DOI:10.19651/j.cnki.emt.2106752

基于 GoogLeNet-GMP 网络的自适应图像水印方法*

熊丽婷
(南昌交通学院 人工智能学院 南昌 330100)

摘 要: 为提高水印方案的抗攻击能力和自适应性,提出一种盲水印的 GoogLeNet-GMP 神经网络方案。首先,所提网络较为简约,最深的路径(即通过预处理网络、嵌入网络和提取网络的路径)仅包含 17 层。通过在水印预处理网络中提高水印分辨率来保持宿主图像的分辨率,由此增强了水印的透明性。同时,在水印预处理网络中使用平均池化,将水印数据的二进制值与宿主图像结合在一起,从而增强了水印的透明性。最后,提取器使用交叉熵作为损失函数,实现嵌入器和提取器之间的训练平衡。实验结果表明,所提方案性能出色,水印容量为 0.003 8,数据集中的 PSNR 均值为 40.57 dB。在有意义攻击下的性能优于其他先进方法。

关键词: 图像水印;GoogLeNet;预处理网络;神经网络;损失函数;分辨率
中图分类号: TP391.41 **文献标识码:** A **国家标准学科分类代码:** 520.6020

Adaptive image watermarking method based on GoogLeNet-GMP network

Xiong Liting
(College of Artifical Intelligence, Nanchang Jiaotong Institute, Nanchang 330100, China)

Abstract: To improve the anti attack ability and adaptability of the watermarking scheme, a blind watermarking scheme based on GoogLeNet-GMP is proposed. Firstly, the proposed network is relatively simple, and the deepest path (that is the path through preprocessing network, embedding network and extracting network) only contains 17 layers. The resolution of the host image is maintained by increasing the watermark resolution in the watermark preprocessing network, thus enhancing the transparency of the watermark. The average pooling is used in the watermark preprocessing network to combine the binary value of the watermark data with the host image properly, so it can enhance the transparency of the watermark. Finally, The extractor uses cross entropy as the loss function to achieve the training balance between the embeder and the extractor. The experimental results show that the performance of the proposed scheme is excellent, the watermark capacity is 0.003 8, and the average PSNR in the dataset is 40.57 dB. The performance under meaningful attack is better than other advanced methods.

Keywords: watermarking;GoogLeNet;preprocessing network;neural network;loss function;resolution

0 引 言

随着数字数据和互联网的广泛使用,侵犯知识产权的行为屡见不鲜,例如非法使用、复制和盗窃数字内容等。数字图像包含高附加值内容,水印技术[1]将所有者信息(水印)嵌入到图像中,可以保护其知识产权。但目前水印技术面临的威胁也较多,主要包括损坏或移除水印信息的恶意攻击,或为实现存储或分发内容的非恶意攻击[2]。

目前,很多水印研究基于一些基本的视觉特征,如文献[3]采用离散小波变换-奇异值分解算法作为数字水印嵌入、提取方法,通过摄像头读取打印的含水印图片信息,在处理器中直接进行水印检测。文献[4]提出一种空间纹理和频域的数字水印方法。文献[5]提出一种基于视觉显著性与量化指数调制的图像鲁棒水印方法,兼顾了水印透明性和抗几何变换的能力。文献[6]提出一种变换域的基于 DWT 水印方法,该算法在图像的高频部分嵌入水印,在次级高频上随机选择一些分散的嵌入点。上述这几类水印方法大多采用变换域方法或者底层视觉特征,均没有使用深度学习框架,因此,水印的透明性不佳。

近期,一些研究者提出基于神经网络的水印方法,利用深度学习将水印提取和水印嵌入的关系描述为损失函数[7]的形式。如文献[8]基于 Adaline 神经网络,确定一个准确

