

基于图像混沌块置乱和DWT变换的无载体信息隐藏研究

谭云^{1,2}, 秦姣华², 黄丽霞¹, 向旭宇², 刘 强²

(1. 湖南应用技术学院, 常德 415000; 2. 中南林业科技大学计算机与信息工程学院, 长沙 410004)

摘要: 无载体隐写通过提取载体特征, 与信息序列进行映射, 从而无需修改载体即可实现对秘密信息的隐藏, 因此, 具有极强的抗隐写分析能力, 但是已有算法在隐藏容量方面仍然有限, 且大多需要构建大样本图像库。本文提出一种基于混沌块置乱和离散小波变换(Discrete wavelet transform, DWT)的无载体信息隐藏算法, 从密钥中提取混沌变换的相关参数, 对载体图像进行混沌块置乱生成多张新图像, 再对其进行分块DWT变换, 根据相邻图像块低频DWT系数之间的关系生成对应的哈希序列, 并构建相应索引库。将载体图像及密钥发送给接收方, 实现秘密信息的传递。实验表明, 与现有算法相比, 该算法获得了隐藏容量和隐藏成功率的较大提升, 具有较强的鲁棒性。同时, 该算法架构简单, 传输负载小, 具有较强的实用价值。

关键词: 无载体信息隐藏; 混沌映射; 图像置乱; DWT变换

中图分类号: TP309.7 **文献标志码:** A

Coverless Information Hiding Based on Chaotic Scrambling of Image Blocks and DWT Transform

TAN Yun^{1,2}, QIN Jiaohua², HUANG Lixia¹, XIANG Xuyu², LIU Qiang²

(1. Hunan Applied Technology University, Changde 415000, China; 2. College of Computer Science and Information Technology, Central South University of Forestry Technology, Changsha 410004, China)

Abstract: Coverless steganography can hide the secret information without modifying the carrier by extracting the features of the carrier and mapping with the information sequence. Therefore, it has strong ability of anti-steganalysis, but the existing algorithms are still limited in hiding capacity, and most of them need to construct a library with large number of images. In this paper, a coverless steganography algorithm based on image block chaos scrambling and discrete wavelet transform (DWT) is proposed. The parameters of chaos transform are extracted from secret key, and the cover image is scrambled to generate multiple new images. Then, block DWT transform is used to generate the corresponding hash sequence according to the relationship between the low-frequency DWT coefficients of adjacent image blocks, and corresponding index library is constructed. The cover image and secret key are sent to the receiver to realize the transmission of secret information. Experimental results show that compared with the existing algorithms, the proposed algorithm not only has a great improvement on the capacity and success rate of information hiding, but also has strong robustness. At the same time, the algorithm has a simple architecture and small transmission load, which shows strong practical value for application.

Key words: coverless information hiding; chaotic map; image scramble; DWT transform

引 言

传统信息隐藏方法利用人类感官对数字信号的感觉冗余,在载体中嵌入秘密信息,会导致载体特征不同程度的改变,给攻击者留下了破解的漏洞^[1]。无载体信息隐藏无需对载体进行修改,具有极强的抗隐写分析能力,是近年来的研究热点。

目前,无载体信息隐藏的方法主要包括构造生成式和特征映射式两种^[2]。基于构造生成的方法主要包括发送端载体构造和接收端秘密信息构造两种。前者包括纹理合成、基于生成对抗网络(Generative adversarial networks, GAN)等各种载体生成方法。其中,纹理合成方法通过采样原始纹理图像,生成任意大小、与原始图像具有类似局部外观的新纹理图像,在纹理合成过程中对信息进行隐藏^[3-5]。基于GAN的方法则是将秘密信息输入到生成模型中,生成新的图像^[6-7]。通过最大化判别网络区分度,尽可能使生成图像和真实图像无法区分。接收端秘密信息构造方法是从自然图像库中检索与秘密图像相似的补丁块,将其进行组合,从而实现秘密图像近似恢复^[8-9]。

