级的灰度图像而言，其信息熵为：

$$S(I) = -\sum_{j=1}^{j=256} p(x_j)\log p(x_j) \tag{2}$$

式中：$p(x_j)$表示图像 I 中灰度值为 j 的像素出现的概率.

步骤 6 将骤计 5 算出的特征值作为水印，采用基于 DCT 变换的算法[14]嵌入到题目规则引导图像中，再将完成拼接的含密图片与嵌入了特征水印的题目规则图片拼接、合成为一张题目图像，作为最终的含密图像供发送方在社交网络上进行传递.

2.3 提取算法

提取秘密信息的流程示意图如图 4 所示，其具体的实现步骤如下：

步骤 1 对含密图片的题目规则部分进行截取并检测特征水印是否存在，若存在则证明此图是发送方发出的含密图片，且未被攻击者所攻击，可以进行接下来的提取步骤. 若不存在则说明此图不是发送方发出的图片或含密图片已经遭受了某种攻击被破坏，可以选择不继续进行提取操作.

步骤 2 对检测通过的每一张含密图片的拼接部分的每一张子图进行预处理，处理后得到 227×227 大小的图片按自上而下、由左向右的顺序依次输入到训练好的卷积神经网络中进行识别分类得到物体的类别标签，由类别标签和映射关系得到二进制序列 R.

步骤 3 将二进制序列 R 的的标志位取出，得到转换为二进制序列的秘密信息的长度 L、输入类型 K 和图像的顺序序号 N. 由截取 R 的前 L 长度 bit 作为含密二进制序列，最后将若干秘密信息按照其对应的顺序序号 N_1、N_2、N_3 按顺序连接得到秘密信息，再由输入类型 K 直接转换得到原秘密信息.

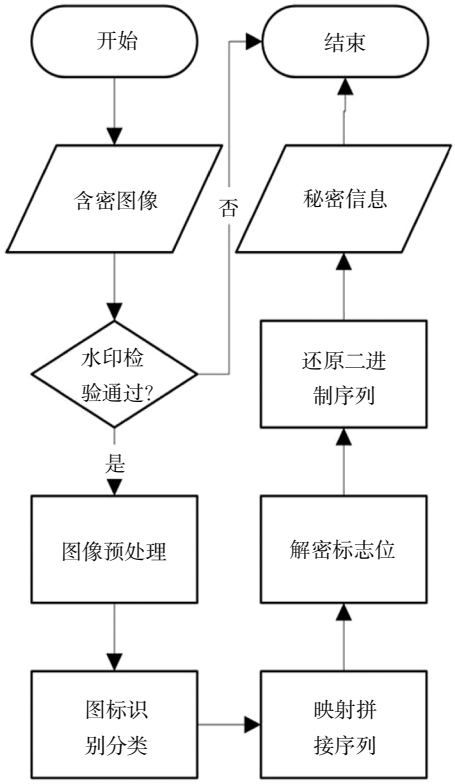

图 4 秘密信息提取流程图

Fig.4 Flow chart of secret information extraction

3 实验结果与分析

3.1 训练神经网络

3.1.1 数据集的建立

为提高识别率和抗攻击性，训练数据集中包含了 32 种物体的图片和这 32 种物体经过各种攻击后的图片，如采用高斯噪声、椒盐噪声、均值滤波、中值滤波、JPEG 压缩和灰度化等攻击手段生成的攻击样本. 其中高斯白噪声的均值为零，方差从 0.001 变化到 1，单位间隔为 0.001，方差越大，噪声强度越大；椒盐噪声的均值为零，方差从 0.001 变化到 1，单位间隔为 0.001，噪声强度随着方差越来越大；滤波攻击的滤波器尺寸参数从 1×1 到 9×9，单位间隔为 1×1，滤波器尺寸越大，滤波攻击强度越大；JPEG 压缩质量因子从 1 变化到 99，单位间隔为 0.1；32 种类别每种都包含 6 041 张图片，整个训练数据集包含 193 312 张图片.

3.1.2 训练参数的初始化及微调

对第 8 层中的 25 小层即全连接层的学习率进

行设置:参数的学习率的大小直接影响该参数的变化快慢,考虑权重和偏置的变化快慢适中的需求,权重因子学习率被设置为 10,权重因子初始值设置为 1,偏置学习率因子设置为 20 时,权重因子设置为 0. 在基本训练参数中,MaxEpoch 是计算的轮数, 它的值越大越容易收敛, 此处设置为 30;InitialLearRate 是学习率,太大模型可能不会收敛,太小则收敛的太慢, 本文设置为 0.000 1. MiniBatchSize 是每次处理的数据的个数,设置为 8;训练网络环境用 GPU 进行训练以极大的提高运行速度,参数中设置训练方式为随机梯度下降法(sgdm)[15].

