

载体独立的深度光照水印算法

陈浩^{1,2}, 王峰^{1,2}, 张卫明^{1,2}, 俞能海^{1,2}

(1. 中国科学技术大学网络空间安全学院, 安徽 合肥 230001;

2. 中国科学技术大学中国科学院电磁空间信息重点实验室, 安徽 合肥 230001)

摘要: 随着多媒体技术的发展与完善, 数字产品的版权保护需求逐步增大。数字水印是一种保护数字产品版权的有效手段, 它一般是通过在数字载体(如文本、图像等)中添加重要标识信息(即数字水印), 使载体带有标识信息, 但又不影响载体的正常使用。常见的数字水印嵌入方案是通过采用特定算法对载体进行修改来嵌入水印信息的。而在实际的应用场景中, 有很多待保护的图像或物件(如艺术画作等)是不允许修改的。基于此背景, 提出了一种新的载体独立的深度光照水印算法, 在嵌入端通过可见光调制的方法来表达水印信息, 从而实现在不对原始载体进行修改的前提下进行水印信息嵌入, 并达到版权保护的目的。通过对人眼视觉系统进行分析, 提出了基于交替式投影的水印模板图案来嵌入水印信息, 使嵌入过程既不需要对原始载体进行修改, 也不会影响人眼的视觉感官。而在提取端, 设计了基于残差连接的水印提取网络, 对采集的水印图像经透视变换后送入该网络来进行水印信息提取。实验在多种条件下进行, 并与3种基准算法进行了对比。实验结果表明, 所提算法生成的水印图像具有较小的视觉失真, 且对“投影-拍摄”过程具有很强的鲁棒性。在不同距离、角度、光照等条件下, 水印提取网络具有很高的水印信息提取准确率, 且相比其他通用网络具有一定的优越性。

关键词: 数字水印; 人眼视觉系统; 光照水印; 深度神经网络

中图分类号: TP309.2

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022056

Carrier-independent deep optical watermarking algorithm

CHEN Hao^{1,2}, WANG Feng^{1,2}, ZHANG Weiming^{1,2}, YU Nenghai^{1,2}

1. School of Cyber Science and Technology, University of Science and Technology of China, Hefei 230001, China

2. CAS Key Laboratory of Electromagnetic Space Information, University of Science and Technology of China, Hefei 230001, China

Abstract: With the development of multimedia techniques, the demand for copyright protection of digital products has also gradually risen. Digital watermarking is an effective means to protect the copyright of digital products. It is generally made by adding important identification information (i.e., digital watermark) to a digital carrier (e.g., text, image, etc.), so that the carrier carries the identification information but does not affect the normal use of the carrier.

收稿日期: 2022-02-08; **修回日期:** 2022-05-19

通信作者: 俞能海, ynh@ustc.edu.cn

基金项目: 国家自然科学基金(U20B2047, 62121002)

Foundation Item: The National Natural Science Foundation of China(U20B2047, 62121002)

引用格式: 陈浩, 王峰, 张卫明, 等. 载体独立的深度光照水印算法[J]. 网络与信息安全学报, 2022, 8(4): 110-118.

Citation Format: CHEN H, WANG F, ZHANG W M, et al. Carrier-independent deep optical watermarking algorithm[J]. Chinese Journal of Network and Information Security, 2022, 8(4): 110-118.

The common digital watermark embedding scheme is to embed the watermark information by modifying the carrier via specific algorithms. In the actual application scenarios, there are many images or objects to be protected (such as art paintings, etc.) that are not allowed to be modified. Based on this background, a new carrier-independent deep optical watermarking algorithm was proposed, which can realize watermark information embedding without modifying the original carrier and achieve the purpose of copyright protection. Specifically, a new watermark template expression scheme at the embedding end was proposed, which expressed the watermark information by visible light modulation. By analyzing the visual system of human eyes, a watermark template pattern based on alternating projection was proposed to embed the watermark information, which made the embedding process neither require modification of the original carrier nor affect the visual senses of human eyes. At the extraction end, a watermark extraction network based on residual connection was designed, and the captured watermarked images were fed into this network after perspective transformation to extract the watermark information. The experiments were conducted under various conditions and comparisons with three baseline algorithms were made. The experimental results show that the proposed algorithm generates watermarked images with less visual distortion and is robust to the "projecting-shooting" process. The watermark extraction network has high accuracy in extracting watermark information at different distances, angles and illumination conditions, and has certain advantages over other general networks.