基于特征映射的方法是目前应用最广泛的无载体信息隐藏方法,通过对载体特征进行分析和提取,建立一定的规则使其与秘密信息产生对应关系。在接收端,利用该特征映射关系即可从载体中提取秘密信息。该方法于2015年首次提出^[10],根据生成的鲁棒散列序列建立索引,从图像库中选择哈希序列与秘密信息段相同的图像,将其作为含秘图像传送给接收方,接收方从中提取秘密信息。随后,周志立等^[11]利用词袋(Bag of words, BOW)模型提取图像集中所有图像的视觉关键词(Visual words, VW),并建立隐藏文本信息与VW的映射关系库,利用子图像的VW作为传递秘密信息的载体。Zheng等^[12]使用尺度不变特征变换(Scale invariant feature transform, SIFT)特征点的方向信息来设计图像哈希,并采用二叉树结构的倒排索引,从而获得容量和检索效率的提升。Zou等^[13]提出基于子图像的平均像素值的信息隐藏方法,生成散列序列,再构建映射字典和哈希数组。吴建斌等^[14]提出基于离散余弦变换(Discrete cosine transform, DCT)和混沌序列的零隐藏算法,利用混沌序列对秘密信息进行加密,同时建立DCT系数与已加密的秘密信息的关系文档。文献^[15]利用基于定向梯度直方图(Histogram of oriented gradient, HOG)的散列算法从图像的非重叠块获得散列序列,直接从大规模数据库中选择散列序列等于秘密信息的原始图像,利用其基于HOG哈希算法的直方图作为载体图像。近来,有研究者对图像进行分块DCT^[16]和离散小波变换(Discrete wavelet transform, DWT)^[17]之后,利用相邻块直流系数之间的关系生成鲁棒特征序列,并与秘密信息进行映射,获得了较好的鲁棒特性。通过对图像分块来提高隐藏信息容量,但是分块越小,鲁棒性越差。Meng等^[18]和Zhou等^[19]提出了基于目标检测和关系映射的隐写算法,通过映射目标类型、颜色和秘密信息来实现无载体信息隐藏,获得了安全性和鲁棒性的提升,但是算法复杂度较大。

目前已有研究中,各种无载体信息隐藏方法在隐藏容量方面均有所提高,但仍然难满足实际需求。隐藏容量不够大、需要构建大样本数据库是目前已有算法的两个主要问题。为改善这两个问题,本文提出一种基于混沌块置乱和DWT变换的无载体信息隐藏算法。首先,对载体图像进行混沌块置乱,随后,对置乱后的图像分块进行DWT变换,根据相邻图像块的低频DWT系数之间的关系生成对应的哈希序列,实现秘密信息的隐藏。不同的混沌序列参数可以生成不同的置乱图像,可映射为不同的秘密信息,因此通过设置不同的密钥,每张载体图像可以承载的秘密信息容量获得极大提升。实验结果表明,本文提出的算法方案简单,极大改善了目前已有方案中的信息容量不够和依赖大样本数据库的问题,且具有很好的鲁棒性和隐藏成功率,具有较强的实用价值。

1 相关算法

1.1 混沌映射

混沌系统对初值和控制参数具有很高灵敏度,且具有较好的伪随机性和状态遍历性,因此,被广泛用于信息加密算法中。Zhou等^[20]提出一种集成两个一维混沌映射的混沌系统架构,如基于Logistic映射和Sine映射构成LSS(Logistic-Sine system)系统,结构如图1所示。

图1中, $L(a, X_n)$ 和 $S(b, X_n)$ 分别为Logistic映射和Sine映射,参数分别为 a 和 b , n 为系统迭代次数,mod为模运算,从而使输出数据范围为 $[0, 1]$ 。因此,系统输出函数可以表示为

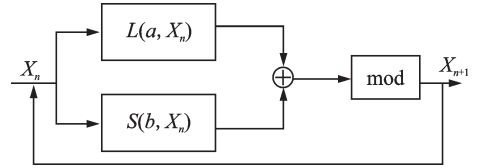


图1 LSS系统架构

Fig.1 Logistic-Sine system architecture

$$X_{n+1} = (L(r, X_n) + S((4-r), X_n)) \bmod 1 = (rX_n(1-X_n) + (4-r)\sin(\pi X_n)/4) \bmod 1 \quad (1)$$

式中: r 为整数且 $r \in (0, 4]$, $\{X_1, X_2, \dots, X_n\}$ 为生成的混沌序列。该LSS系统的混沌行为存在于整个参数设置范围内,其混沌序列在 $[0, 1]$ 范围内均匀分布。由于系统中包含两个种子映射,因此当其中一个种子映射超过混沌范围时,系统依然具有很好的混沌行为。