收稿日期:2021-05-21
* 基金项目:江西省教育厅科学技术研究项目(GJJ191583)、华东交通大学理工学院校级课题(xjjg2019-3)资助

的预测系数,构建线性预测函数,对交流系数误差完成二进制表示,根据水印信息对误差进行扩展。该水印算法具有较好的不可知性和高保真度。文献[9]提出一种码本方案的深度学习水印方法,在水印嵌入过程中生成码本,并在水印提取过程中使用该码本。文献[10]提出了一个联合网络方案,包含水印嵌入网络、攻击模拟网络和水印提取网络。在宿主图像进入网络前,将宿主图像的分辨率降低至水印图像的分辨率,并在离散余弦变换(DCT)网络中进行训练。但该方案抗攻击的类型很少。文献[11]提出了两阶段(可分拆深度学习)训练方案,在无对抗网络的情况下仅对提取器进行重训练,但该方案仅针对特定攻击和强度下的测试。文献[12]结合超混沌系统和 RBF 神经网络,提出一种基于超混沌的 RBF 神经网络模型水印算法。但总体复杂度不属于轻量级,测试的攻击类型较少。

为了尽可能在数字图像内容中插入更多的水印内容,尽可能减少不同攻击造成的水印信息丢失,本文提出一种抗攻击的透明盲水印 GoogLeNet-GMP 网络,该网络可以自适应宿主图像分辨率和水印信息,训练过程中使用随机生成的数据作为水印信息。为了调整透明性和抗攻击能力之间的平衡,还提出了强度因子,作为神经网络的一个超参数。结果验证了所提方法具有优秀性能。该方法是 GoogLeNet 网络的一个应用,对盲水印的开发具有一定借鉴意义。

1　深度学习水印方法存在的问题

大部分深度学习水印方法都为盲水印方法,使用空间域数据,且针对特定的宿主图像分辨率和水印信息。通过分析以往深度学习水印方案,可得出如下结论。

1)如果在训练中使用了特定水印,那么在需要使用新水印的情况下必须进行额外训练。

2)全连接(FC)层的使用限制了宿主图像的分辨率。这些方法不能确保适用于其他分辨率的宿主图像。

3)一些方法没有实现透明性和抗攻击性之间的权衡关系的可控性,由此降低了实用价值。

针对上述 3 个问题,本文提出了一个 GoogLeNet-GMP 神经网络结构,旨在实现宿主图像分辨率自适应性,水印内容自适应性,以及透明性和抗攻击能力,具体如下。

1)宿主图像分辨率自适应性:深度学习网络能够在所有分辨率的宿主图像中嵌入水印。

2)水印内容自适应性:深度学习网络能够改变要插入的水印内容且无需重新训练。

3)透明性和抗攻击能力可控性:深度学习网络可控制视觉可见性和水印强度。

2　提出的水印方法

2.1　整体水印框架

本文水印嵌入和水印提取架构如图 1 所示,其中,嵌入器如图 1(a)所示,提取器如图 1(b)所示。在将 RGB 图像转换为 YCbCr 后,仅处理一个通道(即 Y 分量)。在输入前先将其归一化到[-1, 1]。水印数据为二进制数据,利用密钥进行置乱。对归一化宿主图像数据和置乱水印数据进行预处理,并将结果串联在一起。在嵌入网络中处理串联后的结果,以输出加水印数据,对其进行去归一化,并利用转换后的 Cb 和 Cr 分量将其转换为 RGB 格式,以形成加水印宿主图像。

