文章编号:1671-4229(2021)04-0056-07

智慧家居中轻量灵活的图像隐私遮蔽模型

刘锦强[1], 唐春明[2], 刘忆宁[1*]
(1. 桂林电子科技大学 计算机与信息安全学院, 广西 桂林 541004;
2. 广州大学 数学与信息科学学院, 广东 广州 510006)

摘 要: 基于5G的智能家居系统中,智能摄像头拍摄的视频在上传到云端的过程中存在隐私泄露的问题。通常,智能摄像头是一种计算资源受限的设备,因此,在保证视频流低延时传输以及图像一定可用性的条件下对图像隐私信息进行保护具有一定的挑战性。传统的图像隐私保护方法通常是设计复杂的图像加密算法对整张图进行加密,然而图像中的隐私通常只是图像中的部分内容,如果对全图进行加密,不仅缺乏灵活性,还造成了资源浪费。文章首先采用YOLO v5算法获取用户定义的敏感区域,然后基于DNA加密技术以及整数向量同态加密技术提出了一种遮蔽算法对敏感区域进行遮蔽。该遮蔽算法提供了基于用户需求的动态遮蔽策略,算法轻巧灵活且可以满足用户可定制化隐私保护需求。实验表明,该模型可以应用于智能家居环境中。

关键词: 智能摄像头; 图像隐私; 云平台; 遮蔽操作; 膜
中图分类号: TP 309.2 **文献标志码**: A

Lightweight and flexible image privacy masking scheme in smart home

LIU Jin-qiang[1], *TANG Chun-ming*[2], *LIU Yi-ning*[1*]
(1. School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin 541004, China;
2. School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China)

Abstract: In 5G-based smart home systems, videos taken by smart cameras are usually uploaded to the cloud, which may lead to leakage of user privacy. Generally, a smart camera is a device with limited computing resources. Therefore, it is challenging to protect image privacy information while ensuring low-latency transmission of video and certain availability of images. The traditional image privacy protection methods mainly employ design complex image encryption algorithms to encrypt the entire image. However, the privacy area in the image is usually only part of the image. If the entire image is encrypted, it is inflexible. At the same time, it will waste resources. At first, this paper used the YOLO v5 algorithm to pick up the sensitive areas based on a user-definition, and then a masking algorithm is proposed to mask the sensitive areas based on DNA encryption technology and a VHE algorithm. The masking algorithm provides a dynamic masking strategy based on user needs. The algorithm is lightweight and flexible, and it can meet the needs of users for customizable privacy protection. Experiments prove that the scheme can be applied to the smart home environment.

Key words: smart camera; image privacy; cloud; masking; membrane

基金项目: 国家自然科学基金资助项目(62072133);广西自然科学基金重点资助项目(2018GXNSFDA281040)
作者简介: 刘锦强(1995—),男,硕士研究生. E-mail:jqliu000@gmail.com
* 通信作者. E-mail:ynliu@guet.edu.cn
引文格式: 刘锦强, 唐春明, 刘忆宁. 智慧家居中轻量灵活的图像隐私遮蔽模型[J]. 广州大学学报(自然科学版),2021,20(4):56-62.

随着 5G 物联网设备的发展,智能家居系统得到了广泛的应用[1-2]。在智能家居系统中,用户可以通过物联网设备对房屋环境进行监控及控制,例如,通过智能空调控制温度,通过智能窗帘控制室内光线,使用物联网摄像头监控房屋等[3-4]。然而,物联网设备收集的数据包含大量用户的隐私信息,尤其是物联网监控摄像头收集的图像数据包含大量的用户日常生活信息,这些信息发生泄漏的后果将会十分严重,因此,必须对图像中的隐私信息进行保护[5]。

传统的图像隐私保护方法主要通过采用加密算法打乱相邻像素间的相关性,使图像中的信息无法被识别。传统的数据加密算法包括 AES 和 DES,这 2 种算法主要用于数据加密并且具有较高的安全性[6]。由于智能摄像头拍摄了大量包含用户日常生活的图像信息,若直接使用 AES 和 DES,则需要大量的计算资源,其加密效率十分低下[7-8]。

