

基于传统引导机制的深度鲁棒水印算法

郭学镜, 方毅翔, 赵怡, 张天助, 曾文超, 王俊祥

(景德镇陶瓷大学机械电子工程学院, 江西 景德镇 333000)

摘要: 随着网络 and 多媒体技术的发展, 多媒体数据逐渐成为人们获取信息的重要来源, 数字媒体逐渐成为版权保护和防伪溯源主战场, 版权保护新技术的重要性日益凸显, 数字水印技术作为其中一种重要的版权保护手段得到重视。在信息传递过程中, 含密数字媒体信息可能会受到噪声和外部干扰攻击, 传统鲁棒数字水印技术正是围绕这些问题进行研究。然而, 传统的鲁棒数字水印技术对不同类型攻击的综合抵抗能力有待提升。同时, 由于其嵌入方式的局限性, 传统的鲁棒数字水印算法对不同图像的泛化处理能力较弱。近年来, 深度学习由于其强大的自学习能力被广泛应用于鲁棒数字水印技术研究。基于深度网络的鲁棒数字水印算法的初始化通常来源于随机的参数和特征, 这会导致生成的模型质量不佳、训练时间过长, 甚至无法收敛。结合两者的优点, 采用传统的数字水印技术进行引导, 兼顾深度网络的学习能力和传统鲁棒数字水印技术特征进行设计, 提出一种基于传统引导机制的深度鲁棒数字水印算法。所提算法利用传统的鲁棒数字水印算法生成水印图像, 设计的特征构造能够保证传统水印图像的鲁棒性。再利用 U-Net 结构将传统水印图像融合至深度网络, 生成最终的含密图像。实验结果表明, 所提算法能够提升含密图像抵抗各种攻击的鲁棒性, 并且保证更好的视觉质量。

关键词: 水印技术; 深度网络; 鲁棒水印; U-Net

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023031

Traditional guidance mechanism based deep robust watermarking

GUO Xuejing, FANG Yixiang, ZHAO Yi, ZHANG Tianzhu, ZENG Wenchao, WANG Junxiang

School of Mechanical and Electronic Engineering, Jingdezhen Ceramic University, Jingdezhen 333000, China

收稿日期: 2022-09-10; **修回日期:** 2023-02-01

通信作者: 方毅翔, fangyixiang@jci.edu.cn

基金项目: 国家自然科学基金 (62062044, 62063010); 江西省科技合作专项重点项目 (20212BDH80021); 景德镇市级科技计划项目 (2020ZDGG004)

Foundation Items: The National Natural Science Foundation of China (62062044, 62063010), The Science and Technology Cooperation Special Key Project of Jiangxi Province (20212BDH80021), Jingdezhen Municipal Science and Technology Plan Project(2020ZDGG004)

引用格式: 郭学镜, 方毅翔, 赵怡, 等. 基于传统引导机制的深度鲁棒水印算法[J]. 网络与信息安全学报, 2023, 9(2): 175-183.

Citation Format: GUO X J, FANG Y X, ZHAO Y, et al. Traditional guidance mechanism based deep robust watermarking[J]. Chinese Journal of Network and Information Security, 2023, 9(2): 175-183.

Abstract: With the development of network and multimedia technology, multimedia data has gradually become a key source of information for people, making digital media the primary battlefield for copyright protection and anti-counterfeit traceability. Digital watermarking techniques have been widely studied and recognized as important tools for copyright protection. However, the robustness of conventional digital watermarking methods is limited as sensitive digital media can easily be affected by noise and external interference during transmission. Then the existing powerful digital watermarking technology's comprehensive resistance to all forms of attacks must be enhanced. Moreover, the conventional robust digital watermarking algorithm's generalizability across a variety of image types is limited due to its embedding method. Deep learning has been widely used in the development of robust digital watermarking systems due to its self-learning abilities. However, current initialization techniques based on deep neural networks rely on random parameters and features, resulting in low-quality model generation, lengthy training times, and potential convergence issues. To address these challenges, a deep robust digital watermarking algorithm based on a traditional bootstrapping mechanism was proposed. It combined the benefits of both traditional digital watermarking techniques and deep neural networks, taking into account their learning abilities and robust characteristics. The algorithm used the classic robust digital watermarking algorithm to make watermarked photos, and the constructed feature guaranteed the resilience of traditional watermarked images. The final dense image was produced by fusing the conventionally watermarked image with the deep network using the U-Net structure. The testing results demonstrate that the technique can increase the stego image's resistance to various attacks and provide superior visual quality compared to the conventional algorithm.