Keywords: digital watermarking, human visual system, optical watermarking, deep neural network

0 引言

网络技术的快速发展加快了图像、音视频等数字产品的传播效率,但同时引起了非法复制的版权纠纷问题。因此,在这些环境中数字产品的产权保护成为紧迫问题,而应用于数字图像产权保护的数字水印技术被广泛研究^[1-12]。数字水印技术一般是通过对数字载体进行修改,实现水印信息的嵌入。而为了实现对不同传输信道失真的鲁棒性,往往会有不同的嵌入方式。但这些方案的共同缺点在于嵌入过程本身需要对载体进行修改。当面临无法修改载体的水印需求时,这些方案的用处往往受限。例如,当需要保护博物馆中的艺术画作时,无法对艺术画作本身进行修改,实现一种与载体独立的数字水印方案尤为重要。

本文着眼于“载体独立”的应用需求,旨在提供一种无须修改载体的数字水印方案来保护数字媒体的版权,即基于光照水印的技术^[13-21]。光照水印指的是将含水印信息的光照投射到目标区域,当有光照的载体被相机拍摄时,能从采集到的图像中提取出嵌入的水印信息。该方法通常用一些特殊设计的光照模式表示水印信息,并将这些模式投射到目标图像上,实现水印的嵌入过程。而在提取端,通过一定的图像处理过程,将投影

的水印模式从拍摄的图像中提取出来,从而实现水印信息解码。

理想的光照水印应该同时满足3个特性:高视觉质量、高嵌入效率和传输鲁棒性。对于视觉质量的需求,光照投影的前后不应有明显的视觉失真,要达到足够的透明性。而嵌入效率的需求指的是水印嵌入端应尽可能地避免过多的计算,从而满足高效的嵌入过程。传输鲁棒性指的是对算法解码端的要求,水印在嵌入过后还经过了投影-拍摄信道,需要保证在经历了失真后仍然能够进行提取。

传统的光照水印方案主要是基于频域信息变换来实现的,不能同时满足上述3个特性。手机拍摄信道较为复杂,传统的图像处理操作不能很好地模拟传输信道的失真,这导致如果想要得到较高的提取准确率,就得保证较大的嵌入强度,但这样又会引起较差的视觉质量。因此,算法的关键在于如何更好地兼顾视觉质量和传输鲁棒性。

为了满足视觉质量的需求,本文设计了一种基于人眼视觉模型(HVS, human visual system)的水印嵌入方案,当以较高的频率观察颜色互补的彩色区域时,人眼会出现视觉疲劳,在大脑中自动对彩色区域进行加工,使整体区域看起来趋于一致。因此,本文设计了一种基于颜色分解的

新编码方案, 该方案通过创建两个互补颜色的水印图案来编码“0/1”比特。为了从错综复杂的信道失真中恢复出嵌入的水印信号, 本文选择使用深度神经网络作为水印的提取端。利用深度学习强大的特征提取能力, 通过卷积神经网络的输出分析水印模板类别, 从而实现消息的准确提取。

为了展示所提方法的有效性和优越性, 本文在不同的拍摄环境(如不同的距离、不同角度和不同光照强度)下进行了大量的实验。实验结果表明, 该方法在保证视觉质量的同时, 始终可以实现出色的鲁棒性。

综上所述, 本文的主要贡献有以下 3 个方面。

1) 提出了一种基于深度学习的光照水印方案, 该方案能有效地实现载体无关的水印嵌入过程, 并应用于艺术作品的版权保护。

2) 结合 BCH (Bose-Chaudhuri-Hocquenghem) 编码, 设计了一种高效的水印叠加嵌入方案, 并设计了基于深度神经网络的提取方案, 两者结合能有效地兼顾水印的鲁棒性与透明性。

3) 大量实验表明, 本文提出的算法在鲁棒性和视觉质量上优于已有算法。

1 相关工作

光照水印最早由 Uehira^[15]等提出, 利用固定大小的图像块表示 1 bit 信息, 即对于 $N \times N$ 大小的频域图像模板 F , 分别记直流分量和最高频分量为 DC、HC, 并根据信息比特对高频分量的符号进行调整。

$$F(0,0) = \text{DC} \quad (1)$$

$$F(N-1, N-1) = \begin{cases} \text{HC, '1'} \\ -\text{HC, '0'} \end{cases} \quad (2)$$

对于其他区域的元素, 令 $F(u,v) = 0$, 然后利用离散余弦变换 (DCT, discrete cosine transform) 反变换得到空域模板, 计算如下:

$$f(x,y) = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} C(u)C(v)F(u,v) \cos\left[\frac{(x+0.5)\pi}{N}u\right] \cdot \cos\left[\frac{(y+0.5)\pi}{N}v\right] \quad (3)$$

