

LightLSB: 算力受限环境下大规模生物特征图像的轻量级安全传输机制

张登辉^{1,2}, 沈圣尚¹, 姚捷凤¹, 李默涵¹, 李爱平³

(1. 广州大学网络空间安全学院, 广东 广州 510006;

2. 齐鲁工业大学(山东省科学院)算力互联网与信息安全教育部重点实验室, 山东 济南 250353;

3. 国防科技大学计算机学院, 湖南 长沙 410073)

摘要:近年来, 以人脸识别为代表的生物特征识别技术越来越多地出现在社会生活中。物联网智能终端之间的互联互通使随时随地大规模收集用户生物特征数据成为可能, 也为海量数据的安全应用带来新的挑战。与通用计算设备相比, 物联网终端设备日趋小型化和轻量化, 难以支撑标准密码学所需的复杂运算。生物特征技术的广泛使用加剧了社会对个人隐私泄露的担忧。针对上述问题, 提出了一种基于可视密码的轻量级生物特征图像安全传输机制LightLSB。LightLSB复用现有可视密码方法, 在预处理和后处理过程中逐步提升解密图像质量。通过将敏感生物特征图像分割为多张与原始图像无关的分存图像, 在不可信网络中实现了大规模生物特征图像的安全传输。在5个典型的生物特征数据集上开展了实验, 实验结果表明, 所提架构可以在加密数据集上实现与普通数据集相同的识别性能。

关键词: 物联网; 隐私保护; 可视密码; 图像安全

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025016

LightLSB: a lightweight secure transmission mechanism for large-scale biometric images in computing limited environment

ZHANG Denghui^{1,2}, SHEN Shengshang¹, YAO Jiefeng¹, LI Mohan¹, LI Aiping³

1. Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, China

2. Key Laboratory of Computing Power Network and Information Security, Ministry of Education, Qilu University of Technology (Shandong Academy of Sciences), Jinan 250353, China

3. College of Computer Science and Technology, National University of Defense Technology, Changsha 410073, China

收稿日期: 2024-12-25; **修回日期:** 2025-02-28

通信作者: 李爱平, liaiping@nudt.edu.cn

基金项目: 国家重点研发计划(2019YFB1706003); 广东省自然科学基金(2214050004382); 教育部人文社科青年基金项目(23YJCZH291); 算力互联网与信息安全教育部重点实验室课题(2023ZD02)

Foundation Items: The National Key R&D Program of China (2019YFB1706003), The Natural Science Foundation of Guangdong Province (2214050004382), Youth Program of Humanities and Social Sciences of the MoE (23YJCZH291), Key Laboratory Project of Computing Power Network and Information Security, Ministry of Education (2023ZD02)

引用格式: 张登辉, 沈圣尚, 姚捷凤, 等. LightLSB: 算力受限环境下大规模生物特征图像的轻量级安全传输机制[J]. 网络与信息安全学报, 2025, 11(2): 61-75.

Citation Format: ZHANG D H, SHEN S S, YAO J F, et al. LightLSB: a lightweight secure transmission mechanism for large-scale biometric images in computing limited environment[J]. Chinese Journal of Network and Information Security, 2025, 11(2): 61-75.

Abstract: In recent years, face recognition and other biometric recognition technologies have been increasingly appearing in social life. The interconnection of intelligent terminals in the Internet of things (IoT) has made it possible to collect biometrics on a large scale anytime and anywhere, which has also brought new challenges to the privacy protection of massive data. Compared with general computing devices, IoT terminal equipment has been becoming smaller and lighter, making it difficult to support the complex operations required by standard cryptography. The widespread use of biometric recognition has intensified social concerns about personal privacy disclosure. To address these problems, a lightweight secure transmission mechanism for large-scale biometric images (LightLSB) was proposed. The existing visual cryptography algorithm was reused, and the quality of decrypted images was gradually improved during preprocessing and post-processing. By dividing sensitive biometric images into multiple shares unrelated to the original image, the secure transmission of large-scale biometric images was realized in untrusted networks. Experiments were carried out on three typical biometric datasets, and the results showed that the proposed framework could achieve the same recognition performance on encrypted datasets as on ordinary datasets.

Keywords: IoT, privacy protection, visual cryptography, image security

0 引言

近年来,随着物联网技术的快速发展与移动智能终端的普及^[1],以人脸识别为代表的生物特征识别技术越来越多地出现在社会生活中。生物特征识别是一种利用人体生物特性(如人脸、指纹和步态等)进行身份认证的技术。基于密码学和物理身份的传统身份识别和认证技术存在易伪造、易遗忘和应用场景受限等缺点^[2]。生物特征识别技术弥补了传统基于密码学认证方式的缺陷,能够在不可信网络环境下确保用户数字身份与物理身份的统一,已成为当前最受关注的身份认证技术之一^[3]。当前新型生物特征应用和范式不断涌现,在电子商务、移动支付、智能安防等领域取得了巨大成功^[4]。

智能终端设备之间的互联互通使随时随地大规模收集生物特征图像成为可能,也为海量数据的安全应用带来了新的挑战^[5]。当在不受信任的开放网络传输敏感生物特征数据时,由于其唯一性和持久性,一旦泄露可能会造成永久损失。生物特征保护技术主要分为特征变换和特征加密两类。其中,特征变换方法也称为可撤销方法^[6]。它对特征进行不可逆变换,在不降低特征唯一性的前提下认证身份,如果模板丢失或其信息泄露,可以重新生成模板。由于同一模板的不同变换不会泄露原始模板的任何信息,因此即使变换特征信息泄露,更改参数再次变换仍可保护原始数据,但对比时依赖预存在数据库中的密钥。针对双因子可撤销模板保护方法中的用户因子易丢

失和遗忘问题,孔小景等^[7]用预定义的滑动窗替换不同的辅助数据,提出了一种基于单因子的可撤销生物特征认证方法,该方法能抵御多种安全攻击。特征加密方法将密钥与生物特征互相绑定,利用辅助信息在不泄露生物特征模板信息的前提下认证,但为满足可撤销特性又产生了密钥管理问题。Elrefaie等^[8]将模糊承诺方法应用于基于机器视觉的步态识别系统。此外,Rathgeb等^[9]基于模糊保险箱方法通过将实数特征向量映射为整数值特征向量,提出了一种与生物特征无关的变换方法。Shahreza等^[10]将同态加密用于生物特征模板保护,但该方法运行效率低、通信开销大,尚未达到实用要求。

与通用计算设备不同,物联网终端设备日趋小型化和轻量化,难以在相机和指纹采集器中执行复杂的标准密码学操作^[11]。海量数据的出现使人们更加依赖强大的算力来分析和识别生物特征。而节能和可持续性已成为物联网低功耗终端用户体验的关键^[12]。大规模数据的应用效益与个人隐私保护的矛盾已成为生物特征识别技术的应用壁垒。

作为一种针对图像的秘密共享方法,可视密码(visual cryptography, VC)提供了一种图像与密码学相结合的轻量级安全传输方法^[13-15],阈值特性使得单独的加密图像不会泄露原始图像的任何信息^[16]。VC去除了加密过程中的复杂计算与密钥依赖,是一种低算力场景下图像加密替代方法^[17]。Gayathri等^[18]将像素混洗特征提取技术与秘密共享网络相结合,实现了多模态生物特征认证。Muhammed等^[19]设计了单点弹性分布式指纹

模板存储方法,融合秘密共享与逆半色调(半调)技术,实现了指纹模板的安全重构。然而,VC技术一直受到像素扩展和质量下降等问题的困扰。这些限制不但增加了图像传输的负担,而且损害了下游生物特征识别任务的精度^[20-21]。

针对上述问题,本文提出了一种大规模生物特征图像的轻量级安全传输机制LightLSB,以实现加密方法在资源受限的物联网中的可用性。

本文提出的有意义非扩展VC方法(extended visual cryptography scheme, EVCS)加解密实验效果如图1所示,本文提出的EVCS不但超越了现有的无意义随机网格VC方法(RG-VC)^[22-23],而

且能够恢复出高清图像。LightLSB的架构如图2所示,LightLSB首先通过重新映射颜色空间和灰度值,预生成用于加密的子块,该操作可以生成图像质量更高的VC解密图像;然后,使用高斯滤波器平滑背景区域噪声,使用双边滤波器增强纹理细节,从而提升解密图像质量。最后,本文开发了一个孪生网络识别模型,通过表示学习实现了有损加密图像的高精度识别。

