

一种新型的基于图像哈希的无载体隐写方案

黄承, 钱振兴, 张新鹏

(复旦大学 计算机科学技术学院, 上海 200444)

摘 要: 提出了一种新型的基于载体选择的无载体隐写方案. 发送端以迭代量化哈希为基础建立秘密信息与载体图像的联系, 并根据此联系从图像库中选择合适的载体进行秘密信息传输, 接收端根据事先约定好的规则, 使用图像哈希技术从图像中提取出秘密信息. 实验证明此方案在安全性方面优于传统的基于信息嵌入的隐写方案, 且在鲁棒性与隐写容量方面略优于其他的无载体隐写方案.

关键词: 载体选择; 无载体隐写; 图像哈希

中图分类号: TP309.7 **文献标志码:** A **文章编号:** 1001-0645(2020)12-1302-06

DOI: 10.15918/j.tbit.1001-0645.2019.265

A Novel Coverless Steganography Method Based on Image Hashing

HUANG Cheng, QIAN Zhen-xing, ZHANG Xin-peng

(School of Computer Science, Fudan University, Shanghai 200444, China)

Abstract: A novel coverless steganography method based on cover selection was proposed. The sender was arranged firstly to establish a connection between the secret information and the cover image based on the iterative quantization hashing, and then to select the appropriate cover from the image set to transmit the secret information according to the connection. According to the pre-agreed rules, the receiver was arranged to extract the secret information from the image based on the image hashing technique. Experiments show that this method is superior to the traditional information-embedded steganography method in terms of security, and is slightly better than other coverless steganography methods in terms of robustness and steganographic capacity.

Key words: cover selection; coverless steganography; image hashing

信息隐藏技术是信息安全的一个重要研究领域, 这种技术目的是将秘密信息隐藏于数字媒体之中同时不让对手发现这种行为. 作为信息隐藏的一个重要分支, 隐写术在近年来引起了学者们的广泛关注, 隐写术常被用于隐秘通信之中, 通过将信息隐藏在图像、视频、音频之中, 从而为发送端与接收端之间提供一种不被对手察觉的通信手段^[1]. 虽然隐写术的迅速发展使得其得到了广泛应用, 但是与此同时学者们也提出了一种用于对抗隐写术的技术, 称之为隐写分析, 隐写分析技术通过对载体进行特

征提取与特征分析, 从而来判断载体中是否存在隐写行为. 这种技术的出现对隐写术在安全性方面提出了更高的要求, 一种安全性能优秀的隐写术不仅需要视觉效果上不让人察觉, 而且需要具有抗隐写分析性.

传统的隐写术通常通过对载体进行修改来隐藏信息, 这种方法被称为基于信息嵌入的隐写术. 例如 LSB^[2]方法将秘密信息隐藏于图像像素的最后一位来实现隐写, 为了提高隐写容量与隐写安全性, 一种改进的 LSB 方法也被提出^[3]. 随着学者们对隐

收稿日期: 2019-10-20

基金项目: 国家自然科学基金资助项目(61572308, U1736213, U1636206)

作者简介: 黄承(1995—), 男, 硕士生, E-mail: xiaguol36@163.com.

通信作者: 钱振兴(1981—), 男, 教授, 博士生导师, E-mail: zxqian@fudan.edu.cn.

写术的研究日益深入,更多容量高、安全性好、具有鲁棒性的隐写方法随之出现了。直至今日,基于 STC 嵌入的方法^[4]被认为是最为有效的隐写方法,STC 方法使用定义好的失真函数来实现最小加性失真,使得隐写安全性达到最优。近年来,学者们提出许多基于 STC 嵌入的方法,如 WOW, UNI-WARD, HILL, MiPOD 等方法^[5-8],这些方法使用的失真函数各不相同,但目的都是为了实现最小加性失真。