混沌系统最早由 Lorenz 提出[9],此后构建的混沌映射系统得到了重要应用[10-11]。近年来,混沌映射算法因其具有伪随机性、遍历性和初值敏感性等特点,在图像加密算法中得到了广泛应用。混沌映射算法主要分为一维、两维及多维混沌映射算法[12]。Ahmad 等[13]提出一种基于混沌映射和正交矩阵的图像加密方案。Muhammad 等[14]提出一种应用于物联网环境中的工业监控隐私保护方案,该方案使用基于二维正弦的混沌系统,对监控视频中的关键帧进行加密。虽然这些混沌映射算法的安全性很高,但由于大多数算法仍比较复杂,并不适用于物联网摄像机。此外,大部分混沌映射算法对整幅图像进行加密,尽管提高了图像的安全级别,但是缺乏灵活性,并且浪费了计算资源。

与混沌映射算法的高安全性相比,近年来,基于置换的图像加密算法引起了研究人员的广泛关注。基于置换的图像加密算法通常分为 3 类:像素替换算法、位置替换算法和块替换算法[15]。像素替换算法和位置替换算法相较于块替换法需要更多的加密时间。块替换算法需要处理的图像块越小,加密效果越好。这些基于置换的图像加密算法虽然加密时间较快,但是安全性较差,并且这些算法大多对整张图像进行加密,缺乏灵活性。

考虑到图像加密算法的安全性和灵活性,Lv 等[16]提出一种基于动态膜的加密模型。在该模型中,云平台首先生成一个矩阵作为遮蔽膜,然后由物联网摄像头使用遮蔽膜遮蔽图像中的敏感区域。尽管 Lv 等的方案灵活性以及效率较高,但是由于云平台可以获得全部的遮蔽膜及敏感区域信息,因此,存在云平台与恶意用户合谋的可能,这将是不安全的。

尽管研究人员提出了众多的图像加密算法,但这些算法并不能直接应用于智能家居环境。原因如下:①家用摄像头拍摄的视频每秒 25 到 30 帧,由于智能摄像头的计算资源受限,且持续获取图像,因此,对每一帧进行加密是不合理的;②家庭监控摄像头拍摄的内容是日常生活,图像中的场景单一,并非整个图像都包含敏感信息,加密整个图像会浪费计算资源;③不同用户对隐私的定义不同,传统加密算法无法提供自适应加密策略。

在此背景下,本文提出一种应用于智能家居环境中的轻量、灵活的智能家居图像隐私保护方案,该方案充分考虑了监控摄像头的计算能力和用户的隐私要求。具体来说,在用户选择隐私标签后,智能摄像头会根据用户的隐私要求自动检测和拾取敏感区域,然后使用轻量级遮蔽算法对图像中的敏感区域进行遮蔽。为了减少计算资源的损耗,保证加密算法的灵活性,只有当某帧中出现用户自定义的敏感区域时,才会进行遮蔽,其他帧不进行任何操作。此外,本方案充分考虑了物联网监控摄像头的计算能力,提出的遮蔽算法是轻量级的,去除掩码后的加密图像与原始图像一致。

本文的贡献如下:

(1)提出了一种用于智能家居的轻量级图像隐私保护方法,该方案可以自动识别视频流中的敏感帧并保护敏感帧的隐私;

(2)提出的方法充分考虑了用户的隐私需求,可以根据不同用户的隐私需求动态保护特定区域的隐私;

(3)进行了充足实验,实验表明,所提出的方法适用于智能家居环境。

1 预备知识

1.1 Logistic 映射算法

Logistic 映射算法[17]是混沌系统中常用的一种算法,广泛应用于图像加密中。算法原理如下:

$$x_{n+1}=\mu x_n(1-x_n),$$

其中,$0<\mu<4$,当 $\mu\in(3.75,4]$时,图像为混沌图,$n=0,1,2,3\cdots$然而,用于实数域值的 Logistic 映射具有一定的局限性。