其中

$$C(u) = \begin{cases} \sqrt{\frac{1}{N}}, u=0 \\ \sqrt{\frac{2}{N}}, u \neq 0 \end{cases} \quad (4)$$

再由投影仪将水印模板投射到目标图像上。而水印提取过程则完全相反, 将拍摄图片切块后进行 DCT 变换得到频域块, 并根据每个频域块的高频成分 $F(N-1, N-1)$ 的正负号来判断该图像块所嵌入的水印信息。

此后, Ishikawa^[16]等提出不同的光照水印模板, 利用沃尔什-哈达玛变换 (WHT, Walsh-Hadamard transform) 反变换生成对应的水印空域模板, 如式(5)所示。

$$f(x,y) = \frac{1}{N} \sum_u \sum_v F(u,v) \text{wh}(x,u) \text{wh}(v,y) \quad (5)$$

其中, $\text{wh}(i,j)$ 表示沃尔什-哈达玛矩阵分量。

Uehira^[17]等提出了视觉质量更好、水印提取误码率更低的色差调制方案。在频域模板经过 DCT 反变换后并没有直接进行投射, 而是将变换后的图像当作 YCbCr 色彩空间中的 Cb 通道, 与固定数值的 Y、Cr 通道组合后变换成 RGB 图像, 最后通过投影仪投射到目标图像上。

前述方法仅考虑提取信息的准确性, 这使嵌入的视觉质量较差, 而降低嵌入强度时, 频域的嵌入方式又不能很好地抵抗拍照失真, 无法满足光照水印的需求。

2 基于深度学习的光照水印方法

光照水印系统框架如图 1 所示, 该框架包含两个部分(水印嵌入过程和水印提取过程), 左上方为水印信息编码排布过程, 右侧为水印提取网络, 其主要结构为 ResNet 残差网络。首先使用 BCH^[22]编码和循环冗余校验^[23] (CRC, cyclical redundancy check) 对消息序列进行编码, 然后对编码后的消息序列重新排列以生成要嵌入的消息矩阵。根据消息矩阵生成光照模板并对光源进行调制, 最后照射到目标图像上。在提取方面, 首先对拍摄图像进行透视变换矫正, 然后将矫正的图像输入残差神经网络进行提取以恢复消息矩阵, 之后对提取的消息矩阵进行 BCH 解码和 CRC 校验。若未检测到 CRC 错误, 则为最终

