



## 基于深度学习的联合变换相关器光学图像加密系统去噪方法

郎利影 陆佳磊 于娜娜 席思星 王雪光 张雷 焦小雪

### In depth learning based method of denoising joint transform correlator optical image encryption system

Lang Li-Ying Lu Jia-Lei Yu Na-Na Xi Si-Xing Wang Xue-Guang Zhang Lei Jiao Xiao-Xue

引用信息 Citation: *Acta Physica Sinica*, 69, 244204 (2020) DOI: 10.7498/aps.69.20200805

在线阅读 View online: <https://doi.org/10.7498/aps.69.20200805>

当期内容 View table of contents: <http://wulixb.iphy.ac.cn>

---

## 您可能感兴趣的其他文章

### Articles you may be interested in

#### 基于深度学习压缩感知与复合混沌系统的通用图像加密算法

General image encryption algorithm based on deep learning compressed sensing and compound chaotic system

物理学报. 2020, 69(24): 240502 <https://doi.org/10.7498/aps.69.20201019>

#### 基于多模光纤散斑的压缩感知在光学图像加密中的应用

Application of compressive sensing based on multimode fiber specklegram in optical image encryption

物理学报. 2020, 69(3): 034203 <https://doi.org/10.7498/aps.69.20191143>

#### 基于机器学习构建的环三亚甲基三硝胺晶体势

Energetic potential of hexogen constructed by machine learning

物理学报. 2020, 69(23): 238702 <https://doi.org/10.7498/aps.69.20200690>

#### 基于空间角度复用和双随机相位的多图像光学加密方法

Multiple-image encryption method based on spatial angle multiplexing and double random phase encoding

物理学报. 2019, 68(24): 240503 <https://doi.org/10.7498/aps.68.20191362>

#### 基于计算全息和 $\theta$ 调制的彩色图像加密方法

Color image encryption method based on computer generated hologram and  $\theta$  modulation

物理学报. 2019, 68(11): 110502 <https://doi.org/10.7498/aps.68.20182264>

#### 一种基于压缩感知和多维混沌系统的多过程图像加密方案

Multi-process image encryption scheme based on compressed sensing and multi-dimensional chaotic system

物理学报. 2019, 68(20): 200501 <https://doi.org/10.7498/aps.68.20190553>

# 基于深度学习的联合变换相关器光学图像加密系统去噪方法\*

郎利影<sup>1)</sup> 陆佳磊<sup>2)</sup> 于娜娜<sup>2)</sup> 席思星<sup>2)†</sup> 王雪光<sup>2)</sup> 张雷<sup>2)</sup> 焦小雪<sup>2)</sup>

1) (河北工业大学先进激光技术研究中心, 天津 300401)

2) (河北工程大学, 邯郸 056038)

(2020年5月28日收到; 2020年7月9日收到修改稿)

提出了一种基于深度学习的联合变换相关器 (JTC) 光学图像加密系统新型去噪方法. 针对 JTC 光学图像加密系统中解密图像噪声的问题, 设计了一种基于生成对抗网络的去噪框架, 并使用密集模块加强特征信息复用, 提高了网络的性能. 该方法通过引入通道注意力机制使网络区分不同通道的权重, 学习各通道之间的关联, 使网络能选择性的加强有用特征信息并抑制无用特征信息; 在损失函数方面, 加入非对抗损失部分, 结合对抗损失和生成器模型提高了解密噪声图像中高频信息的恢复质量; 最后重建出高质量的解密图像. 将该方法用于传统的 JTC 光学图像加密系统, 数值计算和模拟实验结果表明, 该方法可极大地消除 JTC 光学图像加密系统中噪声影响, 有效地提高 JTC 光学图像加密系统用于高质量图像加密的有效性和可行性.

**关键词:** 光学图像加密, 深度学习, 信息安全, 神经网络, 联合变换相关器

**PACS:** 42.30.Va, 42.30.Wb, 07.05.Mh

**DOI:** 10.7498/aps.69.20200805

## 1 引言

自 1995 年 Refregier 等<sup>[1]</sup> 提出双随机相位光学加密系统以来, 光学图像加密技术得到了迅速发展, 并在信息安全领域展示出巨大的应用潜力. 但在基于  $4f$  系统的双随机相位光学图像加密技术中, 两个相位掩模必须在空间位置上精确对准, 而且加密结果为复振幅分布, 难以记录及传输<sup>[2]</sup>. 这些缺陷限制了该技术和应用, 于是人们提出了利用数字全息<sup>[3]</sup> 的加密方法<sup>[4]</sup> 来解决此类问题. 虽然数字全息能够记录图像加密结果的复振幅, 但由于参考光的引入, 加密系统的复杂程度和实验操作难度大大增加, 而且解密时的共轭图像影响了解密图像质量, 也没有解决随机相位掩模的精确对准问

题. 因此, Javidi 和 Nomura<sup>[4]</sup> 提出了一种基于联合变换相关器 (JTC) 的光学图像加密系统. 该系统结构简单, 不需要对随机相位掩模进行精确校准, 加密后的图像是 1 个联合功率谱, 即强度图像, 便于记录和传输, 因此成为学者们<sup>[5-7]</sup> 的研究热点. 但这种加密方法的主要缺点是解密图像存在严重的噪声, 导致其质量不能满足一般加密图像的精度要求. 虽然学者们采用 Gerchberg-Saxton (G-S) 算法和基于模糊控制理论的迭代算法 (IAFC) 来设计相位密钥<sup>[8,9]</sup>, 使随机相位密钥的傅里叶谱尽可能均匀, 在一定程度上提高了解密图像的质量. 但这些方法需要复杂的数学计算和编程, 且解密图像质量仍需提高.