本文的主要贡献如下。

1) 提出一种基于秘密共享(secret sharing, SS)的传输模型,实现海量敏感数据图像在物联网终端设备的实时传输。

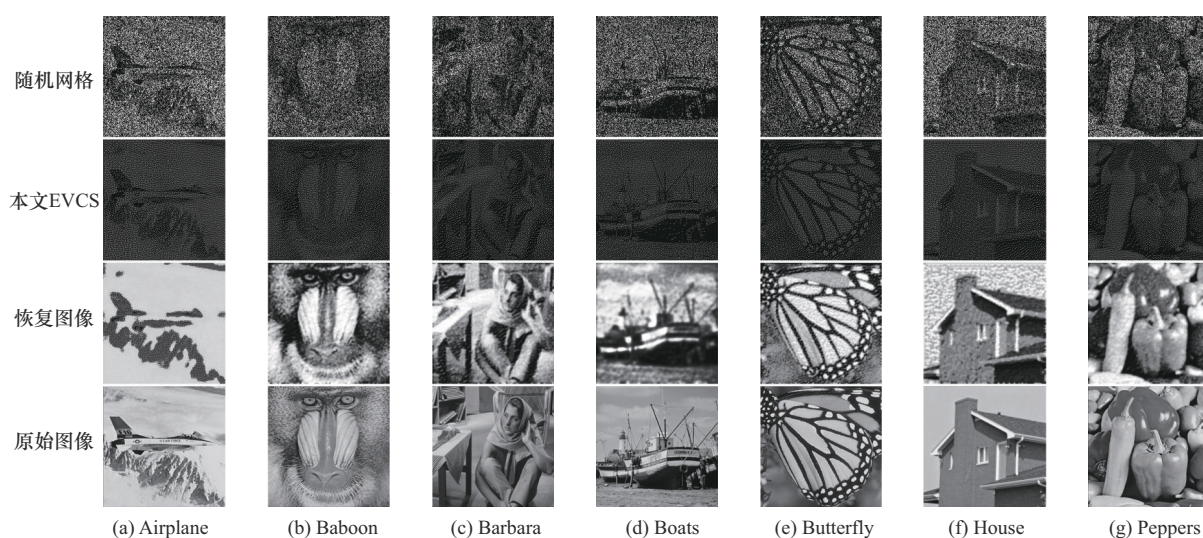


图1 EVCS加解密实验效果
Figure 1 The experimental effects of EVCS on encryption and decryption

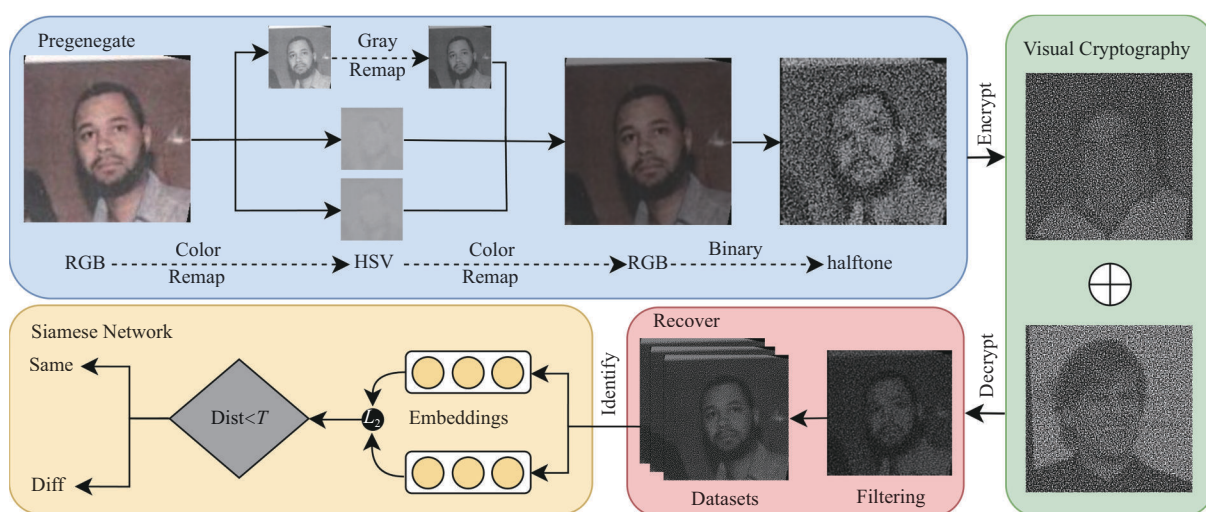


图2 LightLSB的架构
Figure 2 Architecture of LightLSB

2) 利用灰度重映射和双边滤波器提高有损生物特征图像的可感知性, 减小解密图像中不可避免的噪声, 从而提高图像质量。

3) 基于 5 个典型生物特征数据集进行了综合实验, 证明所提出的架构可以在加密数据集上实现与普通数据集相同的识别性能。

1 先验知识

1.1 可视密码加密方法

1.1.1 经典可视密码方法

VC 是一种利用人眼视觉特性来加密和解密图像的技术, 最初由 Naor Moni 和 Shamir Adi 提出, 核心思想是将一张秘密图像分割成多张随机的分存图像, 每张分存图像不包含有关原始图像的任何信息, 解密时只需将加密的分存图像打印在透明的胶片上进行重叠, 通过人眼视觉系统即可恢复出原始图像中的秘密信息。

VC 是一种 (k, n) 的 SS 方法, 可以将黑白秘密图像加密为 n 份分存图像。SS 的阈值特性使得 k ($k \leq n$) 或更多参与者将各自持有的分存图像堆叠在一起时才能恢复秘密图像。若待加密的像素为黑色 (用 1 表示), 对应封面图像中的两个像素为 1 和 0 (用白色表示), 则通过对基矩阵的任意列进行置换即可得到加密矩阵。

1.1.2 有意义可视密码方法

针对传统 VC 方法无法识别噪声分存带来的管理困难问题, 本文选择了分存有意义的 EVCS

作为基座加密模型。在尺寸上, 原始 EVCS 分存图像是加密图像的 1/4。可视密码黑白像素分发过程如图 3 所示, 首先将分存图像转换成半色调图像, 接着将每个像素点拓展成 4 个像素点。在有意义分存图像加密过程中, 分存图像中的白色像素点被拓展成两个白色像素点和两个黑色像素点所组成的像素块。分存图像中的黑色像素点被拓展成 1 个白色像素点和 3 个黑色像素点所组成的像素块。在无意义分存加密过程中, 每张加密图像中的 4 个像素点会被加密成 2 个白色像素点和 2 个黑色像素点所组成的像素块。

1.2 误差扩散半色调方法

使用 VC 技术需要将图像转为二值图像。以灰度图像为例, 半色调会将图像的像素值从 $0 \sim 255$ 转换为 $\{0, 255\}$, 即只用白色像素或黑色像素表示一种图像。目前最常用的半色调方法是误差扩散 (error diffusion, ED)。ED 方法会将当前像素的误差以特定的比例扩散到周围的像素, 以减少图像细节的丢失。

以灰度图像为例, 首先将图像的像素值标准化为 $[0, 1]$; 然后, 利用式(1)对当前位置的标准化像素值进行二值化, 并使用式(2)计算误差 e , 其中, h 和 p 分别表示二值化像素值和标准化灰度像素值; 最后, 通过式(3)将误差扩散到当前像素的邻域中。

$$h(x, y) = \begin{cases} 0, & p(x, y) < 0.5 \\ 1, & p(x, y) \geq 0.5 \end{cases} \quad (1)$$

