



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

陈炜 郭媛 敬世伟

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

Chen Wei Guo Yuan Jing Shi-Wei

引用信息 Citation: *Acta Physica Sinica*, 69, 240502 (2020) DOI: 10.7498/aps.69.20201019

在线阅读 View online: <https://doi.org/10.7498/aps.69.20201019>

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

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>

基于渐进添边的准循环压缩感知时延估计算法

A quasi-cyclic compressed sensing delay estimation algorithm based on progressive edge-growth

物理学报. 2017, 66(9): 090703 <https://doi.org/10.7498/aps.66.090703>

基于两级压缩感知的脉冲星时延估计方法

Pulsar time delay estimation method based on two-level compressed sensing

物理学报. 2018, 67(9): 099701 <https://doi.org/10.7498/aps.67.20172100>

一种基于压缩感知的三维导体目标电磁散射问题的快速求解方法

Compressed sensing based fast method of solving the electromagnetic scattering problems for three-dimensional conductor targets

物理学报. 2018, 67(10): 100201 <https://doi.org/10.7498/aps.67.20172543>

基于新的五维多环多翼超混沌系统的图像加密算法

Image encryption algorithm based on new five-dimensional multi-ring multi-wing hyperchaotic system

物理学报. 2020, 69(4): 040502 <https://doi.org/10.7498/aps.69.20191342>

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*

陈炜 郭媛[†] 敬世伟

(齐齐哈尔大学计算机与控制工程学院, 齐齐哈尔 161006)

(2020年6月29日收到; 2020年8月10日收到修改稿)

提出一种适用于灰度图像与RGB格式彩色图像的通用图像加密算法. 利用双线性插值 Bilinear 与卷积神经网络对图像进行压缩, 再使用二维云模型与 Logistic 组成的复合混沌系统对压缩图像加解密(滑动置乱与矢量分解), 最后对解密图像进行重构. 重构网络中, 由卷积神经网络与双线性插值 Bilinear 主要负责重构轮廓信息, 全连接层主要负责重构颜色信息. 实验结果表明, 该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在数据处理质量和计算量上有着很大优势. 由于复合混沌系统有着足够大的密钥空间且将明文哈希值与密钥关联, 可实现一图一密的加密效果, 能有效抵抗暴力攻击与选择明文攻击, 与对比文献相比, 相关系数更接近理想值且信息熵与明文敏感性指标也都在临界值范围内, 其加密算法有着更高的安全性.

关键词: 深度学习, 压缩感知, 加密, 复合混沌系统

PACS: 05.45.Ac, 05.45.Vx, 05.45.Gg

DOI: 10.7498/aps.69.20201019

1 引言

随着互联网技术的飞速发展, 数字图像已成为信息传输的重要载体. 由 Candes, Romberg, Tao 和 Donoho 等^[1-3]提出的压缩感知理论, 利用信号在某些变换中满足稀疏性的特点, 使采样率在远低于奈奎斯特采样率的情况下对信号进行压缩与重构. 传统压缩感知重构方法基于稀疏先验知识, 从一个欠定方程组中寻找最优解来重构图像, 然而真实图像在某些变换中并不精确满足稀疏性, 使得重构质量不高且多次迭代求解, 耗时长. 而基于深度学习的压缩感知算法采用纯数据驱动的方式提取测量值并重构, 放宽了对图像信号稀疏性的假设条件. Mousavi 等^[4]利用堆降噪自编码模型设计了两种网络, 第一种采用线性的重构方法, 耗时短但

重构质量较低; 第二种采用非线性端到端的方法, 耗时略长但重构质量提高明显. MSRNet^[5], ReconNet^[6], DR²-Net^[7]也是基于深度学习的压缩感知算法, 与传统压缩感知算法相比, 耗时短且重构质量高, 但他们的重点都放在重构网络上, 使用随机高斯矩阵压缩的图像质量差, 限制了图像的重构质量.

混沌学是在非线性动力学的基础上发展起来的, 在确定性系统中做不可预测的随机运动, 细微的改变就能造成巨大误差. 混沌系统由于具有伪随机性、遍历性和非周期性等特点, 在图像加密中被广泛运用^[8-10], 虽能获得很好的加密效果, 但存在着耗时长且不利于传输等问题. 有研究^[11-13]将压缩感知与图像加密结合, 便于图像的存储、传输且安全性也得到保证, 但使用的都是传统压缩感知, 总耗时比在原图上直接加密的时间还长, 且都只适用于灰度图像.

* 国家自然科学基金(批准号: 61872204)、黑龙江省自然科学基金(批准号: F2017029)、黑龙江省省属高等学校基本科研业务费(批准号: 135109236)和研究生创新研究项目(批准号: YJSCX2019042)资助的课题.

[†] 通信作者. E-mail: guoyuan171@126.com

本文提出一种通用的图像压缩加密算法, 在压缩与加密的性能上都有所提升. 贡献有如下 5 点: 首先在压缩网络上使用双线性插值 Bilinear 对图像的宽高压缩, 再通过卷积神经网络将 3 通道压缩为 1 通道, 使压缩网络对采样率没有限制并获得高质量的压缩图像. 第二, 在重构网络上使用双线性插值 Bilinear 与卷积神经网络组成的模型 (bilinear convolutional neural network, BCNN) 重构图像的轮廓信息, 使用全连接层重构图像的颜色信息, 可得到高质量的重构图像. 第三, 压缩重构网络默认使用的是 RGB 格式彩色图像, 可将灰度图复制为 3 通道后再压缩, 重构后求 3 通道对应位置的平均值, 变为 1 通道, 使整个网络也适用于灰度图像. 虽然网络训练使用的是彩色图像, 但灰度图像重构质量依然优于其他算法. 第四, 加密算法上复合混沌系统由二维云模型与 Logistic 级联产生, 密钥空间大且序列更随机. 第五, 置乱方法使用滑动置乱, 与像素点置乱、行列置乱相比, 置乱次数与置乱效果能达到很好的平衡.

2 基本理论

2.1 压缩感知

对于 $h \times w$ 维的原始图像 \mathbf{x} , 取测量矩阵 Φ 对原始图像 \mathbf{x} 进行采样:

$$\mathbf{y} = \Phi \mathbf{x}, \quad (1)$$

(1) 式中, Φ 为 $n \times h$ 维的矩阵且 $n \ll h$, \mathbf{y} 为 $n \times w$ 维的矩阵, 所以矩阵 \mathbf{x} 的元素个数远大于矩阵 \mathbf{y} 的元素个数, 方程组有无数解, 需将 \mathbf{x} 转化为

$$\mathbf{x} = \Psi \mathbf{s}, \quad (2)$$

其中, $\Psi \in \mathbb{R}^{h \times h}$ 和 $\mathbf{s} \in \mathbb{R}^{h \times w}$ 分别是稀疏表示矩阵和 k 稀疏矩阵, k 稀疏矩阵是指矩阵 \mathbf{s} 中每列最多有 k 个非零值且 $k \ll h$. 根据 (2) 式, 可将 (1) 式转化为

$$\mathbf{y} = \Phi \Psi \mathbf{s}, \quad (3)$$

(3) 式中, 已知测量值 \mathbf{y} 、测量矩阵 Φ 和稀疏表示矩阵 Ψ , 可通过 l_1 范数来近似逼近 l_0 范数求解 \mathbf{s} :

$$\min \|\mathbf{s}\|_1 \quad \text{s.t.} \quad \mathbf{y} = \Phi \Psi \mathbf{s}. \quad (4)$$

传统压缩感知方法需要对 (4) 式多次迭代求解, 运算时间长, 而基于深度学习的压缩感知方法不需要迭代优化且有 GPU 硬件条件的支持, 运算时间得到保障.