针对上述问题, 本文提出一种基于深度学习的 JTC 光学图像加密系统新型降噪方法. 近年来,

\* 国家自然科学基金 (批准号: 11904073)、河北省自然科学基金 (批准号: F2019402351)、河北省教育厅青年拔尖人才项目 (批准号: BJ2020028) 和河北省科技计划 (批准号: 20371802D) 资助课题.

† 通信作者. E-mail: xisixing@126.com

随着硬件设备的不断发展和计算能力的不断提高,深度学习算法取得了长足的发展,并被广泛应用于各个领域.例如在目标检测<sup>[10]</sup>中通过深度学习算法进行图像中目标的类别和位置预测;在图像分割<sup>[11]</sup>中通过深度卷积神经网络进行图像中每个像素的类别预测;在图像描述<sup>[12]</sup>中通过深度学习提取图像特征,在循环神经网络中生成图像的描述.随着深度学习算法研究<sup>[13]</sup>的不断深入,一些新颖的网络结构和激活函数被提出,例如 VGG, GoogLeNet, ResNet 等网络和 Maxout, PReLU, ELU 等非线性激活函数.深度学习算法可通过在大规模图像识别数据集上训练来学习合适的图像特征表达,进而实现退化图像的恢复和还原.2016年 Isola 等<sup>[14]</sup>提出了一种图像到图像翻译的一般框架,将图像输入到生成网络代替原始的随机分布,这样可以有效地监督网络生成数据样本.相比传统的生成模型,生成对抗网络拟合真实的数据分布,能生成质量更好的图片.在此基础上,本文提出的 JTC 光学图像加密系统降噪方法是一种基于生成对抗网络的降噪模型一般框架,在网络中加入密集模块和通道注意力模块提取图像的特征信息以提高恢复图像的质量,建立携带噪声的退化解密图像和原始图像之间的图像到图像的映射关系,通过大量的训练样本学习到相应的权重参数,并通过训练好的权重参数进行退化解密图像的恢复.最终消除 JTC 光学图像加密系统中的噪声影响,使得 JTC 光学图像加密系统能够有效应用于高质量图像加密和解密.

## 2 JTC 光学图像加密原理

基于 JTC 的光学图像加密系统如图 1 所示,其中傅里叶透镜的焦距为  $f$ .扩束准直激光照射输

入平面,输入平面的  $(b, 0)$  处放置紧密贴合的待加密图像  $o(x, y)$  和随机相位密钥  $p_1(x, y)$ , 输入平面的  $(-b, 0)$  处则放置随机相位密钥  $p_2(x, y)$ , 即两者对称置于输入平面光轴的两侧.经过傅里叶变换后,傅里叶透镜后焦面放置的电荷耦合器件 (CCD) 记录联合功率谱为加密图像,可表示为

$$\begin{aligned} I(u, v) &= |\mathbb{F}[o(x-b, y)p_1(x-b, y) + p_2(x+b, y)]|^2 \\ &= |O(u, v) * P_1(u, v)|^2 + |P_2(u, v)|^2 \\ &\quad + O(u, v) * P_1(u, v)P_2^*(u, v) \exp(-i4\pi bu) \\ &\quad + [O(u, v) * P_1(u, v)]^* P_2(u, v) \exp(i4\pi bu). \end{aligned} \quad (1)$$

其中,  $\mathbb{F}[\cdot]$  表示傅里叶变换,  $(\cdot) * (\cdot)$  表示卷积运算,  $(\cdot)^*$  表示复共轭;  $O(u, v)$ ,  $P_1(u, v)$  和  $P_2(u, v)$  分别为  $o(x, y)$ ,  $p_1(x, y)$  和  $p_2(x, y)$  的傅里叶变换;  $b$  为待加密图像距光轴的距离.

解密系统为图 2 所示的  $4f$  系统,其中随机相位密钥  $p_2(x, y)$  仍然放置于输入平面  $(-b, 0)$  处,加密图像  $I(u, v)$  则放置于频谱面  $(0, 0)$  处.

扩束准直激光照射随机相位密钥,经过傅里叶变换后照射放置于频谱面的加密图像,得到光场分布为

$$\begin{aligned} E(u, v) &= P_2(u, v) \exp(i2\pi ub)I(u, v) \\ &= (|O(u, v) * P_1(u, v)|^2 + |P_2(u, v)|^2) \\ &\quad \times P_2(u, v) \exp(-i2\pi ub) \\ &\quad + O(u, v) * P_1(u, v) \exp(-i2\pi bu) \\ &\quad + [O(u, v) * P_1(u, v)]^* (P_2(u, v))^2 \exp(i6\pi bu). \end{aligned} \quad (2)$$

最后  $E(u, v)$  经过傅里叶变换后被 CCD 记录,其中第 3 项即为解密图像,位置是  $(b, 0)$ .但在实际 JTC 加密系统中密钥模板面积有限,为一截断纯