3.2 鲁棒性分析

本实验分别采用高斯噪声、椒盐噪声、JPEG 压缩、均值滤波和中值滤波以及灰度化手段对构造的含密图像进行攻击,然后对受到攻击的含密图像进行解密以提取秘密信息,并通过计算其误码率来判断算法的鲁棒性. 误码率(Bit Error Rate,BER)为传输中错误信息的码数 p 与传输的秘密信息的总码数 q 的比值.

$$BER = p/q \times 100\% \quad (3)$$

3.2.1 抗噪声测试

在抗高斯噪声攻击实验中,噪声均值 μ 为 0,方差 σ^2 从 0 变化到 1, $\sigma^2 = 1$ 时,噪声强度最高. 在本测试中,σ^2 从 0.1 递增到 1,间隔为 0.1. 图 5 为本文算法误码率在不同强度的高斯噪声攻击下的误码率的变化折线图. 表 1 展示了本文算法与 CSD(chaotic sequences and image DCT algorithm) 算法[16]、CBZS (chaos based zero-steganography)算法[17]的抗高斯白噪声攻击能力的比较. 通过 20 次重复实验,结果证明,随着高斯噪声方差的增加,误码率始终为零,因而本算法具备良好的抗高斯噪声攻击的能力,性能优于 CBZS、CSD 算法.

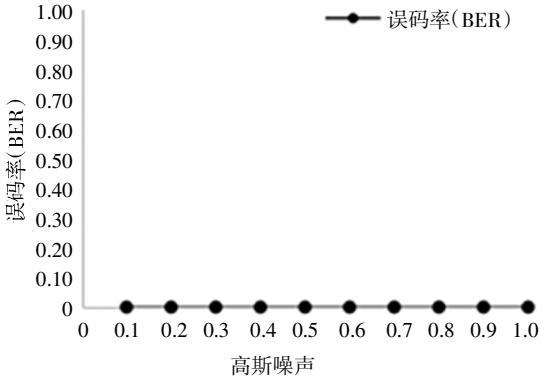

图 5 高斯噪声攻击

Fig.5 Gauss noise attack

表 1 CBZS 算法、CSD 算法与本文算法之间抗 Gaussian 噪声攻击能力比较

Tab.1 The comparison of Gaussian noise attack capability between CBZS algorithm, CSD algorithm and the algorithm in this paper

σ^2	CBZS	CSD	本文算法
0.1	0.18	0.14	0
0.2	0.19	0.24	0
0.5	0.21	0.25	0
0.6	0.21	0.26	0
0.9	0.22	0.31	0
1.0	0.22	0.33	0

图 6 给出了算法在不同强度的椒盐噪声攻击下的误码率折线图,椒盐噪声强度从 0.01 递增到 1,单位距离为 0.01. 由图 6 可知, 在噪声强度低于 0.7 时,BER 始终为零, 在噪声强度为 0.7 至 0.83 之间时 BER 不超过 3.2%. 当噪声强度高于 0.84 时 BER 才基本沿直线上升, 但此时图像已经不具有实际的意义,人类视觉系统基本完全无法识别其内容. 由表 2 可知在噪声强度较低时 BER 基本为零,本文算法的抗椒盐噪声能力在低噪声强度攻击时优于 CBZS、CSD 算法.

3.2.2 抗 JPEG 压缩测试

JPEG 压缩作为一种有损压缩方法通常被第三方用来攻击含密图像. 本文选取的 JPEG 压缩质量因子的范围从 10 递增到 90,单位间隔为 10,通过对每个点的 BER 的计算来算法抗 JPEG 压缩的性能. 每个点的 BER 取 20 次实验的平均值. 横坐标代表压缩质量因子,纵坐标代表通过 JPEG 压缩攻击后,恢复秘密信息时的误码率.

