DOI:10.16136/j.joel.2022.10.0002

一种基于Arnold置乱和DCT编码的无载体信息隐藏方法

郭晨飞，张春玉*，苟沛东，刘海伦，单莉颖，吴秀琪

(西藏民族大学 信息工程学院，陕西 咸阳 712082)

摘要：近年来十分火热的搜索映射式无载体信息隐藏虽具有一定的鲁棒性，但其隐藏容量较低、传输负载大且算法复杂度高。针对以上问题，该文章提出一种基于Arnold置乱和离散余弦变换(discrete cosine transform，DCT)编码的无载体信息隐藏方法。该算法先对图片进行Arnold置乱，再对DCT后的低频系数进行编码，接着更换置乱参数来构建索引表。选择索引表中与秘密信息相同的编码值所对应的参数构建候选队列，最后筛选出鲁棒性强的参数作为密钥发送给接收方。实验结果表明，该方法与现有方法相比大大提高了嵌入容量，拥有更强的抗JPEG压缩性能。并且减少了传输负载，算法简捷，具有较强的应用价值。

关键词：Arnold置乱；DCT编码；低频系数；鲁棒性筛选；无载体信息隐藏

中图分类号：TP391 **文献标识码**：A **文章编号**：1005-0086(2022)10-1094-09

A carrier free information hiding method based on Arnold scrambling and DCT coding

GUO Chenfei, ZHANG Chunyu*, GOU Peidong, LIU Hailun, SHAN Liying, WU Xiuqi

(School of Information Engineering, Xizangminzu University, Xianyang, Shaanxi 712082, China)

Abstract: In recent years, search mapping carrier free information hiding is very popular. Although it has certain robustness, it has low hiding capacity, large transmission load and high algorithm complexity. To solve the above problems, this paper proposes a carrier free information hiding method based on Arnold scrambling and discrete cosine transform (DCT) coding. The algorithm first completes Arnold scrambling of the pictures, then encodes the low-frequency coefficients after DCT, and then changes the scrambling parameters to build the index table. The algorithm selects the parameters corresponding to the same coding value as the secret information in the index table to build a candidate queue, and finally filters out the parameters with strong robustness and send them to the receiver as a key. Experimental results show that compared with the existing methods, this method greatly improves the embedding capacity and has stronger anti JPEG compression performance. The algorithm reduces transmission load, is simple and has strong application value.

Key words: Arnold scrambling; DCT coding; low frequency coefficient; robustness screening; carrier free information hiding

1 引 言

互联网时代，信息安全至关重要，信息隐藏作为信息安全的分支也备受关注。信息隐藏技术是一种将数据嵌入数字媒体以保护版权或秘密通信的技术[1]。近些年来针对传统信息隐藏的隐写分析层出不穷，传统信息隐藏在嵌入秘密信息时均对载体进行修改，很难抵抗隐写分析，因此无载体

* E-mail：zcy@xzmu.edu.cn

收稿日期：2022-01-01 修订日期：2022-03-07

基金项目：国家自然科学基金(62262022)、西藏自治区自然科学基金重点项目(2016ZR-MZ-01)、大学生创新创业训练项目和基于藏传佛教纹饰符号构造纹理的信息隐藏方法(202110695027)资助项目

信息隐藏思想被提出[2]。无载体信息隐藏不是没有载体,而是在嵌入秘密的时候不需要对载体进行任何修改。

无载体信息隐藏近年来成为新的研究热点,其主要分为生成式和基于关系映射的搜索式两大类[3]。生成式包括纹理构造式、纹理合成式和基于生成对抗网络(generative adversarial networks,GAN)等方法。纹理构造式是将秘密信息放在白纸上,再添加干扰元素,最后使用可逆变换生成非自然纹理图案对秘密信息进行掩盖[4-7]。纹理合成式是在源纹理图片合成大块纹理图片的过程中进行信息隐藏。纹理合成式信息隐藏主要分为逐像素点合成的信息隐藏[8-9]和基于块拼接式的信息隐藏[10-12]。基于 GAN 的方法是将秘密信息作为模型的输入,然后生成载体图像[13-15]。