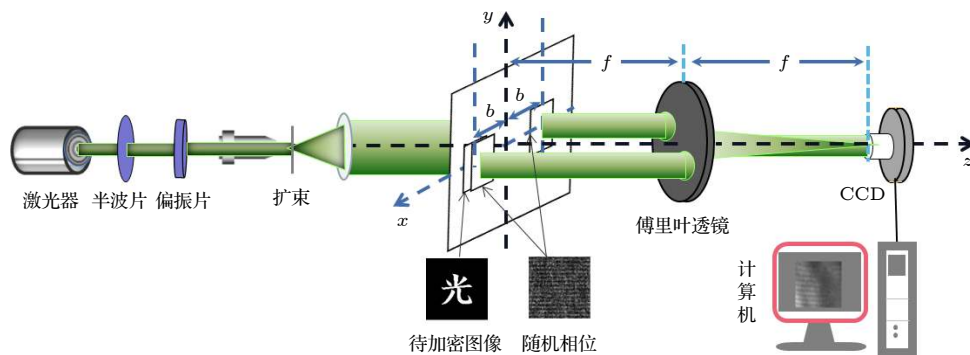


图 1 JTC 光学图像加密系统 ( $f$  是透镜焦距)

Fig. 1. Optical setup of image encryption based on JTC, where  $f$  is focal length.

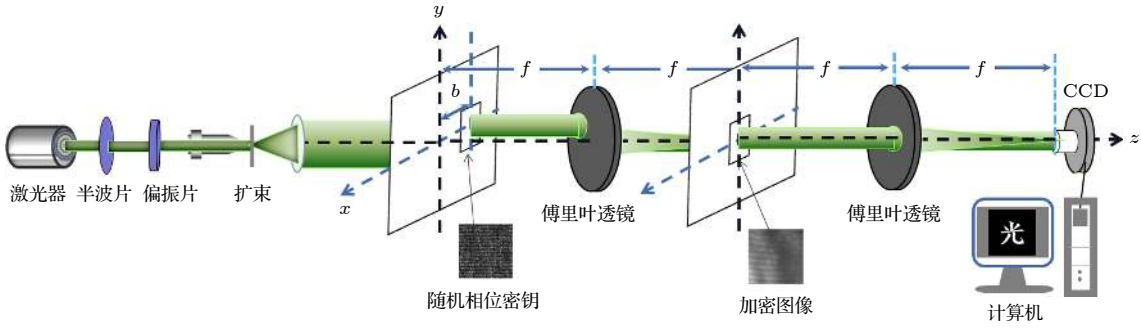


图2 图像解密光学系统

Fig. 2. Optical setup of image decryption.

相位模板, 因此其傅里叶谱不可能是一纯相位函数, 即随机相位密钥功率谱  $|P_2(u, v)|^2 \neq 1$ , (2) 式应修改为

$$\begin{aligned} E'(u, v) &= P_2(u, v) \exp(i2\pi ub) I(u, v) \\ &= (|O(u, v) * P_1(u, v)|^2 + |P_2(u, v)|^2) \\ &\quad \times P_2(u, v) \exp(i2\pi ub) \\ &\quad + O(u, v) * P_1(u, v) |P_2(u, v)|^2 \exp(-i2\pi bu) \\ &\quad + [O(u, v) * P_1(u, v)]^* (P_2(u, v))^2 \exp(i6\pi bu). \end{aligned} \quad (3)$$

所以 (3) 式中第 3 项被 CCD 接收的解密图像可表示为

$$\begin{aligned} e_3(x, y) &= F[O(u, v) * P_1(u, v) |P_2(u, v)|^2 \exp(-i2\pi bu)] \\ &= o(x + b, y) p_1(x + b, y) * p_2(x + b, y) \\ &\quad \otimes p_2(x + b, y), \end{aligned} \quad (4)$$

其中  $(\cdot) \otimes (\cdot)$  表示相关. 由 (4) 式可见, 解密图像为原始图像和随机相位密钥相关函数的卷积, 解密图像中存在严重噪声, 不能完全恢复出原始图像. 传统 JTC 光学图像加密结果如图 3 所示, 其中图 3(a) 为原始图像, 图 3(b) 为加密结果图像, 图 3(c) 为解密结果图像.

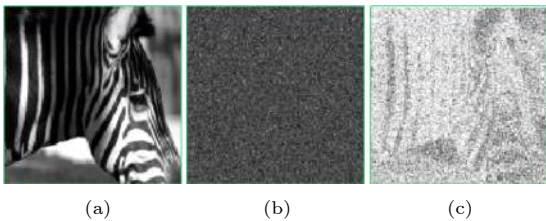


图3 (a) 原始图像; (b) 加密图像; (c) 解密图像

Fig. 3. (a) Image to be encrypted; (b) encrypted image; (c) decrypted image.

因此, 本文提出一种基于深度学习的降噪方法解决 JTC 图像加密系统的弊端, 提高解密图像的质量, 并且不需要复杂的迭代数学运算和编程, 使

其在实现高质量图像的加密和解密时更有效性和实用性.