在实际的计算机应用中,由于需要计算浮点数,该算法可能会使计算资源的消耗增加 1 倍。为了解决浮点计算引起的计算量增加的问题,Miyazaki 等[18]提出了一种适用于整数的逻辑映射算法,具体如下:

$$f_{lnt}^{(n)}(X)=\lceil \mu X(2^n-X)/2^n \rfloor_{251},$$

其中,$X\in[0,2^n]$,$n=0,1,2,3\cdots\lfloor . \rfloor$为向下取整。

Muhammad 等[19]定义了有限域上的逻辑映射,具体如下:

$$X_{i+1}=f_{Z_N}(X_i)=\mu_N X_i(X_i+1)(\mathrm{mod}\,N),$$

其中,控制参数 $\mu_N\in[1,N-1]$,$X_i\in[0,N-1]$,$i=1,2,3,\cdots$

1.2 整数向量同态加密算法(Integer Vector Homomorphic Encryption algorithm, VHE)

整数向量加密算法[20]是一种高效的加密算法,该算法被广泛地应用于云计算环境中。本文中,VHE 算法将被用于遮蔽膜的生成,VHE 算法的细节如下:

(1)密钥生成阶段

实体 A 生成一个大小为 $m\times n$ 的矩阵 $\boldsymbol{S}$,然后发送矩阵 $\boldsymbol{S}$ 给实体 B,其中,$\boldsymbol{S}$ 中的元素均为整数。

(2)加密阶段

步骤 1:实体 A 产生一个大整数 w,其中,$w<<|\boldsymbol{S}|$,$|\boldsymbol{S}|:=\max_i\{|S|_{ij}\}$,然后向实体 B 发送 w。

步骤 2:实体 A 利用向量 $\beta=(b_1,b_2,\cdots,b_m)^{\mathrm{T}}$ 计算 $w\beta$,其中,β 代表明文,$b_1,b_2,\cdots,b_m$ 为整数。

步骤 3:实体 A 计算向量 $\alpha=(a_1,a_2,\cdots,a_n)^{\mathrm{T}}$,该向量满足 $\boldsymbol{S}\alpha=w\beta+e$,其中,$a_1,a_2,\cdots,a_n$ 均为整数,e 是一个作为噪声向量的误差项,其元素值小于 $\frac{w}{2}$,然后将 α 发送给实体 B。

(3)解密阶段

实体 B 计算$\lceil\frac{\boldsymbol{S}\alpha}{w}\rfloor$从而恢复明文信息,其中,$\lceil\frac{\boldsymbol{S}\alpha}{w}\rfloor$是$\frac{\boldsymbol{S}\alpha}{w}$邻近的整数。

1.3 DNA 加密算法

脱氧核糖核酸含有蛋白质和 RNA 生物合成所必需的遗传信息,是一种重要的生物大分子。DNA 包含 4 个碱基,即腺嘌呤(A)、鸟嘌呤(G)、胞嘧啶(C)和胸腺嘧啶(T)。DNA 中的 4 个碱基有特定的分配规则,其中,A 与 T 配对,C 与 G 配对。该配对原则对应于计算机中 0 和 1 的互补原则。因此,研究人员根据 DNA 的配对原理设计了 DNA 加密算法[21]。DNA 加密算法的编码原理如表 1 所示。

表 1 DNA 加密算法编码原理

Table 1 Coding principle of DNA encryption algorithm

碱基	A	T	C	G
A	A	T	C	G
T	T	A	G	C
C	C	G	A	T
G	G	C	T	A

DNA 的编码规则采用八进制,每 2 位对应 1 个碱基。由于不知道对应的规则,所以对应的规则有 8 个,如表 2 所示。

表 2 DNA 加密算法可能的编码规则

Table 2 Coding rules of DNA encryption algorithm

规则	A	T	C	G
Rule 1	00	11	10	01
Rule 2	00	11	01	10
Rule 3	11	00	10	01
Rule 4	11	00	01	10
Rule 5	10	01	00	11
Rule 6	01	10	00	11
Rule 7	10	01	11	00
Rule 8	01	10	11	00