Keywords: watermarking technology, deep network, robust watermarking, U-Net

0 引言

随着多媒体信息技术的快速发展,信息的传输变得方便快捷和多样化。然而,信息来源的有效性和安全性受到许多不法分子的威胁,如图片盗用、商标窃取等。因此,信息的溯源和认证成为信息安全领域的一大挑战。为了解决上述问题,数字水印技术^[1]被提出。水印技术包括编码端和解码端,编码端需要将水印嵌入载体中生成含密信息。相应地,水印将在解码端从含密信息中提取出来。在实际传输过程中,含密信息可能会受到信道的噪声干扰甚至不法分子的恶意攻击,从而破坏水印的提取过程。基于此,鲁棒水印技术被提出。鲁棒水印技术保证了水印在含密信息受到噪声或恶意攻击后仍能被准确提取。鲁棒性、视觉质量以及嵌入容量是衡量鲁棒水印技术的重要指标。

传统的鲁棒水印技术大致可以分为3类:基于像素域的方法^[2-3]、基于变换域的方法^[4-15]、基于几何不变域的方法^[16-22]。基于像素域的方法通过改变非重叠块中相邻像素间的空间关系实现了在像素域中的鲁棒水印嵌入,该方法能够抵抗常

见的一些图像处理攻击,如模糊、滤波等。随着研究的进行,许多学者发现变换域相比于像素域更具鲁棒性。Cox等^[4]提出了基于变换域的鲁棒水印技术,该方法通过改变离散余弦变换后的频域系数来嵌入方法,其能在一定程度上抵抗有损压缩和滤波。Hsu等^[5]在文献[4]的基础上进行了算法改进,将水印嵌入每一个非重叠图像块中的中频系数以提升含密图像的质量。此外,针对变换域鲁棒水印的研究有许多(如离散余弦变换(DCT)^[6-9]、离散小波变换(DWT)^[10-11]、奇异值分解(SVD)^[12-13]、提升小波变换(LWT)^[14-15])。尽管上述方法对常见的噪声、滤波、模糊、有损压缩等攻击达到了一定程度的鲁棒性,但对几何攻击(如旋转或缩放)的抵抗力仍然具有很大的挑战。为了解决这个问题,基于几何不变域的方法被提出。文献[16-17]中的方法利用不变的区域产生Harris三角形网格来嵌入水印。此外,几何不变域由于其受几何攻击前后系数不变的特性被应用于鲁棒水印以抵抗旋转、剪切和缩放等几何攻击。基于几何不变域的方法有傅里叶梅林域^[18-19]、

Zernike 矩^[20-22]、非径向单位映射矩^[23]。这些方法通过对不变矩系数的修改来嵌入水印以达到抵抗几何攻击的目的。不难发现,传统的鲁棒水印技术一般是通过针对已知攻击的程度来设计或构造能够抵抗该攻击的特征系数,其优势在于将人工先验知识作为基础展开探索和设计。然而,传统的鲁棒水印对不同种类型攻击的综合抵抗能力仍然有待提升。此外,由于嵌入方式的局限性,传统鲁棒水印算法对不同图像的泛化处理能力较弱。

近年来,深度学习由于其强大的自学习能力被广泛应用于鲁棒水印技术领域。Zhu 等^[24]提出一个基于端对端的深度神经网络水印算法,其利用生成对抗网络(GAN)^[25]的对抗生成理念来训练以得到最佳的编码解码网络。Hidden^[24]的端对端网络的特点在于新的失真可以直接合并到训练过程中而无须设计新的专用算法。文献[26]提出的 StegaStamp 模型在文献[24]的方法基础上将真实物理世界的模拟攻击加入噪声层并且进行了多类型攻击叠加训练,其实验表明了模型具有良好的鲁棒性和视觉质量。然而,基于深度网络的鲁棒水印算法的初始化通常来源于随机的参数和特征,所以常会导致生成的模型质量不佳、训练时间过长,甚至无法收敛的情况。基于此,本文拟结合传统算法的特征设计优势以及深度网络在搜索和优化方面的强大能力,设计一种基于传统引导机制的深度鲁棒水印算法。本文的主要贡献如下:

- 1) 提出基于传统引导机制的深度鲁棒水印算法;
- 2) 为所提出的算法设计新的损失函数;
- 3) 设计不同程度水印的传统含密图像加入引导机制以探索最佳的模型构造。