## 3 深度学习去噪算法

### 3.1 深度学习网络结构

本文提出的深度学习生成对抗网络结构包括生成网络和判别网络两部分. 生成网络主体采用基于编码器和解码器的 U-net<sup>[15]</sup> 架构, 包括 5 个由注意力模块和密集模块组成的密集通道注意力模块 (DCAB). 其中注意力模块可以使网络将注意力集中在需要侧重的信息, 从而忽略无用信息, 而密集模块用于减少网络参数和提升网络容量, 以及复用图像样本的特征信息. 密集模块和注意力机制通过残差<sup>[16]</sup>的方式结合. 同时网络中增加了跳跃连接来弥补因为网络深度增加而导致的梯度弱化问题.

传统深度学习方法平等的对待各通道信息, 会浪费计算资源, 抑制网络的性能, 为了解决这一问题, 使网络自适应的学习到各通道的特征信息, 本文使用注意力机制<sup>[17]</sup>来对各通道之间关系建模, 增强网络性能, 其通道注意力模块如图 4 所示.

首先向注意力机制模块中输入通道特征图, 用  $x = \{x_1, x_2, x_3, \dots, x_c\}$  表示, 特征图数量为  $c$ , 大小为  $H \times W$ ,  $H$  和  $W$  分别表示高度和宽度. 将每个通道空间信息压缩为局部特征信息, 对得到的特征信息作全局平均池化, 通过聚合的方式得到  $1 \times 1 \times c$  的特征图, 用  $x_c(i, j)$  表示第  $c$  个特征值在  $(i, j)$  处的值,  $z \in \mathbf{R}^c$  表示经过压缩后的特征信息, 其中  $z$  的第  $c$  个元素可以表示为

$$z_c = P(x_c) = \frac{1}{H \times W} \sum_{i=1}^H \sum_{j=1}^W x_c(i, j). \quad (5)$$

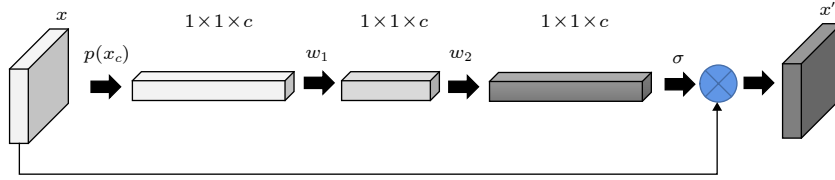


图 4 通道注意力模块, 其中  $x$  表示特征图,  $c$  表示特征图 (通道) 数量,  $w_1$  和  $w_2$  分别表示降维前后的权重,  $\sigma$  是 sigmoid 激活函数,  $p(x_c)$  表示全局池化功能

Fig. 4. Channel attention (CA), Where  $x$  is the feature map,  $c$  is the channel,  $w_1$  and  $w_2$  are the weight set of low-dimension,  $\sigma$  is the sigmoid activation function and  $p(x_c)$  is global pooling function.

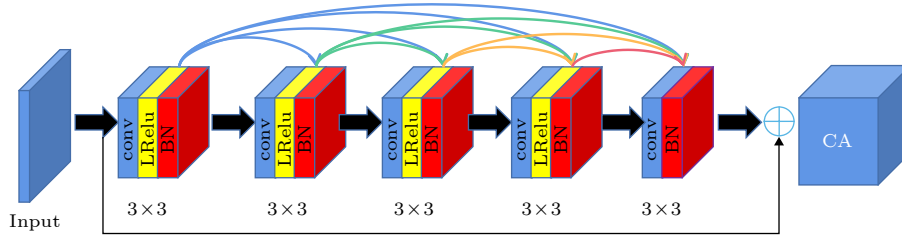


图 5 密集通道注意力模块

Fig. 5. Dense channel attention block (DCAB).

然后利用各通道的特征描述进行建模, 并加入 ReLU 激活函数, 以保障学习到通道间的非线性关系. 为了降低模型的复杂性, 可对  $c$  个通道除以降维系数进行降维, 降维后的通道数量用  $c'$  表示. 最后对比原始特征图与学习到的特征图, 可学习到不同通道的权重. 经过注意力模块后的特征信息  $S$  可表示为

$$s = \sigma(w_2 \text{ReLU}(w_1 z_c)). \quad (6)$$

在生成网络模型中加入密集模块<sup>[18]</sup>, 可以增强特征复用, 有效提取图像中的特征和细节. 密集模块和注意力模块组合成 1 个 DCAB 综合模块, 如图 5 所示, 其中密集模块 5 个卷积层互相连接且共享特征信息, 并结合 LeakyRelu 激活函数和 BN (Batch normalization)<sup>[19]</sup> 层做归一化处理. 在 DCAB 综合模块中, 开始将特征信息流输入到 1 个  $3 \times 3$  的卷积核中, 再经过密集模块和通道注意力模块, 最后将输入 DCAB 模块的特征信息和输出 DCAB 模块的特征信息相加得到新的特征信息.

网络的整体结构如图 6 所示, 首先  $128 \times 128$  像素的噪声解密图像样本  $y$  输入到生成网络中, 经过 2 个 DCAB 综合模块, 期间使用最大池化进行下采样. 因为在网络设计过程中发现多的下采样会导致图像分辨率降低, 本文将网络的下采样次数设置为 2, 保证输出图像的质量. 经过 2 个 DCAB 模块和 2 次反卷积后, 输入图像的尺寸与输出图像的

尺寸一致. 此外, 本文的网络结构使用了跳跃连接将相同维度下的特征信息连接在一起, 以保证低频信息不被丢失, 从而保障输出图像的质量. 最后网络使用  $3 \times 3$  的卷积核结合 tanh 激活函数输出恢复图像  $x_f = G(y)$ .