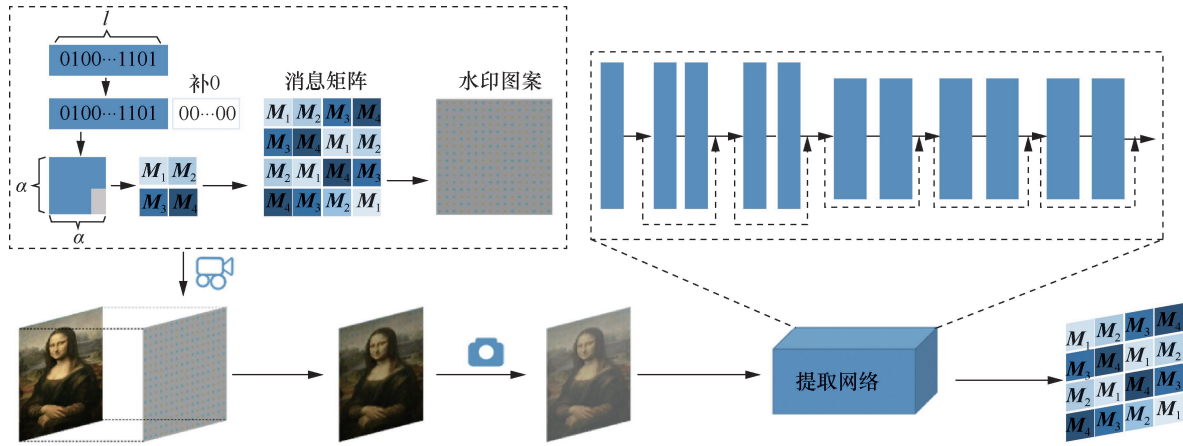


图 1 光照水印系统框架
Figure 1 Optical watermarking system framework

消息序列。若出现 CRC 错误，则重新选择消息序列并进行相同的解码过程，直到未检测到错误或尝试了所有组合。

2.1 消息矩阵生成

在从嵌入水印信息的目标图像到相机的过程中，可能会出现各种失真，并且不同的失真会从不同的角度影响图像内容，如摩尔纹和光照失真可能影响一片区域，产生不可逆的失真。为了保证消息的可提取性，需要将完整的水印单元多次重复地进行嵌入。基于以上分析，本文设计了一种鲁棒的消息生成方案，如图 1 的左上角所示。具体来说，给定原始信息序列，首先通过 CRC 和 BCH 编码，生成具有检错和纠错能力的长为 l 的序列 m ；然后将 m 序列调整为 $a \times a$ 的矩阵（将 $a \times a - l$ 部分置零）；之后，将矩阵分为 M_1 、 M_2 、 M_3 和 M_4 ，并执行图 1 中的排列规则以生成完整的消息矩阵 M 。需要注意的是， M_1 、 M_2 、 M_3 和 M_4 的任何组合都将包含一个完整的消息序列，理想情况下矩阵 M 包含 4 组完整的消息序列，可避免潜在的局部信息丢失。

2.2 基于叠加的水印嵌入

图 2 为水印图案生成过程，本文中，1 bit 消息由一个 $b \times b$ 的图像块进行表示，不同比特的图像块的生成过程如下所示。

$$P_B(x, y) = \begin{cases} 1 - \frac{D(x, y)}{b/4}, & D(x, y) \leq \frac{b}{4} \\ 0, & \text{其他} \end{cases} \quad (6)$$

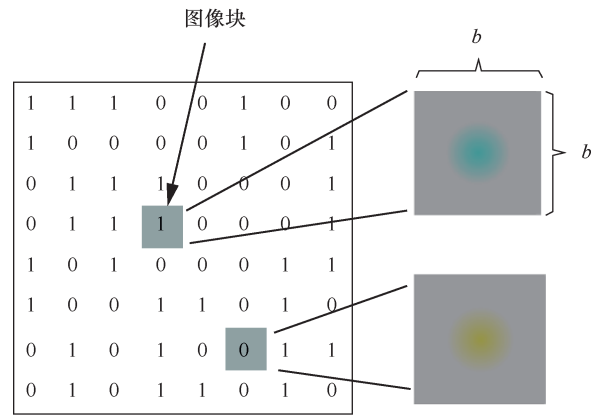


图 2 水印图案生成过程
Figure 2 Watermark pattern generation process

其中

$$D(x, y) = \sqrt{(x - b/2)^2 + (y - b/2)^2} \quad (7)$$

(x, y) 表示图像块的像素坐标。由于人类视觉系统对色度的敏感程度弱于亮度，所以设计的光照模板使用色度渐变的 RGB 图像。水印嵌入区域亮度先设置为背景灰度，当嵌入数据为“1”时对 R 通道进行调制，使 R 通道的像素值从圆周到圆心逐渐变化。同理，当嵌入数据为“0”时，对 B 通道进行调制，使 B 通道的像素值从圆周到圆心逐渐变化。

由于只对单通道进行调制，所以不同数据生成的块色度差距会很小，这样“0/1”比特对应模板图案之间的差距几乎不可见，反映到透射光源中也几乎与普通单色光没有差别。当使用足够频率的光源交替播放互补水印图案时，嵌入的水印

图像很难被人类视觉系统察觉到,同时它可以很容易地被神经网络提取出来。

2.3 水印提取

当使用手机拍摄含水印的图像时,水印图像随着图像载体本身被手机的摄像头记录下来。而在拍摄过程中,由于拍摄角度不同,图像会产生不同的透视畸变,所以在水印提取之前,需要对失真图像进行透视变换。透视变换公式为

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} & h_{13} \\ h_{21} & h_{22} & h_{23} \\ h_{31} & h_{32} & h_{33} \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} \quad (8)$$

其中,光源目标点为 $[x,y,1]$,移动到的目标点为 $[X,Y,Z]$ 。在图像校正之后,将图像分成 $b \times b$ 的像素块,每一个像素块表示 1 bit 消息,然后将像素块送入设计的提取网络中进行消息的分类。