1 相关工作

1.1 StegaStamp 算法

StegaStamp^[26]是一种基于深度网络的数字图像水印算法,其以接近不可感知的方式将任意超链接位串进行鲁棒编码和解码。StegaStamp 包含一个端对端的深度神经网络,它被用来学习抵抗近似于真实印刷和摄影造成的扭曲空间扰动的图像编码/解码算法。StegaStamp 算法的框架如图 1 所示,主要由编码器、噪声层、解码器等构成。编码器将水印信息以视觉不可见的效果嵌入原始图像中并生成载密图像。噪声层模拟图 1 中载密图像拍摄后至受损图像的过程。解码器期望从受损图像中尽可能完整地提取出嵌入的水印信息。该算法的损失函数如下:

$$L = \lambda_R L_R + \lambda_P L_P + \lambda_C L_C + \lambda_M L_M \quad (1)$$

式(1)表明该算法的训练目标可以概括为:最小化输入图像与含密图像的视觉误差(L_2 范数残差正则化 L_R 、学习感知损失 L_P 、判别损失 L_C),最小化解码信息与原始秘密信息的距离(交叉熵损失 L_M)。 λ 表示对应损失的权重,目标函数由上述损失的加权和构成。

1.2 基于 DCT 域的鲁棒水印算法

文献[9]提出了一种基于 DCT 域的鲁棒水印算法,该算法的框架如图 2 所示。

该算法首先将输入的彩色图像转化为 YUV 形式,然后对 Y 通道图像即亮度通道的图像进行离散余弦变换得到 DCT 系数矩阵。被选中的 DCT 系数将通过一种量化索引调制(QIM)的算法嵌入水印信息。

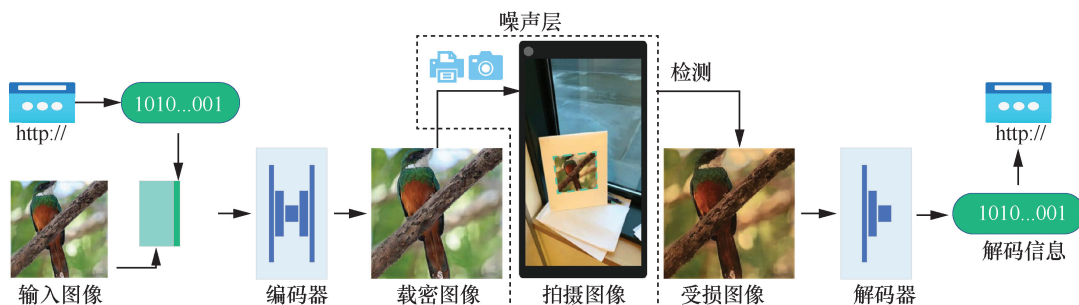


图1 StegaStamp 算法的框架
Figure 1 The framework of StegaStamp algorithm

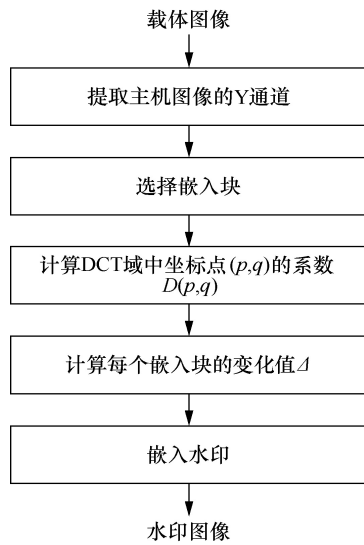


图2 基于DCT域的鲁棒水印算法的框架
Figure 2 The framework of robust watermarking algorithm based on DCT domain

具体的水印嵌入公式如式(2)所示。此外,该算法通过调节量化步长 Q_{step} 的大小来控制含密图像的鲁棒性以及视觉质量。越大的 Q_{step} 获取越强的鲁棒性,然而视觉质量会越差。

$$D' = \begin{cases} \text{round}\left(\frac{D}{Q_{step}}\right) \cdot Q_{step} + \frac{Q_{step}}{2}, (R \bmod 2) \text{ x or } (w) = 0 \\ \text{round}\left(\frac{D}{Q_{step}}\right) \cdot Q_{step} - \frac{Q_{step}}{2}, (R \bmod 2) \text{ x or } (w) = 1 \end{cases}$$

(2)

2 本文算法

为了促进深度学习的能力,并且融合传统算法在特征设计上的优势,本文提出一种基于传统引导机制的深度鲁棒水印算法。如图3所示,该框架主要由传统编码器、深度编码器、噪声层以及解码器组成。

在该算法中,原始彩色图像将会在预处理过程中经过传统编码器生成含密的传统水印图像。然后,水印信息与原始彩色图像以及传统水印图像进行通道叠加,作为U-Net^[27]构架的输入。经过U-Net的下采样和上采样网络后,全连接输出同尺寸的含密彩色图像。噪声层被用来模拟真实物理世界中的各种噪声及攻击。含密彩色图经过噪声层被送入解码器中进行水印信息的解码。解码器是一个用来恢复编码后图像中隐藏的水印消息的深度网络。含密彩色图经过噪声层被送入解码器中进行水印信息的解码。