系统的判别网络由 4 个残差块构成, 每个残差块使用 2 个  $3 \times 3$  的卷积核, 步长为 2, 每个卷积层中叠加 LeakyRelu 激活函数和 BN 层, 特征图经过判别网络时, 尺寸会经过  $64 \times 64 \times 64$ ,  $32 \times 32 \times 128$ ,  $16 \times 16 \times 256$  和  $8 \times 8 \times 512$  的变换.

### 3.2 损失函数

网络结构的损失函数由对抗损失和非对抗损失两部分组成. 对抗损失由判别网络训练获得, 而非对抗损失用于保持图像的整体一致性, 通过均方误差 (MSE) 损失函数和 VGG 损失函数计算. 损失函数可表示为

$$l_{\text{total}} = \lambda_1 \times l_{\text{MSE}} + \lambda_2 \times l_{\text{VGG}} + \lambda_3 \times l_{\text{adv}}, \quad (7)$$

其中:  $\lambda_1$ ,  $\lambda_2$  和  $\lambda_3$  分别表示 MSE 损失函数  $l_{\text{MSE}}$ , VGG 损失函数  $l_{\text{VGG}}$  和对抗损失函数  $l_{\text{adv}}$  的权重系数, 本文  $\lambda_1$  参数设置为 1,  $\lambda_2$  参数设置为 0.00004,  $\lambda_3$  参数设置为 0.6. 对抗损失是损失函数的主要部分, 它在生成网络和判别网络不断对抗训练中产生. 判别网络鉴别真实图片的能力在训练中不断增强, 即  $D(x) = 1$ ; 鉴别生成网络生成的图像样本为

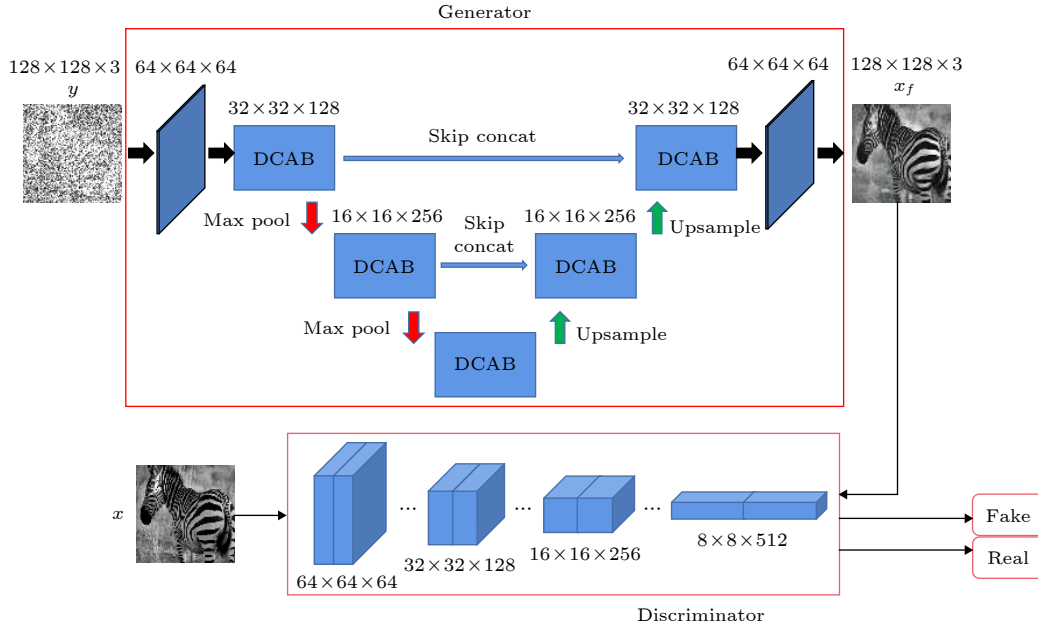


图 6 整体网络结构

Fig. 6. Whole network structure.

假, 即  $D(G(y)) = 0$ . 在与判别网络的不断对抗训练中, 生成网络可以生成欺骗判别网络的样本, 即  $D(G(y))$  不断增大. 因此对抗损失函数可以看作是最大化判别网络的数学期望和最小化生成网络的数学期望, 其表达式为

$$l_{\text{adv}} = \min_G \max_D E_{x \sim p_{\text{data}}(x)} [\log D(x)] + E_{y \sim p_G(y)} [\log(1 - D(G(y)))], \quad (8)$$

其中  $E_{x \sim p_{\text{data}}(x)}$  表示真实图像样本数据分布的期望值,  $E_{y \sim p_G(x)}$  表示噪声图像样本数据分布的期望值,  $\min_G$  表示最小化判别网络判断假图像样本的期望,  $\max_D$  表示最大化判别网络判断真实图像样本的期望.