2.2 复合混沌系统构造

本文利用二维云模型的期望值 (Ex_1, Ex_2) , 熵 (En_1, En_2) , 超熵 (He_1, He_2) 这 6 个数字特征来产生一组具有随机性的隶属度 u_i . (Ex_1, Ex_2) 反映了云滴群的重心位置, (En_1, En_2) 反映了云滴群的随机性, (He_1, He_2) 反映了 (En_1, En_2) 的不确定性度量. 二维云模型正向发生器算法如下所示.

生成两组正态随机数, 以 En_1 与 En_2 为期望值, He_1 与 He_2 为标准差:

$$\begin{cases} y_{1i} = R_n(En_1, He_1), \\ y_{2i} = R_n(En_2, He_2), \end{cases} \quad (5)$$

其中 n 为云滴生成个数. 再生成两组正态随机数, 以 Ex_1 和 Ex_2 为期望值, y_{1i} 和 y_{2i} 为标准差:

$$\begin{cases} x_{1i} = R_n(Ex_1, y_{1i}), \\ x_{2i} = R_n(Ex_2, y_{2i}), \end{cases} \quad (6)$$

最后计算隶属度:

$$u_i = \exp \left[\frac{(x_{1i} - Ex_1)^2}{2 \times y_{1i}^2} - \frac{(x_{2i} - Ex_2)^2}{2 \times y_{2i}^2} \right], \quad 0 < u_i < 1. \quad (7)$$

Logistic 序列表达式为

$$z_i = r \times z_i \times (1 - z_i), \quad 0 < z_i < 1. \quad (8)$$

将隶属度 u_i 与 Logistic 级联得到 C-L 混沌序列:

$$c_i = [(u_i + z_i) \bmod 1] \times 2\pi, \quad 0 < c_i < 2\pi. \quad (9)$$

2.3 滑动置乱

置乱方法中, 像素点置乱虽能很好地打乱图像信息分布, 但处理时间较长. 行列置乱耗时虽短, 但置乱效果不好. 滑动置乱弥补了像素点置乱与行列置乱的缺点, 耗时短且置乱效果好. 本文滑动置乱分两步, 先行滑动再列滑动, 公式如下所示:

$$\begin{cases} rs_i = \text{int}(u_i[0 : h] \times w), \\ cs_i = \text{int}(u_i[h : h + w] \times h), \end{cases} \quad (10)$$

其中, h 和 w 表示图像高宽, rs_i 和 cs_i 表示行列滑动距离.

$$\begin{cases} \text{img}_{rs}[h_i, :] = \text{roll}(\text{img}[h_i, :], rs_i), \\ \text{img}_{cs}[:, w_i] = \text{roll}(\text{img}_{rs}[:, w_i], cs_i). \end{cases} \quad (11)$$

img 是通过压缩网络得到的压缩图像, 具体流程如图 1 所示.

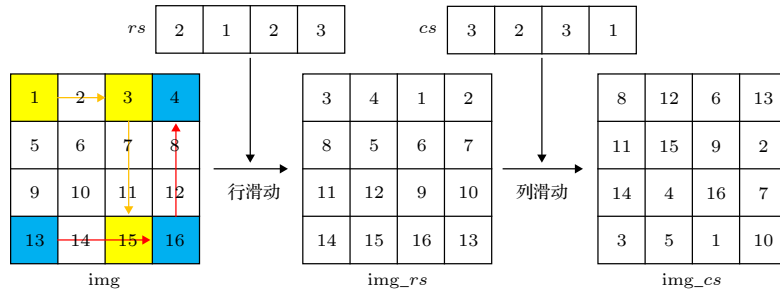


图 1 滑动置乱流程图

Fig. 1. Flow chart for scrambling.

2.4 矢量分解

将置乱后的图像 img_cs 进行矢量分解^[14], 公式可表示为

$$img_cs = |\exp(i\phi) + \exp[i(\phi + \varphi)]|, \quad (12)$$

令 $M_1 = \exp(i\phi)$, $M_2 = \{\text{angle}[\exp[i(\phi + \varphi)] + \pi]\} / (2\pi)$, $0 < M_2 < 1$, $\text{angle}[\cdot]$ 表示相位角. ϕ 是 $[0, 2\pi]$ 上均匀分布的随机序列, 本文使用 C-L 级联混沌序列来代替. φ 的计算公式如下所示:

$$\varphi = \pi - \arccos\left(1 - \frac{img_cs}{2}\right), \quad (13)$$

将分解后的 M_2 作为密文.

3 图像压缩重构方案

本文压缩重构网络 (fully connected layer and bilinear convolutional neural network, FCLB-CNN) 在压缩前需将原图分割为多个大小为 $3 \times 33 \times 33$ 且不重叠的原始图像块, 重构后再拼接成大图. 彩色图像采样率 $MR = 0.18$ 的压缩重构网络如图 2 所示.

3.1 压缩网络

压缩网络由双线性插值 Bilinear 与卷积神经

网络组成, 双线性插值 Bilinear 将图像的宽高压缩, 卷积神经网络将图像 3 通道合并为 1 通道, 卷积核大小分别为 $9 \times 9, 3 \times 3, 3 \times 3, 1 \times 1$. 彩色图像在采样率 $MR = 0.08, 0.03, 0.01, 0.003$ 与灰度图像在 $MR = 0.25, 0.10, 0.04, 0.01$ 时, 压缩图像大小皆为 $1 \times 17 \times 16, 1 \times 10 \times 11, 1 \times 6 \times 7, 1 \times 3 \times 3$. 网络中使用 Relu 激活函数^[15] 来提高网络表达能力, 最后一层使用 Sigmoid 激活函数将值映射到 0—1 之间. 压缩网络 $F^c(\cdot)$ 的输入值为原始图像块 x_i , 卷积层权重 W^c 和压缩图像 y_i 通过 Adam 方法训练得到, 公式如下:

$$y_i = F^c(\text{Bilinear}(x_i), W^c). \quad (14)$$

3.2 重构网络

3.2.1 BCNN 模型

BCNN 模型也是由卷积神经网络与双线性插值 Bilinear 方法组成. 双线性插值 Bilinear 负责上采样, 将网络层宽高放大到 33×33 . 卷积神经网络的卷积核大小分别为 $5 \times 5, 3 \times 3, 3 \times 3, 1 \times 1$. 压缩图像 y_i 通过 BCNN 模型 $F^b(\cdot)$ 重构出原始图像块 x_i 的轮廓信息 x_i^b , 公式如下:

$$x_i^b = F^b(y_i, W^b) = F^b(F^c(\text{Bilinear}(x_i), W^c), W^b). \quad (15)$$

W^b 是 BCNN 模型权重参数.

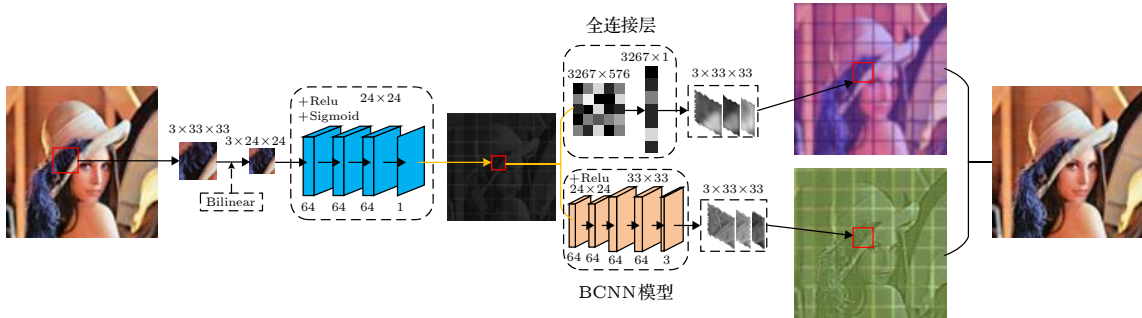


图 2 彩色图像的压缩重构网络 (采样率 $MR = 0.18$)

Fig. 2. Color image compression and reconstruction network, sampling rate $MR = 0.18$.