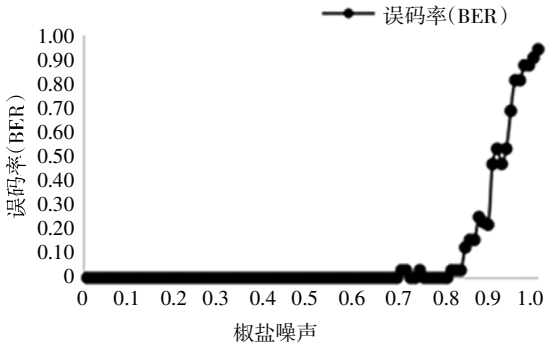

图 6 椒盐噪声攻击

Fig.6 Salt and pepper noise attack

表 2 CBZS 算法、CSD 算法与本文算法之间抗椒盐噪声攻击能力比较

Tab.2 The comparison of Salt and pepper noise attack capability between CBZS algorithm, CSD algorithm and the algorithm in this paper

Noise density	CBZS	CSD	本文算法
0.01	0.18	0.14	0
0.03	0.19	0.24	0
0.05	0.21	0.25	0
0.07	0.21	0.26	0
0.09	0.22	0.31	0
0.10	0.22	0.33	0

测试结果如图 7 所示. 由图 7 可知,本文算法在压缩质量因子变化时能使误码率始终保持为零. 表 3 展示了本文算法与 CBD (Chaos based DCT steganography) 算法 [18]、CBZS 算法、CSD 算法在抗 JPEG 压缩攻击能力上的比较. 数据表明本文算法的抗 JPEG 压缩攻击的能力明显优于另外 3 种算法.

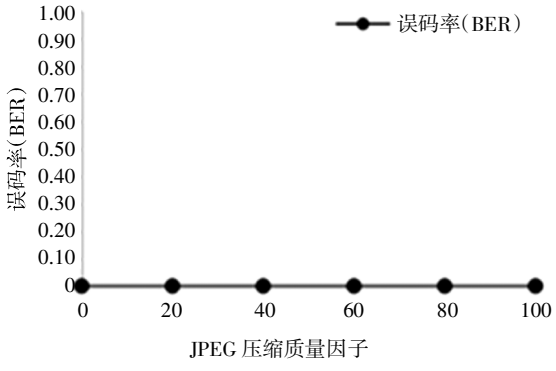

图 7 JPEG 压缩攻击

Fig.7 JPEG compression attack

表 3 CBD 算法、CBZS 算法、CSD 算法与本文算法之间抗 JPEG 压缩攻击能力比较

Tab.3 The comparison of JPEG compression attack capability between CBD algorithm, CBZS algorithm, CSD algorithm and the algorithm in this paper

Quality	CBD	CBZS	CSD	本文算法
90	0.022	0.048	0.002	0
70	0.038	0.080	0.009	0
50	0.151	0.098	0.017	0

3.2.3 抗滤波器攻击测试

对含密图像分别用均值滤波器和中值滤波器进行攻击,计算其误码率来衡量算法抗滤波器攻击的能力[19]. 滤波器尺寸范围从 1×1 递增至 9×9,间隔为 2×2. 测试结果如图 8、图 9 所示. 从图 8 和图 9 可以看出,滤波器尺寸的增大并没有增加误码率,本文算法的误码率始终为零, 具有优秀的抗滤波器攻击能力.