虽然基于信息嵌入的隐写术是当今主流的隐写方法,但是其易于被隐写分析技术所检测的特性往往使得其安全性得不到保障。近年来,无载体隐写术受到人们的关注,无载体隐写术通过载体选择或载体生成来传递秘密信息。本文旨在探究一种基于载体选择的隐写方法,这种方法不直接将秘密信息嵌入到载体当中,而是先使用图像哈希技术在载体图像与秘密信息之间建立联系,然后选择与秘密信息相对应的载体直接传递秘密信息,这种方法难以被隐写分析方法所检测,其安全性远优于基于信息嵌入的隐写术。

1 基于图像哈希的无载体隐写方案原理

1.1 无载体隐写

近年来,一些无载体隐写方法被学者们提出,这些方法不进行信息嵌入,直接使用载体图像来实现秘密信息的传输。具体可分为两类,第一类方法被称为基于载体合成的无载体隐写方法,该方法直接利用秘密信息以及特定的函数关系来生成图像作为载体,例如利用秘密信息直接生成纹理图像作为载体来传输秘密信息^[9]。第二类方法则是基于载体选择的无载体隐写方法,此方法在秘密信息与图像之中建立某种联系,从而选择与秘密信息相对应的图像或其他数字媒体作为载体来传输信息,例如在秘密信息与汉语词汇之间建立联系,用汉语词汇来传输秘密信息^[10]。

虽然无载体隐写方法在安全性能上效果优越,然而相比于基于载体嵌入的隐写方法来说其存在几个普遍的问题。第一个问题是其隐写容量过低,无载体隐写方法中每一张图像所携带秘密信息量远远小于基于信息嵌入的隐写方法。第二个问题是无载体隐写方法普遍缺乏鲁棒性,一些无载体隐写方法仅仅对载体图像做轻微修改便可能丢失秘密信息,从而使得接收端无法提取正确的秘密信息。针对这

几个问题,本文提出了一种基于载体选择的无载体隐写方法。其具体思想为采用图像哈希的方法来建立秘密信息与图像之间的关系,从而选择合适的图像作为载体以传输秘密信息。

1.2 图像哈希

图像哈希^[11-12]常被用于图像检索中,目的是在一个图像库中找到与所给定图像相似的图像。这种方法首先将图像库中的每一张图像以及所给定图像各自转化为一串比特序列,然后通过比对各个比特序列之间的汉明距离,找到距离较小的若干张图像即为与所给定图像相似的图像。为了提高检索速度以及降低表示一张图像所需比特数,学者们提出了一系列的图像哈希方法,例如谱哈希方法^[11]对原始高维数据集进行谱分析,再通过放松限制条件,将问题转换成拉普拉斯特征图的降维问题从而求解,锚点图哈希提出与谱哈希方法相同的优化问题,但用近似邻接矩阵代替邻接矩阵,从而降低了时间复杂度。迭代量化哈希方法^[12]通过交替优化的方法以减少量化误差。

为了提高隐写方法的泛用性与鲁棒性,本文选取了使用最广泛,效果最好的迭代量化哈希方法来建立秘密信息与图像之间的关联,以实现基于载体选择的无载体隐写。

2 隐写方案设计

2.1 方法设计

迭代量化哈希的方法能够将高维的图像数据映射为一串二进制的比特序列,此序列与秘密信息表示的形式相同,因此可以通过图像哈希方法找到哈希后比特序列与秘密信息相类似的图像。在这一思路的基础上,本文提出了一种结合图像哈希且基于载体选择的无载体隐写方法。在通信过程中,存在发送端与接收端,发送端将秘密信息传输给接收端且不让对手发现传输行为。本文设计的方法中,发送端接收到一段秘密信息后,首先将秘密信息进行分段,对于每一段信息,通过基于图像哈希的方法将秘密信息隐藏于 3 张图像之中,将这 3 张图像发送给接收端,接收端接收到这 3 张图像之后,便可通过事先预设好的解码方法得到原秘密信息。每一段信息均如此处理,便可完成秘密信息的传输。在本文中,将秘密信息分为 64 bit 一段,即每 3 张图像传输 64 bit 信息,隐写容量约为 21.3 bit,虽然低于传统的基于信息嵌入的隐写方法,但是相对于其他的无