1.2 图像小波变换

小波变换是基于变换基和小波变换函数的一种变换方法,DWT变换则是通过对连续小波变换的尺度和位移进行离散化得到的,目前已被广泛用于图像处理中。

DWT变换函数为

$$\psi_{j,k}(t) = a_0^{-j/2} \psi(a_0^{-j}t - kb_0) \quad j = 0, \pm 1, \pm 2, \dots; k = 0, \pm 1, \pm 2, \dots \quad (2)$$

式中: $\psi_{j,k}(t)$ 为小波基函数, a_0 和 b_0 为变换因子。对函数 $f(t)$,其离散化变换系数 $c_{j,k}$ 可表示为

$$c_{j,k} = \int_{-\infty}^{\infty} f(t) \psi_{j,k}(t) dt \quad (3)$$

对图像进行DWT分解和变换之后,其高频分量包含图像的细节及边缘特征,低频分量包含图像的主要能量和纹理特征,具有较强的稳定特性和抗干扰性能。因此,可以利用低频分量计算DWT系数为

$$\text{DWT} = \frac{1}{ab} \sum_{x=1}^a \sum_{y=1}^b f(x, y) \quad (4)$$

式中 $f(x, y)$ 为图像变换后的频率分量。

2 基于混沌块置乱的无载体信息隐藏算法

针对现有基于特征映射的无载体信息隐藏方法容量不够、需要构建大样本数据库这两个问题,本文提出一种基于混沌块置乱的无载体信息隐藏算法,具体算法流程如图2所示。对于给定的载体图像,首先将其转换为灰度图,并根据密钥 K 对其进行混沌块置乱。然后,将置乱后的图像分成 J 块,分别进行DWT变换。提取各图像块的低频系数,根据相邻块之间的系数大小关系生成对应的长度为 N 比特的鲁棒哈希序列(图中以 $J=9, N=8$ 为例)。不同密钥值对应不同的置乱方式,生成的哈希序列也不同,因此,需要构建哈希序列与密钥 K 的索引表。当发送方需要进行秘密信息传递时,对秘密信息进行分段预处理之后,在索引表中查询与秘密信息相同的哈希序列所对应的密钥值,将载体图像和密钥值发送给接收方。接收方根据载体图像和密钥即可提取对应的秘密信息。

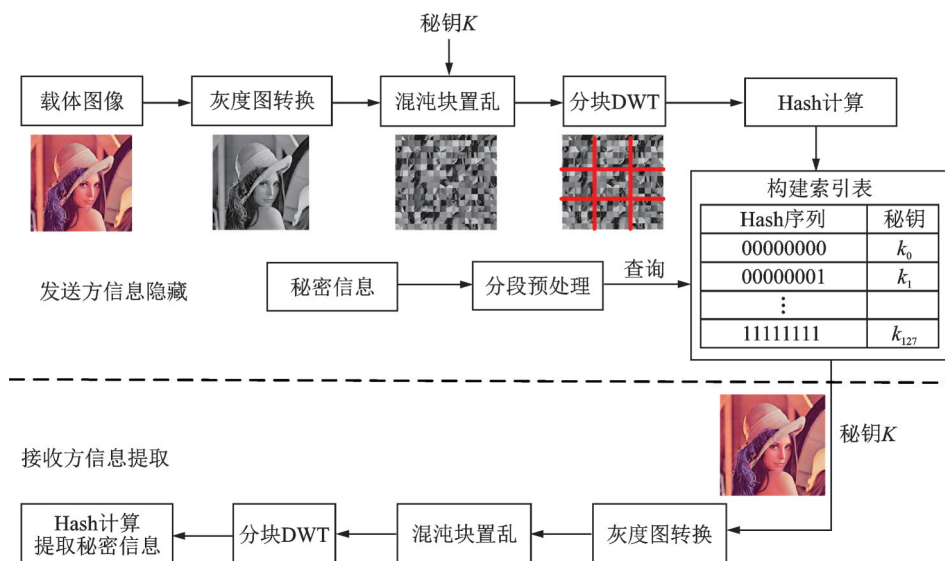


图2 基于图像混沌块置乱的无载体信息隐藏算法

Fig.2 Coverless information hiding based on chaotic scrambling of image blocks

信息隐藏包括以下过程：

(1) 给定载体图像 P_0 , 将其转换成灰度图 P_g 。

(2) 对 P_g 进行混沌块置乱。其中, 混沌系统 LSS 的参数由密钥 K 计算得到^[21]。将密钥 K 转换为 e bit 的二进制数 $b_e b_{e-1} \dots b_1$, 最高 ($e \sim d$) bit 代表映射的各信息段在秘密信息序列中的排列序号, 其余 d 个低比特分别代表混沌映射的各个参数值, 具体含义如图 3 所示。