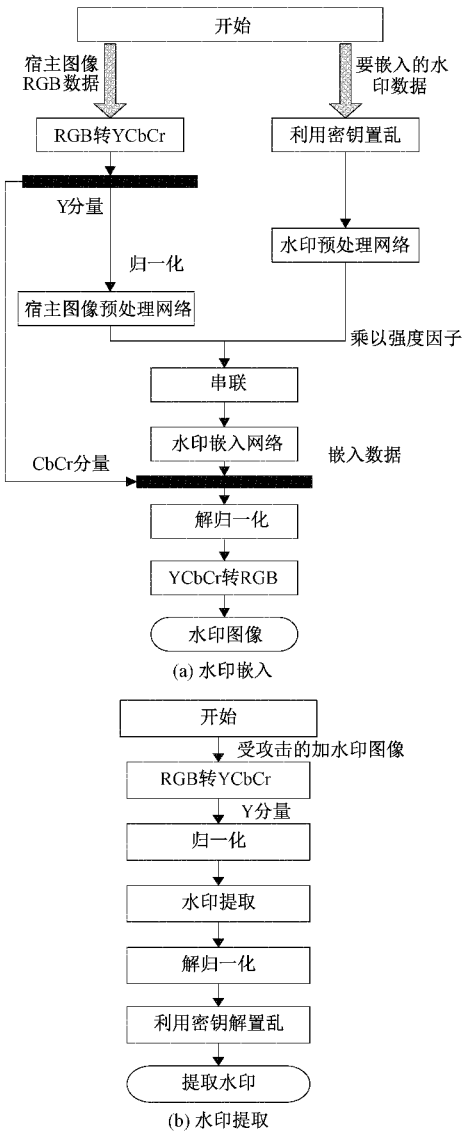

图 1　水印嵌入与水印提取示意图

提取过程接收加水印并受攻击后的 RGB 图像,将其转换为 YCbCr 格式。仅取 Y 分量,并将其归一化到[-1, 1]范围。提取水印信息作为输出,并利用置乱程序中使用的密钥对结果进行去置乱,去置乱后的数据为最终提取出的水印。

2.2　基于 GoogLeNet-GMP 的水印方法

1)整体网络结构

GoogLeNet 由 Google 公司提出,是 2014 年 ImageNet

的竞赛冠军。GoogLeNet 可解决一般卷积神经网络的过大计算量导致的过拟合问题。引入 1×1 卷积，创造性地采用 Inception 模块，其一般结构如图 2 所示，将稀疏矩阵聚类为相对密集的子矩阵，从而降低参数量，节省计算资源。其中 Inception 也有多个版本，其中，Inception v3 将二维卷积进行非对称拆分，拆分成为两个较小的卷积，比如 9×9 卷积可以分解为两个一维的卷积形式(1×9，9×1)，这样就增加了网络的非线性，可以处理更多的空间特征，本文采用 Inception v3 网络结构。

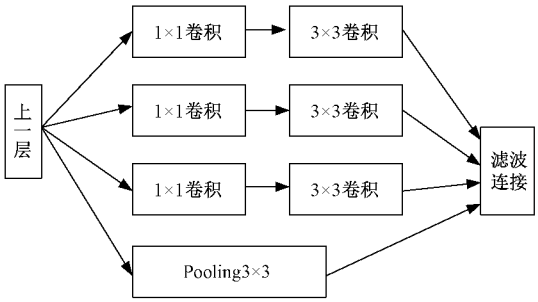

图 2　一般 Inception 模块结构

值得一提，本文的网络设计参考了全局最大池化(global maximum pooling，GMP)网络，网络结构以 GoogLeNet Inception v3 为基础，在 Inception 模块之后增加 GMP 层。CoogLeNet-GMP 网络结构参数如表 1 所示，模块按结构差异分为 5 类。同时，使用 Sigmoid 全连接(FC)层替换原网络的稀疏 FC 层。假设 $f_k(x,y)$ 代表最后一个 CL 层的第 k 个特征图，最终网络中的类别 i 得分为：

$$\boldsymbol{S}_i = Sigmoid\left(\sum_k \omega_k^i m_k - b_i\right) \tag{1}$$

式中：$m_k = \max_{x,y}\{f_k(x,y)\}$，$\omega_k^i$ 表示权重参数，b_i 表示偏置参数。

表 1　CoogLeNet-GMP 结构参数

类型	大小/步长	尺寸
Conv-1	3×3/2	299×299×3
Conv-2	3×3/2	149×149×32
Conv Padded	3×3/1	147×147×32
Pool	3×3/2	147×147×64
Conv-3	3×3/1	73×73×64
Conv-4	3×3/2	73×73×80
Pool	3×3/2	71×71×192
Inception	—	35×35×192
Inception×2	—	35×35×288
Inception×5	—	17×17×768
Inception	—	17×17×768
GMP	—	8×8×2 048
Sigmiod	分类	1×1×2 048