(1) 传统编码器

在本文提出的算法中,原始彩色图像将在预处理过程中通过传统编码器生成彩色的传统鲁棒水印图。具体地,一幅 $400 \times 400 \times 3$ 的原始彩色RGB图像首先被转换成YUV格式,Y通道的亮度分量系数矩阵随后被划分成100个

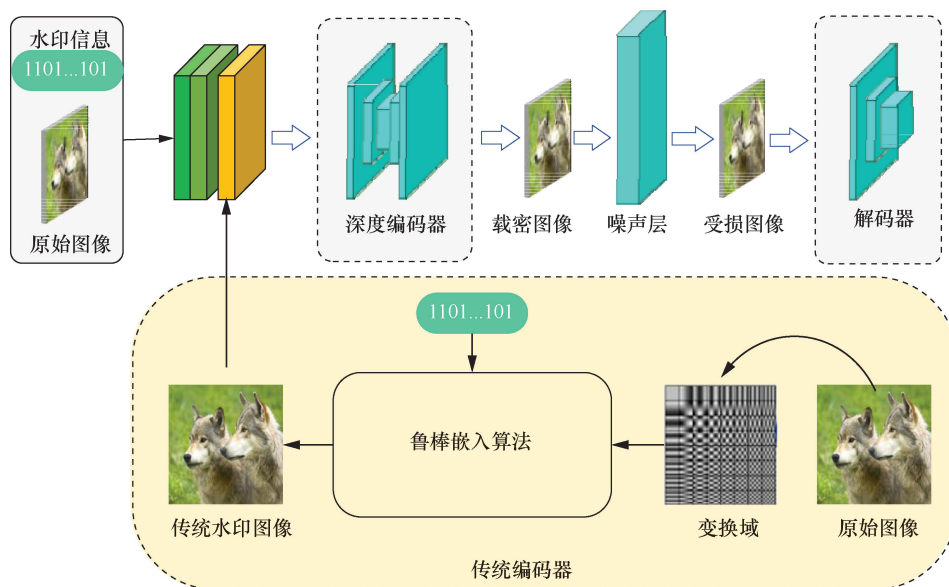


图3 基于传统引导机制的深度鲁棒水印算法的框架
Figure 3 Traditional guidance mechanism based deep robust watermarking algorithm framework

40×40 的非重叠块。每一个非重叠块矩阵通过奇异值分解得到一个最大奇异值（记为 S ）。与 1.2 节水印算法相同， S 通过式(3)被修改为 S' 以嵌入 1 bit 信息 w 。

$$S' = \begin{cases} \text{round}\left(\frac{S}{Q_{\text{step}}}\right) \cdot Q_{\text{step}} + \frac{Q_{\text{step}}}{2}, \\ \left(\text{round}\left(\frac{S}{Q_{\text{step}}}\right) \bmod 2\right) x \text{ or } (w) = 0 \\ \text{round}\left(\frac{S}{Q_{\text{step}}}\right) \cdot Q_{\text{step}} - \frac{Q_{\text{step}}}{2}, \\ \left(\text{round}\left(\frac{S}{Q_{\text{step}}}\right) \bmod 2\right) x \text{ or } (w) = 1 \end{cases} \quad (3)$$

所有的块嵌入完成后， S' 替换原有的 S 并通过奇异值分解的逆过程还原至像素域。最后，YUV 像素格式的传统含密图像被重新转换成 RGB 格式。

(2) 深度编码器

深度编码器被训练以将消息嵌入图像中同时最小化输入图像（图 2 中的原始图像和传统水印图像）与输出图像（图 2 中的载密图像）的感知差异。在本文提出的算法中，3 幅 400×400×3 的图像连接（即一个 400×400×9 的张量）后，三通道的原始彩色图像和三通道的传统鲁棒水印图以及 100 位二进制字符串的水印信息将作为 3 个输入被送入深度编码器（U-Net^[27]风格的架构），其中，水印信息可通过上采样、复制等方式扩展到 400×400×3 的尺寸，以保证与传统的鲁棒水印图像尺寸一致。本文的 U-Net^[27]架构与 StegeStamp 中的类似，通过多个卷积层、池化层、上采样，最终全连接输出三通道的 RGB 残差图像。最终的三通道含密图像将由原始图像与残差图像通过像素叠加生成。