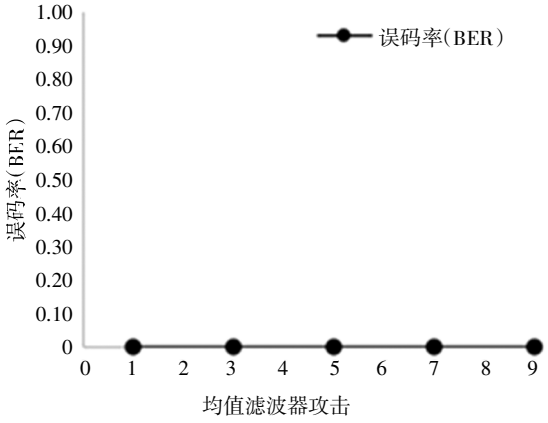

图 8 均值滤波器攻击

Fig.8 Mean filter attack

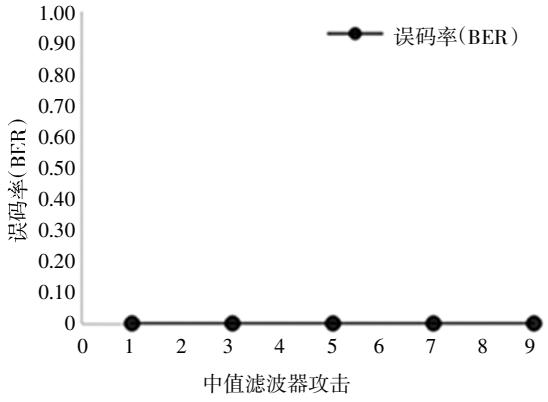

图 9 中值滤波器攻击

Fig.9 Median filter attack

3.3 抗检测性和安全性

本文算法中以人们的社交习惯设计智力题规则, 通过小图标拼接和文字引导使得处理后的拼接图像变得有意义,在内容上符合特定的逻辑表达. 从图 10 可以看出,最终生成的含密图像,内容上具备关联性和合理性,符合人们的行为习惯,不容易被第三方所怀疑,故其安全性较高. 算法为含密图像设计了专有的特征水印, 水印中包含了子图的信息熵特征和位置信息, 故信息接收者可以据此判断含密图

像是否为发送者发出,是否被攻击者进行替换、移位等篡改攻击,进一步提高了算法的安全性. 算法本身未对含密图像作任何改变,故其抗检测能力较强.

已知货架上每行、列商品的总价,求所有商品的总价

图 10　生成的含密图像

Fig.10　Generated dense image

3.4 容量

2^n 张图像只能对应 n 位二进制编码,因此若要单张图像表示尽可能多的二进制数则需要建立相当庞大的图像库来满足要求. 在本文算法中每张小图标图像均编码为 5 位二进制数,图像库中仅需要 32 张图像. 在一般的编码规则下单张 52×52 或 312×312 的图像均代表 5 bit 信息. 而本文算法中将 36 张大小为 52×52 进行拼接得到 312×312 大小的图像则可单次表示 180 bit 信息，减去 10 bit 可表示 170 bit 信息;生成多张图像时减去标志位中占有的 13 bit 也能表示 167 bit 信息，而不用建立图像数量为 2^{167} 张的图像库. 且本文算法考虑到实际传输的秘密信息长度需求更大,因而提供了最多可用 7 张拼接图像作为载体以传输秘密信息,每段信息的顺序已被处理并隐藏于标志位中以保证能解出正确的原始秘密信息. 故本文算法最多一次性可传输 167 × 7 = 1 169 bit 信息，若秘密信息为汉字可传输 77 个汉字,在很多情况下,能用于实际的隐蔽通信. 用数据嵌入率来表示嵌入容量的大小:

$$C = B/D \times 100\% \tag{4}$$

式中:B 为隐藏信息的长度;D 为宿主的长度.

ICS(image coding and stitching)算法[20]的数据嵌入率只有 0.01%,大小为 1 024×1 024 的单张图片的最大容量为 167 bit. GGCM（Grayscale Gradient Co-occurrence Matrix)的数据嵌入率只有 0.01%,大小为 256×256 的单张图片的最大容量为 8 bit. 而本文提出的算法可达 0.18%，单张图片的最大容量可达 170 bit,相比以上两种无载体隐藏算法,数据嵌入率有了较大的提升,单张图片的容量也有所提升.

4 结　论

为提高通信效率和隐藏容量，本文采用数据挖掘技术从社交平台中提取社交行为习惯，并结合深度学习方法进行训练、识别和分类,建立图标库,以行为习惯为构造准则构造出含密图像，实现秘密消息的隐蔽传输. 本文算法 MATLAB 2017b 环境下测试,从实验结果看,本文算法具有良好的隐蔽性和鲁棒性,能抵抗高斯噪声、抗椒盐噪声、抗 JPEG 压缩、抗均值滤波器和抗中值滤波器的攻击，有效地提高了通信效率和秘密消息的隐藏容量.

参考文献

[1] 沈昌祥,张焕国,冯登国. 信息安全综述[J].中国科学,2007,37(2):129—150.
SHEN C X,ZHANG H G,FENG D G. Overview of cyber security [J].Science In China,2007,37(2):129—150.(In Chinese)

[2] INAS J K,PRASHAN P,VIAL P,*et al*. Comprehensive survey of image steganography:techniques,evaluations,and trends in future research [J]. Neurocomputing,2018,335:299—326.

[3] ZHOU Z L,SUN H Y,HARIT R,*et al*. Coverless image steganograph without embedding [C]// International Conference on Cloud Computing and Security. Springer,Cham:Springer,2015:123—132.