如图 3 所示,水印提取网络 $\mathcal{R}$ 用于提取每个

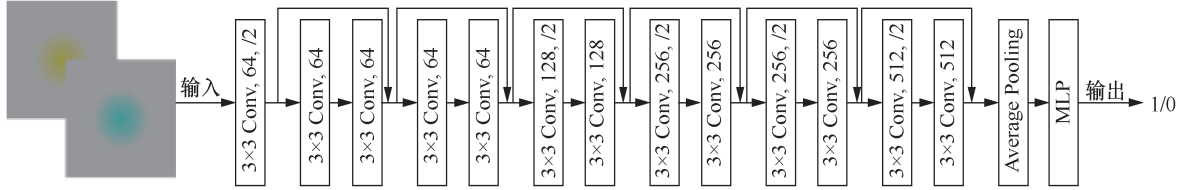


图 3 水印提取网络 $\mathcal{R}$

Figure 3 Watermark extraction network $\mathcal{R}$

3 实验与分析

对于信息序列编码,使用 BCH (64,36) 作为纠错码,其可以纠正 5 bit 错误,CRC 位的长度为 7 bit,其实际消息位为 30 bit。设置消息矩阵大小为 8×8 ,即水印信息为 64 bit,而表示 1 bit 消息的块大小设置为 $b=32$ 。将水印矩阵拆分后,每个消息块 $M_i (i=1,2,3,4)$ 大小为 4×4 。由于进行了水印矩阵的重复排列,实验中的单个水印图像大小为 512×512 。从 COCO 数据集^[25]中随机选择 100 幅图像并嵌入水印信息。然后,将单个比特水印块进行裁剪,从而得到 25 600 个水印块作为训练集。测试数据集采用经典的 USC-SIPI 图像数据集^[26],实验中使用的 DLP (digital light processing) 投影仪光源含有 800×600 像素的分辨率,水印模板被投射到目标图片上,目标图片是

图像块所代表的比特信息,并组合成最终的消息矩阵。具体来说, $\mathcal{R}$ 由一个卷积块 (Conv-BN-ReLU-MaxPooling)、6 个残差块^[24]和全连接层组成。RGB 图像块通过卷积块进行特征提取,然后由全连接层转换成一个个 1 bit 信息并组成最终消息矩阵。提取网络的训练目标是通过更新参数 $\theta_{\mathcal{R}}$ 来最小化输出消息矩阵 M' 和原始消息矩阵 $M \in \{0,1\}^{a \times a}$ 之间的差别。

$$\mathcal{L}_{\mathcal{R}} = \text{MSE}(M', M) = \text{MSE}(M', R(\theta_{\mathcal{R}})) \quad (9)$$

2.4 信息解码

提取出消息矩阵之后,需要组合出一个完整的消息序列以进行 BCH 解码和 CRC 校验。具体来说,根据信息块排布规则,尝试任一种 M_1 、 M_2 、 M_3 和 M_4 的可能组合,并对它们进行解码。如未检测到 CRC 错误,则正确信息已被提取出来,否则尝试下一种组合,直至未检测到 CRC 错误或尝试了所有组合。

以 A4 纸打印的数据集图像,共将 100 个随机水印模板投影到 100 张目标图片上。实验环境如下:目标图片上的水印投影区域为 $105 \text{ mm} \times 105 \text{ mm}$,实验使用的投影仪型号为“NEC CR3117X”,播放频率为 60 Hz,使用的手机型号为 Huawei P30 Pro。

从拍摄图像数据中裁剪出比周围区域更亮的水印嵌入区域,将裁减区域修正成大小为 512×512 像素的正方形后切割成 16×16 个图像块,每块大小为 32×32 像素。100 张图片共切割成 25 600 个图像块,即 25 600 个二进制水印数据,随机选择其中 90% (23 040 块) 作为神经网络的训练集,剩余 10% 作为验证集。选择与本文算法最相关的 DCTCode^[15]、WHTCode^[16]、Color-Difference^[17] 这 3 种水印算法作为对比算法。

3.1 视觉质量比较

为了衡量嵌入水印图像的视觉质量,采用平均主观意见分(MOS)来进行测试。具体来说,为每种光照水印嵌入方案准备16幅随机图像,然后要求50位观察者从1(视觉质量差)到5(视觉质量好)进行打分。从表1中可以发现本文所提算法的MOS远高于其他算法。图4展示了视觉质量的对比效果。



图4 视觉质量的对比效果
Figure 4 Visual quality comparison

表1 不同算法视觉质量比较
Table1 Comparison of visual quality of different algorithms

算法	MOS
DCT ^[10]	2.63
WHT ^[11]	2.87
Color-D ^[13]	3.26
本文算法	4.28

从图5可以看出,对比算法的效果图中可以清晰地看到一些水印图案形成的条纹,非常影响视觉效果。而本文算法充分利用人眼视觉的特性,将原本互补的水印图案进行抵消,从而达到更好的视觉效果。

3.2 鲁棒性测试

为了测试算法在不同拍摄条件下的鲁棒性,在不同的光照强度、拍摄距离、拍摄角度以及JPEG质量因子的前提下进行了拍照和提取实验。同时,在相同条件下将提取出的水印与原始水印进行误码率计算,得到的实验结果如表2~表5所示。