在仅考虑对抗损失的情况下, 整体网络输出的恢复图像质量不能满足要求, 因此在损失函数中加入非对抗损失函数以提升图像的质量. 非对抗损失中, 输出图像与原始图像的均方误差  $l_{\text{MSE}}$  可表示为

$$l_{\text{MES}} = \frac{1}{H \times W} \sum_{x=1}^W \sum_{y=1}^H (p_x - G(p_y))^2, \quad (9)$$

其中,  $p_x$  表示真实图像样本,  $G(p_y)$  表示生成网络生成的假图像样本. 但  $l_{\text{MSE}}$  在提高生成图像高频部分的质量中作用有限, 因高频信息主要为图像的纹理和细节, 对于图像质量至关重要, 因此 VGG 损失函数被引入, 使用经过 ImageNet 分类任务训练

的 VGG19 提取图像高频信息,  $l_{\text{VGG}}$  可表示为

$$l_{\text{VGG}(i,j)} = \frac{1}{H_{i,j} W_{i,j}} \sum_{x=1}^{h_{i,j}} \sum_{y=1}^{w_{i,j}} \left( v(p'_{x,y})_{i,j} - v(G(p_{x,y}))_{i,j} \right)^2, \quad (10)$$

其中  $v(\cdot)_{i,j}$  表示经过 VGG19 中第  $i$  个池化层的第  $j$  个卷积层提取的特征信息.

## 4 实验结果与分析

本文的生成对抗网络训练过程中选用 ImageNet 数据集的汽车、斑马、鸟类和山羊 4 个类别, 以及汉字和二维码 2 个二值图像类别, 每个类别采用 500 张图片作为训练集, 每个类别使用 100 张图片作为测试集, 使用 50 张图片作为验证集. 使用 RTX 2080ti 显卡训练实验数据, 初始学习率设置为 0.0002, 采用自适应的方式下降学习率. 使用 Xavier 为权重初始化, 设置 batch-size 大小为 4.

如图 7(a<sub>1</sub>)—(f<sub>1</sub>) 所示, 在生成对抗网络训练结果的基础上, 选择 4 幅灰度图像和 2 幅二值图像进行加密, 其中多个原始图像尺寸为  $0.5 \text{ cm} \times 0.5 \text{ cm}$ ,  $128 \times 128$  像素, JTC 加密系统中激光波长  $\lambda = 532 \text{ nm}$ , 透镜焦距  $f = 0.3 \text{ m}$ , 待加密图像距光轴的距离  $b = 0.5 \text{ cm}$ . 经过图 1 所示的传统 JTC 光学图

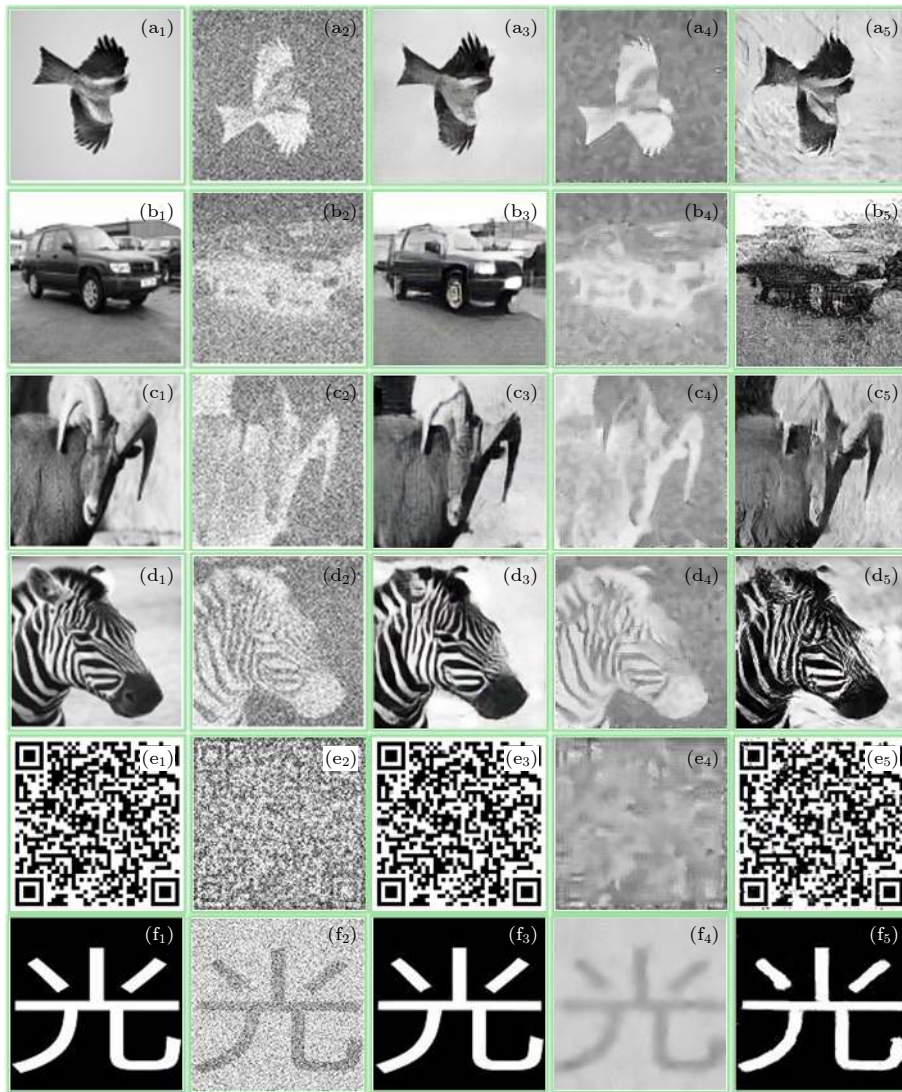


图 7 (a<sub>1</sub>)—(f<sub>1</sub>) 原始的图像; (a<sub>2</sub>)—(f<sub>2</sub>) 经过光学加密的噪声图像; (a<sub>3</sub>)—(f<sub>3</sub>) 本文提出算法去噪图像; (a<sub>4</sub>)—(f<sub>4</sub>) 为 BM3D 去噪图像; (a<sub>5</sub>)—(f<sub>5</sub>) pix2pix 去噪图像