本文网络架构包括宿主图像和水印的预处理网络、水印嵌入网络，以及水印提取网络，整体网络结构如图 3 所示，第 1 个网络结构特征较为简单，仅包含 17 层。第 2 个水印预处理网络将水印分辨率提升至宿主图像分辨率，由此保留了宿主图像信息，提高水印透明性。

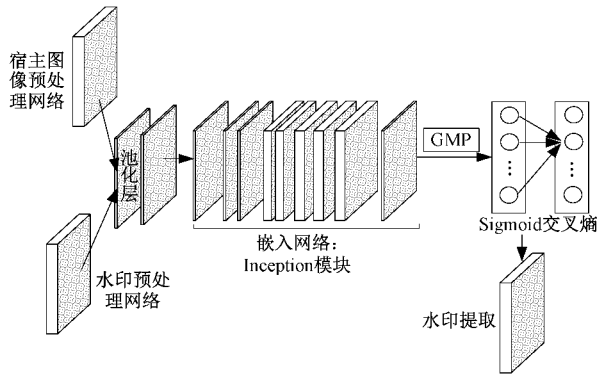

图 3　本文整体网络模型结构

2)宿主图像的预处理网络

宿主图像预处理网络保留原始图像的分辨率，包含 1 个卷积层(CL)及 64 个滤波器，其步长为 1。嵌入网络的输出应与宿主图像基本相同，这样可以避免对宿主图像造成显著损伤。其中，64 个滤波器代表生成的通道有 64 个，这样可以提取尽可能多的宿主图像特征。

3)用于水印的预处理网络

将水印预处理网络配置为逐渐增加分辨率，以匹配宿主图像预处理网络的分辨率，由此增加水印的透明性。该网络由 CL、批归一化(BN)、激活函数(AF)和平均池化(AP)组成，最后一个区块则仅包含 CL 和 AP。激活函数以 Sigmoid 函数为准。

$$Sigmoid(x) = \frac{1}{1+e^{x}} \tag{2}$$

AF 为修正线性单元(ReLU)，AP 为 2×2 滤波器，步长为 1。使用 AP 是因为水印是二进制数据，数值是离散的，但宿主图像数据是连续实值。有必要利用 AP 来平滑水印数据以结合宿主图像数据，保留连续特征。将水印预处理网络的输出与强度比例因子相乘，以控制水印的透明性和抗攻击能力。

4)水印嵌入网络

水印嵌入网络将预处理宿主图像信息的 64 个通道和预处理水印信息的一个通道的结果串联在一起，并作为输入，以输出加水印的图像信息。该网络前 4 个区块包含 ReLU，最后一个区块包含 CL-AF(tanh)。tanh 激活函数保留正值和负值，以满足输入宿主图像信息[−1，1]的数据范围。所有卷积步长为 1，以保持宿主图像的分辨率不变，增加透明性。除最后一个区块外，所有区块均包含 64 个 CL 滤波器；最后一个区块的滤波器数量等于宿主图像通道数，即 1 个。利用交叉熵作为损失函数，其表达式为：

$$CE(x)_i = -\phi_i \ln[f_i(x)] - (1-\phi_i)\ln[-f_i(x)] \tag{3}$$

式中:x 为输入样本,i 为类别个数 5,即每个类别都会有一个交叉熵值,ϕ_i 表示第 i 个类别的真实标签,$f_i(x)$ 表示第 i 个类别的模型输出值。

为了加快图像的训练过程,本文采用批量法,因此,损失函数为:

$$\text{Loss} = \frac{1}{N}\sum_{k=1}^{N} CE(x^{(k)}) \tag{4}$$

式中:N 表示批量的大小。

5)水印提取器网络

提取网络采用与水印预处理网络逆对称的结构,但使用不同数量的滤波器。其降低水印图像和受攻击图像的分辨率,并提取水印信息。该网络包含 3 个 ReLU 区块,以及 CL-AF(tanh)区块,即最后一个区块。在下采样中设所有 CL 步长为 2。值得一提,水印嵌入网络和水印提取网络中,可以使用提取水印和原始水印之间的平均绝对误差作为损失函数。当然,依然可以采用式(3)和(4)作为损失函数。