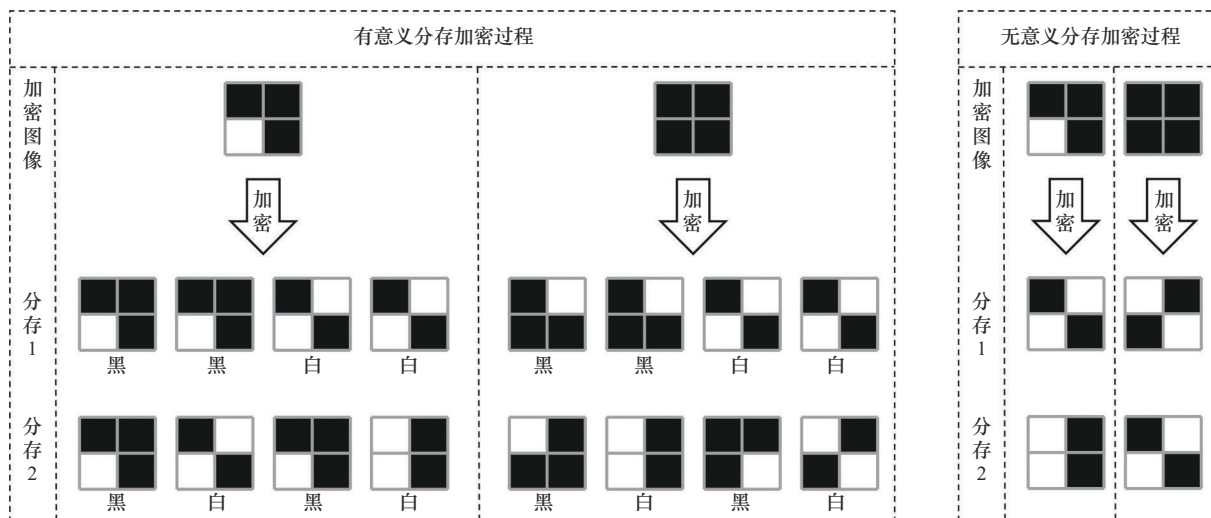


图3 可视密码黑白像素分发过程

Figure 3 Share image distribution process of VC

$$e(x,y) = h(x,y) - p(x,y) \quad (2)$$

$$\begin{cases} p(x+1,y) += \frac{7}{16} \times e(x,y) \\ p(x-1,y+1) += \frac{3}{16} \times e(x,y) \\ p(x,y+1) += \frac{5}{16} \times e(x,y) \\ p(x+1,y+1) += \frac{1}{16} \times e(x,y) \end{cases} \quad (3)$$

其中, $\frac{7}{16}$ 、 $\frac{3}{16}$ 、 $\frac{5}{16}$ 和 $\frac{1}{16}$ 为 Floyd-Steinberg 系数。对所有像素进行处理后得到一张二值化的半色调图像。

2 本文方法

本文提出的基于 VC 的生物特征图像安全传输与高精度识别架构在加密的预处理和解密的后处理过程中提高了图像质量, 并且加密和解密保留了经典流程, 从而可以重用现有的加密结构。

2.1 基于 EVCS 的无扩展图像加密方法

在 VC 的解密过程中, 分存图像叠加会导致黑色像素的不可撤销性, 进而使解密图像的亮度显著降低。针对这一特性, 可以在图像的预处理阶段利用 HSV (hue, saturation, value) 模式的亮度分离优势, 先调低图像的整体亮度。通过调整亮度分量, 可以更加精确地控制图像的明暗程度, 而不影响色调和饱和度。在经典的 RGB 模式中, 颜色由红、绿、蓝 3 个通道组成, 它们相互交织, 难以独立调整亮度。而 HSV 模式能够更直观地表达颜色的明暗程度, 使得亮度的调整变得更加简单和精确。

首先, 将原始图像从 RGB 颜色空间转换为 HSV 颜色空间, 并将亮度值从 0 ~ 255 重新映射到 0 ~ 64; 然后, 将图像转换回 RGB 模式, 并对其进行半色调处理。处理过程通过式(4)进行。

$$I' = I_{\text{ht}}(G_{\text{rc}}(I_{\text{rc}}(\text{RGB}, \text{HSV})/c)) \quad (4)$$

其中, I' 是预生成的图像, G_{rc} 和 I_{rc} 表示颜色和灰度重新映射函数, I_{ht} 表示误差扩散函数。为了满足加密约束, 需要将图像划分为 2×2 的子块, 并确保每个子块中黑色像素的数量为 3 或 4。重映射系数 $c = 4$, 表示将亮度重映射为原始图像的 1/4。通过提供比半色调模式更大的重映射空间, 灰度模式可以增强与秘密子块大小相同的加

密子块的感知。

图像在加解密过程中经常会出现背景噪声和图像失真等现象, 影响图像质量和识别系统的准确性。HSV 模式能够更好地分离颜色信息, 因此在处理背景噪声和图像失真时可以更加精确地定位并修复问题区域, 从而提高图像的整体质量。

2.2 基于滤波器的解密图像质量提升方法

在原始图像中, 白色像素和黑色像素之间的对比度为 1, 并且不存在噪声。对于使用 VC 解密后的图像, 叠加解密图像会造成黑色像素覆盖白色像素, 白色像素被解密为灰色块, 从而导致图像质量下降。使用高斯滤波器和双边滤波器可以有效减少背景噪声并增强前景主体的细节。

高斯滤波器可以减小背景噪声的影响, 从而增强图像的视觉效果。当对图像进行半色调处理时, ED 算法会将噪声引入高频区域。图像的边缘和细节可能会被误认为是半色调噪声而被滤除。低通滤波器不仅可以消除半色调噪声, 还可以使图像边缘变细。为了尽可能还原解密图像的清晰度, 采用式(5)中的双边滤波器消除噪声和失真, 同时保留图像中的边缘细节信息。

$$I'_p = \frac{1}{W_p} \sum_{q \in S} I_q \cdot f_r(\|I_p - I_q\|) \cdot G_s(\|p - q\|) \quad (5)$$

$$W_p = \sum_{q \in S} f_r(\|I_p - I_q\|) \cdot G_s(\|p - q\|) \quad (6)$$

其中, I'_p 表示在区域 p 中经过双边滤波器处理后的像素值; I_q 表示区域 q 处的原始图像像素值; S 表示区域 p 的邻域; f_r 是强度差的高斯函数, 用于衡量 I_p 和 I_q 之间的相似度; G_s 是空间距离的高斯函数, 用于衡量像素 p 和 q 的接近程度。双边滤波器通过 f_r 保留边缘细节信息, 并通过 G_s 控制平滑度和减少噪声, 同时保留图像的重要结构特征。通过式(6)计算出一个标准化因子 W_p , 用于确保滤波器的输出值和为 1。

解密后的图像缺少包含 2 ~ 4 个白色像素的子块, 这些子块无法通过叠加进行解密, 从而导致图像整体偏黑。通过直方图均衡可以确保即使是暗图像也能实现几乎均匀的亮度, 从而改善这种黑化效应并创造一致的亮度条件。由于直方图缺乏特定限制, 恢复后的图像亮度过高, 丢失了大量信息, 因此使用自适应直方图均衡来解决这

个问题。加密图像生成与解密图像增强方法过程如算法 1 所示。

算法 1 加密图像生成与解密图像增强

输入 输入图像 (img, cover1, cover2),

超参数(radius, sigma, cnts)

输出 增强后的解密图像 img_{enh}

1) $img \leftarrow (0, 255/4)$;

2) $img_{enc} \leftarrow \text{Rectify}(\text{Halftone}(img))$;

3) Resize cover1 and cover2 to 1/4 of img_{enc} and Halftone;

4) Divide (img_{enc} , cover1, cover2) into 2×2 blocks;

5) (share1, share2) $\leftarrow$ empty shares where size as img_{enc} ;

6) for block in img_{enc} do

7) | (share1, share2) $\leftarrow$ Encrypt (block);

8) end

9) $img_{dec} \leftarrow \text{share1} \& \text{share2}$;

10) $I \leftarrow \text{Gaussian blur}(img_{dec}, (\text{radius}, \text{radius}), 0)$;

11) for $i \leftarrow 1$ to cnts do

12) | $I \leftarrow \text{Bilateral filter}(I, \text{radius}, \text{sigma}, \text{sigma})$;

13) end

14) $enh \leftarrow \text{Equalize histogram}(I)$

2.3 基于神经网络的质量提升因子预测方法

深度学习的泛化能力使得有损加密图像识别成为可能。深度学习可以从变换或低质图像中提取有效特征^[24-25]。使用基于滤波器的解密图像质量提升方法,需要先找到 3 个超参数,然后设置滤波器。这 3 个超参数分别如下。