3.2.2 全连接层

与轮廓信息相比, 颜色信息更加复杂, 需要更多的权重参数. 卷积神经网络虽能很好地重构图像轮廓信息, 但权重参数有限, 过多的网络层又会造成重构时间增长. 全连接层有足够多的参数, 以彩色图像 $MR = 0.18$ 为例, 将 $1 \times 24 \times 24 = 576$ 的向量放大到 $3 \times 33 \times 33 = 3267$, 共有 1881792 个权重参数可以用来重构颜色信息. 压缩图像 y_i 通过全连接层 $F^l(\cdot)$ 重构出原始图像块 x_i 颜色信息 x_i^l , 公式如下:

$$x_i^l = F^l(y_i, W^l) = F^l(F^c(\text{Bilinear}(x_i), W^c), W^l). \quad (16)$$

W^l 是全连接层权重参数. BCNN 模型与全连接层重构出的图像如图 3 所示.

由于 BCNN 模型与全连接层重构的图像很多像素值不在 0—1 之间, 为了能直观展示出来, 对图像像素值进行归一化处理. 从图 3 可知, BCNN 模型重构出的图像颜色虽然单调, 但轮廓非常清晰. 全连接层重构出的图像较模糊, 但颜色更加丰富.

3.2.3 损失函数

压缩图像 y_i 通过 BCNN 模型和全连接层后, 合并颜色信息 x_i^l 和结构信息 x_i^b , 得到图像块的近似解 x_i' :

$$x_i' = x_i^l + x_i^b, \quad (17)$$

损失函数使用均方误差函数:

$$L(W^c, W^l, W^b) = \frac{1}{N} \sum_{i=1}^N \|x_i' - x_i\|_2^2 \\ = \frac{1}{N} \sum_{i=1}^N \|F^l(y_i, W^l) + F^b(y_i, W^b) - x_i\|_2^2. \quad (18)$$

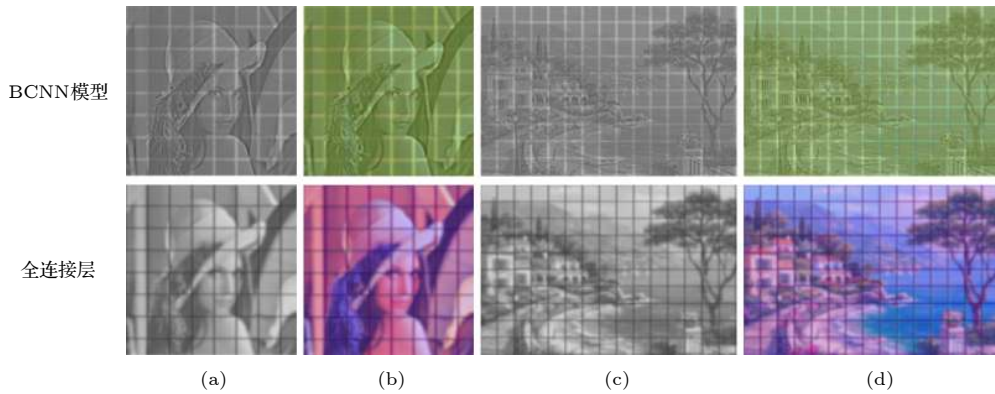


图 3 BCNN 模型与全连接层分别重构的 Lena 和 Sea 图像 (a) Lena (灰度); (b) Lena (彩色); (c) Sea (灰度); (d) Sea (彩色)

Fig. 3. Lena and Sea images reconstructed from BCNN model and fully connected layer respectively: (a) Lena (gray); (b) Lena (color); (c) Sea (gray); (d) Sea (color).

3.3 网络训练数据集与配置

先将 91 张彩色图像^[5]按 0.75, 1 和 1.5 的比例缩放, 再将图像分块, 大小为 $3 \times 33 \times 33$ 且取步长为 14, 共 87104 块小图像, 作为训练数据集. 使用 Pytorch 开源工具训练网络, 设备主要配置为 Intel Core i5-8500 CPU, 内存 16 GB, 显卡 GTX 2080ti.

3.4 网络训练参数设置

全连接层 $F^l(\cdot)$ 使用默认的初始化权重. 压缩网络 $F^c(\cdot)$ 和 BCNN 模型 $F^b(\cdot)$ 使用 Xavier 方法初始化权重. 使用 Adam 方法训练整个网络, 学习率设为 0.001, 每 100000 次学习率降低为原来的 1/2, 共训练 500000 次. 为了提高网络的抗噪能力, 训练时可在压缩图像上添加强度 $\sigma = 0.10$ 的高斯噪声.

4 加解密算法

4.1 加密

本文的通用图像压缩加密方案, 详细流程如图 4 所示.

详细的加密步骤如下所示.

步骤 1: 将彩色图像设置成 RGB 格式, 灰度图可以先转成 3 通道且对应位置的值相同. 经过压缩网络压缩后, 压缩图像块 y_i 是 4 维的, 在加密之前需拼接并转成 2 维的图像 img.

步骤 2: 先根据 SHA256 算法计算原始图像的哈希值, 将哈希值按步长为 2 切割并转十进制, 得到 32 个范围在 1—256 的值, 再从前往后进行异或处理, 最后除以 256, 得到 0—1 之间的一个小数作为原始图像的密钥 k_1 .

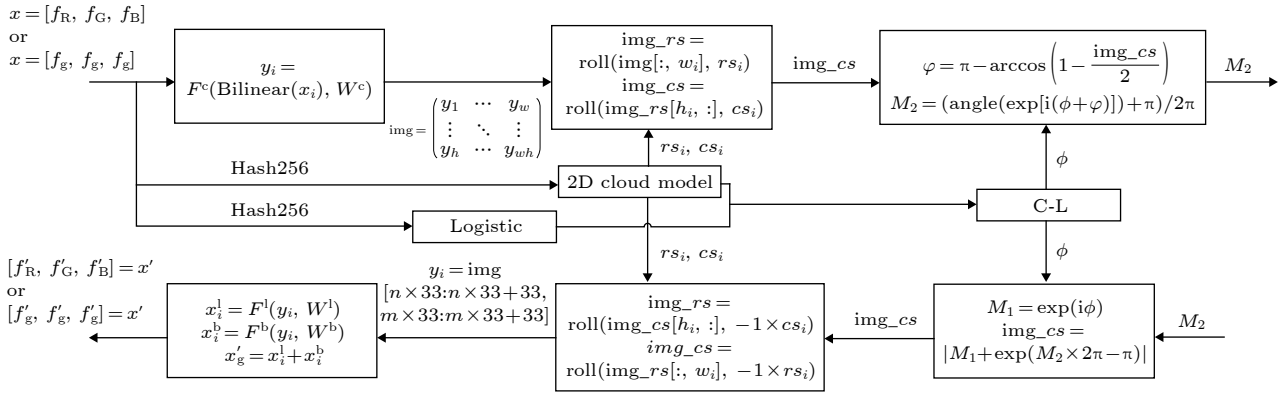


图 4 整个算法流程图

Fig. 4. Entire algorithm flow chart.