载体隐写方法,此方法隐写容量并不逊色.相对于普通的基于载体选择的无载体隐写方法,此方法所需要的图像数量明显减少.例如对于 64 bit 的秘密信息,普通方法需要 2^{64} 张图像,远超实验中常用的图像库中图像数量,而本文所提出的方法所需图像仅为 3 万张左右,可从常用图像库中找到合适的库.

2.2 迭代量化哈希

迭代量化哈希是使用最为广泛的一种图像哈希算法,同样它也是性能最为优越的哈希算法之一,本文以迭代量化哈希作为基础建立秘密信息与载体图像之间的联系.其基本步骤可分为 3 步:第 1 步对数据进行中心化,第 2 步对数据采用 PCA 的方法进行降维,第 3 步将降维后的数据进行二值量化.前 2 个步骤均易于理解,在此节中主要详细介绍第 3 个步骤.

对于原始数据 $\mathbf{X} \in \mathbf{R}^{n \times d}$ 通过 PCA 降维处理之后,得到的数据为 $\mathbf{V} \in \mathbf{R}^{n \times c}$. 迭代量化哈希第 3 个步骤将 $\mathbf{V}$ 进行二值处理以得到相应比特序列的过程可以看作将数据映射到一个二进制超立方体的顶点上.在这个过程中,为了得到最优的二进制编码,需要使得对应的量化误差最小化,而迭代量化哈希方法采用旋转数据矩阵的方法来达到这个目标.

假设所要求解的旋转矩阵为 $\mathbf{R}$,经过二值处理最终得到的哈希序列表示为 $\mathbf{B}$,由此可以得知 $\mathbf{B} = \text{sgn} \mathbf{V}$. 其量化损失函数为

$$Q(\mathbf{B}, \mathbf{R}) = \|\mathbf{B} - \mathbf{VR}\|_2^2. \quad (1)$$

迭代量化哈希首先对 $\mathbf{R}$ 进行随机初始化,然后通过迭代来交替更新 $\mathbf{R}$ 与 $\mathbf{B}$. 可分为以下两个过程:

固定 $\mathbf{R}$,对 $\mathbf{B}$ 进行更新

$$\mathbf{B} = \text{sgn}(\mathbf{VR}). \quad (2)$$

固定 $\mathbf{B}$,对 $\mathbf{R}$ 进行更新

$$\mathbf{C} = \mathbf{B}^T \mathbf{V}, \quad (3)$$

$$[\mathbf{U}_B, \mathbf{S}, \mathbf{U}_A] = \text{svd}(\mathbf{C}), \quad (4)$$

$$\mathbf{R} = \mathbf{U}_A \mathbf{U}_B^T. \quad (5)$$

这一部分的求解过程可以看作将求解一个正交 Procrustes 问题,在本文中利用简单奇异值分解的方法对此问题进行求解.

通过若干次迭代进行这两个步骤即可得到旋转矩阵 $\mathbf{R}$,从而可以将每一张图像都转化为比特序列.

2.3 步骤详解

对于发送端来说,所执行的步骤可分为 5 步,如图 1 所示.

① 将秘密信息分段,每一段为 64 bit,当最后一段不足 64 bit 时,不足的位随机填充至 64 bit 并且记录下最后一段的长度 L .

② 对于每一段来说,将所拥有图像库中每一张图像通过迭代量化哈希方法转换为 64 bit 的比特序列,并且将秘密信息与每一个图像的比特序列进行对比,找到汉明距离最小的两张图像,值得注意的是,此处必须保证这两张图像与秘密信息不同的位不在同一个位置,所以这一步骤相当于在满足这一条件的情况下找到距离小的两张图像.