1) radius: 双边滤波器的半径,表示滤波器的大小。radius 值越大,滤波效果越强。

2) sigma: 双边滤波器的空间标准差,表示滤波器在空间域中的权重分布。sigma 值越大,滤波器对远离中心的像素的考虑越多。

3) cnts: 滤波器的迭代次数。迭代次数越多,滤波效果越强。

为了达到最优的恢复效果,需要通过迭代的方式花费大量的算力和时间计算最优的 3 个超参数,这在算力紧缺的边缘设备上难以实现的。

为了快速计算能够有效提升解密图像质量的超参数组合,引入了深度卷积神经网络(deep convolutional neural network, DCNN)进行超参数预测。

不同超参数组合下的 PSNR 值如图 4 所示。X 轴、Y 轴、Z 轴分别表示 3 个超参数(radius, sigma, cnts)的值。图中的颜色显示了各组合下逆半色调图像与原始图像的 PSNR 值的差异。图中的多个驻点表明,通过迭代搜索确定最优超参数组合既耗时又困难。因此,采用 DCNN 进行超参数预测是必要的。

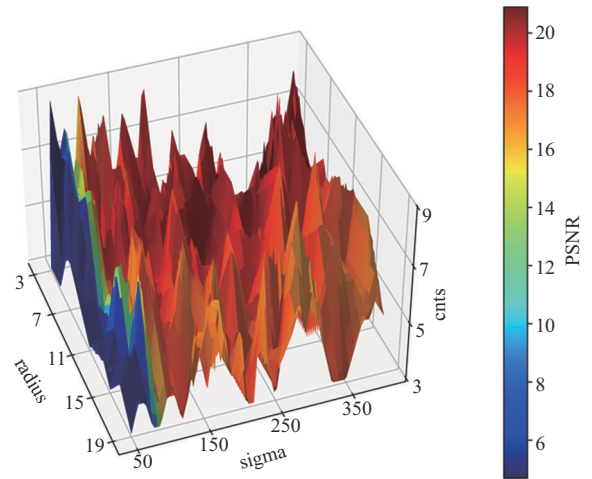


图 4 不同超参数组合下的 PSNR 值

Figure 4 PSNR values under different hyperparameters combination

DCNN 由主干网络和线性输出层组成。首先,主干网络从输入的有损解密图像中提取特征,这些特征用嵌入向量表示;然后,线性输出层将这些高维嵌入向量转换为三维向量,作为 DCNN 预测的超参数值;最后,使用式 (7) 中的 SmoothL1 损失函数计算预测值与真实值之间的误差。这种方法本质上是把超参数搜索问题转化为回归问题。

$$L_{\text{SmoothL1}} = \begin{cases} 0.5(x_n - y_n)^2/t, & |x_n - y_n| < t \\ |x_n - y_n| - 0.5t, & \text{其他} \end{cases} \quad (7)$$

其中, n 为每轮训练的批处理大小, x_n 与 y_n 分别表示预测值与真实值。

超参数预测 DCNN 训练过程如算法 2 所示。在 DCNN 结构设计上,采用了在 ImageNet 数据集上预训练的 MobileNetV2^[26]作为解密图像的特征提取主干网络,并将全连接层替换为一个 256

维的中间隐藏层和一个3维的输出层。MobileNetV2{Sandler, 2018 #35}是一种轻量级DCNN, 适用于算力有限的物联网场景。

算法2 超参数预测DCNN训练过程

输入 解密图像img
输出 预测的超参数 (radius, sigma, cnts)_{pred}

```

1) Backbone  $\leftarrow$  DCNN;
2) Linear layer  $\leftarrow$  (256,3);
3) Loss  $\leftarrow$  SmoothL1;
4) lossbest  $\leftarrow \infty$ , early stop  $\leftarrow$  0;
5) for epoch  $\leftarrow$  1 to  $N_{\max}$  do
6) | Train  $M$  on trainset;
7) | Evaluate  $M$  on validset;
8) | if lossval < lossbest then
9) | | lossbest  $\leftarrow$  lossval
10) | | early stop  $\leftarrow$  0;
11) | |  $M_{\text{best}} \leftarrow M$ ;
12) | else
13) | | early stop += 1;
14) | | if early stop  $\geq S_{\max}$  then
15) | | | break
16) | | end
17) | end
18)end
19)(radius, sigma, cnts)pred  $\leftarrow M_{\text{best}}$  (img)

```

3 实验

为了证明本文的加密方法适用于一般的生物特征识别场景。本文选取了以下5个常用的生物特征数据集进行实验^[27]。

1) Celebrity Face Image Dataset: 该数据集包含18位名人共1 800张人脸图像。

2) LFW: 人脸识别任务的常用数据集, 该数据集包含5 749位名人共13 233张人脸图像。

3) FVC2000: 生物指纹图像数据集, 包含10类共800张指纹图像。

4) CASIA-PalmprintV1: 生物掌纹图像数据集, 包含312位个体共5 502张掌纹图像。

5) CASIA-Iris-Syn: 生物虹膜图像数据集, 包含1 000类合成的虹膜图像, 本文选取其中1 000张虹膜图像。

3.1 实验设置

本文使用峰值信噪比 (peak signal-to-noise ratio, PSNR) 和结构相似度 (structural similarity, SSIM) 作为解密图像恢复质量与DCNN预测性能的评估指标。两幅图像越相似, PSNR值越大。SSIM的取值为[-1,1]。当两幅图像相同时, SSIM值为1。

实验时, 首先将Celebrity Face Image Dataset中的每张图像转换为解密图像, 并针对每张解密图像在特定范围内计算出3个超参数取值下的最优PSNR值; 然后, 随机选取1 260张图像作为训练集、360张图像作为验证集、180张图像作为测试集, 用于DCNN的训练。

模型的训练过程采用Adam优化器, 学习率为 1×10^{-3} , 权重衰减为 1×10^{-5} 。引入学习率调度器优化训练过程, 当验证损失在连续10个训练周期没有改善时, 将学习率降低到原来的 $\frac{1}{10}$ 。训练时, 批处理大小 n 取值为256, 式(7)中的 t 取值为1。为了防止模型过拟合, 在训练过程中采用早停机制。当验证损失在20个训练周期内没有改善时, 停止训练。模型训练的实现均使用Python和PyTorch框架。训练和测试的实验环境为Ubuntu, GPU配置为两块16 G NVIDIA Tesla T4。

3.2 图像质量提升效果分析

在模型测试阶段, 采用训练后的DCNN对测试集中的180张解密图像进行预测, 得到每张图像的3个超参数预测值。超参数预测DCNN的网络结构包含5个卷积层和1个线性层, 其具体组成及各层的输出尺寸和参数量如表1所示。

表1 超参数预测DCNN的结构与参数量
Table 1 Structure and parameters of DCNN

结构	输出尺寸	参数量
Conv1	[96, 112, 112]	7 104
Conv2	[144, 56, 56]	31 968
Conv3	[192, 28, 28]	59 488
Conv4	[576, 14, 14]	1 043 120
Conv5	[1280, 7, 7]	2 083 712
Linear	[3]	1 069 574

图5展示了在测试集中分别使用默认超参数、迭代搜索和DCNN预测的超参数得到的部分

恢复图像与原始图像的对比,并在表2中给出了不同超参数获取方法下恢复图像与原始图像的平均PSNR与SSIM。



图5 图像恢复效果比较

Figure 5 Comparison of images recovery effects

表2 超参数的恢复性能对比
Table 2 Comparison of hyperparameters recovery performance

超参数获取方法	平均PSNR	平均SSIM
默认设置	14.466	0.232
迭代搜索	16.307	0.406
DCNN 预测	16.366	0.399

结果显示,使用DCNN预测的超参数进行逆半色调的解密图像在PSNR指标上表现最优,但在SSIM指标上略微低于迭代搜索方法。造成这种现象的可能原因如下。

1) 在迭代搜索过程中,需要尝试大量的参数组合,为了减少时间复杂度,超参数的搜索并非连续的。相比之下,DCNN能够在更广泛的参数空间内进行搜索,因为DCNN可以预测连续的数值,因此可能找到更优的超参数组合。

2) DCNN在训练过程中更倾向于优化PSNR指标,因为SmoothL1损失函数的计算是基于PSNR获取的超参数。因此,DCNN在预测超参数时更加注重提高PSNR,而对SSIM指标的优化相对较少。

3.3 损失函数分析

为了进一步强化DCNN的超参数拟合能力,本文尝试将式(7)中的损失函数替换为均方误差(mean squared error, MSE)损失函数。MSE损失函数通过增加对误差的惩罚尝试来提高模型的预测性能。MSE损失通过 $L_n = (x_n - y_n)^2$ 计算。