步骤 3: 根据原始图像的密钥 k_1 再产生与压缩图像 img 大小一样的二维云模型序列、Logistic 序列和 C-L 序列。二维云模型初始值 $(Ex_1, Ex_2) = (11, 22)$, $(En_1, En_2) = (33, 44)$, $(He_1, He_2) = (10, 30)$, 生成正态随机数之前, 先分别产生 (Ex_1, Ex_2) , (En_1, En_2) , (He_1, He_2) 的哈希值, 将这 3 组哈希值相加, 再按步长为 2 切割并转十进制, 然后求平均值, 与原始图像密钥 k_1 结合作为随机种子。Logistic 序列的参数 $r = 3.999$, 初始值为原始图像的密钥 k_1 。

步骤 4: 将二维云模型产生的随机序列放大取整后, 对压缩图像 img 进行行和列的滑动置乱, 得到置乱后的图像 img_{cs} 。

步骤 5: 将 C-L 序列作为矢量分解的夹角 ϕ , 与图像 img_{cs} 进行矢量分解得到相位分布矩阵 M_2 , 并将 M_2 作为密文。

4.2 解密

解密过程是加密过程的逆过程, 具体公式图 4 中已给出, 详细步骤如下所示。

步骤 1: 通过 C-L 级联混沌序列求出 M_1 。已知 M_1 与密文 M_2 , 根据 (12) 式得到置乱后的图像 img_{cs} 。

步骤 2: 根据 (10) 式产生的序列对图像 img_{cs} 进行列和行的逆向滑动, 得到 2 维的压缩图像 img , 再拼接成 4 维的图像块 y_i 。

步骤 3: 得到图像块 y_i 后, 再通过重构网络重构出图像。

5 实验与算法性能分析

5.1 重构质量分析

在重构质量上与 TVAL3^[16], NLR-CS^[17], D-

AMP^[18], ReconNet, DR²-Net, MSRNet 这些算法比较。前三种是基于传统的压缩感知算法, 后三种是基于深度学习的压缩感知算法。本节通过引入一些指标来衡量图像重构质量的高低。峰值信噪比 (peak signal to noise ratio, PSNR) 作为重构质量的评估指标, 值越大表示图像重构的质量越高。PSNR 的公式如下:

$$\text{PSNR} = 10 \times \lg \left(\frac{\text{MAX}^2}{\text{MSE}} \right) = 20 \times \lg \left(\frac{\text{MAX}}{\sqrt{\text{MSE}}} \right), \quad (19)$$

其中, MAX 表示图像像素可取的最大值, MSE 表示均方差。均方差的公式如下:

$$\text{MSE} = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [f(i, j) - f'(i, j)]^2. \quad (20)$$

式中, m 和 n 表示图像的宽高, $f(i, j)$ 表示原始图像像素值, $f'(i, j)$ 表示重构图像像素值。结构相似性 (structural similarity, SSIM) 从亮度、对比度和结构 3 个层次比较是否相似, 值在 0—1 之间, 越接近 1 表示两幅图像越相似。SSIM 的公式如下:

$$\text{SSIM}(X, Y) = L(X, Y) \times C(X, Y) \times S(X, Y), \quad (21)$$

其中, X 与 Y 表示对比的两张图像, $L(X, Y)$ 表示亮度的对比结果, $C(X, Y)$ 表示对比度的对比结果, $S(X, Y)$ 表示结构的对比结果。

$$\begin{cases} L(X, Y) = \frac{2u_X u_Y + C_1}{u_X^2 + u_Y^2 + C_1}, \\ C(X, Y) = \frac{2\sigma_X \sigma_Y + C_2}{\sigma_X^2 + \sigma_Y^2 + C_2}, \\ S(X, Y) = \frac{\sigma_{XY} + C_3}{\sigma_X \sigma_Y + C_3}, \end{cases} \quad (22)$$

其中 u_X 和 u_Y 分别是图像 X 和图像 Y 的均值, σ_X 和 σ_Y 分别是图像 X 和图像 Y 的方差, σ_{XY} 是图像 X

和图像 Y 的协方差, $C_1 = (k_1 \times j)^2$, $C_2 = (k_2 \times j)^2$, $C_3 = C_1/2$, $k_1 = 0.01$, $k_2 = 0.03$, $j = 255$.

$$\begin{cases} u_X = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} X(i, j), \\ \sigma_X^2 = \frac{1}{m \times n - 1} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (X(i, j) - u_X)^2, \\ \sigma_{XY} = \frac{1}{m \times n - 1} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (X(i, j) - u_X)(Y(i, j) - u_Y), \end{cases} \quad (23)$$

其中 m 和 n 表示图像的宽高.

使用 11 张灰度图像^[5]进行测试, 表 1 列出了采样率 $MR = 0.25, 0.10, 0.04, 0.01$ 的重构结果.

表 1 列出了 3 张灰度图像的 PSNR 与 11 张灰度图像的平均 PSNR. 从表 1 可以看出, 基于深度学习的算法 ReconNet 在 $MR = 0.25$ 时, 重构质量低于前三种传统压缩感知算法, 但 DR²-Net, MSRNet 和 FCLBCNN 的重构质量高于传统的 3 个算法, 且 FCLBCNN 在 4 个采样率上的重构图像平均 PSNR 值最高.

在数据集 BSD500 上测试算法的泛化能力, 共 500 张图像. 测试结果如表 2 所列.

表 2 为各算法在数据集 BSD500 上的 PSNR 与 SSIM 值 (“—”表示空). 采样率 $MR = 0.25, 0.10$ 时, FCLBCNN (gray) 的 PSNR 和 SSIM 值都是最高的, 重构性能优于基于深度学习的 ReconNet, DR²-Net 和 MSRNet. FCLBCNN (color) 的采样率 $MR = 0.08, 0.18$ 对应 FCLBCNN(gray) 的采样率 $MR = 0.25, 0.53$, 且他们的 PSNR 和 SSIM 值相差不大, 说明 FCLBCNN 通过彩色图像训练的网络也适用于灰度图像, 不需要重新训练网络. 实验表明, 本文 FCLBCNN 与其他算法相比, 重构质量更高且有着很好的泛化能力.

表 1 重构的灰度图像在不同算法、不同采样率下的 PSNR

Table 1. PSNR of reconstructed gray images under different algorithms and different sampling rates.

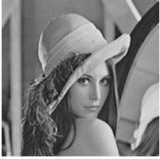







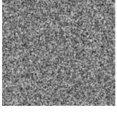

采样率	算法	Lena	Monarch	Flinstones	平均PSNR
0.25	TVAL3	28.67	27.77	24.05	27.84
	NLR-CS	29.39	25.91	22.43	28.05
	D-AMP	28.00	26.39	25.02	28.17
	ReconNet	26.54	24.31	22.45	25.54
	DR ² -Net	29.42	27.95	26.19	28.66
	MSRNet	30.21	28.90	26.67	29.48
FCLBCNN		31.09	29.97	27.57	29.71
0.10	TVAL3	24.16	21.16	18.88	22.84
	NLR-CS	15.30	14.59	12.18	14.19
	D-AMP	22.51	19.00	16.94	21.14
	ReconNet	23.83	21.10	18.92	22.68
	DR ² -Net	25.39	23.10	21.09	24.32
	MSRNet	26.28	23.98	21.72	25.16
FCLBCNN		26.93	24.58	22.08	25.41
0.04	TVAL3	19.46	16.73	14.88	18.39
	NLR-CS	11.61	11.62	8.96	10.58
	D-AMP	16.52	14.57	12.93	15.49
	ReconNet	21.28	18.19	16.30	19.99
	DR ² -Net	22.13	18.93	16.93	20.80
	MSRNet	22.76	19.26	17.28	21.41
FCLBCNN		23.33	19.59	17.17	21.51
0.01	TVAL3	11.87	11.09	9.75	11.31
	NLR-CS	5.95	6.38	4.45	5.30
	D-AMP	5.73	6.20	4.33	5.19
	ReconNet	17.87	15.39	13.96	17.27
	DR ² -Net	17.97	15.33	14.01	17.44
	MSRNet	18.06	15.41	13.83	17.54
FCLBCNN		18.12	15.63	13.90	17.62

256 × 256 的 Lena 图像在各阶段效果如表 3 所列.