基于关系映射的搜索式信息隐藏是先建立载体特征与秘密信息的关系映射,然后再根据秘密信息选择发送相应的载体,接收方根据特征映射关系和接收到的载体来提取秘密信息。2015 年,周等[16]提出了一种新的隐写框架。首先采集大量的图片构成数据库,接着生成哈希序列对这些图片进行索引。然后将秘密信息分成段,从数据库中选取哈希序列与秘密信息段相同的图像作为隐藏图像。周志立等[17]提出一种基于 BOW(bag-of-words)模型的无载体信息隐藏方法。利用 BOW 模型提取图片中的视觉关键词,构建图片视觉关键词与文本信息的关键词的映射关系库。根据待隐藏的文本信息选择相应的图片作为隐藏图片。为了提高容量、鲁棒性,ZHENG 等[18]利用尺度不变特征变换(scale-invariant feature transform,SIFT)特征点的方向信息,设计了一种高效稳定的图像哈希算法。为了提高哈希系统的检索和匹配效率,使用了一种四叉树结构的倒排序索引。ZHOU 等[19]将自然图像数据库中的图片划分成若干不重叠的子图片,提取子图片的特征值并建立索引,在数据库中搜索秘密图片的子图片来获得隐写图片。该方法的秘密信息只能为图片形式。ZOU[20]等提出一种基于子图像平均像素值的方法。构建关系映射和哈希数组,建立多级索引结构来有效检索。为了提高搜索式无载体信息隐藏的安全性和鲁棒性,ZHANG[21]等提出了一种基于离散余弦变换(discrete cosine transform,DCT)和潜在狄利克雷分配(latent Dirichlet allocation,LDA)主题分类的无载体信息隐藏,传送同一主题的图片来提高安全性,对图片进行 DCT 变换,使用相邻块之间直流系数的关系生成鲁棒性序列。WU[22]等提出了一种基于灰度梯度共生矩阵的方法。利用灰度梯度共生矩阵对图像进行编码,能较好抵抗 JPEG 压缩攻击和低通滤波攻击。LIU 等[23]提出一种基于 DenseNet 特征图像检索和离散小波变换(discrete wavelet transform,DWT)序列映射的方法。使用 DenseNet 卷积神经网络模型提取图像数据集特征,采用监督学习方法对图像进行检索,并且对图像进行分块,使用块变换后的低频分量计算 DWT 系数来生成鲁棒特征序列。ZHOU 等[24]提出了一种基于快速区域卷积神经网络(faster region-based convolutional neural network,Faster-RCNN)的无载体信息隐藏方法,利用 Faster-RCNN 来检测和定位图像中的物体,使用这些物体的标签来表达秘密信息。为了解决图像库建立困难、传输图片开销大的问题,王亚宁等[25]提出一种面向无载体信息隐藏的映射关系智能搜索方法。从已有的图像库出发,自动搜索一套高容量、高覆盖率的映射关系。为了提高隐藏容量和隐藏成功率,谭云等[26]提出了一种基于图像混沌块置乱和 DWT 变换的方法,对载体图像进行置乱生成多张新图片,再进行分块 DWT 变换,使用相邻块的 DWT 系数关系来生成对应的哈希序列。

当前的搜索式无载体信息隐藏方法,隐藏容量小,且需要大量的图片来建立图像库。在传递秘密信息时需要发送大量的图片,传输负载巨大且增大了被检测的风险。此类算法鲁棒性较好,但抗 JPEG 压缩能力不强,在提取秘密时误码率并不乐观。基于这些问题,本文提出了一种基于 Arnold 置乱和 DCT 编码的无载体信息隐藏方法。首先对图像进行 Arnold 置乱,然后对其进行 DCT 变换,使用 DCT 低频系数对其进行编码,改变置乱参数构建编码值与参数的索引表。在隐藏秘密信息时进行鲁棒性筛选得到最佳参数并将其作为密钥发送给接收方。实验结果表明,该方法与现有典型算法相比大大提高了嵌入容量,不需要建立图像库,只需要传输一张图片即可,减小了传输负载,提高了安全性。在抵抗 JPEG 压缩方面性能尤为显著,有更强的应用价值。

2　Arnold 置乱和 DCT 低频系数编码

2.1　Arnold 置乱

Arnold 变换是俄国数学家弗拉基米尔·阿诺德(Vladimir Igorevich Arnold)在遍历理论的研究中提出的一种裁剪变换。Arnold 变换可以把图像中的像素点位置进行置换,因此在图像置乱和图像加密中应用广泛。狭义的 Arnold 变换公式和广义的 Arnold 变换公式分别如式(1)和(2)所示:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod(N), \tag{1}$$

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod(N), \tag{2}$$

式中，(x_n, y_n)是原图像中像素点的位置坐标，(x_{n+1}, y_{n+1})是变换后该像素点对应的坐标，mod 为取模运算，参数 a，b 为正整数，N 为数字图像矩阵的阶数。狭义的 Arnold 变换还具有周期性，其周期性与图像的尺寸有关。几种大小为 $N\times N$ 的图像的二维 Arnold 变换周期如表 1 所示。

表 1　二维图像的 Arnold 变换周期

Tab. 1　Arnold transformation period of two-dimensional image

n	4	8	10	16	24	32	40	48	64	128	256	512
Period	3	6	30	12	12	24	30	12	48	96	192	384

对于 $N\times N$ 的图像，广义的 Arnold 变换没有周期，因此在该算法中置乱次数在 $1-N$ 之间选取即可。

2.2　DCT 低频系数编码方案

DCT 变换是与傅里叶变换相关的一种变换，在信号处理和图像处理的方面应用广泛，主要应用于信号和图像的有损压缩。二维 DCT 的变换公式如式(3)和式(4)所示：

$$T(u,v) = \sum_{x=0}^{n-1}\sum_{y=0}^{n-1} f(x,y)\alpha(u)\alpha(v) \cos\left(\frac{(2x+1)\pi u}{2n}\right)\cos\left(\frac{(2x+1)\pi v}{2n}\right), \tag{3}$$

$$\alpha(u) = \begin{cases} \sqrt{\dfrac{1}{n}}, u = 0 \\ \sqrt{\dfrac{2}{n}}, u \neq 0 \end{cases}, \tag{4}$$

式中，$f(x,y)$为图像中的像素值，$x, y = 0, 1, 2\cdots, N-1$，$T(u,v)$为计算后得到的变换域矩阵，$u, v = 0, 1, 2\cdots, N-1$，$n$ 为块长度，实际中常采用 8×8 的子块，故 n 一般为 8。

本文算法使用 DCT 变换后的低频系数来编码。先将图片分成 8×8 的小块，然后进行 DCT 变换得到低频系数，最后利用与直流分量最近的 8 个低频系数(Z 形扫描)的正负进行编码。当低频系数大于 0 时，表示 1，否则表示 0。编码示例如图 1 所示。