3　实验与分析

本文在 PC 机配置为 Intel (R) Core (TM) i3 CPU@2.5 GHz,8 GB RAM 上进行实验。显卡型号为 NVIDIA Quadro M2000,显存为 2.0 GB。通过不同实验进行定量和定性评估,以评价水印方案的透明性和抗攻击能力。

对于嵌入网络和提取网络,使用 Adam 优化器[13],学习率分别为 0.000 1 和 0.000 01。训练中,将强度因子 μ 设为 1,权重衰减率为 0.01。每小批的宿主图像数量为 100 个,最大迭代次数为 4 000(直到损失函数区域稳定)。

3.1　数据集

本文使用 BOSS 数据集[14]作为训练数据集,该数据集包含 10 000 张分辨率为 512×512 的灰度图像。BOSS 数据集广泛用于各种深度学习相关的应用和技术。其中,有 50 张分辨率为 512×512 的灰度图像的标准数据集[15]作为评估数据集。实验使用分辨率为 8×8 像素的二进制图像作为水印。训练过程中,每次迭代生成一个随机水印,并以相应密钥进行置乱。这些随机生成的水印使网络能够适应水印信息,并降低了训练过程中的过拟合。此外,除了标准灰度图像,采用虹膜图像库[16]也是可行的。

3.2　性能评估度量

本文利用式(5)中的峰值信噪比(PSNR)对透明性进行量化评估。由于水印嵌入器输出的归一化像素值范围为[−1, 1]。将其转换为[0, 255]中的一个整数,作为透明性评估中的最终水印图像。

$$PSNR = 20\lg\left(\frac{255^2}{\sqrt{MSE}}\right) \tag{5}$$

通过提取出的水印误码率(BER)来评估透明性。水印信息包含两类(原始二进制水印与提取的二进制水印),若两者相同,则水印信息的像素值为 1;若两者不同,则像素值为 0。BER 的定义为:

$$BER(\%) = \frac{1}{XY}\sum_{i,j}^{XY}\delta(WM_o(i,j), WM_e(i,j)) \times 100\% \tag{6}$$

式中:WM_o 表示二进制原始水印信息;WM_e 表示提取的二进制水印信息,$\delta(x,y) = \begin{cases} 0, & x \neq y \\ 1, & x = y \end{cases}$。

此外,水印容量是水印分辨率与宿主图像分辨率之比。其水印和宿主图像的分辨率分别为(X, Y)和(M, N)。本文将水印容量固定为 0.003 8。

3.3　水印图像的透明性

根据训练结果,当强度因子 $\mu=1$ 时,加水印图像相对于原始宿主图像的平均 PSNR 为 43.09 dB。本文对评估数据集应用训练权重集,得出的 PSNR 范围为[37.37 dB, 42.25 dB],均值为 40.57 dB。一些测试数据集的样例如图 4 所示,其中,宿主图像如图 4(a)所示,加水印的图像如图 4(b)所示,差异图像如图 4(c)所示。这些样例分别表示最低(第 1 行)、中间(第 2 行)和最高(第 3 行)透明性。即使对于最低透明性的样例,原始图像和加水印图像的差异也是肉眼难以分辨的。由此证明本文方法实现了极高的透明性。

(a) 宿主图像　(b) 加水印图像　(c) 差异放大图像

图 4　水印图像透明性的展示

3.4　面对各种攻击的稳健性

本文在评价数据集上,针对各种不同类型的攻击及强度,基于训练权重集进行实验分析。攻击的目的是通过恶意或非恶意攻击消除水印,在无所有权的情况下使用图像。

当 $\mu=1$ 时,不同攻击下提取水印的平均误码率情况如表 2 所示,其中,BER 值取评估数据集中所有图像的均值。从中可发现,对于每种类型的攻击,BER 数值会随着攻击强度的增加呈上升趋势。旋转攻击在 45°时会对图像信息造成最大干扰。因此,BER 随着旋转角度的增加而上升,