表 2 在 BSD500 测试集上不同算法、不同采样率下的平均 PSNR 和平均 SSIM
Table 2. Mean PSNR and SSIM of different algorithms and different sampling rates on the BSD500 test set.

算法	$MR = 0.08$		$MR = 0.10$		$MR = 0.18$		$MR = 0.25$		$MR = 0.53$	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
ReconNet	—	—	23.28	0.6121	—	—	25.48	0.7241	—	—
DR ² -Net	—	—	24.26	0.6603	—	—	27.56	0.7961	—	—
MSRNet	—	—	24.73	0.6837	—	—	27.93	0.8121	—	—
FCLBCNN (gray)	—	—	24.83	0.7056	—	—	28.19	0.8400	32.87	0.9392
FCLBCNN (color)	27.94	0.8252	—	—	32.07	0.9279	—	—	—	—

表 3 Lena 图像在各阶段的效果 (采样率 $MR = 0.53$ (灰度), 0.18 (彩色))
Table 3. Lena image effects at various stages, sampling rate $MR = 0.53$ (gray), 0.18 (color).

原图	采样率	压缩图像	置乱图像	密文图像	重构图像	PSNR	SSIM
	0.53					36.4387	0.9715
	0.18					32.5516	0.9456

从表 3 可以看出, Lena 在采样率 $MR = 0.53$ (灰度), 0.18 (彩色) 时, 密文图像已看不出原图轮廓, 重构出的图像也与原始图像非常接近, 具有良好的视觉效果, 所以下列的性能分析皆使用这两个采样率.

5.2 密钥空间分析

一般情况下, 密钥空间足够大时, 图像加密算法才能有效抵御暴力破解. 本文使用的混沌系统中, Logistic 序列的密钥有 r 与 $z[0]$, 二维云模型的密钥有随机种子 k_1 , (Ex_1, Ex_2) , (En_1, En_2) 和 (He_1, He_2) , 共 9 个密钥. 仿真设备精度为 10^{15} , 精确位数为 15 位, 密钥空间为 $10^{15 \times 9} = 10^{135}$, 而密钥空间 $\geq 2^{100} \approx 10^{30}$ 就能满足安全要求 [19], 所以本文加密算法的密钥空间足够大, 暴力破解无法对加密图像进行有效解密.

5.3 相关性分析

一般来说, 原始图像相邻像素值的相关性会比

较高, 但对于一个理想的密文图像, 相邻像素值的相关性应该为 0. 因此, 密文图像的相邻像素值的相关系数是加密算法优劣的一个重要指标. 相关系数分为水平、垂直和斜线 3 个方向, 计算公式如下:

$$r = \frac{\sum_{i=1}^N (x_i - \bar{x}) \times (y_i - \bar{y})}{\sqrt{\sum_{i=1}^N (x_i - \bar{x})^2} \times \sqrt{\sum_{i=1}^N (y_i - \bar{y})^2}}. \quad (24)$$

其中, \bar{x} 和 \bar{y} 分别为 x_i 和 y_i 的平均值. 表 4 所列为本文与文献 [20, 21] 在 3 个方向上的相关系数, 密文图像上的绝对值最小值已用粗体标出.

从表 4 可以看出, 本文算法在相关系数的平均值上更接近 0, 优于其他算法. 同时, 为了更直观的展现图像相邻像素值的相关性, 引入 Lena (gray) 的明文图像与密文图像在 3 个方向上的相关性分布图如图 5 所示.

从图 5 上可以看出, 本文算法得到的密文图像在 3 个方向上的像素点成随机性分布, 已显著破坏了相邻像素点的相关性, 增强了保密性.

表 4 不同加密算法的相关系数比较

Table 4. Comparison of correlation coefficients of different encryption algorithms.

测试图像	方向	明文(gray)	密文			
			本文(gray)	本文(color)	文献[20]	文献[21]
Lena	水平	0.9396	0.0010	-0.0024	-0.0048	0.0011
	竖直	0.9639	-0.0066	0.0012	-0.0112	0.0098
	斜线	0.9189	-0.0039	0.0035	-0.0045	-0.0227
Peppers	水平	0.9769	-0.0004	-0.0023	-0.0056	0.0071
	竖直	0.9772	0.0089	0.0063	-0.0162	-0.0065
	斜线	0.9625	-0.0077	0.0004	-0.0113	-0.0165
平均值	水平	—	0.0003	-0.0024	-0.0052	0.0041
	竖直	—	0.0012	0.0038	-0.0137	0.0017
	斜线	—	-0.0058	0.0020	-0.0079	-0.0196

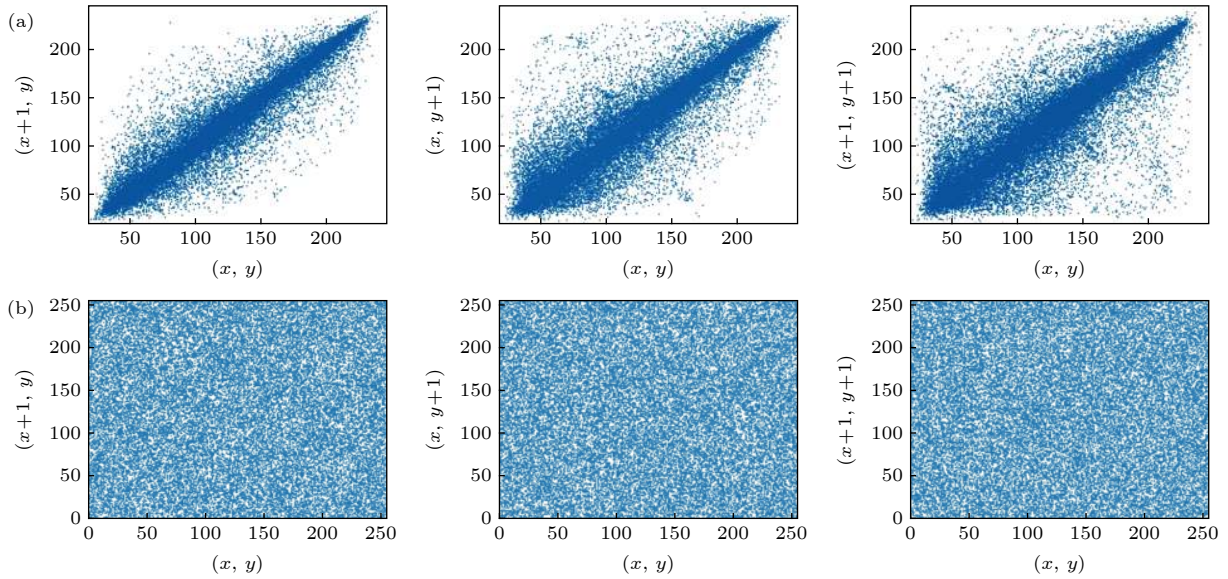


图 5 Lena (gray) 图像明文与密文在水平、竖直、斜线 3 个方向的相关分布图 (a) 明文图像的相关分布图; (b) 密文图像的相关分布图

Fig. 5. Correlation distribution of the plaintext and ciphertext in the horizontal, vertical and oblique directions of Lena (gray) images: (a) Correlation distribution of plaintext; (b) correlation distribution of ciphertext.

5.4 信息熵分析

全局信息熵反映了整个图像像素值的混乱程度, 其信息熵越大, 表示图像所包含的信息越混乱, 全局信息熵的公式如下所示:

$$en = - \sum_{i=1}^L p(i) \log_2 p(i). \quad (25)$$

其中, L 表示图像的灰度等级, 本文使用的图片灰度级皆为 256, $p(i)$ 表示像素值出现的概率, en 的理想值为 8. 本文与其他算法在 Lena, Peppers 上的全局信息熵如表 5 所列, 密文图像的全局信息熵最大值已用粗体标出.