对于光照强度实验,本文选择的光照强度为50~200 cd/m²(坎德拉/平方米),其中,数值越大,代表光照强度越强。将不同强度的光照射在

载体图片中,再使用手机拍摄后进行提取水印,不同光照强度下的误码率如表2所示。由表2可知,随着光照强度的增强,算法的误码率逐渐降低,在光照强度为200 cd/m²时误码率仅有3.24%,且对于50~200 cd/m²的光照强度,算法的误码率均小于10%。这意味着提取出的水印能被纠错码进行纠错。与此同时,在相同的光照强度下,本文算法相比其他算法有明显的优势。对于不同拍摄距离下的实验,本文选择的距离为30~70 cm。由表3可知,随着拍摄距离增加,其他算法的误码率明显上升,本文所提算法虽然也有上升,但仍在10%以内,性能优势显而易见。

表2 不同光照强度下的误码率
Table 2 Bit error rate under different illumination intensity

光照强度/ (cd/m ²)	误码率			
	DCT ^[15] 算法	WHT ^[16] 算法	Color-D ^[17] 算法	本文算法
50	23.53%	24.07%	19.53%	7.23%
100	19.78%	24.33%	17.69%	5.49%
150	14.25%	11.05%	12.42%	4.88%
200	14.38%	12.26%	9.07%	3.24%

表3 不同拍摄距离下的误码率
Table 3 Bit error rate under different shooting Distance

距离/cm	误码率			
	DCT ^[15] 算法	WHT ^[16] 算法	Color-D ^[17] 算法	本文算法
30	8.29%	9.38%	7.26%	1.26%
40	12.16%	10.26%	10.33%	1.33%
50	23.05%	20.02%	15.01%	3.41%
60	22.09%	19.03%	20.21%	5.71%
70	27.65%	22.70%	23.52%	9.24%

对于拍摄角度实验,本文选择在目标图片中心的上、下、左、右以15°、30°、40°的角度进行拍摄。不同拍摄角度下的误码率如表4所示,在各个方向上都是角度越大,误码率越高,且本文算法误码率均低于其他算法。其中,拍摄角度大于15°时误码率上升明显,一方面是由于水印模板失真严重,另一方面是提取网络没有以大角度拍摄下的数据集进行训练。因此要使其对大角度拍摄更加鲁棒,还需添加更多样的训练数据集。

表 4 不同拍摄角度下的误码率
Table 4 Bit error rate at different shooting angles

角度	误码率			本文算法
	DCT ^[15] 算法	WHT ^[16] 算法	Color-D ^[17] 算法	
左 40°	23.75%	19.28%	19.35%	13.24%
左 30°	20.09%	19.05%	17.26%	6.43%
左 15°	14.27%	16.93%	11.28%	5.27%
右 15°	13.73%	24.65%	14.38%	7.26%
右 30°	18.22%	20.96%	15.33%	11.48%
右 40°	30.35%	22.49%	23.26%	15.33%
上 40°	22.44%	19.72%	20.20%	17.96%
上 30°	24.96%	21.04%	12.33%	7.24%
上 15°	16.28%	20.62%	9.03%	3.23%
下 15°	17.96%	12.53%	11.24%	7.96%
下 30°	20.35 %	22.01%	18.73%	12.48%
下 40°	30.05%	26.28%	28.62%	17.39%

对于 JPEG 压缩实验,本文选择 JPEG 压缩质量因子 QF (QF = 10, 20, 30) 进行实验, QF 值越小代表压缩率越高,对应的图像失真越严重。从表 5 可以看出本文所提算法几乎不受 JPEG 压缩质量因子的影响,在较高的压缩率下依然能够保证良好性能。这是因为提取网络主要从空域的水印模板图案上提取水印信息,本身几乎不受 JPEG 压缩的影响,从而在 3 种压缩条件下会得到相近的实验结果。而其他算法利用传统的数字图像处理技术提取水印信息,非常依赖图像的高频信息,而在高强度的 JPEG 压缩下图像的高频信息损失非常严重,因此在高压压缩率下的鲁棒性较差。

表 5 不同 JPEG 压缩质量因子下的误码率
Table 5 Bit error rate under different JPEG compression quality factors

JPEG 压缩 质量因子	误码率			本文算法
	DCT ^[15] 算法	WHT ^[16] 算法	Color-D ^[17] 算法	
10	19.62%	15.30%	17.64%	4.07%
20	11.45%	9.22%	10.23%	3.69%
30	9.73%	9.09%	7.64%	4.24%

3.3 提取网络比较

为了凸显本文提取网络的优势,对本文网络和现存流行的分类网络 (GoogLeNet^[27]、MobileNet^[28]、LeNet^[29]、PNASNet^[30]、VGGNet^[31]、

EfficientNet^[32]、DenseNet^[33]、DPN^[34]) 进行了提取实验,并进行对比。为了公平比较,对所有网络结构用相同的数据集进行训练,得到的水印信息提取误码率如表 6 所示。