(3) 噪声层

为了模拟真实物理世界中图像传输或者在拍摄打印时会遭受的攻击，噪声层的设计参考了文献[26]。噪声层大致可分为像素型扰动和空间型扰动。像素型扰动通常指常见的噪声干扰以及 JPEG 压缩等，空间型扰动则一般指几何攻击等。与 StegaStamp 相同，本文的噪声层干扰包括噪

声、色彩变换、JPEG 压缩、透视扭曲以及模糊处理。

(4) 损失函数

由于本文提出的算法基于传统鲁棒水印算法，预期通过训练达到深度网络与传统鲁棒水印算法优势融合，使得最终水印图像的综合性能（如视觉质量、鲁棒性）得以提升。本文设计的损失函数如式(4)所示。

$$L = \lambda_{R1}L_{R1} + \lambda_{R2}L_{R2} + \lambda_P L_P + \lambda_C L_C + \lambda_M L_M \quad (4)$$

为了保证深度网络与传统鲁棒水印算法的融合学习。本文在视觉质量上要求最小化载密图像与原始图像的视觉误差为 L_{R1} ，同时在融合过程中也要求含密图像与传统水印图像的视觉误差为 L_{R2} 。 L_{R1} 和 L_{R2} 都表示 L_2 范数残差正则化损失。

3 实验设计与结果分析

为了证明本文算法的优势，本文进行了一系列测试。首先，依据本文算法与 StegaStamp 算法构建的模型（分别简称为本文模型与 StegaStamp 模型）在同样的条件下进行了测试对比。本文随机从 MIRFLICKR 数据集^[28]中挑选 4 500 幅自然图像作为训练集，另随机挑选 500 幅自然图像作为测试图像集。训练过程中 100 bit 的水印信息将被嵌入图像中生成最终的含密图像（也称水印图像）。

3.1 实验方案及评估参数设计

由于引入的传统鲁棒水印算法中量化步长 Q_{step} 的变化能够对嵌入的鲁棒强度和视觉质量产生影响，本文通过设计不同的嵌入强度（ Q_{step} 的取值）进行测试以观察不同参数下传统鲁棒水印图像对深度模型的影响。此外，本文对传统含密图像与深度的融合比例（引入的传统水印图像嵌入区域的占比）进行了设置以探索不同融入比例对模型的影响。融入传统水印图的设计如图 4 所示。

如图 4 所示，本文模型将融合比例和嵌入强度分别设为 100%、100，作为提出的基本模型（记为 Proposed）。此外在强度为 100 时，分别设置融合比例为 80%、60%作为两组对照模型（分别

记为 Pro-80%、Pro-60%)。类似地, 在融合比例为 100% 时, 嵌入强度设为 150 和 200 的模型也作为两组对照模型 (分别记为 Pro-150、Pro-200)。

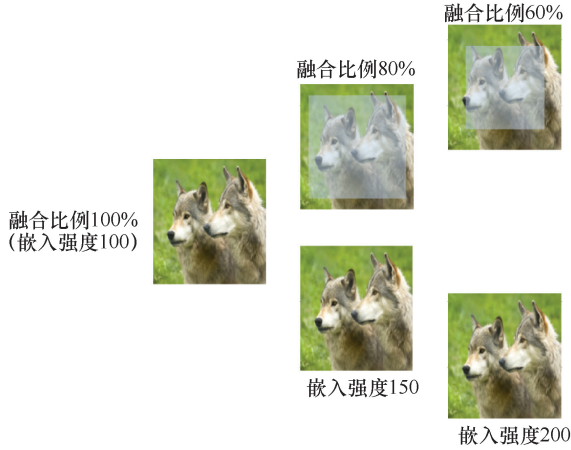
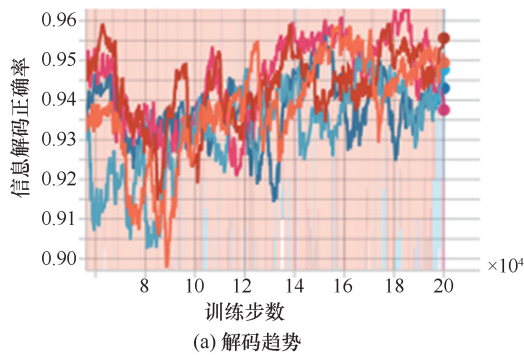


图4 融入传统水印图的设计

Figure 4 Design-integrated traditional stego-image

视觉质量和鲁棒性是评估鲁棒水印算法模型性能的两个重要指标。其中视觉质量由峰值信噪比 (PSNR, peak signal to noise ratio) 来衡量, 如式(5)所示。

$$\text{PSNR} = 10 \lg \left(\frac{255^2 rc}{\sum_{i=1}^r \sum_{j=1}^c (I(x, y) - I_w(x, y))^2} \right) \quad (5)$$