基于局部信息熵的图像随机性统计检验方法 [22] 是对全局信息熵的扩展, 通过计算多个非重叠且随机选择的图像块上信息熵的样本均值来衡量图像的随机性. 使用共 30 个大小为 44×44 的不重叠图像块, 本文算法在 Lena, Peppers 上密文的局部信息熵如表 6 所列.

表 5 不同加密算法得到的信息熵的比较

Table 5. Comparison of the entropy obtained by different encryption algorithms.

测试图像	明文(gray)	密文		
		本文(gary)	本文(color)	文献[12]
Lena	7.3035	7.9949	7.9944	7.9544
Peppers	7.4344	7.9956	7.9952	7.9633

从表 5 可以看出, 本文算法的全局信息熵更接近 8. 表 6 中, 局部信息熵的值也都在临界范围内. 因此, 可以认为本文算法得到的密文像素值分布非常混乱, 能更好地掩盖明文图像信息.

5.5 明文敏感性分析

本文加密算法使用的密钥与明文有关且明文对密文非常敏感, 使轻微修改明文后得到的密文与原密文相差很大, 无法破译密码系统. 本节引入像素改变率 (number of pixels change rate, NPCR) 和一致平均改变密度 (unified average changing

表 6 不同加密算法得到的局部信息熵比较

Table 6. Comparison of the local entropy obtained by different encryption algorithms.

测试图像	局部信息熵(gray/color)	临界值		
		$u_{0.05}^{*-}$ = 7.9019	$u_{0.01}^{*-}$ = 7.9017	$u_{0.001}^{*-}$ = 7.9015
		$u_{0.05}^{*+}$ = 7.9030	$u_{0.01}^{*+}$ = 7.9032	$u_{0.001}^{*+}$ = 7.9034
Lena	7.9024/7.9027	Pass	Pass	Pass
Peppers	7.9027/7.9023	Pass	Pass	Pass

intensity, UACI) 来评估加密算法抵抗差分攻击的能力, 公式如下所示:

$$\text{NPCR} = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N [|\text{sign}(P_1(i, j) - P_2(i, j))| \times 100\%], \quad (26)$$

$$\text{sign}(x) = \begin{cases} 1, & x \geq 0, \\ 0, & x = 0, \\ -1, & x \leq 0. \end{cases} \quad (27)$$

$$\text{UACI} = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N \frac{|P_1(i, j) - P_2(i, j)|}{255 - 0} \times 100\%, \quad (28)$$

其中, $P_1(i, j)$ 为密文图像 P_1 的像素值, $P_2(i, j)$ 为密文图像 P_2 的像素值.

本文与其他算法在 Lena, Peppers 密文上的 NPCR 与 UACI 对比如表 7 和表 8 所列.

从表 7 和表 8 可以看出, 本文算法在 NPCR 与 UACI 上都处于临界范围内, 说明本文加密算法能够更好地抵御差分攻击.

5.6 鲁棒性分析

为了验证本文算法的压缩重构网络在训练时

添加高斯噪声能提高鲁棒性, 网络在训练时添加了强度 $\sigma = 0.10$ 的高斯噪声与网络在训练时没有添加高斯噪声的算法, 对高斯噪声、椒盐噪声和剪切攻击的对比如图 6 和图 7 所示.

图 6 中, 由于重构 (a) 和 (b) 图像的网络在训练时没有添加高斯噪声, 解密与重构后图像已看不清轮廓. 重构 (c) 和 (d) 图像的网络在训练时添加了高斯噪声, 解密与重构后图像依然能看清轮廓. 图 7 中, 密文图像被剪切后, 重构出的 (d) 和 (e) 图像质量优于 (b) 和 (c) 图像质量. 从图 6 和图 7 可以看出, 训练网络时在压缩图像上添加高斯噪声, 能抵抗一定程度的噪声污染与剪切攻击.

5.7 选择明文攻击分析

选择明文攻击是指通过特殊的明文与对应的密文推导出中间密钥, 本节通过一个简单的实验来验证本文算法能抵御选择明文攻击. 定义一个像素点全为 0 的灰度图 P_1 , 图像 P_2 与 P_1 只有一个像素值不一样, C_1, C_2 分别为 P_1, P_2 的密文图像. 定义 $P_3 = |P_1 - P_2|$, $C_3 = |C_1 - C_2|$. 在明文上找一个像素点并修改像素值, P_1, P_2, P_3 与 C_1, C_2, C_3 如图 8 所示.

表 7 不同加密算法得到的 NPCR 比较

Table 7. Comparison of NPCR obtained by different encryption algorithms.

测试图像	NPCR (gray/color)	NPCR理论临界值		
		$N_{0.05}^* = 99.5693\%$	$N_{0.01}^* = 99.5527\%$	$N_{0.001}^* = 99.5341\%$
Lena	0.9960/0.9961	Pass	Pass	Pass
Lena ^[12]	0.9954/—	Fail	Fail	Pass
Lena ^[20]	0.9962/—	Pass	Pass	Pass
Peppers	0.9959/0.9957	Pass	Pass	Pass
Peppers ^[12]	0.9944/—	Fail	Fail	Fail
Peppers ^[20]	0.9963/—	Pass	Pass	Pass

表 8 不同加密算法得到的 UACI 比较

Table 8. Comparison of UACI obtained by different encryption algorithms.

测试图像	UACI (gray/color)	UACI理论临界值		
		$u_{0.05}^{*-} = 33.2824\%$ $u_{0.05}^{*+} = 33.6447\%$	$u_{0.01}^{*-} = 33.2255\%$ $u_{0.01}^{*+} = 33.7016\%$	$u_{0.001}^{*-} = 33.1594\%$ $u_{0.001}^{*+} = 33.7677\%$
Lena	0.3352/0.3357	Pass	Pass	Pass
Lena ^[12]	0.3303/—	Fail	Fail	Fail
Lena ^[20]	0.3370/—	Fail	Pass	Pass
Peppers	0.3333/0.3331	Pass	Pass	Pass
Peppers ^[12]	0.3305/—	Fail	Fail	Fail
Peppers ^[20]	0.3369/—	Fail	Pass	Pass

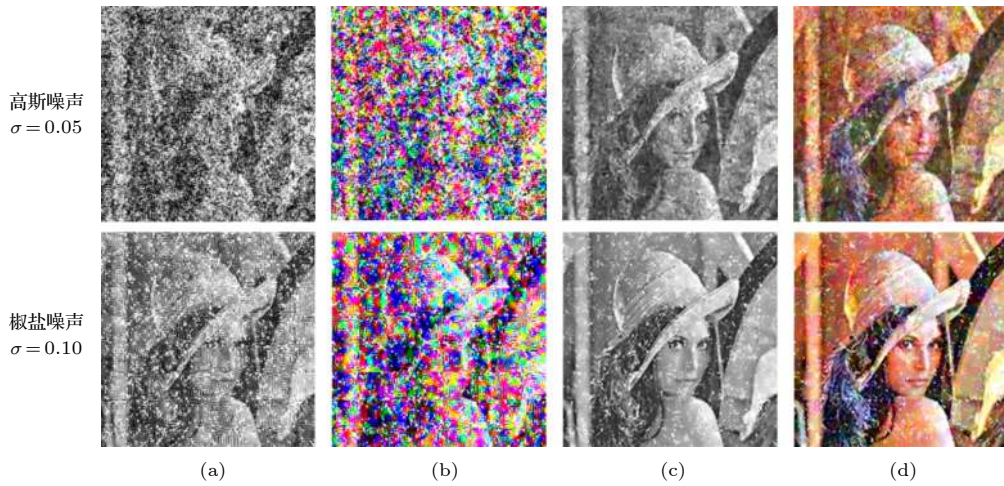


图 6 在密文图像上添加高斯噪声或椒盐噪声后重构出的 Lena 图像 (a), (b) 使用的网络在训练时没有添加高斯噪声; (c), (d) 使用的网络在训练时添加了强度为 0.10 的高斯噪声

Fig. 6. Lena image reconstructed by adding Gaussian noise or salt and pepper noise to the ciphertext image: The networks used in (a) and (b) did not add Gaussian noise during training; the networks used in (c) and (d) are trained with Gaussian noise with an intensity of 0.10.