表 6 不同网络下水印信息提取误码率
Table 6 Bit error rate of watermark information extraction in different networks

网络	误码率
GoogLeNet ^[27]	3.56%
MobileNet ^[28]	4.58%
LeNet ^[29]	6.37%
PNASNet ^[30]	4.93%
VGGNet ^[31]	4.65%
EfficientNet ^[32]	4.73%
DenseNet ^[33]	4.54%
DPN ^[34]	4.77%
本文网络	1.97%

由表 6 可知,本文提出的提取网络误码率低于其他网络,由于残差网络的跳连结构能很好地保证特征的连续性,本文的提取网络能有效提取出设计模板的特征。

5 结束语

本文提出了一种新的载体独立的深度光照水印算法,以满足载体无关条件下的水印嵌入和提取过程,从而能有效保护如博物馆艺术画作等载体的版权。出于对 HVS 的研究和嵌入效率的考虑,本文提出了一种基于空域叠加的水印表达和嵌入方案。利用光照模板表达水印信息投影到图片上实现水印的嵌入过程。在提取端,为了抵抗拍摄过程产生的失真,本文设计了基于残差模块的神经网络来进行模板的分类,即消息的提取。实验表明,所提算法比现存的流行算法有较高的鲁棒性,且在水印的不可见性上有较大的优势。

参考文献:

- [1] 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.
- [2] SWANSON M D, KOBAYASHI M, TEWFIK A H. Multimedia data-embedding and watermarking technologies[J]. Proceedings of the IEEE, 1998, 86(6): 1064-1087.