但超过 45°后，会随着角度增加而下降。这意味着本文网络训练结果较好，不存在对特定强度攻击的过拟合问题。

表 2　不同攻击下提取水印的平均误码率

攻击类型	攻击	强度	BER/%		
			WM1 随机(平均)	WM2 	WM3 
像素值改变攻击	无攻击	—	0.701 6	0.668 7	0.668 7
	高斯滤波	3×3	1.591 3	1.754 3	2.008 3
		5×5	7.525 1	7.305 3	8.452 4
		7×7	11.511 6	11.287 6	11.512 1
		9×9	18.467 1	19.197 1	17.507 3
	均值滤波	3×3	4.273 0	3.958 2	4.113 5
		5×5	5.228 1	5.359 2	4.783 2
	中值滤波	3×3	8.419 3	7.878 6	7.876 3
		5×5	10.551 7	10.842 9	11.096 9
	椒盐噪声添加	0.01	0.862 2	0.797 9	0.797 2
		0.03	1.179 0	1.020 1	1.116 1
		0.05	1.403 3	1.242 7	1.339 3
		0.07	1.818 1	1.537 8	1.849 5
		0.09	2.583 4	3.126 0	2.040 8
	高斯噪声添加	σ=0.01	0.828 8	0.798 1	0.733 4
		σ=0.03	1.976 0	1.659 0	1.977 0
		σ=0.05	6.091 1	6.887 2	5.641 1
		σ=0.08	11.986 3	12.856 8	13.329 1
	锐化	5-像素点模板	3.285 1	3.669 1	3.571 4
		9-像素点模板	3.923 5	4.627 3	4.368 6
	JPEG	90	0.957 4	0.861 6	0.765 3
		70	4.242 9	3.989 0	4.241 1
		50	8.063 0	7.909 1	9.056 1
		30	14.892 7	15.115 0	14.827 8
		10	31.474 6	31.825 3	33.418 4
几何攻击	旋转	15	2.073 9	1.886 0	1.913 3
		30	4.915 7	4.819 8	5.229 6
		45	5.036 3	5.114 7	5.739 8
		60	3.821 1	3.668 2	4.719 4
		75	1.782 9	1.818 3	1.945 2
	Crop	0.9	0.707 6	1.178 9	0.924 7
		0.7	2.139 6	4.337 1	13.456 6
		0.5	14.637 4	16.742 3	11.479 6
		0.3	24.965 8	21.398 9	29.177 3
		0.1	39.639 7	48.507 8	38.361 0
	Cropout	0.1	2.201 2	3.029 9	1.753 8
		0.3	9.059 7	12.437 6	9.088 0
		0.5	17.027 8	24.264 1	20.918 4
		0.7	24.045 7	33.416 3	25.478 3
		0.9	34.854 3	44.928 7	37.372 4
	Dropout	0.9	9.927 9	0.925 1	1.052 3
		0.7	2.458 6	2.201 2	2.327 8
		0.5	6.250 1	5.453 1	5.516 6
		0.3	14.897 9	15.562 7	15.114 8
		0.1	34.118 7	37.309 1	34.757 7

由表 2 还可知，除了高斯滤波攻击(7×7 及以上的滤波器)、高斯噪声攻击(σ 大于 0.08)和 JPEG 攻击(压缩比 40 以上)之外，本文方案能够较好地抵御大部分像素值改变攻击(BER 低于 10%)。具体来说，本文方案能够很好抵

御椒盐噪声攻击。对于几何攻击,所提方案在面对旋转攻击时表现极好,但在面对 Crop(50%以上)和 Cropout 攻击(30%以上)时 BER 较高。但这些攻击会对宿主图像造成极大损害,没有实际价值。因此,所提方案能够很好地抵御有意义的攻击。