图 1 中左边的矩阵为 Lenna 灰度图像左上角 8×8 的像素块，右边的矩阵为经过 DCT 变换后的矩阵。黑色边框内是以 Zigzag 扫描顺序选取的 8 位低频系数，对其进行编码，结果如表 2 所示。

$$\begin{bmatrix} 34 & 34 & 34 & 33 & 34 & 28 & 35 & 32 \\ 34 & 34 & 34 & 33 & 34 & 28 & 35 & 32 \\ 34 & 34 & 34 & 33 & 34 & 28 & 35 & 32 \\ 34 & 34 & 34 & 33 & 34 & 28 & 35 & 32 \\ 34 & 34 & 34 & 33 & 34 & 28 & 35 & 32 \\ 36 & 36 & 29 & 27 & 33 & 31 & 30 & 31 \\ 32 & 32 & 25 & 30 & 32 & 33 & 31 & 27 \\ 30 & 30 & 27 & 28 & 30 & 30 & 28 & 29 \end{bmatrix} \xrightarrow{\text{DCT}} \begin{bmatrix} 257.1 & 6.4 & 2.5 & -0.3 & 0.4 & 0.1 & -6.0 & 6.9 \\ 8.4 & 0.0 & 0.5 & -5.0 & 1.9 & 3.4 & -4.2 & 3.3 \\ -5.3 & -1.0 & -1.4 & 1.3 & -0.7 & -0.5 & 2.1 & -1.7 \\ 2.4 & 1.7 & 1.5 & 1.5 & -0.6 & -1.5 & 0.2 & 0.4 \\ -1.1 & -1.6 & -0.2 & -1.8 & 1.6 & 1.2 & -1.4 & -0.1 \\ 1.4 & 0.9 & -1.9 & -0.1 & -2.0 & 0.9 & 1.5 & 0.7 \\ -2.0 & -0.1 & 3.1 & 2.0 & 1.8 & -2.7 & -0.9 & -1.3 \\ 1.5 & -0.2 & -2.3 & -1.9 & -1.0 & 2.3 & 0.3 & 1.1 \end{bmatrix}$$

图 1　经过 DCT 变换后的矩阵

Fig. 1　Matrix after DCT transformation

表 2　低频系数对应的编码

Tab. 2　Codes corresponding to low frequency coefficients

Low frequency coefficient	6.4	8.4	−5.3	0.0	2.5	−0.3	0.5	−1.0
Corresponding code	1	1	0	0	1	0	1	0

3　提出的算法

本文提出了一种基于 Arnold 置乱和 DCT 编码的无载体信息隐藏方法。该方法首先选择一张载体图片，将其转换为灰度图，接着对图片进行 Arnold 置乱。将置乱后的图片分成 8×8 的小块，接着对每一个小块进行 DCT 变换。对变换后的每一个小块按照第 2 节的编码方案进行编码，然后更改置乱参数和置乱次数，构建参数与每一个小块的对应编码值的索引表。在隐藏信息的时候，对秘密信息进行分段处理，将索引表中所有对应该秘密信息的参数放在一个候选队列里，对该候选队列里的所有参数进行鲁棒性筛选。将最佳参数作为密钥和载体图片一起发送给接收方。

在提取秘密信息的时候，根据对应的参数进行相应的 Arnold 置乱，再将置乱后的图片分成 8×8 的小块，接着进行 DCT 变换，最后解码得到秘密信息。算法流程如图 2 所示。

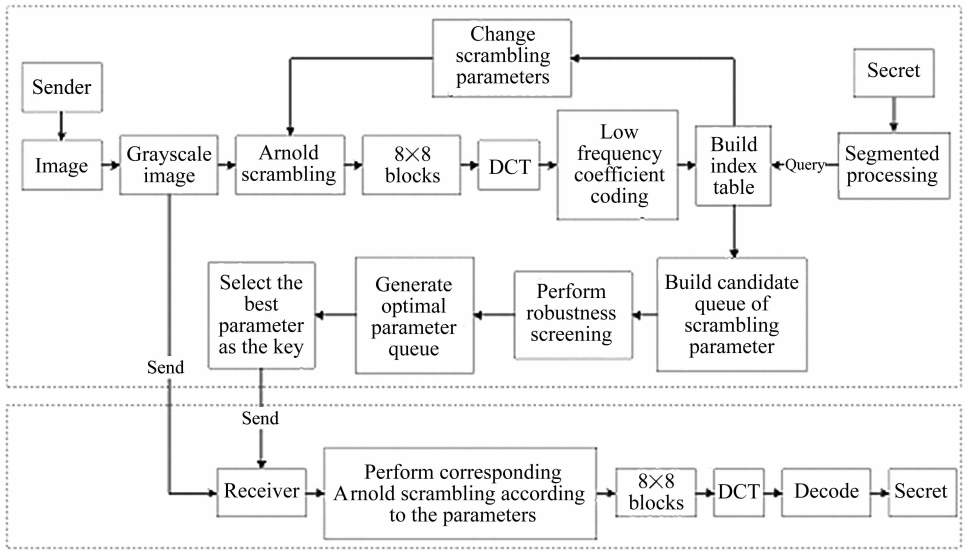

图 2　算法流程

Fig. 2　Algorithm flow

3.1　隐写算法

本节以 64×64 大小的图片,每个小块隐藏 7 位为例来说明,具体的隐写算法步骤如下:

Step1　选取一张载体图片,将其大小调整为 64×64 大小的图片,再转换成灰度图;

Step2　对图片进行参数为 a,b,N 的 Arnold 置乱;

Step3　将置乱后的图片分成 64 个 8×8 的小块,如图 3 所示,接着进行 DCT 变换得到低频系数,每一个小块都使用第 2 节的方法进行编码;