③ 找出步骤②中两张图像中不同的位,将它们的值依次排列作为为首若干位,并在这些位之后随机填充,组成一个新的长度为 64 bit 的信息,将这个新信息与每一张图像哈希后的比特序列进行对比,找到一张哈希后为首若干位与此信息为首若干位相同的图像,并记录下来.

④ 依次传输②中找到的两张图像以及③中找到的一张图像,便完成了一段 64 bit 的秘密信息的传输.

⑤ 对每一段信息,重复②③④来传输所有秘密信息,相当于每 64 bit 的秘密信息用 3 张图像作为载体进行传输.在所有信息传输完成后,将长度 L 用基于信息嵌入的隐写方法传输给接收端.

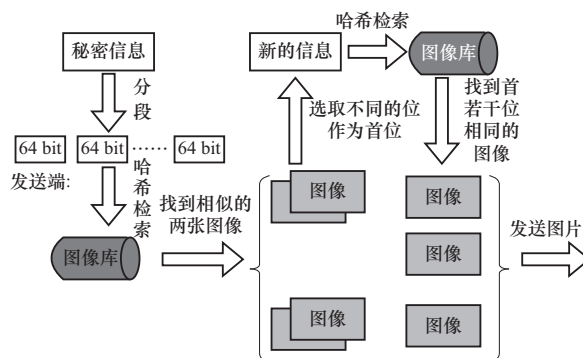


图 1 发送端操作步骤

Fig. 1 Sender operation steps

对于接收端来说,还原秘密信息可分为 3 个步骤,如图 2 所示.

① 将每 3 张图像分为一组,对于每一组图像,以迭代量化哈希的方法将图像转换为 64 bit 的比特序列,找到前两个比特序列相同的位,这些位的值即为原秘密信息的值,称为信息 1.

② 对于前两个比特序列不相同的若干位,取第 3 个比特序列为首若干位,形成信息 2,组合信息 1 与信息 2 还原出一段 64 bit 的秘密信息,这段信息是原

秘密信息的一段。

③ 重复执行①②得到每一段秘密信息并且依序相组合便得到了最终的秘密信息。值得注意的是最后一段秘密信息仅取前 L 位。

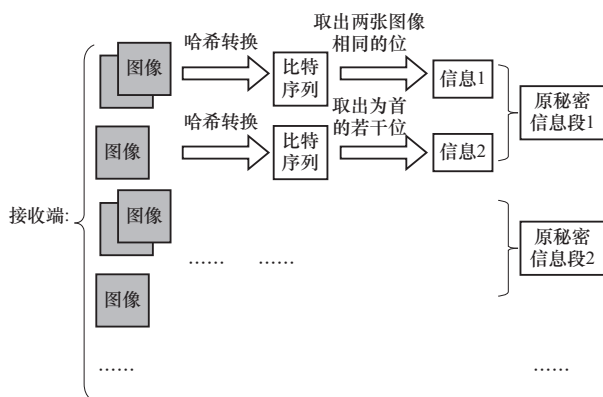


图 2 接收端操作步骤

Fig. 2 Receiver operation steps

3 实验与性能分析

3.1 信息提取正确性分析

第一部分的实验目的在于验证 2.3 节所描述方法是否能够正确提取秘密信息。在这一部分，选取了不同长度的比特序列作为秘密信息，然后将这些秘密信息分别通过 2.3 节所描述方法进行信息传输与提取，将提取所得信息与原秘密信息相比较，得到结果如表 1 所示，虽然每个信息的比特长度不同，但都能够被本文所提出方法正确提取，证明此方法在信息提取的正确性上具有优越的性能，有一定的实用性。

表 1 不同长度的秘密信息下信息提取的错误率

Tab. 1 Error rate of information extraction under secret information with different lengths