3.5 水印自适应性

一个好的水印方案必须能够适应不同类型的水印数据。本文使用新生成的随机数据作为训练中每个小批的水印信息,由此实现水印自适应性。在表 2 的结果中,"随机(平均)"表示使用所有水印数据的均值,WM2 和 WM3 表示两个特定水印数据。表 2 的结果表明本文方案可应用不同类型的水印数据,且可以实现类似的抗攻击能力。

3.6 宿主图像自适应性

提出的方案未使用任何依赖于宿主图像分辨率的网络层(例如 FC 层),因此对宿主图像分辨率具有自适应性。通过将宿主图像分辨率从 64×64 逐步变更至 512×512,评估水印透明性和抗攻击能力,具体测量结果如表 3 所示,其中水印容量固定为 0.003 8。虽然存在抗攻击能力随分辨率增加而下降的案例,但其下降比例很小(或增加的 BER 值并不高),即降低后的抗攻击能力依然较高。由此可得出结论,本文方法适用于不同分辨率的宿主图像。

表 3　水印分辨率、宿主图像分辨率和透明性测量

宿主图像分辨率	水印分辨率	透明性/dB
64×64	4×4	39.96
128×128	8×8	40.59
256×256	16×16	41.45
512×512	32×32	42.39

3.7 与当前先进方法比较

该小节将所提方案与其他先进方法(文献[9])进行比较。由于文献[9]给出了精确数值结果,首先比较其与所提方案在各种攻击下的结果。为公平起见,本文对强度因子 μ 进行了调整,以使用与其他方法相似的 PSNR。其中,μ 调整为 1,PSNR 为 40.87 dB。针对特定攻击的比较结果如表 4 所示,攻击类型参照文献[9],从中可发现,所提方案在高斯噪声攻击之外的所有攻击中均取得较优性能。

其他比较方法并未给出精确数值。为此,比较文献[10-12]在特定攻击集合下的水印结果。与其他先进方法的比较结果如表 5 所示。其中,所提方案的强度因子 μ 设为 2.75,PSNR 为 33.5 dB。结果表明,所提方案在 Crop(0.035)攻击之外均取得比文献[12]和[10]更好的性能。但与文献[11]相比,所提方案仅在 JPEG 压缩攻击中取得更好结果。Crop(0.035)攻击仅使用加水印图像的 3.5%来提取水印信息,不具备实践意义。此外,文献[11]在训练中使用了相同类型的攻击和强度,这意味着其实验评价中仅考虑训练过的攻击。因此,该方案不能确保结果

表 4　针对特定攻击的比较结果

攻击	强度	文献[9]	本文方案
PSNR/dB		40.24	40.87
无攻击	—	—	0.701 5
高斯滤波	半径=1	8.6	7.142 1
	半径=1.6	39	9.725 3
	半径=2	—	12.723 4
中值滤波	3×3	13.4	8.418 6
	5×5	—	10.554 7
椒盐噪声添加	0.02	2.9	1.020 1
	0.6	4.5	1.530 3
	0.1	9.1	3.188 4
高斯噪声添加	5%	2.4	5.994 6
	15%	14.5	27
	25%	25.6	38.169 7
锐化	半径=1	0.9	0.988 6
	半径=5	2.4	1.721 8
	半径=10	3.2	2.008 7
JPEG	90	1.6	0.956 7
	70	4.2	4.24
	50	11.8	8.067 9
Cropout	0.1	7.7	2.136 3
	0.2	13.1	5.325 2
	0.3	18.8	8.673 3

适用于其他类型和其他强度的攻击,不能证明其在实际应用中的抗攻击能力。本文方案实用价值较高,在除高斯噪声添加攻击和高强度 Crop 攻击(这两种攻击会导致图像失去使用意义)之外的所有攻击中均表现较好性能。

表 5　与其他先进方法的比较

攻击类型	文献[10]	文献[11]	文献[12]	本文(μ=2.75)
训练数据集	Pascal VOC	COCO	灰度图像标准数据集	BOSS
PSNR	—	33.5	—	33.5
JPEG	25.4	23.8	37	0.669 6
Cropout	7.5	2.7	6	5.835 5
Dropout	8	2.6	7	4.719 4
Crop	0	11	12	44.132 7
高斯滤波	50	1.4	4	4.304 8