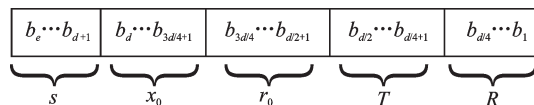


图3 密钥 K 各比特的含义

Fig.3 Meaning of each bit of secret key K

混沌映射参数计算如下

$$x_0 = \sum_{i=1}^{n/4} b_i \times 2^{-i} \tag{5}$$

$$r_0 = \sum_{i=n/4+1}^{n/2} b_i \times 2^{-i-n/4} \tag{6}$$

$$T = \sum_{i=n/2+1}^{3n/4} b_i \times 2^{i-1-n/2} \tag{7}$$

$$R = \sum_{i=3n/4+1}^n b_i \times 2^{-i-3n/4} \tag{8}$$

$$X_0 = (x_0 + R) \times T \bmod 1 \tag{9}$$

$$r = (r_0 + R) \times T \bmod 4 \tag{10}$$

$$s = \sum_{i=d+1}^e b_i \times 2^{i-d-1} \tag{11}$$

式中 s 表示各信息段排列序号, 用于接收端对秘密信息的恢复。具体流程如算法 1 所示。

算法 1 混沌块置乱

输入: 灰度图像 P_g , 密钥 K 。

输出:块置乱图像 P_s 。

(a) 将 P_g 大小调整为512像素 \times 512像素,并将其分成 $M \times M$ 块;

(b) 根据式(5~10),从密钥 K 计算混沌序列的各个参数,并生成混沌序列 $L=LSS(X_0, r)$, L 的长度为 $2M$;

(c) 将 L 分成两个长度为 M 的序列 L_1 和 L_2 ,并分别对其按元素大小排序,生成索引向量 I_1 和 I_2 ;

(d) 由向量 I_1 和 I_2 进行循环内移后,生成置乱矩阵;

(e) 根据置乱矩阵,实现对载体图像 P_g 置乱,生成置乱图像 P_s 。

(3) 将块置乱图像 P_s 分成 J 块,分别对每块图像 p_i 进行DWT变换,采用的小波基为rbio1.1,并取其低频分量

$$LF_i = \text{DWT}(p_i) \quad i \in \{1, 2, \dots, J\} \quad (12)$$

(4) 计算各图像块的低频分量的系数平均值 d_i 。

(5) 根据相邻块 d_i 值的大小关系,生成鲁棒哈希序列 $h_1 h_2, \dots, h_N$ 。

$$h_i = \begin{cases} 0 & d_{i+1} < d_i \\ 1 & d_{i+1} \geq d_i \end{cases} \quad i = \{1, 2, \dots, N\} \quad (13)$$

(6) 修改密钥 K ,重复步骤(1~5),构建索引表,不同的哈希序列对应不同的密钥 K 值。

(7) 对秘密信息进行预处理,将其分成每 N bit为一段,不足 N 比特时在序列尾部填充“0”。针对每一段 N bit序列,从索引表中查询其对应 K 值。

(8) 将载体图像及密钥 K 发送给秘密信息接收方。

(9) 秘密信息接收方根据步骤(1~5)进行各秘密信息段的提取,同时,根据式(11)可从密钥 K 计算各信息段的排列序号,从而成功恢复完整的秘密信息。

3 性能测试

本文从信息隐藏容量、隐藏成功率、算法鲁棒性及计算效率4个方面对算法进行了性能测试和分析,并复现了现有的基于像素(Pixel-based)计算的算法^[10]、基于SIFT特征哈希(Hash-based)^[12]的算法、基于DCT变换(DCT-based)的算法^[16]和基于DWT变换(DWT-based)的算法^[17],与本文算法进行了性能对比。

测试中的实验环境为: Intel(R) Core(TM) i7-6500CPU@2.50 GHz, 16.00 GB RAM, 采用的软件是 Matlab2018 和 MySQL Workbench6.3。