[4] 张新鹏,钱振兴,李晟.信息隐藏研究展望[J]. 应用科学学报,2016,34(5):476—484.
ZHANG X P,QIAN Z X,LI S .Prospect of digital steganographyresearch [J]. Journal of Applied Sciences,2016,34(5):476—484.(In Chinese)

[5] 刘健,袁谦,吴广,等.卷积神经网络综述[J].计算机时代,2018,11:19—23.
LIU J,YUAN Q,WU G,*et al*. Review of convolutional neural networks [J].Computer Era,2018,11:19—23.(In Chinese)

[6] KRIZHEVSKY A,SUTSKEVER I,HINTON G E. ImageNet classification with deep convolutional neural networks [J]. Communica-

tions of the ACM,2017,60(6):84—90.

[7] ZEGEDY C,LIU W,JIA Y Q,*et al*. Going deeper with convolutions.[C]//Proceedings of the 2015 IEEE Conference on Computer Vision and Pattern Recognition. Boston,MA: IEEE,2015:1—9.

[8] SIMONYAN K,ZISSERMAN A. Very deep convolutional networks for large-scale image recognition [C]//The Hilton San Diego Resort & Spa. San Diego:ICLR,2015:1—14.

[9] 冉鹏,王灵,李昕,等. 改进 Softmax 分类器的深度卷积神经网络及其在人脸识别中的应用[J].上海大学学报(自然科学版),2018,24(3):353—366.
RAN P,WANG L,LI X,*et al*. Improved Softmax classifier for deep convolution neural networks and its application in face recognition [J]. Journal of Shanghai University (Natural Science),2018,24(3):353—366. (In Chinese)

[10] 蒋昂波,王维维. ReLU 激活函数优化研究[J].传感器与微系统,2018,37(2):50—52.
JIANG A B,WANG W W. Research on optimization of ReLU activation function [J]. Transducer and Microsystem Technologies,2018,37(2):50—52. (In Chinese)

[11] 周林勇,谢晓尧,刘志杰,等. 卷积神经网络池化方法研究[J].计算机工程,2019,45(4):211—216.
ZHOU L Y,XIE X Y,LIU Z J,*et al*. Research on pooling method of convolution neural network [J]. Computer Engineering,2019,45(4):211—216. (In Chinese)

[12] 刘鑫鹏,栾悉,谢毓湘,等. 迁移学习研究和算法综述[J].长沙大学学报,2018:32(5):29—36.
LIU X P,LUAN X,XIE Y X,*et al*. Transfer learning research and algorithm review[J]. Journal of Changsha University,2018,32(5):29—36. (In Chinese)

[13] 谭耀麟. 图像信息系统原理[M]. 北京:清华大学出版社,2006:326—335.
TAN Y L. Principle of image information system [M]. Beijing:Tsinghua University Press,2006:326—335. (In Chinese)

[14] KEKRE H B,SARODE T K,THEPADE S D. Color-texture feature based image retrieval using DCT applied on Kekre´s median codebook [J]. International Journal of Imaging & Robotics TM,2009,2(9):54—65.

[15] 王功鹏,段萌,牛常勇. 基于卷积神经网络的随机梯度下降算法[J].计算机工程与设计,2018,39(2):442—462.
WANG G P,DUAN M,NIU C Y. Stochastic gradient descent algorithm based on convolution neural network [J].Computer Engineering and Desigh,2018,39(2):442—462. (In Chinese)

[16] 吴建斌,费潇潇,王年丰. 基于混沌序列和 DCT 变换的图像零隐藏算法研究[J]. 电子测量技术,2017,40(5):174—179.
WU J B,FEI X X,WANG N F. Zero-steganography algorithm research based on chaotic sequences and image DCT transform [J]. Electronic Measurement Technology,2017,40 (5):174—179. (In Chinese)

[17] BILAL M,IMTIAZ S,ABDUL W,*et al*. Chaos based Zero - steganography algorithm [J]. Multimedia Tools & Applications,2014,72(2):1073—1079.

[18] SINGH S,SIDDIQUI T J. A security enhanced robust steganography algorithm for data hiding [J]. International Journal of Computer Science Issues,2012,9(3):131—139.

[19] WU J B,LIU Y W,DAI Z Y,*et al*. A coverless information hiding algorithm based on grayscale gradient co-occurrence matrix [J]. I-ETE Technical Review,2018,35:23—33.

[20] 吴建斌,贾炎柯,刘逸雯. 基于图像编码及拼接的无载体信息隐藏[J].华南理工大学学报(自然科学版),2018,46(5):32—39.
WU J B,JIA Y K,LIU Y W. Coverless information hiding algorithm based on image coding and stitching [J]. Journal of South China University of Technology (Nature Science Edition),2018,46(5):32—39. (In Chinese)