(a) 解码趋势

Name	Smoothed	Value	Step	Time	Relative
train	0.9497	0.9425	192.6k	Tue Feb 22, 17:27:50	1d 2h 5m 21s
train_150	0.9474	0.975	192.6k	Sat Feb 26, 02:43:54	1d 4h 15m 46s
train_200	0.9407	0.93	192.6k	Tue Mar 1, 13:31:45	1d 5h 0m 33s
train_60%	0.9572	1	192.6k	Fri Mar 4, 19:06:52	1d 4h 39m 52s
train_80%	0.9419	0.9875	192.6k	Thu Feb 24, 17:55:45	1d 3h 20m 24s

(c) 解码正确率

其中, r 和 c 分别表示图像的长和宽, I 表示原始图像, I_w 表示最终载密图像。

另外, 误码率 (BER, bit error ratio) 用来衡量模型的鲁棒性, 其计算公式如式(6)所示。

$$\text{BER} = \frac{L_{\text{error}}}{L_{\text{origin}}} \quad (6)$$

3.2 模型训练效果

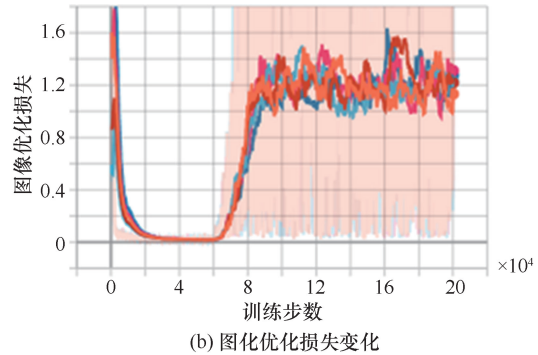
本文对不同的模型进行训练, 训练结果如图 5 所示。

从图 5 可以看出, 所有模型在 20 万步都能够收敛至较理想的效果。针对不同 Q_{step} , 不难发现嵌入强度为 150 的情况下训练效果相对较好, 比特正确率可达到 97.5%。同样, 从不同融合比例来看, 80% 的融合比例训练效果较好, 比特正确率可达到 98.75%, 说明 80% 的融合比例下融合效果相对较好。

3.3 模型测试效果

本节主要对本文模型与 StegaStamp 模型做了简单的对比, 在测试图中随机取一幅, 其模型测试的图像视觉效果如图 6 所示。

两个模型的训练均能保证信息嵌入前后有较好的视觉不可见性。为进一步证实本文模型的有效性及其优势, 将借助峰值信噪比 (PSNR) 和结构相似度 (SSIM, structural similarity) 两个参数对本文模型与 StegaStamp 模型进行比较。



(b) 图化优化损失变化

Name	Smoothed	Value	Step	Time	Relative
train	1.132	4.836	200k	Tue Feb 22, 18:39:48	1d 3h 17m 19s
train_150	1.218	1.455	200k	Sat Feb 26, 03:52:18	1d 5h 24m 10s
train_200	1.225	2.3	200k	Tue Mar 1, 14:33:25	1d 6h 2m 13s
train_60%	1.308	1.127	200k	Fri Mar 4, 20:08:52	1d 5h 41m 52s
train_80%	1.276	1.35	200k	Thu Feb 24, 18:58:23	1d 4h 23m 2s