信息长度/bit	64	128	1 000	10 000	100 000
提取错误率/%	0	0	0	0	0

3.2 隐写安全性分析

这一部分的实验验证此方法的安全性能，隐写方法安全性的评价标准在于其是否能抵抗隐写分析技术。因此，本文主要采取的措施为使用隐写分析方法对此隐写方法进行测试，检测此方法是否能够对抗一些经典的隐写分析方法，并将其安全性与一些传统的基于信息嵌入的隐写方法进行对比，此实验采取的隐写分析方法有 SRM^[13]，maxSRM^[14]，Ye Net^[15]。实验结果如表 2 所示， P_E 表示隐写分析器的平均错误率，此值越高时，证明隐写方法安全性

能越好。从表 2 可以看出，对于 WOW，HILL，S-UNIWARD 3 种基于信息嵌入的隐写方法来说，隐写分析器的错误率较低，证明隐写分析器一定程度上能够分析出载体是否进行了隐写，而对于此文所提出的方法来说，3 种隐写分析器的平均错误率均为 50% 左右，难以分辨出图像是否进行了隐写。因此，在安全性方面，本文设计的隐写方法优于传统的基于信息嵌入的隐写方法，不容易被隐写分析方法所检测。

表 2 隐写分析方法检测的平均错误率

Tab. 2 Average error rate detected by Steganalysis

算法	SRM	maxSRMd2	Ye Net
WOW	0.345 4	0.301 2	0.245 3
HILL	0.354 2	0.323 4	0.253 4
S-UNIWARD	0.386 1	0.340 9	0.281 2
本文方法	0.521 3	0.499 8	0.517 6

3.3 隐写容量分析

隐写方法性能评价的另一个重要标准是隐写容量，在这部分的实验对此方法的隐写容量进行了测试。分析可得，此隐写方法的容量主要受限于图像库中图像的数量，增大容量会导致所需图像库图像数量增大，因此须在两者之间找到均衡点。由 2.3 节描述可知，每一段比特序列长度决定了隐写容量大小，若每一段为 64 bit 信息，则隐写容量为每张图像携带约 21.3 bit。在此部分，为每一段比特序列选取了不同的长度，并且分别计算各个长度的比特序列下图像库所需图像的数量。结果如表 3 所示，当比特序列分为 64 bit 一段时，图像库所需最少图像数量约为 3 万张，而当序列长度上升到 128 bit 时，所需最少图像数量约为 50 万张，这是一个庞大的图像数据库，远远高于一般图像数据库的图像数量，因此若选取 128 bit 作为序列长度，在实际使用场景中难以找到一个合适的图像数据库。经上述分析，从可行性的标准考虑，采用 64 bit 作为一段的长度是较为合适的方案，在此方案下，图像库所需图像数量最少约为 3 万张，隐写容量约为每张图像携带 21.3 bit。

表 3 隐写容量与图像数量的关系分析

Tab. 3 The relationship between steganographic capacity and number of images

比特序列长度/bit	32	48	64	128
所需图像数量/万张	0.1	1.2	3.0	50.0

3.4 鲁棒性分析

隐写方法的鲁棒性是验证隐写方法实用性的重要标准。在发送端向接收端传输隐写载体时,载体可能会被各种不同的方法所修改,例如添加噪声、旋转、压缩、裁剪等操作,在经过这些操作后,需要验证秘密信息是否依然能被正确提取,鲁棒性正是衡量这一问题的标准^[16-19]。在此部分,对传输的载体图像进行4种不同的操作,而后对操作后的图像进行信息提取,计算秘密信息提取的错误率,并与其它两种无载体隐写方法对比,本文称为方案1^[16]与方案2^[17]。结果如表4所示,从表4中可以看出对于压缩与噪声干扰,本文所提出方法具体优越的鲁棒性,基本能够正确提取相关信息,而对于旋转以及裁剪操作而言,当操作对原图像改变规模较小时,鲁棒性较好,而当改变规模增大时,鲁棒性较差。总体来说,本文所提出方法在针对压缩与噪声干扰情况下时的鲁棒性优于另外两种方法,在旋转与裁剪操作情况下鲁棒性较差。