Step4　改变置乱参数和次数,其中参数 a,b 取值区间为[1,14],置乱次数 N 的取值区间为[1,64]。重复步骤 2 和步骤 3 来构建 a,b 和 N 与每一个小块的对应编码值的索引表,即不同的 a,b,N 对应着索引表的编码值 0000000 到 1111111。索引表中会有多个 a,b,N 对应着同一个编码值;

Step5　对要嵌入的二进制秘密信息进行分段处理,每 7 位分成一段;

Step6 在索引表中找到与一段秘密信息相等的编码值,将其对应的所有 a,b,N 放在一个候选队列里面;

Step7　对候选队列里的 a,b,N 进行鲁棒性筛选,得到最佳参数 a,b,N;

Step8　重复步骤 6 和步骤 7,得到每一段秘密信息对应的最佳参数 a,b,N,将其作为密钥,一共 64 组;

Step9　将载体图片和密钥发送给接收方。

鲁棒性筛选先将载体图片进行质量因子为 10,30,50,70,90 的 JPEG 压缩,接着使用候选队列里的参数 a,b,N 对压缩后的图片分别进行相应的置乱,再分别进行 DCT 变换并进行编码,如果编码值与秘密信息相等,则说明该参数 a,b,N 对应的置乱方式可以抵抗该质量因子的 JPEG 压缩,选择可以同时抵抗质量因子为 10,30,50,70,90 的参数并将其放入最佳参数队列里;反之,放弃该参数。最后在最佳参数队列里面任选一个参数作为最佳参数。

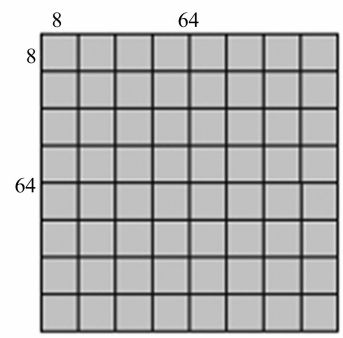

图 3　图片分块示意图

Fig. 3　Schematic diagram of picture blocking

3.2　提取算法

提取算法的过程如下:

Step1　根据得到的参数 a,b,N 对图片进行相应的 Arnold 置乱;

Step2　将置乱后的图片分成 64 个 8×8 的小块,再进行 DCT 变换,使用第 2 节的方法进行解码;

Step3　更换得到的参数 a,b,N,重复步骤 2 和步骤 3,得到每一个小块所表示的编码;

Step4　将所有编码进行合并得到秘密信息。

4　实验结果与分析

4.1　信息隐藏容量

每一张图片隐藏的相对容量与其图片大小和可隐藏的信息位数相关。该方法的信息隐藏位数与 8×8 小块的数目和每一个 8×8 小块可以表示的秘密信息位数相关。本文使用 bbp(bit per pixel)来计算相对隐藏容量 C。计算公式如下:

$$C=\frac{K\times L}{W\times H},\tag{5}$$

式中,W 为图片的宽度,H 为图片的高度,L 为 8×8 的小块数目,K 为每一个 8×8 小块可以表示的秘密信息位数。K 的取值与参数有关,参数 a,b 的取值区间不同,每张图片所能表示的位数也不同,为了得到 K 值,本文从 256_ObjectCategories 数据集中随机选取了 300 张图片,并将所有的图片大小进行修改,以 48×48 图片为例进行测试。测试结果如图 4 所示。

从图 4 可以看出,当 a,b 最大取值为 1 时,可以表示 1 位的图片数量最多;当 a,b 最大取值为[2, 3]时,可以表示 2 位的图片数量最多;当 a,b 最大取值为4时,可以表示4位的图片数量最多;当a,b最大取值为[5,7]时,可以表示5位的图片数量最多;当 a,b 最大取值为[8,13]时,可以表示 6 位的图片数量最多;当 a,b 最大取值为[14,21]时,可以表示 7 位的图片数量最多。

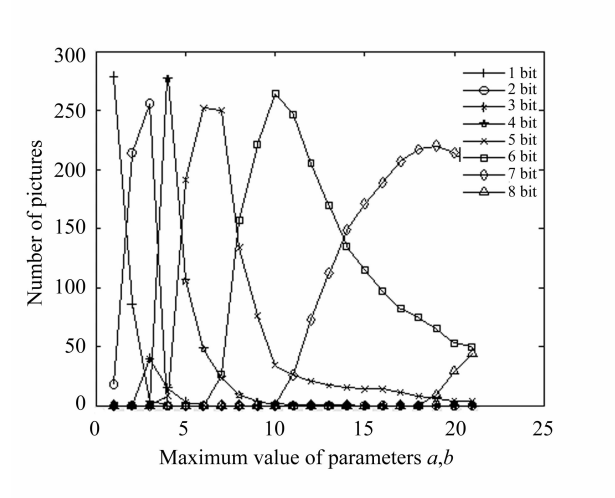

图 4　参数 a,b 的取值区间与图片数量的关系

Fig. 4　Relationship between the value range of parameters a and b and the number of pictures

在实验中,虽然随着参数取值区间的增加,每个图片可以表示的位数也在增加,但是建立索引表所需的时间也在增加,即算法复杂度也在上升。因此在本文中选取参数 a,$b\in[1,8]$的 48×48 的图片和参数 a,$b\in[1,14]$的 64×64 的图片为例进行测试。测试结果如图 5 所示。