2 采用的方法

为保护智慧家居环境中图像的隐私,本文提出了一种具有灵活性特点的轻量级图像隐私保护模型,如图 1 所示。该模型由图像采集与预处理部分和遮蔽算法 2 个部分组成。在遮蔽算法部分,本研究提出了一种图像中敏感区域的遮蔽算法。

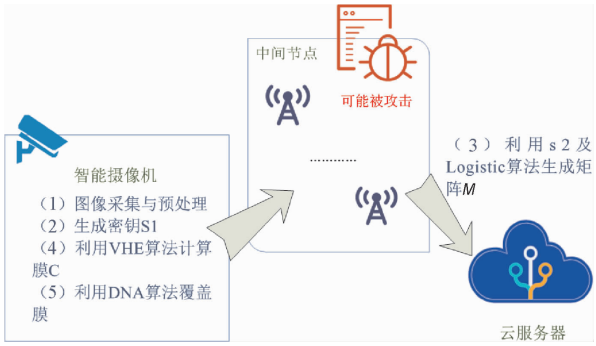

图 1　系统模型图

Fig. 1　Scheme proposed

2.1　图像采集与预处理

在智能家居环境中,不同用户对于图像中隐私区域的定义是不同的,例如为了获得来访者来访预警服务,但不泄露来访者的人脸信息,用户可以设置人脸信息作为隐私区域,也可以将眼部设置为隐私区域。这些区域将会作为隐私标签用于后续敏感区域的隐私遮蔽。

物联网摄像头采集图像并上传到云服务器前,首先向用户提供一些设定好的隐私标签以提供个性化的隐私服务,如来访者的全部人脸、眼部信息或者是来访人员的车牌等,然后利用已部署好的 YOLO v5 算法[22]来获取图像的敏感信息区域,并输出符合用户隐私要求的隐私目标信息。选择使用 YOLO v5 算法的原因是它比其他目标检测算法具有更快的检测速度及更高的准确率,适合应用于智能家居环境中。

2.2　遮蔽算法

2.2.1　加密

步骤 1:智慧摄像头识别敏感区域位置 $SA_r \times SA_c$,然后生成一个序列 $\boldsymbol{S}1$,$S1_i \in \{2^0, 2^1, \cdots 2^8\}$,其中,$i \in (0, 1, \cdots, SA_r \times SA_c)$;

步骤 2:云服务器根据获取的敏感区域信息以及密钥 $\boldsymbol{S}2$ 利用逻辑映射算法生成 $M_i \in \{2^0, 2^1, \cdots 2^8\}$,其中,$i \in (0, 1, \cdots, SA_r \times SA_c)$,然后云服务器向智能摄像头发送 $\boldsymbol{M}$;

步骤 3:智能摄像头执行 VHE 算法计算矩阵 $\boldsymbol{C}$ 的具体细节如公式(1)所示,其中,e 是一个误差项;

$$\boldsymbol{C} = \boldsymbol{S}1^{-1}(\boldsymbol{W}\boldsymbol{M} + e) \tag{1}$$

步骤 4:智能摄像头定位图像中的敏感区域后,利用步骤 3 得到的矩阵 $\boldsymbol{C}$ 与图像中的敏感区域所对应的矩阵执行 DNA 加密算法,对图像中的敏感区域进行遮蔽;

步骤 5:智能摄像头向云服务器发送加密图。

2.2.2　解密

步骤 1:根据密钥 $\boldsymbol{S}1$ 以及 $\boldsymbol{S}2$ 计算矩阵 $\boldsymbol{C}$;

步骤 2:执行 DNA 解密算法。

3　实验与仿真

本节对采用的实验环境及实验结果进行了详细描述。采集和预处理部分在系统配置为 2.3 GHz 处理器和 Windows 10 的云实例上使用 Python 进行。其中,所选择的图像均为灰度图像,实验图像名称、原图大小以及敏感区域大小如表 3 所示。

表 3　实验图尺寸

Table 3　The size of experiment image

图像名称	加密图尺寸	敏感区域尺寸
Barbara	512 × 512	304 × 512
AL	512 × 512	242 × 324
Lena	512 × 512	110 × 36

本文以 3 幅图像为例来验证所提出的模型。如图 2 所示.