(d) 图像优化损失值

图5 模型训练结果

Figure 5 The result of model training

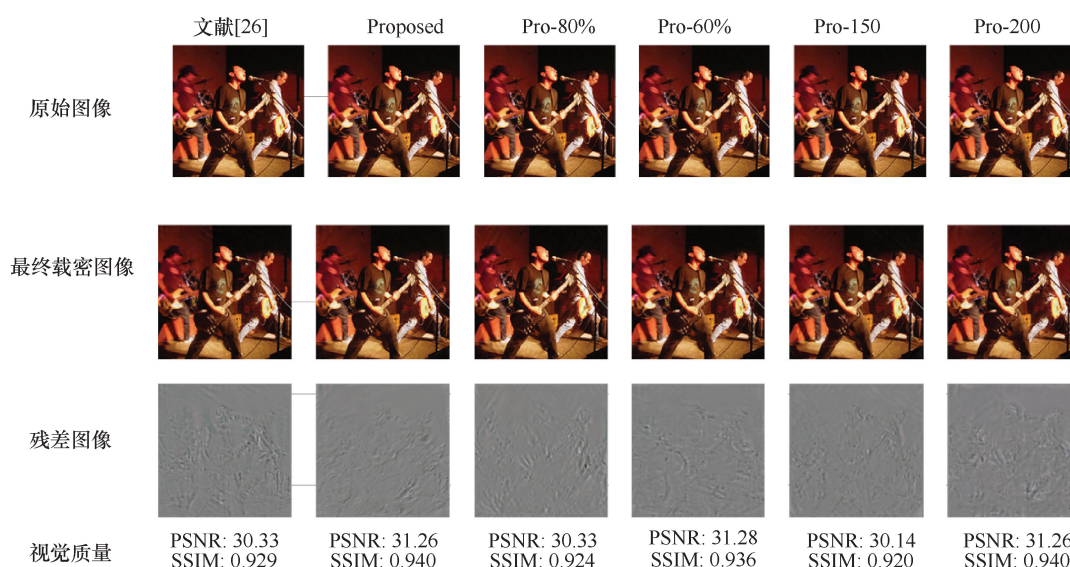


图 6 模型测试的图像视觉效果
Figure 6 Image visualization for model testing

显然，如表 1 所示，本文提出的所有模型与 StegaStamp 模型都有着接近的 PSNR 和 SSIM。其中最显著的是 Q_{step} 设为 150 时的模型，其 PSNR 均高于 StegaStamp 模型。

表 1 视觉质量对比
Table 1 Visual Quality Comparison

模型方案	平均 PSNR/dB
StegaStamp	30.926
Proposed	31.848
Pro-80%	31.496
Pro-60%	31.838
Pro-150	31.632
Pro-200	31.016

在模型的鲁棒性测试实验中，所有模型均分别遭受噪声层中 5 种攻击类型的独立攻击和叠加攻击。所有模型对 500 幅测试集图像经过攻击后

的解码平均误码率如表 2 所示。

相比 StegaStamp 模型，本文提出的模型拥有更低的误比特率和更强的鲁棒性。其中，StegaStamp 对于叠加攻击的 BER 为 4.16%，而本文提出的 Pro-150 的 BER 达到了 2.72%。此外，Pro-150 对所有独立攻击的 BER 都低于 StegaStamp 模型。

从视觉质量和鲁棒性等综合性能上分析，本文提出的基于传统引导机制的深度鲁棒水印模型能够有效提升水印算法的鲁棒性和视觉质量。

4 结束语

随着鲁棒水印技术在实际应用环境中不断受到挑战，本文提出一个基于传统引导机制的深度鲁棒水印算法。该算法在沿用 StegaStamp 算法的基础上融合传统鲁棒水印算法在特征设计方面的优

表 2 平均误码率
Table 2 Average BER

攻击类型	StegaStamp	Proposed	Pro-80%	Pro-60%	Pro-150	Pro-200
All	4.16%	3.79%	2.68%	2.72%	2.72%	3.36%
Warp	1.42%	1.04%	0.22%	0.18%	0.18%	0.56%
Blur	0.05%	0.02%	0.03%	0.02%	0.02%	0.03%
Noise	0.04%	0.02%	0.05%	0.03%	0.03%	0.03%
Color	1.15%	1.56%	1.48%	1.12%	1.12%	1.99%
JPEG	0.08%	0.02%	0.05%	0.02%	0.02%	0.17%

势,并探索不同融合程度对框架性能的影响。实验结果表明,本文提出的模型能够有效地提升算法的视觉质量和鲁棒性。后续将会考虑探索不同的传统鲁棒水印算法与深度模型的优化匹配问题。

参考文献:

- [1] BARNI M, BARTOLINI F, COX I J, et al. Digital watermarking for copyright protection: communications perspective[J]. IEEE Communications Magazine, 2001, 39(8): 90-91.
- [2] NIKOLAIDIS N, et al. Robust image watermarking in the spatial domain[J]. Signal Processing, 1998, 66(3): 385-403.
- [3] ZHANG W Y. Semi-fragile spatial watermarking based on local binary pattern operators[J]. Optics Communications, 2011, 284(16/17): 3904-3912.
- [4] COX I J, KILIAN J, LEIGHTON F T, et al. Secure spread spectrum watermarking for multimedia[J]. IEEE Transactions on Image Processing, 1997, 6(12): 1673-1687.
- [5] HSU C T, WU J L. Hidden digital watermarks in images[J]. IEEE Transactions on Image Processing, 1999, 8(1): 58-68.
- [6] HUANG J W, SHI Y Q, SHI Y. Embedding image watermarks in dc components[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2000, 10(6): 974-979.
- [7] CHU W C. DCT-based image watermarking using subsampling[J]. IEEE Transactions on Multimedia, 2003, 5(1): 34-38.
- [8] AHMED N, NATARAJAN T, RAO K R. Discrete cosine transform[J]. IEEE Transactions on Computers, 1974, 23(1): 90-93.
- [9] BYUN S W, SON H S, LEE S P. Fast and robust watermarking method based on DCT specific location[J]. IEEE Access, 2019, 7: 100706-100718.
- [10] COX I, MILLER M, BLOOM J, et al. Digital watermarking and steganography[M]. Morgan Kaufmann Publishers Inc, 2007.
- [11] NEZHADARYA E, WANG Z J, WARD R K. Robust image watermarking based on multiscale gradient direction quantization[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(4): 1200-1213.
- [12] CHANG C C. SVD-based digital image watermarking scheme[J]. Pattern Recognition Letters, 2005, 26(10): 1577-1586.
- [13] MOHAMMAD A A, ALHAT S S. An improved SVD-based watermarking scheme for protecting rightful ownership[J]. Signal Processing, 2008, 88(9): 2158-2180.
- [14] NI R R, RUAN Q Q, LIU J Q. Tampering estimation watermarking based on lifting wavelet and chaotic sequence[C]//Proceedings of 2006 8th International Conference on Signal Processing. 2006.
- [15] GU Q L, GAP T G. A novel reversible robust watermarking algorithm based on chaotic system[J]. Digital Signal Processing, 2013, 23(1): 213-217.
- [16] SEO J S, YOO C D. Image watermarking based on invariant regions of scale-space representation[J]. IEEE Transactions on Signal Processing, 2006, 54(4): 1537-1549.
- [17] LU C S, SUN S W, HSU C Y, et al. Media hash-dependent image watermarking resilient against both geometric attacks and estimation attacks based on false positive-oriented detection[J]. IEEE Transactions on Multimedia, 2006, 8(4): 668-685.
- [18] LIN C Y, WU M, BLOOM J A, et al. Rotation, scale, and translation resilient watermarking for images[J]. IEEE Transactions on Image Processing: a Publication of the IEEE Signal Processing Society, 2001, 10(5): 767-782.
- [19] ZHENG D, ZHAO J, EL SADDIK A. RST-invariant digital image watermarking based on log-polar mapping and phase correlation[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(8): 753-765.
- [20] KIM H S, LEE H K. Invariant image watermark using Zernike moments[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(8): 766-775.
- [21] XIN Y Q, LIAO S, PAWLAK M. A multibit geometrically robust image watermark based on Zernike moments[C]//Proceedings of the 17th International Conference on Pattern Recognition. 2004: 861-864.
- [22] XIN Y, LIAO S, PAWLAK M. Geometrically robust image watermarking on a circular domain[J]. Pattern Recognition, 2007, 40(1): 3740-3752.
- [23] GOLABI S. Non-unit mapped radial moments platform for robust, geometric invariant image watermarking and reversible data hiding[J]. Information Sciences, 2018, 447: 104-116.
- [24] ZHU J, RUSSELL K, JUSTIN J, et al. Hidden: hiding data with deep networks[C]//Proceedings of ECCV. 2018: 682-697.
- [25] GOODFELLOW I J, JEAN P A, MEHDI M, et al. Generative adversarial nets[C]//Proceedings of the 27th International Conference on Neural Information Processing Systems. 2014: 2672-2680.
- [26] TANCIK M, MILDENHALL B, NG R. StegaStamp: invisible hyperlinks in physical photographs[C]//Proceedings of 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2020: 2114-2123.
- [27] RONNEBERGER O, FISCHER P, BROX T. U-Net: convolutional networks for biomedical image segmentation[C]//Proceedings of Medical Image Computing and Computer-Assisted Intervention-MICCAI 2015. 2015: 234-241.
- [28] HUISKES M J, LEW M S. The MIR flickr retrieval evaluation[C]//Proceedings of the 1st ACM International Conference on Multimedia Information Retrieval. 2008: 39-43.

[作者简介]



郭学镜（1996- ），男，江西上饶人，景德镇陶瓷大学硕士生，主要研究方向为信息安全与数字图像处理。



张天助（1993- ），男，江西上饶人，景德镇陶瓷大学助理讲师，主要研究方向为信息安全与数字图像处理。



方毅翔（1987- ），男，江西景德镇人，景德镇陶瓷大学讲师，主要研究方向为信息安全与数字图像处理。



曾文超（1996- ），男，湖北宜昌人，景德镇陶瓷大学硕士生，主要研究方向为信息安全与数字图像处理。



赵怡（1985- ），女，江西南昌人，景德镇陶瓷大学实验师，主要研究方向为信息安全与数字图像处理。



王俊祥（1985- ），男，江西景德镇人，景德镇陶瓷大学教授，主要研究方向为信息安全与数字图像处理。