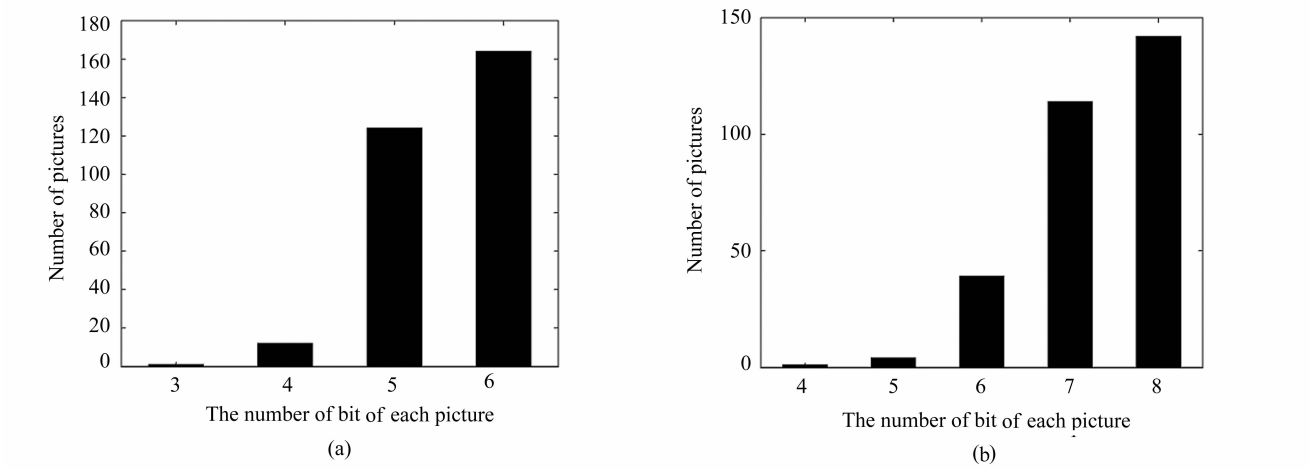

图 5　表示不同位数的图片数量:(a) 48×48 的图片;(b) 64×64 的图片

Fig. 5　The number of pictures with different bits: (a) 48×48 pictures; (b) 64×64 pictures

图 5(a),(b)分别为 48×48 和 64×64 的图片测试结果,可以看出:对于大多数 48×48 图片都可以表示 5 位或 6 位,只有个别图片只能表示 3 位或 4 位;对于大多数 64×64 图片都可以表示 7 位或 8 位,只有个别图片只能表示 4 位或 5 位。

当使用 64×64 的图片时,K 为 8,L 为 64。该方法与其他几种方法的容量对比如表 3 所示。

表 3　信息隐藏容量对比表

Tab. 3　Comparison of information hiding capacity

Method	Hidden digits /bits	Picture size /pixel	Relative capacity/ (bit/pixel)
Pixel[16]	8	512×512	3.82×10^{-5}
SIFT_BOF[19]	8	512×512	3.05×10^{-5}
DCT_LDA[21]	15	512×512	5.7×10^{-5}
DenseNet_DWT[23]	8	128×128	4.88×10^{-4}
O_GAN[15]	300	64×64	7.32×10^{-2}
LSS_DWT[26]	4 608	512×512	1.76×10^{-2}
The algorithm	8×64	64×64	1.25×10^{-1}

4.2　信息隐藏成功率

该算法在最佳参数选择的时候进行了鲁棒性筛选。在筛选的时候有可能会出现没有一个参数能够同时抵抗质量因子为 10,30,50,70,90 的 JPEG 压缩的情况。对于这种情况,本文放弃在该块隐藏信息。为了统计该情况出现的概率,使用信息隐藏成功率来衡量。假设一张图片能够通过鲁棒性筛选的块数为 B_K,该图片一共可以分成 B 块,那么信息隐藏成功率 S 为:

$$S=\frac{B_{\mathrm{K}}}{B}。\tag{6}$$

本文从 256_Object Categories 数据集中选择了 100 张图片,并将所有的图片大小进行修改,以 48×48 和 64×64 的图片为例进行测试。对于 48×48 的图片,以每个块隐藏 6 位为例进行鲁棒性筛选测试。对于 64×64 的图片,以每个块隐藏 7 位为例进行鲁棒性筛选测试。测试结果如图 6 所示。

图 6 中(a),(b)分别为 48×48 和 64×64 的图片测试结果,其中虚线为所有图片的平均隐藏成功率,可以看到图(a)中平均隐藏成功率 93%左右,图(b)中平均隐藏成功率已经超过 99%,即在鲁棒性筛选的时候基本上都可以找对应的参数,不能通过鲁棒性筛选的块只是极个别情况。