表4 进行干扰操作后秘密信息提取的错误率

Tab. 4 Error rate of secret information extraction after interference operation

扰动操作	方案1/%	方案2/%	本文方案/%
旋转 30°	20.67	36.35	25.43
旋转 60°	40.18	28.22	48.29
压缩(品质因数 50)	50.34	1.99	1.21
压缩(品质因数 90)	45.12	1.33	1.54
中心裁剪 10%	40.88	32.28	43.96
中心裁剪 50%	85.12	88.66	60.23
高斯噪声 $\sigma(0.01)$	0.72	5.67	0.22
高斯噪声 $\sigma(0.1)$	3.54	6.22	0.87

4 结 论

本文提出了一种基于载体选择的无载体隐写方法,此方法以图像哈希技术为基础,在载体图像与秘密信息建立联系,发送端将载体图像传递给接收端之后,接收端通过这种联系还原出秘密信息。此外,本文通过实验验证了该方法的有效性与安全性,并对隐写容量以及鲁棒性进行了分析,实验证明此方法在隐写容量方面与现有的几种无载体隐写方案相当,在部分情况下鲁棒性上优于现有的几种无载体隐写方案。

此方法的局限性在于隐写容量较小且需要的图

像库过大,今后的工作将在这一方面进行改进,在减少图像库大小的同时提高隐写容量。

参考文献:

- [1] Fridrich J. Steganography in digital media: principles, algorithms, and applications [M]. Cambridge: Cambridge University Press, 2009.
- [2] Chan C K, Cheng L M. Hiding data in images by simple LSB substitution[J]. Pattern Recognition, 2004, 37(3): 469 - 474.
- [3] Mielikainen J. LSB matching revisited[J]. IEEE Signal Processing Letters, 2006, 13(5): 285 - 287.
- [4] 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.
- [5] Holub V, Fridrich J. Designing steganographic distortion using directional filters[C]// Proceedings of 2012 IEEE International Workshop on Information Forensics and Security (WIFS). [S. l.]: IEEE, 2012: 234 - 239.
- [6] Holub V, Fridrich J, Denemark T. Universal distortion function for steganography in an arbitrary domain[J]. EURASIP Journal on Information Security, 2014, 2014(1): 1 - 10.
- [7] Li B, Wang M, Huang J, et al. A new cost function for spatial image steganography[C]// Proceedings of 2014 IEEE International Conference on Image Processing (ICIP). [S. l.]: IEEE, 2014: 4206 - 4210.
- [8] Sedighi V, Cogan R, Fridrich J. Content-adaptive steganography by minimizing statistical detectability[J]. IEEE Transactions on Information Forensics and Security, 2015, 11(2): 221 - 234.
- [9] Wu K C, Wang C M. Steganography using reversible texture synthesis[J]. IEEE Transactions on Image Processing, 2014, 24(1): 130 - 139.
- [10] Chen X, Chen S, Wu Y. Coverless information hiding method based on the chinese character encoding[J]. Journal of Internet Technology, 2017, 18(2): 313 - 320.
- [11] Weiss Y, Torralba A, Fergus R. Spectral hashing[C]// Proceedings of Advances in Neural Information Processing Systems. [S. l.]: IEEE, 2009: 1753 - 1760.
- [12] Gong Y, Lazebnik S, Gordo A, et al. Iterative quantization: a procrustean approach to learning binary codes for large-scale image retrieval[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2012, 35(12): 2916 - 2929.