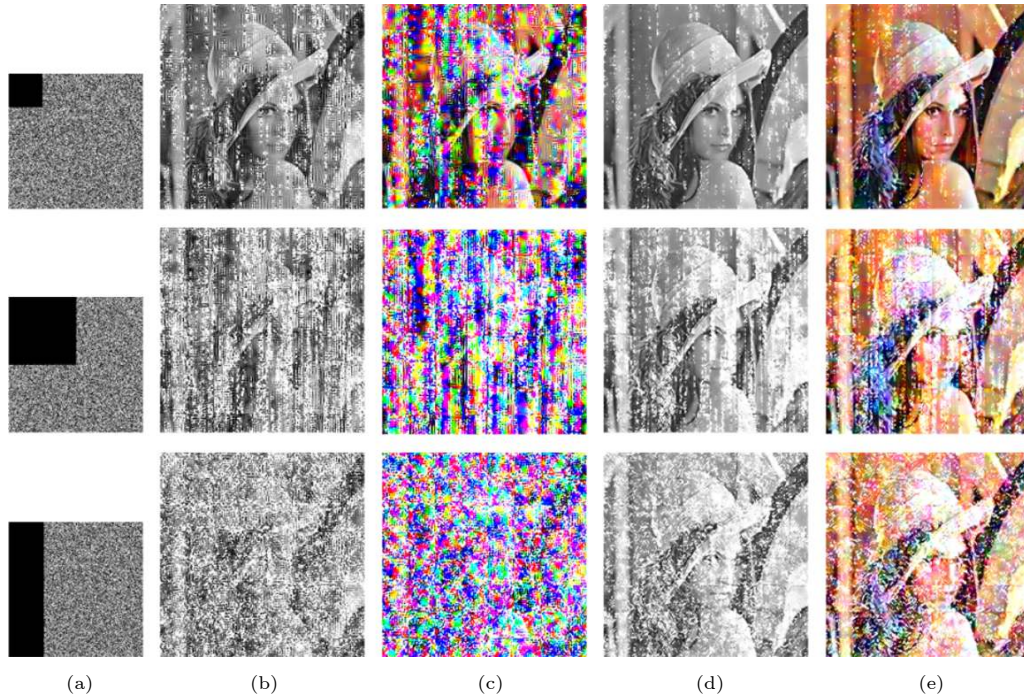


图 7 Lena 图像的密文被剪切后的重构结果 (a) 剪切不同大小后的密文; (b), (c) 使用的网络在训练时没有添加高斯噪声; (d), (e) 使用的网络在训练时添加了强度为 0.10 的高斯噪声

Fig. 7. Reconstruction result after ciphertext cut of Lena image: (a) Cut ciphertexts of different sizes; the networks used in (b) and (c) did not add Gaussian noise during training; the networks used in (d) and (e) are trained with Gaussian noise with an intensity of 0.10.

从图 8 可知, 外界无法从 C_3 上获得任何有效信息, 说明本文加密算法能有效抵御选择明文攻击.

5.8 直方图分析

直方图反映了图像中每种灰度级的像素个数, 越均匀说明加密效果越好, 本节通过明文和密文的

直方图对本文算法进行评估, Lena, Peppers 在灰度图像和彩色图像上的直方图如图 9 所示.

图 9 中, Lena 和 Peppers 的明文图像直方图有着明显的像素值分布特性, 而密文图像的直方图非常均匀, 很好地隐藏了明文图像的像素值分布特性. 说明本文算法可以很好地抵抗统计攻击.

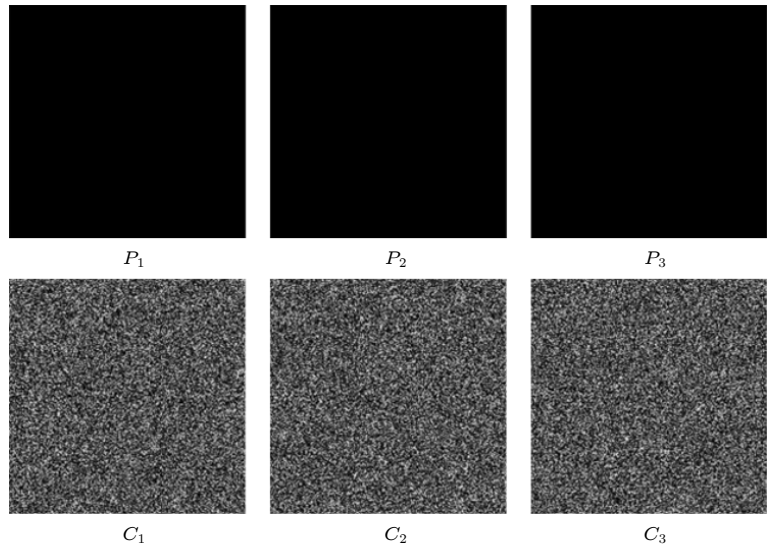


图 8 选择明文攻击效果图

Fig. 8. Effect pictures of chosen plaintext attack.

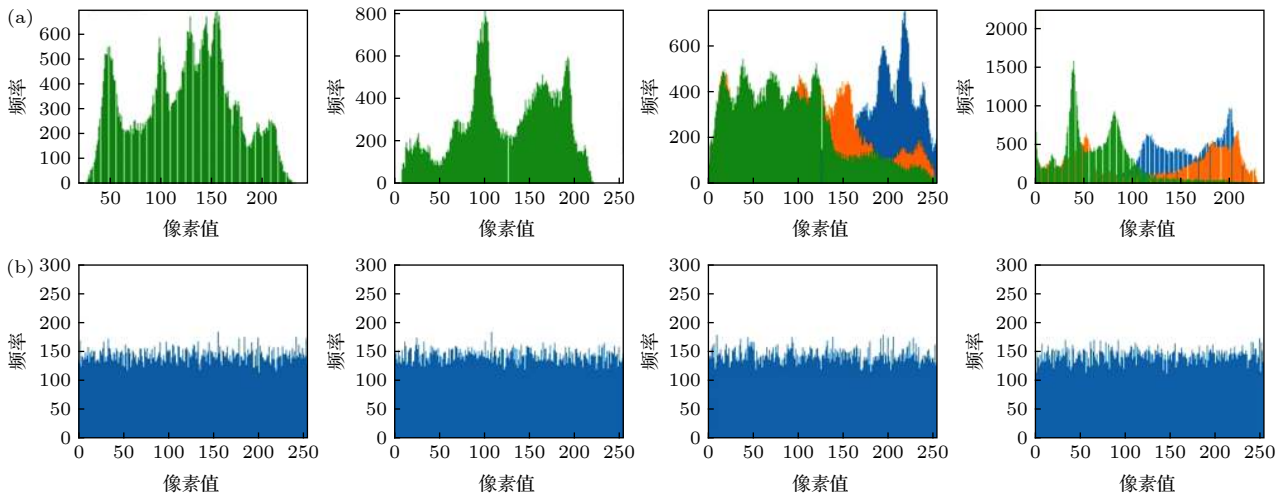


图 9 Lena (gray), Peppers (gray), Lena (color), Peppers (color) 图像在明文与密文上的直方图 (a) 明文直方图; (b) 密文直方图
Fig. 9. Histograms of Lena (gray), Peppers (gray), Lena (color), Peppers (color) images in plain text and ciphertext: (a) Plain text histogram; (b) ciphertext histogram.