4　结　　论

本文提出一种基于 GoogLeNet-GMP 的图像水印方法。该方法利用强度因子调整透明性和抗攻击能力之间的权衡关系。其中,水印预处理网络将水印分辨率增至宿

主图像分辨率，以确保水印透明性；嵌入网络利用 GoogLeNet 保持分辨率不变，输出加水印图像。由于本文不使用依赖于分辨率的网络层，因此，实现了对输入图像分辨率的自适应性。在有意义攻击下的性能优于其他先进方法，有较大应用价值。

未来，本文将基于用户需求，对透明性和抗攻击能力之间进行适当控制，进一步提升方案的有效性。

参考文献

[1] 刘贻明，张重雄. 伪 3D-DCT 域的视频零水印算法[J]. 电子测量技术，2019，42(24)：162-166，171.

[2] 李良旭. 区块链技术在数字版权中的研究与应用[D]. 北京：北方工业大学，2018.

[3] 曾台英，余正轩. 基于 ARM 的数字水印检测终端的设计实现[J]. 国外电子测量技术，2019，38(2)：144-148.

[4] ZHANG L，YAN H，ZHU R，et al. Combinational spatial and frequency domains watermarking for 2D vector maps[J]. Multimedia Tools and Applications，2020，79(1-2)：1-13.

[5] 钟瑞泽，谢海波. 基于视觉显著性与量化指数调制的图像鲁棒水印算法[J]. 电子测量与仪器学报，2020，34(3)：22-32.

[6] 张勤，崔丽. 基于 DWT 的一种数字水印算法[J]. 北京师范大学学报(自然科学版)，2015，51(1)：19-22.

[7] ZARRABI H，EMAMI A，KHADIVI P，et al. BlessMark：A blind diagnostically-lossless watermarking framework for medical applications based on deep neural networks[J]. Multimedia Tools and Applications，2020，79(17)：1-23.

[8] 王洪，王聪，余金暇. 基于 Walsh-Hadamard 变换与预测误差扩展的图像水印算法[J]. 光学技术，2018，44(4)：487-494.

[9] KANDI H，MISHRA D，GORTHI S R. Exploring the learning capabilities of convolutional neural networks for robust image watermarking [J]. Computers & Security，2017，65：247-268.

[10] AHMADI M，NOROUZI A，SOROUSHMEHR S，et al. Redmark：Framework for residual diffusion watermarking on deep networks[J]. ArXiv，2018，45(4)：7248-7256.

[11] LIU Y，GUO M，ZHANG J，et al. A novel two-stage separable deep learning framework for practical blind watermarking [C]. International Conference on Multimedia，Nice，France，IEEE Press，2019：1509-1517.

[12] 杨树国，刘庆亮，熊鹏程. 基于超混沌的 RBF 神经网络图像自适应水印算法[J]. 青岛科技大学学报(自然科学版)，2018，39(5)：106-110，118.

[13] 杨观赐，杨静，李少波，等. 基于 Dopout 与 ADAM 优化器的改进 CNN 算法[J]. 华中科技大学学报(自然科学版)，2018，46(7)：122-127.

[14] BAS P，FILLER T，PEVNY T. Break our steganographic system：The ins and outs of organizing BOSS[C]. International Workshop on Information Hiding，Springer：Berlin/Heidelberg，Germany，2011：59-70.

[15] RAJPAL A，MISHRA A，BALA R. Multiple scaling factors based Semi-Blind watermarking of grayscale images using OS-ELM neural network [C]. International Conference on Signal Processing，Communications and Computing，IEEE，2016：1-6.

[16] 刘笑楠，张文云，高艳娜. 局部置乱结合双随机相位编码的双虹膜身份模板保护方法[J]. 仪器仪表学报，2020，41(6)：235-241.

作者简介

熊丽婷，副教授，主要研究方向为神经网络、图像处理、数据挖掘等。

E-mail：ilovebear0000@163.com