Fig. 7. (a<sub>1</sub>)–(f<sub>1</sub>) Ground truth; (a<sub>2</sub>)–(f<sub>2</sub>) image encrypted image; (a<sub>3</sub>)–(f<sub>3</sub>) image deoised by the algorithm proposed in this paper; (a<sub>4</sub>)–(f<sub>4</sub>) deoised by BM3D; (a<sub>5</sub>)–(f<sub>5</sub>) image deoised by pix2pix.

像加密系统和图 2 所示的解密系统, 解密结果图像如图 7(a<sub>2</sub>)—(f<sub>2</sub>) 所示, 可见解密图像中含有严重噪声, 很多情况下图像质量不能满足要求, 限制了传统 JTC 光学图像加密系统的应用. 经过本文提出的深度学习新型降噪算法处理的结果如图 7(a<sub>3</sub>)—(f<sub>3</sub>) 所示, 可见该方法很好地降低了传统 JTC 光学图像加密系统解密图像的噪声, 极大地提高了解密图像质量, 对于二值图像的去噪效果要优于灰度图像. 为了验证本文提出的去噪方法有效性, 将传统的 BM3D 去噪方法和基于深度学习的 pix2pix 去噪方法应用于 JTC 光学图像加密系统并进行对比. 其中 BM3D 去噪方法处理解密图像的结果如图 7(a<sub>4</sub>)—(f<sub>4</sub>) 所示, 而基于深度学习的 pix2pix

去噪方法处理解密图像的结果如图 7(a<sub>5</sub>)—(f<sub>5</sub>) 所示. 通过图 7 的对比可见, 本文方法明显优于传统去噪方法.

最后, 分别使用峰值信噪比 (PSNR)、结构相似性 (SSIM) 和 MSE 函数评估了本文去噪方法和传统去噪方法的优劣, 包括传统的 BM3D 和 pix2pix 去噪方法及基于 G-S 算法和 IAFC 设计相位密钥提高解密图像质量的方法<sup>[20]</sup>. 计算结果如表 1 所列, 根据计算结果, 本文提出的去噪方法处理的解密图像在质量、鲁棒性和图像的结构相似性方面都优于传统去噪方法, 在降低传统 JTC 光学图像加密系统中噪声影响, 提高 JTC 光学图像加密系统用于高质量图像加密的有效性方面具有极大优势.

表 1 5 种去噪方法结果对比  
Table 1. Comparison of experimental data results.

	指标		
	PSNR	MSE	SSIM
BM3D	11.4615	4708.7266	0.0556
pix2pix	17.4363	1334.5201	0.4285
G-S	12.4521	3834.3358	0.1598
IAFC	19.0561	731.2579	0.5784
本文方法	22.4049	421.0133	0.7398

## 5 结 论

本文提出了一种用于传统 JTC 图像加密系统的对抗生成网络去噪模型, 通过将密集模块和注意力模块相结合引入生成网络中, 有效提取图像的特征信息. 损失函数方面, 非对抗损失使用 VGG-19 网络来恢复图像中的纹理和细节, 实验结果表明, 本文提出的去噪方法优于传统的 BM3D 去噪算法和 pix2pix 模型, 也优于基于 G-S 算法和 IAFC 设计相位密钥提高解密图像质量的方法, 且在各项指标上均有明显的提高. 该方法极大地消除了 JTC 光学图像加密系统中的噪声影响, 有效地提高了 JTC 光学图像加密系统用于高质量图像加密的有效性和可行性, 推动了深度学习算法在光学图像加密降噪领域的应用.