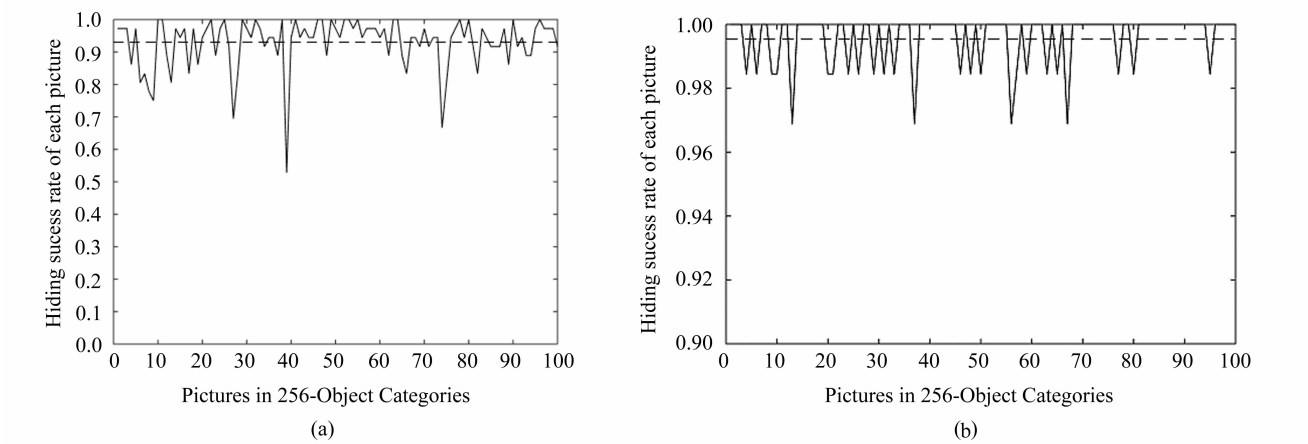

图 6　信息隐藏成功率:(a) 48×48 的图片; (b) 64×64 的图片

Fig. 6　Success rate of information hiding: (a) 48×48 picture; (b) 64×64 picture

4.3　鲁棒性测试

鲁棒性是信息隐藏中的一个重要评价指标。本文在 256_Object Categories 数据集中选取了 100 张图片,并对图片大小调整。以 64×64 的图片为例测试了算法在噪声、滤波和裁剪等攻击下的鲁棒性。使用错误率 BER 来作为衡量标准,错误率 BER 表示如下:

$$BER=\frac{P_{\mathrm{E}}}{P},\tag{7}$$

式中,P_{E} 为提取秘密信息错误的块数,P 为所有用来表示秘密信息的块数。

由于该算法进行了鲁棒性筛选,故可以抵抗质量因子为 10,30,50,70,90 的 JPEG 压缩。将该算法的测试结果与其他方法进行比较,结果如表 4 所示。

从表中可见,该方法与其他算法相比,抵抗 JPEG 压缩攻击能力尤为显著。在抵抗椒盐噪声、中心裁剪和边缘裁剪等攻击方面的性能优于其他算法。

表4 不同无载体方法的提取错误率(%)

Tab. 4 Extraction error rate of different carrier free methods(%)

Project	Parameter	DCT_LDA[21]	DenseNet_DWT[23]	LSS_DWT[26]	The algorithm
JPEG compression	Q=10	15.00	13.70	9.60	0.00
	Q=30	9.00	8.50	6.20	0.00
	Q=50	8.70	5.00	11.80	0.00
	Q=70	5.20	5.50	0.40	0.00
	Q=90	1.50	1.50	9.00	0.00
Gaussian white noise	0.001	29.50	22.40	15.6	50.39
Salt and pepper noise	0.001	19.50	18.00	9.00	1.72
Gaussian low-pass filtering	[3 3]	0.70	1.50	3.2	8.05
Center clipping	20%	95.7	95.7	69.00	41.88
Edge cutting	20%	76.5	75.7	88.8	65.16

4.4 算法复杂度分析

本文从时间复杂度和空间复杂度的角度来对该算法的复杂度进行分析，并对 LSS_DWT[26] 的方法按其所述进行了复现，与该方法进行了对比。实验环境为：Intel(R) Core(TM) i7-7700 CPU @ 3.60 GHz，16.00 GB RAM。使用的软件为 Matlab2018a。

4.4.1 时间复杂度分析

本文算法的时间复杂度与图片的大小、参数的选取以及每个小块所表示的位数相关。以参数 a，b [1，8]，每个小块表示 6 位为例，与 LSS_DWT[26] 算法的复杂度进行对比。两种方法建立索引表的伪代码如下所示：

算法 1 Arnold_ DCT($n\times n$)

输入 image

输出 Index table

1. for a=1：8

2. for b=1：8

3. for N=1：48//1，2，3 的复杂度为 8×8×48

4. Arnold_image＝Arnold(image)//Arnold 变换，复杂度为 $n\times n$

5. DCT_image＝dct2(Arnold_image)//dct 变换，复杂度为 $n\times\log2^n$

6. Index_table(a，b，N)＝encoded(DCT_image)//dct 编码，复杂度为 $(n/8)^2\times6$

7. end

8. end

9. end

算法 2 LSS_DWT[26]($n\times n$)

输入 image1，image2…image$N$

输出 Index table

1. for i=1：N//复杂度为 30

2. for j=1：W//复杂度为 24×24

3. Scrambled_image＝scrambling(image(i))//进行混沌块置乱，复杂度为 $n\times n$

4. Blocked_image＝block(Scrambled_image)//分块，复杂度为 $n\times n$

5. cA1＝dwt2(Blocked_image)//dwt 变换，复杂度为 $n\times\log2^n$

6. Average_ cA1＝average(cA1)//求 dwt 低频系数的平均值，复杂度为 $n\times n$

7. Index_table(i，j)＝encoded(Average_cA1)//对 dwt 低频系数的平均值进行排序编码，复杂度为 9

8. end

9. end

上面伪代码中 $n\times n$ 为图片大小，Arnold 置乱和块置乱对图片中的每一个像素进行操作，故其复杂度为 $n\times n$。dct2 和 dwt2 的复杂度为 $n\times\log2^n$。Arnold_DCT 算法中可以分成 $(n/8)^2$ 个小块，其中每个小块表示 6 位，故复杂度为 $(n/8)^2\times6$。LSS_DWT 中将 9 个块的平均值进行比较再编码，故复杂度为 9。LSS_DWT[26] 中 N 为建成索引表所需的图片数，W 为经过置乱可以生成的新图片数（该文献中 M＝4）。故两种算法建立索引表的复杂度分