- [3] HARTUNG F, KUTTER M. Multimedia watermarking techniques[J]. *Proceedings of the IEEE*, 1999, 87(7): 1079-1107.
- [4] LANGELAAR G C, SETYAWAN I, LAGENDIJK R L. Watermarking digital image and video data. A state-of-the-art overview[J]. *IEEE Signal Processing Magazine*, 2000, 17(5): 20-46.
- [5] LIU Z. New trends and challenges in digital watermarking technology: applications for printed materials[M]//*Multimedia Watermarking Techniques and Applications*. Auerbach Publications. 2006: 257-305.
- [6] HAITSMAN J, KALKER T. A watermarking scheme for digital cinema[C]//*Proceedings of Proceedings 2001 International Conference on Image Processing (Cat. No.01CH37205)*. 2001: 487-489.
- [7] Digital Cinema Initiatives. Digital Cinema System specification v1.2[R]. 2008.
- [8] 常玉红, 黄惠芬, 王志红. 检测图像篡改的脆弱水印技术[J]. *网络与信息安全学报*, 2017, 3(7): 47-52.
- CHANG Y H, HUANG H F, WANG Z H. Fragile watermarking technique for detecting image[J]. *Chinese Journal of Network and Information Security*, 2017, 3(7): 47-52.
- [9] 刘文星, 陈伟, 刘渊. 图像四叉树剖分下的自适应数字水印算法[J]. *网络与信息安全学报*, 2017, 3(12): 40-47.
- LIU W X, CHEN W, LIU Y. Adaptive digital watermarking algorithm under image quad-tree partition[J]. *Chinese Journal of Network and Information Security*, 2017, 3(12): 40-47.
- [10] 王志红, 黄惠芬, 常玉红. 基于 SVD 分解和 Hadamard 变换的图像半脆弱水印技术[J]. *网络与信息安全学报*, 2017, 3(5): 26-31.
- WANG Z H, HUANG H F, CHANG Y H. Semi-fragile watermarking technology based on SVD decomposition and Hadamard transform[J]. *Chinese Journal of Network and Information Security*, 2017, 3(5): 26-31.
- [11] GOHSHI S, NAKAMURA H, ITO H, et al. A new watermark surviving after re-shooting the images displayed on a screen[C]//*Knowledge-Based Intelligent Information and Engineering Systems*, 2005: 1099-1107.
- [12] OKIHARA K, INAZUMI Y, KINOSHITA H. A watermarking method that improves the relationship between of the number of embedded bits and image degradation[J]. *The Journal of the Institute of Image Information and Television Engineers*, 2004, 58(10): 1465-1467.
- [13] UEHARA K, SUZUKI K, IKEDA H. Does optoelectronic watermark technology migrate into business and industry in the near Future? Applications of optoelectronic watermarking technology to new business and industry systems utilizing flat-panel displays and smart devices[J]. *IEEE Transactions on Industry Applications*, 2016, 52(1): 511-520.
- [14] UEHARA K, SUZUKI K, IKEDA H. Applications of optoelectronic watermarking technique to new business and industry systems utilizing flat-panel displays and smart devices[C]//*Proceedings of 2014 IEEE Industry Application Society Annual Meeting*. 2014: 1-9.
- [15] UEHARA K, SUZUKI M. Digital watermarking technique using brightness-modulated light[C]//*Proceedings of 2008 IEEE International Conference on Multimedia and Expo*. 2008: 257-260.
- [16] ISHIKAWA Y, UEHARA K, YANAKA K. Practical evaluation of illumination watermarking technique using orthogonal transforms[J]. *Journal of Display Technology*, 2010, 6(9): 351-358.
- [17] UEHARA K, UNNO H. Effects of JPEG compression on reading optical watermarking embedded by using color-difference modulation[J]. *Journal of Computer and Communications*, 2018, 6(1): 56-64.
- [18] OSHITA K, UNNO H, UEHARA K. Optically written watermarking technology using temporally and spatially luminance-modulated light[J]. *Electronic Imaging*, 2016, 28(8): 1-6.
- [19] UNNO H, UEHARA K. Lighting technique for attaching invisible information onto real objects using temporally and spatially color-intensity modulated light[J]. *IEEE Transactions on Industry Applications*, 2020, 56(6): 7202-7207.
- [20] UNNO H, YAMKUM R, BUNPORN C, et al. A new displaying technology for information hiding using temporally brightness modulated pattern[J]. *IEEE Transactions on Industry Applications*, 2017, 53(1): 596-601.
- [21] UNNO H, UEHARA K. Display technique for embedding information in real object images using temporally and spatially luminance-modulated light[J]. *IEEE Transactions on Industry Applications*, 2017, 53(6): 5966-5971.
- [22] BOSE R C, RAY-CHAUDHURI D K. On a class of error correcting binary group codes[J]. *Information and Control*, 1960, 3(1): 68-79.
- [23] PETERSON W W, BROWN D T. Cyclic codes for error detection[J]. *Proceedings of the IRE*, 1961, 49(1): 228-235.
- [24] HE K M, ZHANG X Y, REN S Q, et al. Deep residual learning for image recognition[C]//*Proceedings of 2016 IEEE Conference on Computer Vision and Pattern Recognition*. 2016: 770-778.
- [25] LIN T Y, MAIRE M, BELONGIE S, et al. Microsoft COCO: common objects in context[C]//*Computer Vision – ECCV 2014*. 2014: 740-755.
- [26] The USC-SIPI Image Database[EB].
- [27] SZEGEDY C, LIU W, JIA Y Q, et al. Going deeper with convolutions[C]//*Proceedings of 2015 IEEE Conference on Computer Vision and Pattern Recognition*. 2015: 1-9.
- [28] YANG T J, CHEN Y H, SZE V. Designing energy-efficient convolutional neural networks using energy-aware pruning[C]//*Proceedings of 2017 IEEE Conference on Computer Vision and Pattern Recognition*. 2017: 6071-6079.
- [29] LECUN Y, BOTTOU L, BENGIO Y, et al. Gradient-based learning applied to document recognition[J]. *Proceedings of the IEEE*, 1998,

86(11): 2278-2324.

- [30] LIU C, ZOPH B, NEUMANN M. Progressive neural architecture search[J]. Computer Vision and Pattern Recognition, 2017.
- [31] SIMONYAN K, ZISSERMAN A. Very Deep convolutional networks for large-scale visual recognition[J]. Computer Vision and Pattern Recognition, 2014.
- [32] TAN M, LE Q. EfficientNet: rethinking model scaling for convolutional neural networks[C]// ICML. 2019.
- [33] HUANG G, LIU Z, VAN DER MAATEN L, et al. Densely connected convolutional networks[C]//Proceedings of 2017 IEEE Conference on Computer Vision and Pattern Recognition. 2017: 2261-2269.
- [34] GALLA T. Theory of neural information processing systems[J]. Journal of Physics A, 2006, 39: 3849.

[作者简介]



陈浩（1993-），男，辽宁本溪人，中国科学技术大学硕士生，主要研究方向为信息隐藏。



王锋（1996-），男，安徽潜山人，中国科学技术大学硕士生，主要研究方向为数字水印和深度学习。



张卫明（1976-），男，河北定州人，博士，中国科学技术大学教授、博士生导师，主要研究方向为信息隐藏、密码学、媒体内容安全和人工智能安全。



俞能海（1964-），男，安徽无为，人，博士，中国科学技术大学教授、博士生导师，主要研究方向为图像视频处理与分析、计算机视觉与模式识别、信息隐藏与媒体内容安全、信息检索与数据挖掘。