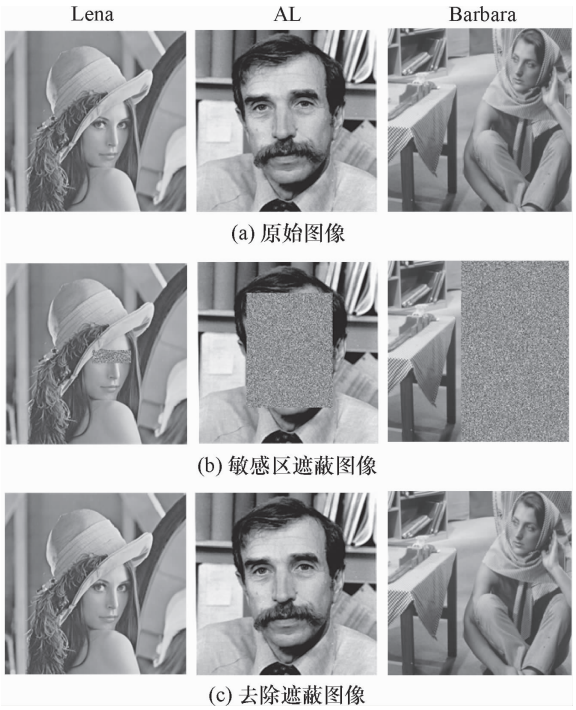

图 2　原始图像加密及解密效果图

Fig. 2　Encryption and decryption of original images

由图 2 可知,经过遮蔽操作后的图像无法识

别出用户所设定的隐私区域内容,图像中的其他区域未经任何处理,这表明该算法具有较好的灵活性,可以满足用户可定制化隐私的需求。

3.1 直方图分析

灰度直方图(图3)可以直观地评价图像的像素色调分布。在直方图中,x 轴和 y 轴表示对应强度级别的像素数。图3(a)、图(b)、图(c)分别是原始图像、原始敏感区域图像和加密敏感区域图像的直方图。