(下转第 1313 页)

参考文献:

- [1] 焦龙龙, 罗森林, 曹伟, 等. 变异策略动态构建的模糊测试数据生成方法[J]. 北京理工大学学报, 2019, 39(5): 539 - 544.
Jiao Longlong, Luo Senlin, Cao Wei, et al. Fuzzing test data generation method based on dynamic construction of mutation strategy[J]. Transactions of Beijing Institute of Technology, 2019, 39(5): 539 - 544. (in Chinese)
- [2] 马锐, 任帅敏, 马科, 等. 基于粒子群优化算法的 Android 应用自动化测试方法[J]. 北京理工大学学报, 2017, 37(12): 1265 - 1270.
Ma Rui, Ren Shuaimin, Ma Ke, et al. Test automation for Android applications based on particle swarm optimization algorithm[J]. Transactions of Beijing Institute of Technology, 2017, 37(12): 1265 - 1270. (in Chinese)
- [3] Zawlewski M. American fuzzy lop (AFL) fuzzer[EB/OL]. [2017 - 05 - 22]. http://lcamtuf.coredump.cx/afl/technical_details.txt.
- [4] Gen Z, Xu Z, Yingqi L, et al. PTfuzz: guided fuzzing with processor trace feedback[J]. IEEE Access, 2018: 37302 - 37313.
- [5] Intel Corporation. Intel processor trace[EB/OL]. [2018 - 01 - 01]. <https://software.intel.com/en-us/blogs/2013/09/18/processortracing>.
- [6] Karamcheti S, Mann G, Rosenberg D. Adaptive grey-box fuzz-testing with Thompson sampling [J]. arXiv: Artificial Intelligence, 2018: 37 - 47.
- [7] Agrawal S, Goyal N. Analysis of Thompson sampling for the multi-armed bandit problem [C] // Proceedings of Conference on Learning Theory. [S. l.]: IEEE, 2012.
- [8] Nadarajah S, Gupta A R. Characterizations of the beta distribution [J]. Communications in Statistics-Theory and Methods, 2004, 33(12): 2941 - 2957.
- [9] Dolan-Gavitt B, Hulin P, Kirda E, et al. LAVA: large-scale automated vulnerability addition[C] // Proceedings of IEEE Security and Privacy. [S. l.]: IEEE, 2016.
(责任编辑: 李兵)
-
- (上接第 1306 页)
- [13] Fridrich J, Kodovsky J. Rich models for steganalysis of digital images[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(3): 868 - 882.
- [14] Denemark T, Sedighi V, Holub V, et al. Selection-channel-aware rich model for steganalysis of digital images [C] // Proceedings of 2014 IEEE International Workshop on Information Forensics and Security (WIFS). [S. l.]: IEEE, 2014: 48 - 53.
- [15] Ye J, Ni J, Yi Y. Deep learning hierarchical representations for image steganalysis[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(11): 2545 - 2557.
- [16] Zheng S, Wang L, Ling B, et al. Coverless information hiding based on robust image hashing[C] // Proceedings of International Conference on Intelligent Computing. [S. l.]: Springer, 2017: 536 - 547.
- [17] 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.
- [18] 周艺华, 曹元大, 魏本杰, 等. 图像检索中基于记忆与半监督的主动相关反馈算法[J]. 北京理工大学学报, 2006, 26(1): 45 - 48.
Zhou Yihua, Cao Yuanda, Wei Benjie, et al. Memorization and semi-supervision based active relevance feedback algorithm for content-based image retrieval[J]. Transactions of Beijing Institute of Technology, 2006, 26(1): 45 - 48. (in Chinese)
- [19] 杨红菊, 张艳, 李凤霞, 等. 基于欧拉向量的彩色图像检索方法[J]. 北京理工大学学报, 2008, 28(8): 697 - 701.
Yang Hongju, Zhang Yan, Li Fengxia, et al. Color image retrieval methods based on euler vector[J]. Transactions of Beijing Institute of Technology, 2008, 28(8): 697 - 701. (in Chinese)
(责任编辑: 李兵)