表3给出了使用不同损失函数训练下DCNN的预测性能。结果显示,模型在使用MSE损失函数后并没有获得更优的预测性能。这表明MSE损失函数并不适用于本文的超参数预测任务。

表3 使用不同损失函数训练下DCNN的预测性能
Table 3 Predictive performance of DCNN is trained with different loss functions

损失函数	PSNR	SSIM	训练损失	验证损失
SmoothL1	16.366	0.399	7.935	18.995
MSE	15.480	0.319	248.981	2 345.723

观察训练损失和验证损失可以发现,使用MSE损失函数会导致DCNN模型的损失过大。造成这种现象的原因可能是超参数数据中存在许多异常值,MSE损失函数会放大部分异常值,导致模型的损失难以收敛。此外,由图4可知,超参数取值存在多个局部最优解,相比SmoothL1损失函数,MSE损失函数更容易陷入局部最优解中。

3.4 图文混排加密实验

由于VC加密可以对黑色像素完美解密,在某些场景中,如电子签名、机密文档等白底黑字的图像文本,使用VC可以做到完美加解密。

图6展示了一个PDF文档经本文的视觉加解密方法和图像质量提升方法处理后的解密图像和恢复图像,可见,本文提出的EVCS方法和图像质量提升方法可以有效复原图像中的文字信息,这表明本文提出的视觉加密方法既能加解密生物图像特征,又能加解密文本信息。



图6 可逆性实验结果展示

Figure 6 Experimental results presentation of reversibility

3.5 加密生物特征识别性能分析

3.5.1 人脸数据集识别性能比较

云边端的图像识别系统可以利用神经网络在

生物特征图像上进行泛化。尽管解密后的生物图像相比原始图像是有损失的,但是恢复图像保留了原始图像的关键特征。因此,这些恢复图像仍然可以进行分类。

为了高精度地识别有损解密数据,本文实验设计了一种擅长比较数据相似性的孪生网络。孪生网络也是一种DCNN,专门用于对输入的恢复图像进行编码,并将编码结果与目标图像进行比较。该网络由两个结构相同的子网络组成,通过共享参数可以方便图像的编码和比较。每个子网络对输入图像独立地提取特征和编码,生成两个特征嵌入向量,并计算这些向量在特征空间中的欧几里得距离。如果计算出的欧几里得距离小于设定的阈值,就可以判定这两幅图像属于同一类别;否则这两幅图像属于不同类别。

对于正样本对,孪生网络的优化目标是通过式(8)中的对比损失函数最小化输出特征嵌入向量在特征空间中的欧几里得距离。相反,对于负样本对,孪生网络的优化目标是最大化输出特征嵌入向量在特征空间中的欧几里得距离。

$$L(Y, X_i, X_j) = \frac{1}{2} \times (1 - Y) \times (D_\theta)^2 + \frac{1}{2} \times Y \times \{\max(0, m - D_\theta)\}^2 \quad (8)$$

其中, Y 表示 X_i, X_j 是否为正样本对, $Y = 1$ 表示为正样本对, 否则为负样本对; D_θ 为 X_i, X_j 在特征空间中的欧几里得距离; m 为边界约束超参数, 表示要求孪生网络将负样本对至少拉开一定的距离, 本文 $m = 5.0$ 。

在有损人脸图像识别实验中, 首先在 LFW 数据集上针对不同的主干网络分别开展了识别训

练实验。其中, 识别性能评估指标选用准确率、精度、召回率和 $F1$ 。指标值越接近 1, 表示性能越好。不同主干网络识别解密图像的性能评估如表 4 所示, 最终选取 EfficientNetV2_M^[28]。

黑白图像的识别相比彩色图像的识别更具挑战性^[29], 因此对解密图像的识别性能均有所下降。表 5 给出了模型在不同 VC 加密方法下的识别性能。

表 5 模型在不同 VC 加密方法下的识别性能
Table 5 The recognition performance of the model under different VC encryption methods

VCS	准确率	精度	召回率	$F1$
VCS-1	0.918	0.941	0.889	0.907
VCS-2	0.930	0.959	0.896	0.919
Prob-VCS	0.942	0.966	0.917	0.935
RG-VCS	0.936	0.949	0.914	0.925
本文方法	0.952	0.970	0.936	0.948

VCS-1 和 VCS-2 分别有 4 倍和 2 倍的尺寸扩展, Prob-VCS^[30]使用了 8 份分存, 理论上生物特征信息的损失更少, 识别性能更高。然而, 本文方法各项指标的表现均为最优。

3.5.2 图像质量比较

为了评估本文方法的加解密图像质量, 选取了 3 种方法进行实验对比。这 3 种方法分别为传统基于拓展 (pixel_extend) 的可视密码方法、基于多像素加密大小不变 (ME-SIVCS) 的可视密码方法^[31]和基于 LAB 颜色空间亮度调节 (Adjust_brightness_LAB) 的可视密码方法。与其他 3 种方法相比, 本文方法可以在保证像素不扩展

表 4 不同主干网络识别解密图像的性能评估

Table 4 Performance evaluation of different backbone networks for recognition and decryption of images

主干网络	原始图像				半色调				RG-VCS				本文方法			
	准确率	精度	召回率	$F1$	准确率	精度	召回率	$F1$	准确率	精度	召回率	$F1$	准确率	精度	召回率	$F1$
MobileNetV2	0.94	0.94	0.94	0.93	0.92	0.91	0.93	0.92	0.84	0.86	0.81	0.84	0.89	0.90	0.89	0.89
VGG19	0.93	0.92	0.95	0.93	0.91	0.93	0.89	0.91	0.85	0.88	0.81	0.83	0.87	0.89	0.85	0.87
ResNet18	0.94	0.94	0.94	0.94	0.91	0.91	0.90	0.91	0.83	0.86	0.77	0.81	0.90	0.91	0.88	0.89
ResNet50	0.97	0.97	0.97	0.97	0.96	0.97	0.95	0.96	0.92	0.92	0.94	0.93	0.92	0.91	0.92	0.91
Inception_v3	0.96	0.96	0.63	0.96	0.96	0.97	0.95	0.96	0.92	0.92	0.92	0.92	0.95	0.95	0.95	0.95
EffinetNet_b3	0.98	0.91	0.89	0.89	0.97	0.94	0.91	0.92	0.95	0.90	0.85	0.86	0.86	0.87	0.82	0.84
EfficientNetV2_M	0.98	0.98	0.96	0.97	0.97	0.99	0.96	0.97	0.94	0.95	0.91	0.92	0.97	0.98	0.96	0.97

的情况下同时保证图像质量。本文方法在 HSV 颜色空间上, 将亮度调整到了原来的 1/4。

图 7 使用了计算机视觉领域中的标准测试图像 (如图 1 所示), 横坐标表示 7 张测试图像, 纵坐标表示对应的图像质量指标数值。在图 7 中, 本文方法图像质量的表现和其他方法相似, 没有显著的质量损失。ME-SIVCS 由于采用无意义加密方法, 在亮度上占有优势, 如果想应用于有意义分存加密场景, 就必须降低亮度。与传统基于拓展的可视密码方法相比, 本文方法在保证图像质量的同时, 解决了像素拓展的问题。LAB 颜色空间虽然精确, 但亮度调整可能会导致颜色通道的非预期变化。HSV 颜色空间的亮度分量与颜色分量相对独立, 可以在不显著改变色彩的情况下调整亮度。