别为:

$$\text{Arnold\_DCT} = 8\times 8\times 48(n\times n+n\times \log 2^n+(n/8)^2\times 6) = 3\,360\times n^2+3072n\log 2^n。\quad (8)$$

$$\text{LSS\_DWT} = 30\times 24\times 24(n\times n+n\times n+n\times \log 2^n+n\times n+9) = 51\,840\times n^2+17\,280\times n\times \log 2^n+155\,520。\quad (9)$$

图 7 为两种算法建立索引表的复杂度对比,可以看出该算法远远小于 LSS_DWT[26]。本文还选取了不同大小的图片和参数进行了测试。对于 64×64 的图片,a,b 分别取 1−10,N 取 64,每个小块表示 7 位;对于 48×48 的图片,a,b 分别取 1−8,N 取 64,每个小块表示 6 位。对于 LSS_DWT[26] 的方法,在 256_Object Categories 数据集中随机选取了 300 张图片,将其大小修改成 512×512 进行测试,并与本文方法进行比较。测试结果如表 5 所示。

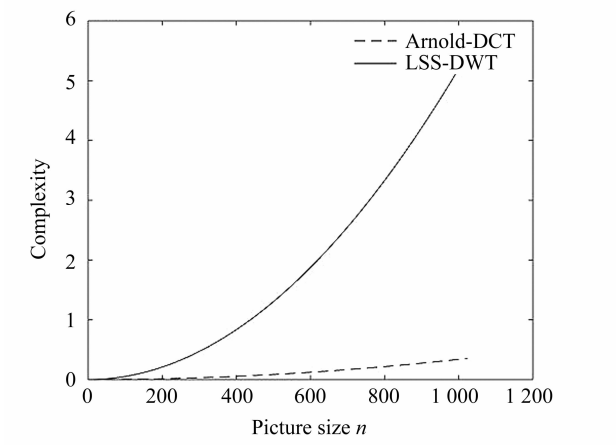

图 7　复杂度对比

Fig. 7　Complexity comparison

表 5　算法耗时对比表

Tab. 5　Comparison of algorithm time consumption

Method	LSS_DWT[26]	The algorithm	
		64×64	48×48
Average time consumption/s	218.49	109.89	34.5

LSS_DWT[26] 算法的主要耗时在构建索引表上。测试中有时仅需 30 张图片就可以完成索引表的构建,但有时需要 90 张。对于我们的算法,当图片大小为 48×48 时,索引表的构建仅需 6 s 左右,其主要耗时在鲁棒性筛选上。从表 5 可以看出,随着图片和参数减小,该方法的平均耗时也越来越少,与 LSS_DWT[26] 相比,本文算法的耗时更少。对于 O_GAN[15]、王亚宁等[25] 的算法,使用神经网络模型来训练构建索引表,也需要消耗大量时间。其中 O_GAN[15] 方法的模型训练时间需要两天才能完成。因此,本文提出的算法更加快速简捷。

4.4.2　空间复杂度分析

基于特征映射的无载体信息隐藏都需要建立图像库,对于不同的算法,映射相同的比特时所需要的图片数也不一样。如要表示 N 位秘密信息,那么至少需要 2^N 张图片来建立一个图像库。由于会出现不同图片表示相同的秘密信息和出现某些秘密信息很难找到对应的图片问题,因此图像库的大小远远大于 2^N。所以图像库的构建往往比较困难,有时会因为索引表的个别编码找不到对应图片,而花费大量时间去寻找能映射该编码的图片。

当 N 取 8 位的时候,LSS_DWT[26] 算法使用 50 张载体图片可以映射 95% 的秘密信息。王亚宁等[25] 的方法也需要 256 张图片才能映射到所有编码。文中方法只需要 1 张图片即可,不需要再建立图像库,并且不需要浪费空间去存储大量的图片,因此该方法的空间复杂度小。在发送秘密信息的时候也不需要去发送大量的图片,其被检测的安全性也大大提高。

5　结　论

该文章提出一种基于 Arnold 置乱和 DCT 编码的无载体信息隐藏。使用 Arnold 置乱的方式和 DCT 低频系数正负来编码的方法相结合使得一张图片能够映射更多的信息,从而避免去建立一个图像库,达到减小图片数量的目的,大大减小了传输负载,降低了被检测的风险,提高了安全性并且增加了信息隐藏容量。使用鲁棒性筛选的方法,选择出能够抵抗 JPEG 压缩的参数,来增强该方法的抗干扰能力。对于噪声和滤波等攻击有着不错的抵抗能力。该方法操作简单,算法复杂度低,具有很强的实用价值。

参考文献:

[1] ZHANG X. Reversible data hiding with optimal value transfer[J]. IEEE Transactions on Multimedia, 2013, 15(2):316-325.

[2] SHI Y Q, CHEN C H, CHEN W. A Markov process based approach to effective attacking JPEG steganography [C]//Information Hiding, July 10-12, 2006, Alexandria, VA, USA. Berlin, Heidelberg: Springer-Verlag, 2006: 249-264.

[3] LI G L, SHAO L P, REN P A. Generative information hiding based on difference clustering and error texture synthesis [J]. Chinese Journal of Image and Graphics, 2019, 24(12):2126-2148.

李国利，邵利平，任平安. 差异聚类和误差纹理合成的生成式信息隐藏[J]. 中国图象图形学报，2019，24(12)：2126-2148.

[4] XU J Y，MAO X Y，JIN X G，et al. Stego-marbling-texture [C]//2013 International Conferenceon Computer-Aided Design and Computer Graphics，November 16-18，2013 Guangzhou，China. New York：IEEE，2013：236-243.

[5] XU J Y，MAO X Y，JIN X G，et al. Hidden message in a deformation-based texture[J]. The Visual Computer，2015，31(12)：1653-1669.