3.1 信息隐藏容量分析

容量问题是目前无载体信息隐藏算法的主要问题,目前已有的基于特征映射的算法大多是将一张图像映射到一个信息序列,因此信息序列的长度 N 越大,对应的隐藏信息容量就越大。但是 N 越大,所需要的样本库越大,算法效率、隐藏成功率和鲁棒性都会降低。

在本文提出的算法中,假设一张原始图像可映射的信息比特数为 N ,将图像 P_g 分成 $M \times M$ 块,则经过块置乱可生成的新图像数量 W 为

$$W = A_M^M \times A_M^M = M^2 \times (M-1)^2 \cdots \times 2^2 \times 1 \quad (14)$$

因此,经过块置乱后可映射的信息比特数为 $W \times N$,隐藏信息容量大大提高。表1是本文算法信息隐藏容量与已有算法的对比,Pixel-based算法^[10]和Hash-based算法^[12]中每张图像映射的信息分别为8 bit和18 bit,DCT-based算法^[16]、DWT-based算法^[17]和本文算法中每张图像映射的信息比特数与图像进行DCT或DWT变换时的分块数目 J 相关,为方便比较,这里均假设 $J=9$ 。基于GAN网络的算法(GAN-based)^[22]中,假设输入的噪声向量维度为100,映射为3位二进制数。

表2比较了不同算法承载同样秘密信息所需图像数量。假设Pixel-based算法、DCT-based算法和DWT-based算法中,每张图像映射的信息量均为 $N=8$ bit,且不考虑信息序列补零等带来的额外信息开销。可见,在传递长度分别为1 Byte、10 Byte、100 Byte和1 KByte的秘密信息时,本文算法所需的载体图像数量远小于其他同类型方案。

表1 每张图像信息隐藏容量比较

算法	容量/bit
Pixel-based	8
Hash-based	18
DCT-based	8
DWT-based	8
GAN-based	300
本文算法($J=9, M=2$)	32
本文算法($J=9, M=4$)	4 608

表2 承载同样秘密信息所需图像数量比较

算法	1 Byte	10 Byte	100 Byte	1 KByte
Pixel-based ($N=8$)	1	10	100	1 024
Hash-based ($N=18$)	1	5	45	456
DCT-based ($N=8$)	1	10	100	1 024
DWT-based ($N=8$)	1	10	100	1 024
本文算法($N=8, M=2$)	1	3	25	256
本文算法($N=8, M=4$)	1	1	1	2

3.2 隐藏成功率分析

对基于特征映射的信息隐藏来说,所提取的特征序列既要保证鲁棒性要求,同时也应该反应特征的差异性,因此,在给定数据库的前提下,信息隐藏成功率也是衡量信息隐藏方案的重要指标。假设每张图像映射 N bit,当前图像库可映射的不同信息段数量为 k ,则信息隐藏成功率为

$$S = \frac{k}{2^N} \quad (15)$$

从256_ObjectCategories数据集中随机选择1 000张图像构成样本库,对Pixel-based算法^[10]、DCT-based算法^[16]、DWT-based算法^[17]和本文算法的隐藏成功率进行了测试。测试中,这4种算法均设置为每张图像映射8 bit信息。结果如图4所示,可见,随着图像样本数的增长,隐藏成功率随之增长。在载体图像数量相同时,本文算法的信息隐藏成功率远远高于其他算法。同时,图像置乱块越小,即置乱分块数 M 越大,可生成的新图像越多,隐藏成功率也越高。当置乱分块数 M 为4时,仅需要50张载体图像,就可达到95%左右的隐藏成功率,而其他算法仅有15%左右的隐藏成功率。因此,本算法用于构建和存储载体图像库的开销远小于其他算法。

3.3 鲁棒性分析

本文分别测试了算法在JPEG压缩、噪声、滤波和裁剪等攻击下的鲁棒性能,并与现有算法进行了对比。在测试中,将每张图像映射的 N bit视为一个信息块,采用误块率作为衡量标准,将其定义为

$$\text{BLER} = \frac{\text{BL}_c}{\text{BL}_s} \quad (16)$$

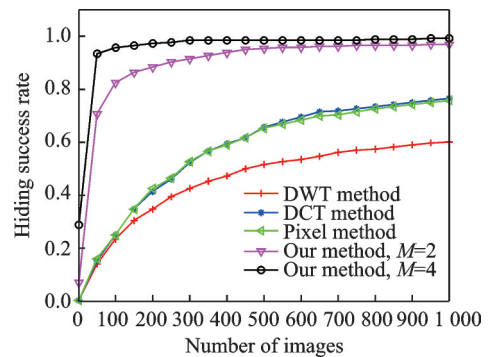


图4 信息隐藏成功率

Fig.4 Success rate of information hiding

式中:BL_c是接收完全正确的信息块数,BL_s为发送的总信息块数。设N=8,从表3可见,本文算法在抗JPEG压缩、高斯噪声、椒盐噪声、散斑噪声、中心裁剪和直方图均衡等攻击上,性能均超过现有算法。