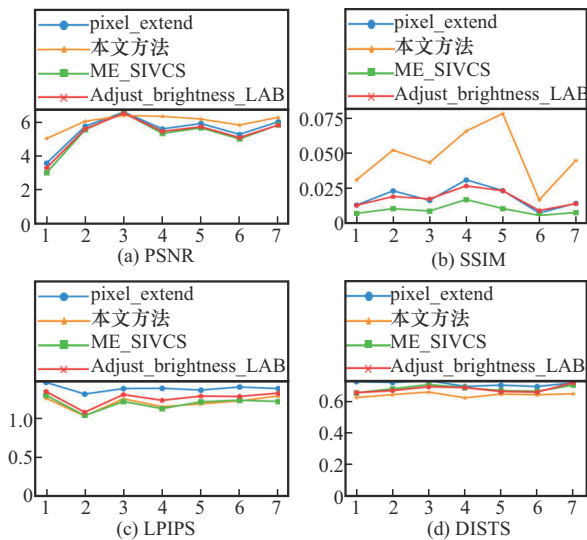


图 7 不同方法的图像质量评估指标

Figure 7 Image quality evaluation indexes of different methods

表 6 对比了不同 VCS 的特性, 整体来看, 本文方法相比其他方法各方面的表现均比较出色。在尺寸方面, pixel_extend 往往需要进行像素扩展, 这不仅会增加存储和传输负担, 还会增加处理复杂度。而本文方法无须进行像素扩展, 能够保持图像的原始尺寸, 从而更加高效和实用。在图像质量提升方面, 本文方法的表现同样优异, 能够保证图像的清晰度和细节。特别是解密后的图像质量, 本文方法确保了图像的可辨识性和视觉效果, 而其他方法的图像质量可能有所下降。在易加解密方面, 本文方法通过使用 OR 运算进行加解密操作, 相比之

下, XOR-VCS 等方法可能需要更复杂的运算和算法支持, 这在实际应用中可能会增加计算和时间成本。在有意义分存方面, 本文方法生成的每个分存不是无意义的噪声图像, 而是具有实际意义的图像信息, 从而增强了加密图像的隐秘性和安全性, 使其在信息安全领域具有显著的应用价值。而 XOR-VCS 和 PCVCS-BW 的分存往往是随机噪声, 无法直接识别和利用。

表 6 不同 VCS 的特性对比

Table 6 Comparison of features of different VCS

VCS	尺寸 不变	质量 提升	易加 解密	有意义 分存
pixel_extend	×	×	√	√
ME_SIVCS	√	√	√	×
本文方法	√	√	√	√
Adjust_brightness_LAB	√	√	√	√
XOR-VCS ^[32]	√	√	×	×
HP-VCS	√	√	√	×
CO-VCS	√	√	√	×
BP-VCS ^[33]	√	√	√	×
PCVCS-BW	√	√	√	×

为了进一步展示本文视觉加密方法的泛用性以及图像质量提升方法的优越性能, 本文在 FVC2000 指纹数据集、CASIA-PalmprintV1 掌纹数据集和 CASIA-Iris-Syn 虹膜数据集上进行了更充分的实验。

结构感知深度神经网络 (structure aware DCNN, SAD) 是目前性能最好的逆半色调方法^[34], 其在原始 DCNN 逆半色调基础上引入了结构感知子网络预测图像的细节结构信息。

首先, 分别使用 SAD 和本文 DCNN (图 8 中的 Ours) 对解密指纹图像进行质量提升。指纹图像质量评估指标如图 8 所示。其中, 横坐标表示 10 类不同的指纹图像, 纵坐标表示每类指纹的平均图像质量指标, 实线表示 SAD 的改进质量, 虚线表示本文逆半色调图像的改进质量。LPIPS、DISTs 和 FID 值越小, 表示图像质量越好。ClipIQA 是无参考的图像质量评估指标^[35]。左侧刻度用于表示 SSIM、LPIPS、DISTs 和 FID 的值, 右侧刻度用于表示 PSNR 和 ClipIQA 的值。

在上述 3 个数据集上, 本文图像质量提升方法的各项指标均优于 SAD。表 7 为基于 CASIA-

PalmprintV1 掌纹数据集和 CASIA-Iris-Syn 虹膜数据集的图像质量评估结果。图9展示了指纹图像恢复效果也优于 SAD。这证明, 尽管超参数的选取是基于 PSNR 指标的, 但最终解密图像的恢复质量在各项指标上都取得了最优值。由此可以推断, SAD 虽然具有强大的拟合能力, 但是无法将有损解密图像直接映射回原始图像。

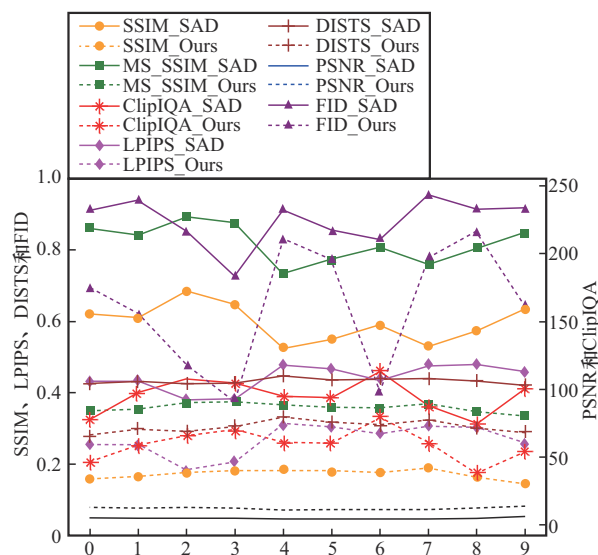


图8 指纹图像质量评估指标

Figure 8 IQA result of fingerprint images

3.5.3 轻量级分析和安全性分析

为了评估 LightLSB 的轻量级, 本文对 7 张测试图像分别使用不同的加密算法 (包括非对称加密算法 RSA、对称加密算法 3DES 和 AES) 进行处理。图像的加解密处理时间与加密前后的空间占用情况如表 8 所示。从实验结果来看, 本文方

表7 掌纹数据集与虹膜数据集图像质量评估结果

Table 7 Quality evaluation results of palmprint dataset and iris dataset

数据集	逆半色调	PSNR	SSIM	LPIPS	DISTS
CASIA-PalmprintV1	SAD	10.04	0.456	0.456	0.360
	本文 DCNN	16.41	0.479	0.436	0.324
CASIA-Iris-Syn	SAD	10.48	0.376	0.555	0.375
	本文 DCNN	12.97	0.456	0.505	0.349



图9 指纹图像加解密效果

Figure 9 Effects of fingerprint images on encryption and decryption

法解密处理所需时间最少, 因为可以通过简单的叠加进行解密, 不需要进行复杂的数学运算。而且, 解密图像是基于半色调二值图像的, 在保留图像原始特征的前提下, 大小相对于原始彩色和灰度图像大幅减小。因此, 本文方法结合目前常用的 AES 加密算法, 能够在减少存储成本的同时在物联网中安全、高效地处理并分发大规模生物特征图像。

本文方法在构建加密分存图像时通过 SS 算

表8 图像加解密处理时间与加密前后空间占用情况

Table 8 The relationship between image encryption/decryption processing time and the spatial occupancy prior to encryption

测试图像	RSA 处理时间/ms		3DES 处理时间/ms		AES 处理时间/ms		本文方法处理时间/ms		加密前后空间占用/KB	
	加密	解密	加密	解密	加密	解密	加密	解密	加密前 (原始)	加密后
Airplane	645.11	1 576.13	2.02	1.91	0.18	0.20	1.48	0.02	40.34	7.26
Baboon	1 020.05	1 577.07	2.01	1.82	0.21	0.19	2.99	0.03	52.62	6.27
Barbara	746.45	1 568.05	2.01	1.83	0.18	0.20	1.43	0.02	43.71	5.94
Boats	1 199.09	1 555.26	2.05	1.82	0.18	0.19	1.46	0.02	40.42	5.98
Butterfly	777.38	1 544.85	2.00	1.82	0.20	0.20	1.46	0.03	43.73	6.19
House	1 760.49	1 581.50	2.01	1.86	0.19	0.19	1.47	0.02	34.55	6.31
Peppers	746.43	1 615.39	2.05	1.86	0.19	0.20	1.63	0.02	39.48	6.20

法确保图像的安全性, 因为从单个分存图像中获取秘密是不可能的, 少于阈值的分存图像不会泄露原始图像的任何秘密信息。攻击者在没有足够分存图像的情况下, 难以恢复原始图像信息。如果攻击者尝试攻击某张分存图像, 错误的分存叠加将导致得到错误的解密图像, 防御系统据此可以检测到攻击者的存在。同时, 本文在加密前进行预处理操作, 预处理过程不涉及加密细节, 仅与当前图像有关, 因此预处理过程不会泄露任何

秘密图像的信息。在随后的加密过程中, 本文复用了现有的 EVCS, 因此整个加密过程是安全的。如果某张分存图像在不安全的信道传输时被窃取, 有意义分存的特性也提供了一定的隐蔽性。分存图像在视觉上是有意义的, 它们可以不包含敏感信息, 从而减少攻击者的注意。攻击者即使意识到这些分存图像是加密图像, 也无法通过单一分存图像推断出原始图像的信息。