[6] PAN L，QIAN Z X，ZHANG X P. Digital steganography based on texture image[J]. Journal of Applied Science，2016，34(5)：625-632.
潘琳，钱振兴，张新鹏. 基于构造纹理图像的数字隐写[J]. 应用科学学报，2016，34(5)：625-632.

[7] QIAN Z X，PAN L，LI S，et al. Steganography by constructing marbling texture [C]//International Conference on Cloud Computing and Security，June 8-10，2018，Haikou，China. Berlin，Heidelberg：Springer-Verlag，2018：428-439.

[8] OTORI H，SHIGERU K. Texture synthesis for mobile data communications[J]. IEEE Computer Graphics and Applications，2009，29(6)：74-81.

[9] ZHAO Y，SHAO L P. Generative information hiding based on pixel by pixel texture synthesis[J]. Journal of Optoelectronics · Laser，2020，31(3)：334-344.
赵艺，邵利平. 逐像素纹理合成的生成式信息隐藏[J]. 光电子 · 激光，2020，31(3)：334-344.

[10] WU K C，WANG C M. Steganography using reversible texture synthesis [J]. IEEE Transactions on Image Processing，2015，24(1)：130-139.

[11] QIAN Z X，ZHOU H，ZHANG W M，et al. Robust steganography using texture synthesis[C]//Advances in Intelligent Information Hiding and Multimedia Signal Processing，November 21-23，2016，Kaohsiung，Taiwan. Berlin，Heidelberg：Springer-Verlag，2017：25-33.

[12] WEI W Y，WANG Y，A C F. A carrier free information hiding method for texture synthesis based on LBP[J]. Computer Engineering and Science，2019，41(11)：1961-1967.
魏伟一，王瑜，阿成凤. 一种基于 LBP 的纹理合成无载体信息隐藏方法[J]. 计算机工程与科学，2019，41(11)：1961-1967.

[13] LIU M M，ZHANG M Q，LIU J，et al. Carrier free information hiding based on generative countermeasure network [J]. Journal of Applied Science，2018，36(2)：371-382.
刘明明，张敏情，刘佳，等. 基于生成对抗网络的无载体信息隐藏[J]. 应用科学学报，2018，36(2)：371-382.

[14] CUI Q，ZHOU Z L，FU Z J，et al. Image steganography based on foreground object generation by generative adversarial networks in mobile edge computing with internet of things[J]. IEEE Access，2019，7：90815-90824.

[15] ZHU Y M，CHEN F，HE H J，et al. Orthogonal gan information hiding model driven by secret information[J]. Journal of Applied Science：2019，37(5)：721-732.
朱翌明，陈帆，和红杰，等. 基于秘密信息驱动的正交 GAN 信息隐藏模型[J]. 应用科学学报，2019，37(5)：721-732.

[16] ZHOU Z L，SUN H Y，HARIT R，et al. Coverless image steganography without embedding [C]//International Conference on Cloud Computing and Security，August 13-15，2015，Nanjing，China. Berlin，Heidelberg：Springer-Verlag，2015：123-132.

[17] ZHOU Z L，CAO Y，SUN X M. Carrier free information hiding based on image bag of words model[J]. Journal of Applied Science，2016，34(5)：527-536.
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[J]. 应用科学学报，2016，34(5)：527-536.

[18] ZHENG S L，LIAN G W，LING B H，et al. Coverless information hiding based on robust image hashing[C]//International Conference on Intelligent Computing，August 7-10，2017，Liverpool，UK. Berlin，Heidelberg：Springer-Verlag，2017：536-547.

[19] ZHOU Z L，MU Y，JONATHAN Q M. Coverless image steganography using partial-duplicate image retrieval [J]. Soft Computing：A Fusion of Foundations，Methodologies and Applications，2019，23(13)：4927-4938.

[20] ZOU L M，SUN J D，GAO M，et al. A novel coverless information hiding method based on the average pixel value of the sub-images[J]. Multimedia Tools and Applications，2019，78(7)：7965-7980.

[21] ZHANG X，PENG F，LONG M. Robust coverless image steganography based on DCT and LDA topic classification[J]. IEEE Transactions on Multimedia，2018，20(12)：3223-3238.

[22] WU J B，LIU Y W，DAI Z W，et al. A coverless information hiding algorithm based on grayscale gradient co-occurrence matrix[J]. IETE Technical Review，2018，35(sup1)：23-33.

[23] LIU Q，XIANG X Y，QIN J H，et al. Coverless steganography based on image retrieval of DenseNet features and DWT sequence mapping[J]. Knowledge-Based Systems，2020，192：105375.

[24] ZHOU Z L，CAO Y，WANG M M，et al. Faster-RCNN based robust coverless information hiding system in cloud environment[J]. IEEE Access，2019，7：179891-179897.

[25] WANG Y N，WU B. Mapping relation intelligent search method for carrier free information hiding[J]. Journal of Information Security，2020，5(3)：48-61.
王亚宁，吴槟. 面向无载体信息隐藏的映射关系智能搜索方法[J]. 信息安全学报，2020，5(3)：48-61.

[26] TAN Y，QIN J H，HUANG L X，et al. Research on carrier free information hiding based on image chaotic block scrambling and DWT transform[J]. Data Acquisition and Processing，2021，36(1)：147-155.
谭云，秦姣华，黄丽霞，等. 基于图像混沌块置乱和 DWT 变换的无载体信息隐藏研究[J]. 数据采集与处理，2021，36(1)：147-155.

作者简介：

张春玉 (1979—)，女，硕士，副教授，硕士生导师，主要从事信息安全方面的研究.