## 参考文献

- [1] Refregier P, Javidi B 1995 *Opt. Lett.* **20** 767
- [2] Javidi B, Carnicer A, Yamaguchi M, Nomura T, Pérez-Cabré E, Millán M S, Nishchal N K, Torroba R, Barrera J F, He W, Peng X, Stern A, Rivenson Y, Alfalou A, Brosseau C, Guo C, Sheridan J T, Situ G, Naruse M, Matsumoto T, Juvells L, Tajahuerce E, Lancis J, Chen W, Chen X, Pinkse P W, Mosk A P, Markman A 2016 *J. Opt.* **18** 083001
- [3] Pan W, Tian Y L 2005 *Opt. Precision Eng.* **13** 15 (in Chinese) [潘武, 田贻丽 2005 光学精密工程 **13** 15]
- [4] Javidi B, Nomura T 2000 *Opt. Lett.* **25** 28
- [5] Rueda E, Barrera J F, Henao R 2009 *Opt. Commun.* **282** 3243
- [6] Rajput S K, Nishchal N K 2012 *Opt. Lasers Eng.* **50** 1474
- [7] Mehra I, Rajput S K, Nishchal N K 2014 *Opt. Lasers Eng.* **52** 167
- [8] Cheng C J, Lin L C, Wang C M 2005 *Opt. Rev.* **12** 367
- [9] Lin L C, Cheng C J 2006 *Opt. Commun.* **258** 144
- [10] Rao J M, Qiao Y J, Ren F, Wang J X, Du Q Y 2017 *Sensors* **17** 1951
- [11] Chen L C, Papandreou G, Kokkinos I 2018 *IEEE T. Pattern Anal.* **40** 834
- [12] Johnson J, Karpathy A, Li F F, Las Vegas N V 2016 *Proceeding of IEEE Conference on Computer Vision and Pattern Recognition* Las Vegas, NV, USA, Dec 12, 2016 p494
- [13] Lateef F, Ruichek Y 2019 *Neurocomputing* **338** 321
- [14] Phyllip I, Zhu J Y, Zhou T H, Alexei A E 2017 *Proc of IEEE Conf. on Computer Vision and Pattern Recognition* Honolulu, HI, United States, Nov 11, 2017 p632
- [15] Ronneberger O, Fischer P, Brox T 2015 *International Conference on Medical Image Computing and Computer Assisted Interventions* Munich, Germany, Nov 18, 2015 p234
- [16] He K, Zhang X, Ren S, Sun J 2016 *Proceeding of IEEE Conference on Computer Vision and Pattern Recognition* Las Vegas N V, United States, June 26–July 1, 2016 p770
- [17] Li K, Wu Z, Peng K C, Ernst J, Fu Y 2018 *Proceeding of IEEE Conference on Computer Vision and Pattern Recognition* Salt Lake City UT, United States, Dec 17, 2018 p9215
- [18] Huang G, Liu Z, Weinberger K Q, Der M 2017 *Proceeding of IEEE Conference on Computer Vision and Pattern Recognition* Honolulu, HI, United States, July 21–26, 2017 p2261
- [19] Ioffe S, Szegedy C 2015 *Proceedings of The 32nd International Conference on Machine Learning (ICML)* Lille France, July 6–11, 2015 p448
- [20] Wu K N, Hu J S, Lin Y 2007 *Opt. Precision Eng.* **4** 577 (in Chinese) [吴克难, 胡家升, 林勇 2007 光学精密工程 **4** 577]

# In depth learning based method of denoising joint transform correlator optical image encryption system\*

Lang Li-Ying<sup>1)</sup> Lu Jia-Lei<sup>2)</sup> Yu Na-Na<sup>2)</sup> Xi Si-Xing<sup>2)†</sup>  
Wang Xue-Guang<sup>2)</sup> Zhang Lei<sup>2)</sup> Jiao Xiao-Xue<sup>2)</sup>

1) (*Advanced Laser Technology Research Center, Hebei University of Technology, Tianjin 300401, China*)

2) (*Hebei University of Engineering, Handan 056038, China*)

( Received 28 May 2020; revised manuscript received 9 July 2020 )

## Abstract

There is serious noise interference in the decryption process of the joint transform correlator (JTC) optical encryption system, so the quality of the decrypted image cannot meet the accuracy requirements in most cases. The quality of decrypted image can be improved to a certain extent when the phase key is designed by the Gerchberg-Saxton algorithm and the iterative algorithm fuzzy control algorithm, but the complexity of the design process is inevitable and the quality of the decrypted image still needs improving. Recently, the in depth learning technology has attracted the attention of scholars in the fields of computer vision, natural language processing and optical information processing. In order to deal with the noise interference in the JTC optical encryption system, combining the current deep learning method, in this paper we propose a new denoising method for JTC optical image encryption system based on in depth learning, the dense modules are added into the generated network to enhance the reuse of feature information and improve the performance of the network. The latest self-attention mechanism area is added into the network to distinguish the weights of different channels and learn the relationship between channel and channel, so that the network can selectively strengthen the useful feature information but suppress useless feature information. The density module and the channel attention module are integrated into a DCAB synthesis module, which can effectively extract the image feature information and improve the performance of the network. The receptive field of the convolution kernel is enlarged by two down-sampling and the feature map is restored to its original size by two up-sampling. The VGG-19 is used to extract high-frequency details and texture features of images, meanwhile, the non-adversarial loss and mean-square error (MSE) loss are added into the loss function to reduce the difference among the image samples. The quality of noise-reduced images in this method are obviously better than that of the existing denoising algorithms by evaluating intuitive visual observation or SSIM (structural similarity), PSNR (peak signal to noise ratio) and MSE. The results of numerical calculation and simulation experiments show that this method can greatly eliminate the influence of noise on the JTC optical image encryption system, and effectively improve the effectiveness and feasibility of JTC optical image encryption system for high-quality image encryption.

**Keywords:** optical image encryption, deep learning, information security, neural networks, joint transform correlator

**PACS:** 42.30.Va, 42.30.Wb, 07.05.Mh

**DOI:** [10.7498/aps.69.20200805](https://doi.org/10.7498/aps.69.20200805)

\* Project supported by the National Natural Science Foundation of China (Grant No.11904073), the Natural Science Foundation of Hebei Province, China (Grant No. F2019402351), the Youth Top-notch Project of Hebei Provincial Education Department, China (Grant No. BJ2020028), and the Science and Technology Program of Hebei Province, China (Grant No. 20371802D).

† Corresponding author. E-mail: [xisixing@126.com](mailto:xisixing@126.com)