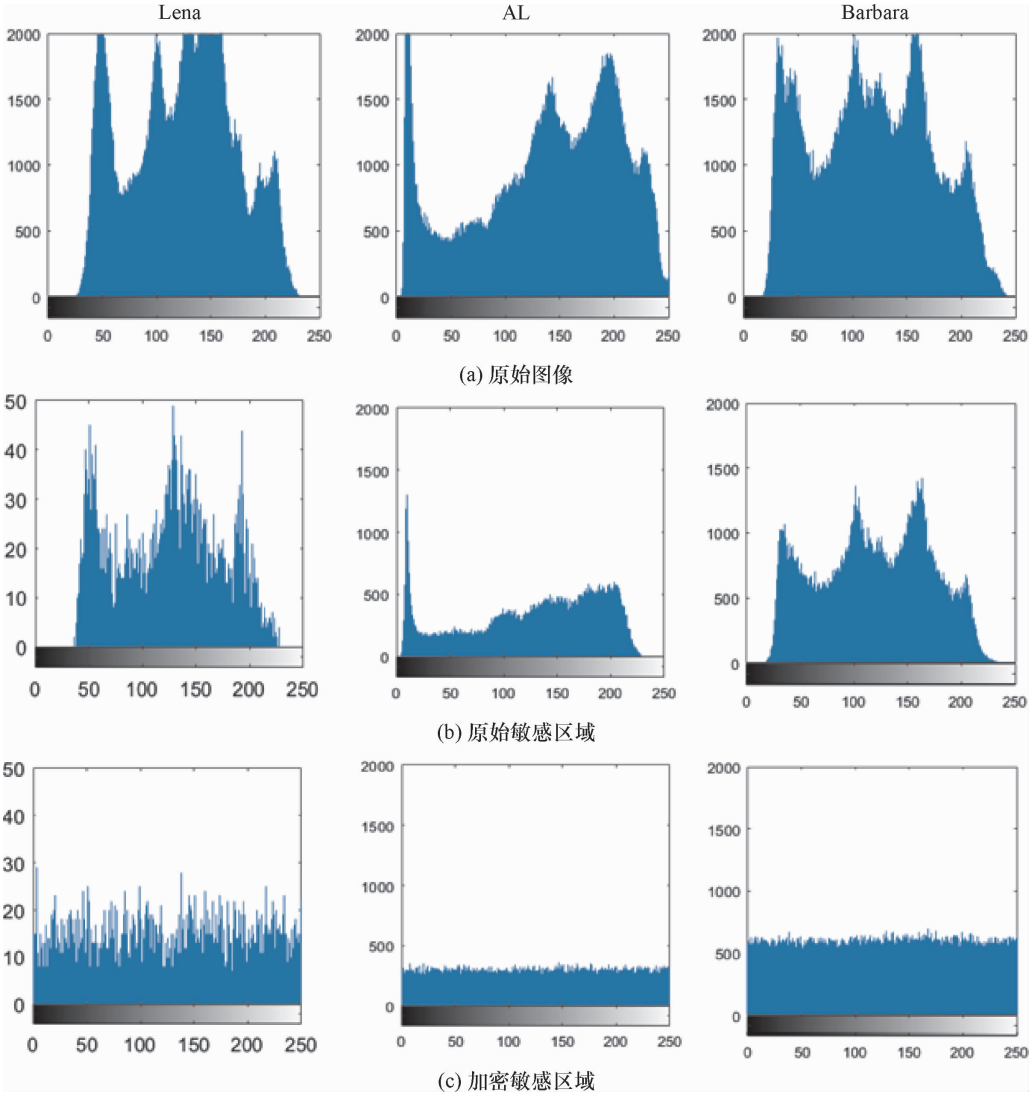

图3 灰度直方图

Fig. 3 Grayscale histogram of the original image

由图3可知,原始图像的灰度直方图是不均匀的,没有经过遮蔽处理的敏感区域的灰度直方图分布不均,被遮蔽后敏感区域的灰度直方图分布均匀,这就证明了被遮蔽的图像不会泄露隐私信息,遮蔽算法具有较好的安全性。

3.2 像素相关性分析

相邻像素的相关性(图4)反映了图像相邻位置像素值的相关程度,如公式(2)所示:

$$c = \frac{\sum_{i=1}^{N}\left(x_i - \frac{1}{N}\sum_{i=1}^{N}x_i\right)\left(y_i - \frac{1}{N}\sum_{i=1}^{N}y_i\right)}{\sqrt{\sum_{i=1}^{N}\left(x_i - \frac{1}{N}\sum_{i=1}^{N}x_i\right) \times \sum_{i=1}^{N}\left(y_i - \frac{1}{N}\sum_{i=1}^{N}y_i\right)}} \tag{2}$$