图 10 展示了原始图像和加密图像的像素点统

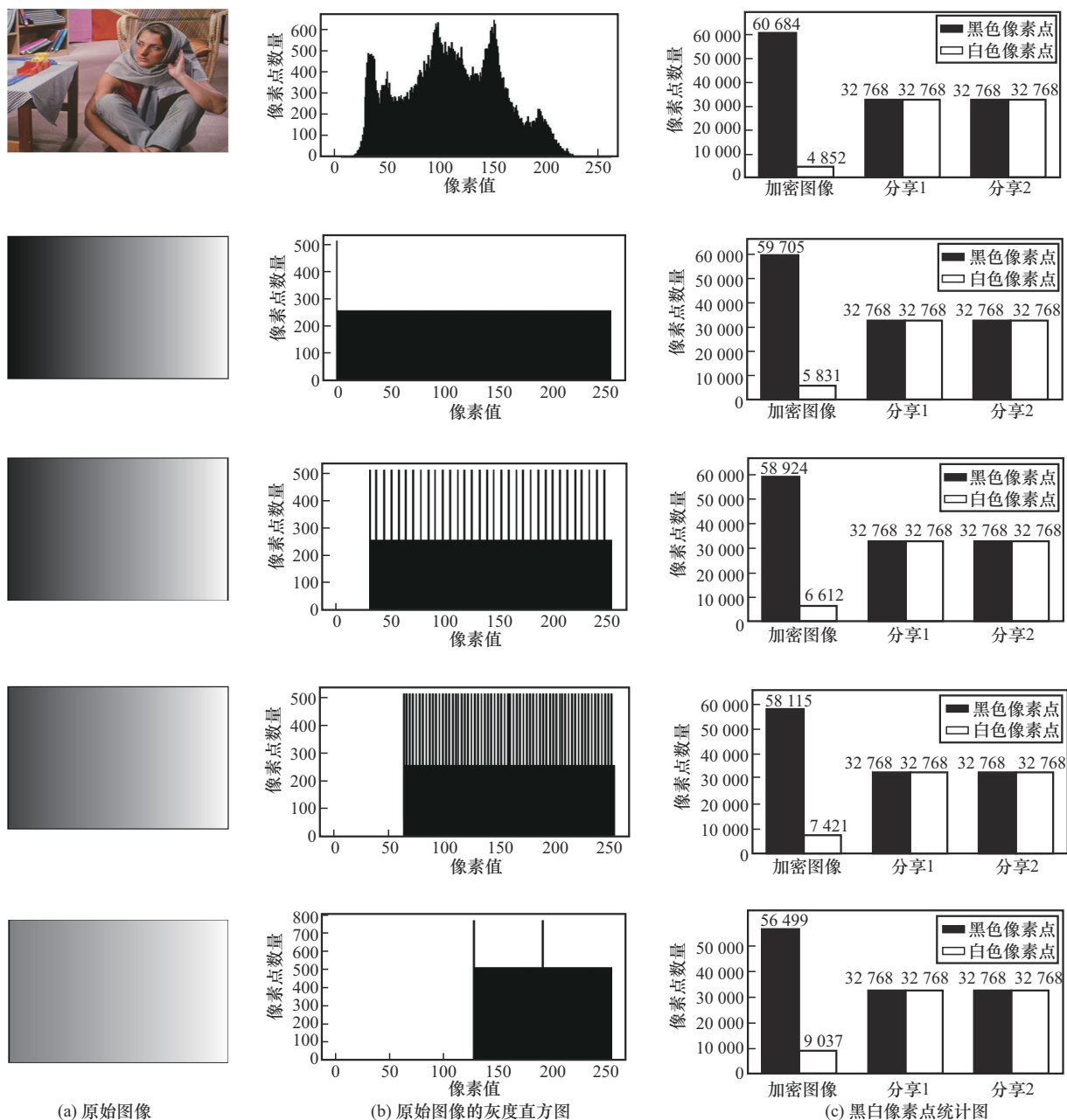


图 10 像素点统计特性

Figure 10 Pixel statistical characteristics

计特性。其中第1列是原始图像,第2列是原始图像的灰度直方图,第3列是加密图像和分存图像的黑白像素点统计图。从图中可以看出,在不同灰度图像中,即使加密图像的像素点不断变化,分存图像的黑白像素点比例始终为1:1。因此,攻击者无法基于模式识别或统计分析的方式进行攻击,从而无法推断出原始图像的任何信息。

图11为LightLSB在物联网中的应用示例。物联网中摄像头拍摄的人脸生物图像在经过轻量级的加密处理后所得到的分存图像,将被分发到不同的边缘节点。每个边缘节点的设备只存储一张分存图像,因此,即使某个边缘节点被攻破,或者其分存图像在传输过程中被攻击者窃取,攻击者没有得到全部分存图像,也就无法获取原始图像的信息。可信用户在获取所有分存图像后,通过叠加这些图像获得解密图像,然后通过超参数预测DCNN提升解密图像的质量,最后使用恢复图像进行身份认证操作。

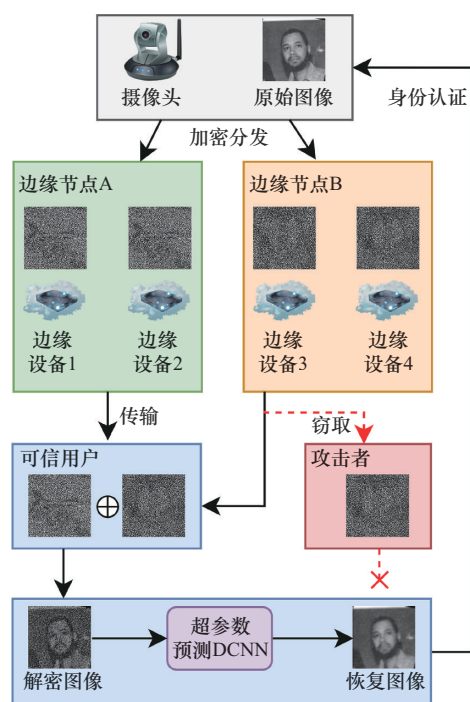


图11 LightLSB在物联网中的应用示例

Figure 11 Example of LightLSB application in the IoT

3.5.4 消融实验

为了验证图像质量提升方法对识别性能的影响,本文基于LFW数据集中有损人脸生物特征图像开展了消融实验。图像质量提升对识别性能

的影响如表9所示,可以看出,经过本文图像质量提升方法处理的图像识别性能接近于原始图像的识别性能。

表9 图像质量提升对识别性能的影响

Table 9 The effect of image quality improvement on recognition performance

方法	准确率	精度	召回率	F1
本文 VCS	0.952	0.970	0.936	0.948
本文 VCS+SAD	0.962	0.975	0.947	0.958
本文 VCS+BF	0.969	0.981	0.957	0.966

4 结束语

当前数据安全与合规、经济发展和技术进步之间的博弈和冲突日趋凸显。与文本信息不同,生物特征图像具有数据量大、冗余度高的特点,因此有必要从图像而不是文本的角度来研究生物特征的加密算法。针对传统生物特征加密算法在算力和密钥管理方面的局限性,本文基于可视密码的秘密共享特性提出了一种轻量级生物特征图像安全传输方法,去除了图像加解密过程中的复杂计算与密钥依赖,实现了生物特征图像的高效、安全传输。评估实验结果表明,本文方法在实现高效、安全传输大规模生物特征图像的同时,能够确保有损加密数据的识别精度和生物特征识别系统的可用性。在未来的研究工作中,将探索基于VC的对抗防御方法,利用加密噪声的随机性去除对抗样本中刻意添加的扰动,实现具有隐私保护特性的对抗攻击防御方法。

参考文献:

- [1] 张宁,臧亚丽,田捷.生物特征与密码技术的融合——一种新的安全身份认证方案[J].密码学报,2015,2(2):159-176.
ZHANG N, ZANG Y L, TIAN J. The integration of biometrics and cryptography: a new solution for secure identity authentication[J]. Journal of Cryptologic Research, 2015, 2(2): 159-176.
- [2] 李高磊,李建华,周志洪,等.面向新型关键基础设施的密码应用安全性评估技术综述[J].网络与信息安全学报,2023,9(6):1-19.
LI G L, LI J H, ZHOU Z H, et al. Review of cryptographic application security evaluation techniques for new critical infrastructures[J]. Chinese Journal of Network and Information Security, 2023, 9(6): 1-19.
- [3] NAOR M, SHAMIR A. Visual cryptography [C]//Proceedings of the Theory and Application of Cryptographic Techniques(Advances in

- Cryptology EUROCRYPT '94). 1994:1-12.
- [4] 孙哲南, 赫然, 王亮, 等. 生物特征识别学科发展报告 [J]. 中国图象图形学报, 2021, 26(6): 1254-1329.
SUN Z N, HE R, WANG L, et al. Overview of biometrics re-search[J]. Journal of Image and Graphics, 2021, 26(6): 1254-1329.
 - [5] 顾天晟, 曾福康, 邵思思, 等. 基于拟态防御和 Paillier 加密的智能物联网终端安全防护方法 [J]. 网络与信息安全学报, 2024, 10(6): 164-176.
GU T S, ZENG F K, SHAO S S, et al. Security protection method based on mimic defense and paillier encryption for smart IoT terminals[J]. Chinese Journal of Network and Information Security, 2024, 10(6): 164-176.
 - [6] KUMAR N M. Cancelable biometrics: a comprehensive survey [J]. Artificial Intelligence Review, 2020, 53(5): 3403-3446.
 - [7] 孔小景, 李学俊, 金哲, 等. 一种单因子的可撤销生物特征认证方法[J]. 自动化学报, 2021, 47(5): 1159-1170.
KONG X J, LI X J, JIN Z, et al. One-factor cancellable biometrics verification scheme[J]. Acta Automatica Sinica, 2021, 47(5): 1159-1170.
 - [8] ELREFAEI L A, AL-MOHAMMADI A M. Machine vision gait-based biometric cryptosystem using a fuzzy commitment scheme[J]. Journal of King Saud University-Computer and Information Sciences, 2022, 34(2): 204-217.
 - [9] RATHGEB C, MERKLE J, SCHOLZ J, et al. Deep face fuzzy vault: implementation and performance [J]. Computers & Security, 2022, 113: 102539.
 - [10] SHAHREZA H O, RATHGEB C, OSORIO-ROIG D, et al. Hybrid protection of biometric templates by combining homomorphic encryption and cancelable biometrics[C]//Proceedings of the 2022 IEEE International Joint Conference on Biometrics (IJCB). Piscataway:IEEE Press, 2022: 1-10.
 - [11] ZHANG D, REN L, SHAFIQ M, et al. A lightweight privacy-preserving system for the security of remote sensing images on IoT [J]. Remote Sensing, 2022, 14(24): 6371.
 - [12] WU X, FANG J, YAN W Q. Contrast optimization for size invariant visual cryptography scheme[C]//Proceedings of IEEE Transactions on Image Processing. Piscataway: IEEE Press, 2023: 2174-2189.
 - [13] XIONG L, ZHONG X, XIONG N N, et al. QR-3S: a high payload QR code secret sharing system for industrial internet of things in 6G networks [J]. IEEE Transactions on Industrial Informatics, 2020, 17(10): 7213-7222.
 - [14] HOLLA M R, PAIS A R. High-performance medical image secret sharing using super-resolution for CAD systems [J]. Applied Intelligence, 2022, 52(14): 16852-16868.
 - [15] WEN W Y, FAN J C, ZHANG Y S, et al. APCAS: autonomous privacy control and authentication sharing in social networks [J]. IEEE Transactions on Computational Social Systems, 2023, 10(6): 3169-3180.
 - [16] YU C, ZHANG X, QIN C, et al. Reversible data hiding in encrypted images with secret sharing and hybrid coding [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2023, 33(11): 6443-6458.
 - [17] 刘雁孝, 吴萍, 孙钦东. 基于区域卷积神经网络的图像秘密共享方案 [J]. 计算机研究与发展, 2021, 58(5): 1065-1074.
LIU Y X, WU P, SUN Q D. Secret image sharing schemes based on region convolution neural network[J]. Journal of Computer Research and Development, 2021, 58(5): 1065-1074.
 - [18] GAYATHRI M, MALATHY C. Novel framework for multimodal biometric image authentication using visual share neural network [J]. Pattern Recognition Letters, 2021, 152: 1-9.
 - [19] MUHAMMED A, PAIS A R. A secure fingerprint template generation mechanism using visual secret sharing with inverse halftoning[J]. Journal of Visual Communication and Image Representation, 2023, 94: 103854.
 - [20] IBRAHIM D R, TEH J S, ABDULLAH R. An overview of visual cryptography techniques[J]. Multimedia Tools and Applications, 2021, 80(21): 31927-31952.
 - [21] ZHANG D, ZHU H, LIU S, et al. HP-VCS: a high-quality and printer-friendly visual cryptography scheme[J]. Journal of Visual Communication and Image Representation, 2021, 78: 103186.
 - [22] LIU L, LU Y, YAN X. A novel (k_1, k_2, n) -threshold two-in-one secret image sharing scheme for multiple secrets[J]. Journal of Visual Communication and Image Representation, 2021, 74: 102971.
 - [23] LEE K H, CHIU P L. An extended visual cryptography algorithm for general access structures[J]. IEEE transactions on information forensics and security, 2011, 7(1): 219-229.
 - [24] ZHOU S, CHAN K, LI C, et al. Towards robust blind face restoration with codebook lookup transformer [J]. Advances in Neural Information Processing Systems, 2022, 35: 30599-30611.
 - [25] SHIM G, PARK J, KWEON I S. Robust reference-based super-resolution with similarity-aware deformable convolution [C]//Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. Piscataway:IEEE Press, 2020: 8422-8431.
 - [26] SANDLER M, HOWARD A, ZHU M, et al. MobileNetV2: inverted residuals and linear bottlenecks[C]//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. Piscataway:IEEE Press, 2018: 4510-4520.
 - [27] MINAEI S, ABDOLRASHIDI A, SU H, et al. Biometrics recognition using deep learning: a survey [J]. Artificial Intelligence Review, 2023, 56(8): 8647-8695.
 - [28] TAN M, LE Q. EfficientNetV2: smaller models and faster training[C]//Proceedings of the 38th International Conference on Machine Learning. 2021: 10096-10106.
 - [29] MA F, JING X Y, ZHU X, et al. True-color and grayscale video person re-identification[J]. IEEE Transactions on Information Forensics and Security, 2019, 15: 115-129.
 - [30] WU X, YANG C N. Probabilistic color visual cryptography schemes for black and white secret images[J]. Journal of Visual Communication and Image Representation, 2020, 70: 102793.
 - [31] LIU F, WU C, QIAN L. Improving the visual quality of size invariant visual cryptography scheme[J]. Journal of Visual Communication and Image Representation, 2012, 23(2): 331-342.
 - [32] CHEN Y-H, SU-TZU J J. XOR-based (n, n) visual cryptography schemes for grayscale or color images with meaningful shares[J]. Applied Sciences, 2022, 12(19): 10096.
 - [33] HOU Y-C, QUAN Z-Y, TSAI C-F, et al. Block-based progressive visual secret sharing [J]. Information Sciences, 2013, 233: 290-304.

- [34] SON C-H. Inverse halftoning through structure-aware deep convolutional neural networks[J]. Signal Processing, 2020, 173: 107591.
- [35] KASTRYULIN S, ZAKIROV J, PROKOPENKO D, et al. PyTorch image quality: metrics for image quality assessment[J]. arXiv preprint arXiv:220814818, 2022.

[作者简介]



张登辉 (1988-), 男, 河南信阳人, 广州大学副教授, 主要研究方向为图像安全和人工智能模型评测。



沈圣尚 (2000-), 男, 广东信宜人, 广州大学硕士生, 主要研究方向为图像安全和有损图像修复。



姚捷凤 (2000-), 男, 广东广州人, 广州大学硕士生, 主要研究方向为视觉秘密共享和图像安全。



李默涵 (1987-), 女, 甘肃兰州人, 广州大学教授, 主要研究方向为人工智能安全和网络入侵检测。



李爱平 (1974-), 男, 山东诸城人, 国防科技大学研究员, 主要研究方向为大数据分析、数据挖掘和网络信息安全。