表3 鲁棒性能对比
Table 3 Comparison of robustness

项目	Pixel-based	Hash-based	DCT-based	DWT-based	本文算法
JPEG压缩(Q=10%)	0.946	0.586	0.953	0.961	0.961
高斯噪声($\mu=0, \sigma=0.001$)	0.963	0.590	0.950	0.949	0.965
椒盐噪声($\mu=0, \sigma=0.001$)	0.986	0.898	0.989	0.992	0.994
散斑噪声 0.01($\mu=0, \sigma=0.01$)	0.966	0.759	0.964	0.966	0.971
中值滤波(3×3)	0.956	0.761	0.962	0.976	0.967
均值滤波(3×3)	0.994	0.871	1.000	0.998	0.987
高斯滤波(3×3)	0.995	0.930	1.000	1.000	0.996
中心裁剪(20%)	0.253	0.086	0.265	0.185	0.282
边缘裁剪(20%)	0.284	0.129	0.278	0.278	0.254
旋转 10°	0.103	0.430	0.099	0.113	0.109
平移(80, 50)	0.061	0.230	0.057	0.046	0.055
缩放(3倍)	0.999	0.963	1.000	1.000	0.999
直方图均衡	0.686	0.231	0.685	0.682	0.687
伽马校正(0.8)	0.916	0.579	0.899	0.920	0.914

3.4 计算效率分析

DCT算法^[16]、DWT算法^[17]和本文算法的计算复杂度都与DCT或DWT变换时的分块数J相关,但本文算法同时增加了对图像进行混沌块置乱的计算开销。假设混沌置乱的分块数为M×M,其计算开销随着M的增大而增加,如表4所示。

表5为平均隐藏1字节秘密信息时,不同算法所需的时间对比,其中DCT算法^[16]、DWT算法^[17]和本文算法中图像分块数J设为8,本文算法中混沌块数M设为32。由于增加了混沌块置乱,因此本文算法时耗略高于其他算法。

表4 混沌块置乱的时耗

Table 4 Time consumption of chaotic block scrambling

M	8	16	32	64	128
时耗/s	0.004 7	0.006 0	0.007 5	0.008 8	0.010 2

表5 算法效率对比

Table 5 Comparison of algorithm efficiency

算法	Pixel-based	Hash-based	DCT-based	DWT-based	本文算法
时耗/s	0.371 7	0.410 5	0.163 8	0.375 8	0.419 6

3.5 安全性分析

从鲁棒性能测试结果可见,在载体图像遭受压缩、噪声和滤波等攻击时,本算法具备较强的抗攻击能力。同时,无载体信息隐藏不会对载体图像进行修改,不易被隐写分析算法检测,因此,具有极高的安全性。

4 结束语

无载体信息隐藏不需要对载体进行修改,具有极强的抗隐写分析能力,但是目前已有的基于特征映射的无载体信息隐藏算法容量有限,且大多需要构建较大样本库。本文提出一种基于混沌块置乱和DWT变换的无载体信息隐藏算法,对载体图像进行混沌块置乱以后可以映射到多个信息序列。实验表明,与现有算法相比,该算法获得了信息隐藏容量和隐藏成功率的较大提升,具有较强的鲁棒性。同时,该算法架构简单、传输负载小,具有较强的应用价值。

参考文献:

- [1] TAN Y, QIN J, XIANG X, et al. A robust watermarking scheme in YCbCr color space based on channel coding[J]. *IEEE Access*, 2019, 7(1): 25026-25036.
- [2] QIN J, LUO Y, XIANG X, et al. Coverless image steganography: A survey[J]. *IEEE Access*, 2019, 7(1): 171372-171394.
- [3] WU K C, WANG C M. Steganography using reversible texture synthesis[J]. *IEEE Transactions on Image Processing*, 2015, 24(1): 130-139.
- [4] QIAN Z, ZHOU H, ZHANG W, et al. Robust steganography using texture synthesis[J]. *Advances in Intelligent Information Hiding and Multimedia Signal Processing*, 2017, 63(1): 25-33.
- [5] ZHOU H, CHEN K, ZHANG W, et al. Targeted attack and security enhancement on texture synthesis based steganography [J]. *Journal of Visual Communication and Image Representation*, 2018, 54(1): 100-107.
- [6] DUAN X, SONG H, QIN C, et al. Coverless steganography for digital images based on a generative model[J]. *Computers Materials & Continua*, 2018, 55(3): 483-493.
- [7] 刘明明,张敏倩,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.
LIU Mingming, ZHANG Minqian, LIU Jia, et al. Coverless information hiding based on generative adversarial networks[J]. *Journal of Applied Sciences*, 2018, 36(2): 371-382.
- [8] ZHOU Z, MU Y, WU Q M J. Coverless image steganography using partial-duplicate image retrieval[J]. *Soft Computing*, 2018, 20(1): 1-12.
- [9] LUO Y, QIN J, XIANG X, et al. Coverless real-time image information hiding based on image block matching and dense convolutional network[J]. *Journal of Real-Time Image Processing*, 2019, 17(1): 125-135.
- [10] ZHOU Z, SUN H, HARIT R, et al. Coverless image steganography without embedding[J]. *International Conference on Cloud Computing and Security*, 2015, 9483(1): 123-132.
- [11] 周志立,曹焱,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.
ZHOU Zhili, CAO Yan, SUN Xingming, Coverless information hiding based on bag-of-words model of image[J]. *Journal of Applied Sciences*, 2016, 34(5): 527-536.
- [12] ZHENG S, WANG L, LING B, et al. Coverless information hiding based on robust image hashing[J]. *International Conference on Intelligent Computing*, 2017, 10363(1): 536-547.
- [13] ZOU L, SUN J, 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*, 2018, 21(1): 1-16.
- [14] 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 Jianbin, FEI Xiaoxiao, WANG Nianfeng. Zero-steganography algorithm research based on chaotic sequences and image DCT transform[J]. *Electronic Measurement Technology*, 2017,40(5): 174-179.
- [15] ZHOU Z, WU Q M J, Yang C N. Coverless image steganography using histograms of oriented gradients-based hashing algorithm[J]. *Journal of Internet Technology*, 2017, 18(5): 1177-1184.
- [16] 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.
- [17] LIU Q, XIANG X, QIN J, et al. Coverless steganography based on image retrieval of DenseNet features and DWT sequence mapping[J]. *Knowledge-Based Systems*, 2020, 192(1): 105375-105389.

- [18] MENG R, ZHOU Z, CUI Q, et al. A novel steganography scheme combining coverless information hiding and steganography [J]. Journal of Information Hiding and Privacy Protection, 2019, 1(1): 43-48.
- [19] ZHOU Z, CAO Y, WANG M, et al. Faster-RCNN based robust coverless information hiding system in cloud environment[J]. IEEE Access, 2019, 7(1): 179891-179897.
- [20] ZHOU Y, BAO L, CHEN C L P. A new 1D chaotic system for image encryption[J]. Signal Processing, 2014, 97: 172-182.
- [21] HUA Z, YI S, ZHOU Y. Medical image encryption using high-speed scrambling and pixel adaptive diffusion[J]. Signal Processing, 2018, 144: 133-144.
- [22] 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.
ZHU Yiming, CHEN Fan, HE Hongjie, et al. Orthogonal GAN information hiding model based on secret information driven [J]. Journal of Applied Sciences, 2019,37(5): 721-732.

作者简介:



谭云(1980-),女,博士、硕士生导师,研究方向:信息隐藏、压缩感知,E-mail: tantanyun@hotmail.com。



秦姣华(1973-),通信作者,女,博士,教授、博士生导师,研究方向:网络信息安全、图像检索、模式识别。



黄丽霞(1981-),女,硕士,副教授,研究方向:物联网信息安全、信号处理。



向旭宇(1972-),男,博士,教授、硕士生导师,研究方向:网络信息安全、图像处理。



刘强(1995-),男,硕士研究生,研究方向:信息隐藏、深度学习。

(编辑:陈琚)