表 9 本文压缩加密算法与在原图上直接使用本文加密算法的耗时对比

Table 9. Time-consuming comparison that the compression encryption algorithm of this article and the encryption algorithm of this article directly used on the original image.

图像大小	压缩重构(gray/color)	加解密(gray/color)	总时间(gray/color)	编程工具	平台
256 × 256	0.21/0.20	0.66/0.65	0.87/0.85	Pycharm + Pytorch	i5-8500 CPU
	—	0.93/2.81	0.93/2.81		
512 × 512	0.91/0.89	2.51/2.51	3.42/3.40		
	—	3.89/11.96	3.89/11.96		
1024 × 1024	4.81/4.62	9.40/9.42	14.21/14.04		
	—	15.84/48.51	15.84/48.51		

5.9 时间复杂度分析

时间复杂度也是衡量算法性能的一个重要指标. 为了验证本文基于深度学习的压缩重构网络能

降低整个算法的耗时, 与在原图上直接使用本文加密算法的耗时对比如表 9 所列, 最快时间已用粗体标出.

从表 9 可以看出, 本文压缩加密算法比在原图上直接使用本文加密算法的总耗时更短, 特别是彩色图像, 说明本文压缩加密算法在时间上有着很大优势.

6 结 论

本文提出了一种基于深度学习的压缩感知与复合混沌的通用图像加密方案, 利用深度学习方法来压缩重构图像, 适用于灰度图像与 RGB 格式的彩色图像, 不需要单独训练网络, 使用复合混沌系统、滑动置乱与矢量分解组成的加密算法对压缩后的图像进行加解密. 通过实验与性能分析, 验证了本文压缩加密算法在图像存储与传输方面的优势, 耗时短、重构质量高、抗噪能力强且安全性高.

参考文献

- [1] Donoho D L 2006 *IEEE Trans. Inf. Theory* **52** 1289
- [2] Candes E J, Romberg J, Tao T 2006 *IEEE Trans. Inf. Theory* **52** 489
- [3] Candes E J, Wakin M B 2008 *IEEE Signal Process. Mag.* **25** 21
- [4] Mousavi A, Patel A B, Baraniuk R G 2015 *53rd Annual Allerton Conference on Communication, Control, and Computing* Monticello, USA, September 29–October 2, 2015 p1336
- [5] Lian Q S, Fu L P, Chen S Z, Shi B S 2019 *Acta Autom. Sin.* **45** 2082 (in Chinese) [练秋生, 富利鹏, 陈书贞, 石保顺 2019 *自动化学报* **45** 2082]
- [6] Kulkarni K, Lohit S, Turaga P, Kerviche R, Ashok A 2016 *IEEE Conference on Computer Vision and Pattern Recognition* Las Vegas, USA, June 26–30, 2016 p449
- [7] Yao H T, Dai F, Zhang S L, Zhang Y D, Tian Q, Xu C S 2019 *Neurocomputing* **359** 483
- [8] Li J, Xian F, Zhang J P 2019 *Int. Electr. Elem.* **27** 84 (in Chinese) [李静, 向菲, 张军朋 2019 *电子设计工程* **27** 84]
- [9] Hu X C, Wei L S, Chen W, Chen Q Q, Guo Y 2020 *IEEE Access* **8** 12452
- [10] Zhuang Z B, Li J, Liu J Y, Chen S Q 2020 *Acta Phys. Sin.* **69** 040502 (in Chinese) [庄志本, 李军, 刘静漪, 陈世强 2020 *物理学报* **69** 040502]
- [11] Zhang D, Liao X F, Yang B, Zhang Y S 2018 *Multim. Tools Appl.* **77** 2191
- [12] Shi H, Wang L D 2019 *Acta Phys. Sin.* **68** 200501 (in Chinese) [石航, 王丽丹 2019 *物理学报* **68** 200501]
- [13] Gong L H, Qiu K D, Deng C Z, Zhou N R 2019 *Opt. Laser Technol.* **115** 257
- [14] Qin W, Peng X 2010 *Opt. Lett.* **35** 118
- [15] Liu Y N, Niu H Q, Li Z L 2019 *Chin. Phys. Lett.* **36** 044302
- [16] Li C B, Yin W T, Jiang H, Zhang Y 2013 *Comput. Optim. Appl.* **56** 507
- [17] Dong W S, Shi G M, Li X, Ma Y, Huang F 2014 *IEEE Trans. Image Process.* **23** 3618
- [18] Metzler C A, Maleki A, Baraniuk R G 2016 *IEEE Trans. Inf. Theory* **62** 5117
- [19] Guo Y, Jing S W, Zhou Y Y, Xu X, Wei L S 2020 *IEEE Access* **8** 9896
- [20] Belazi A, El-Latif A A, Belghith S 2016 *Signal Process.* **128** 155
- [21] Hua Z Y, Zhou Y C, Pun C M, Chen C 2015 *Inf. Sci.* **297** 80
- [22] Wu Y, Zhou Y C, Saveriades G, Agaian S S, Noonan J P, Natarajan P 2013 *Inf. Sci.* **222** 323

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

Chen Wei Guo Yuan[†] Jing Shi-Wei

(*School of Computer and Control Engineering, Qiqihar University, Qiqihar 161006, China*)

(Received 29 June 2020; revised manuscript received 10 August 2020)

Abstract

Many image compression and encryption algorithms based on traditional compressed sensing and chaotic systems are time-consuming, have low reconstruction quality, and are suitable only for grayscale images. In this paper, we propose a general image compression encryption algorithm based on a deep learning compressed sensing and compound chaotic system, which is suitable for grayscale images and RGB format color images. Color images can be directly compressed and encrypted, but grayscale images need copying from 1 channel to 3 channels. First, the original image is divided into multiple $3 \times 33 \times 33$ non-overlapping image blocks and the bilinear interpolation Bilinear and convolutional neural network are used to compress the image, so that the compression network has no restriction on the sampling rate and can obtain high-quality compression of image. Then a composite chaotic system composed of a two-dimensional cloud model and Logistic is used to encrypt and decrypt the compressed image (sliding scrambling and vector decomposition), and finally the decrypted image is reconstructed. In the reconstruction network, the convolutional neural network and bilinear interpolation Bilinear are mainly responsible for reconstructing the contour structure information, and the fully connected layer is mainly responsible for reconstructing and combining the color information to reconstruct a high-quality image. For grayscale images, we also need to calculate the average value of the corresponding positions of the 3 channels of the reconstructed image, and change the 3 channels into 1 channel. The experimental results show that the general image encryption algorithm based on deep learning compressed sensing and compound chaos system has great advantages in data processing quality and computational complexity. Although in the network the color images are used for training, the quality of grayscale image reconstruction is still better than that of other algorithms. The image encryption algorithm has a large enough key space and associates the plaintext hash value with the key, which realizes the encryption effect of one image corresponding to one key, thus being able to effectively resist brute force attacks and selective plaintext attacks. Compared with it in the comparison literature, the correlation coefficient is close to an ideal value, and the information entropy and the clear text sensitivity index are also within a critical range, which enhances the confidentiality of the image.

Keywords: deep learning, compressed sensing, encryption, compound chaotic system

PACS: 05.45.Ac, 05.45.Vx, 05.45.Gg

DOI: [10.7498/aps.69.20201019](https://doi.org/10.7498/aps.69.20201019)

* Project supported by the National Natural Science Foundation of China (Grant No. 61872204), the Natural Science Foundation of Heilongjiang Province, China (Grant No. F2017029), the Fundamental Research Funds for the Higher Education Institutions of Heilongjiang Province, China (Grant No. 135109236), and the Graduate Innovation Research Project, China (Grant No. YJSCX2019042).

[†] Corresponding author. E-mail: guoyuan171@126.com