其中,x_i 和 y_i 是相邻像素值,N 是像素数。

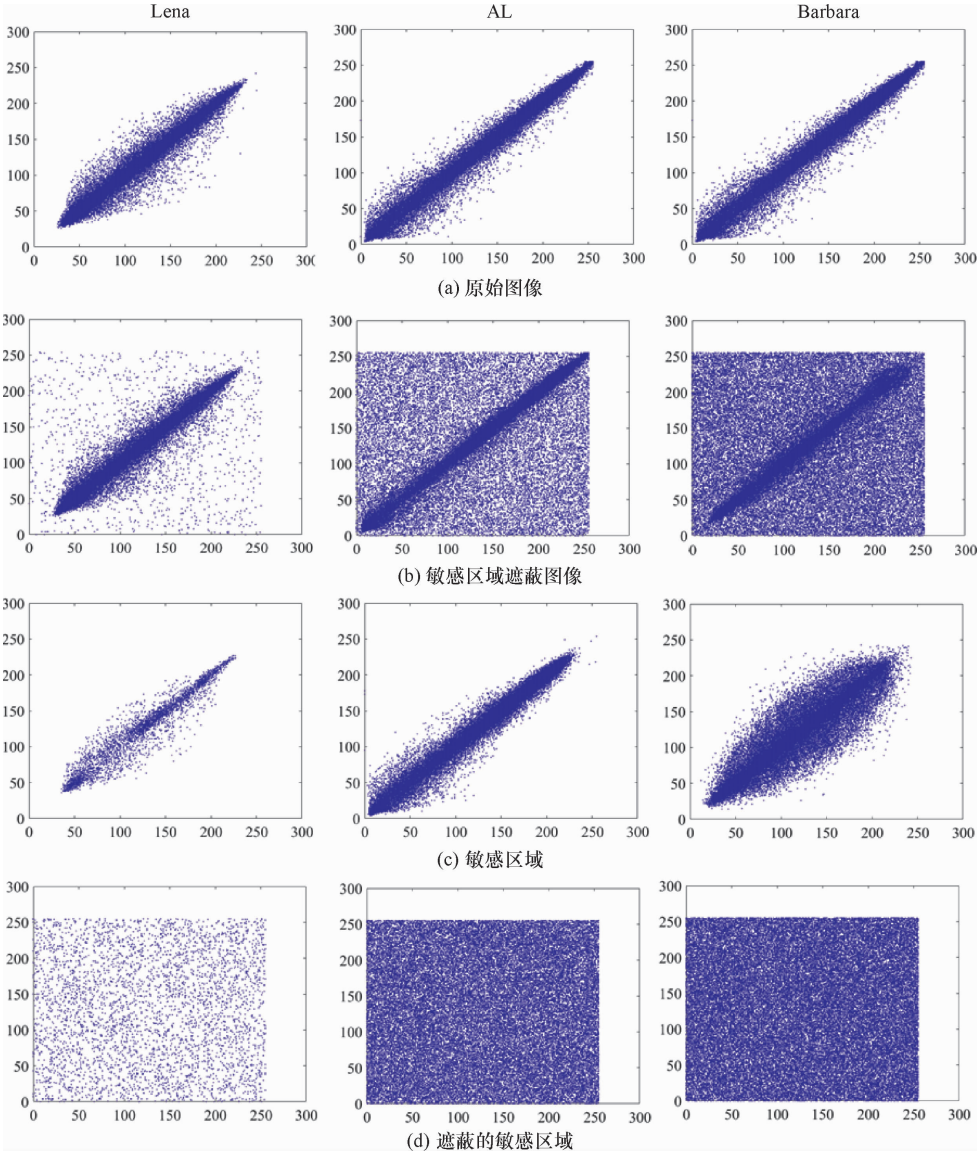

图 4　相邻像素值的相关分析

Fig. 4　Correlation analysis of adjacent pixel values

由图 4 可知,所选图像中的敏感区域被遮蔽后,相邻像素的相关性被完全破坏,这使得通过统计攻击的手段难以对加密图进行预测。说明使用本文提出的方案对图像的敏感区域进行遮蔽后,遮蔽图像的相邻像素分布高度分散,与原始图像的相关性非常低。

3.3　*MSE*, *RMSE* 和 *PSNR*

均方误差(*MSE*)定义了图像 I_1 和 I_2 之间对应像素差的平方,可以用来描述原始图像和恢复掩蔽图像之间的质量差异,可由公式(3)表示:

$$MSE = \frac{1}{H \times W}\sum_{i=1}^{W}\sum_{j=1}^{H}(X(i,j) - Y(i,j))^2 \quad (3)$$

均方根误差(*RMSE*)是 *MSE* 的平方根,可由公式(4)表示:

$$RMSE = \sqrt{MSE} \quad (4)$$

为了验证图像遮蔽操作的效率,使用峰值信噪比(*PSNR*)来验证遮蔽恢复图像的质量,如公式(5)所示:

$$PSNR = 10 \times \log_{10}\left(\frac{(2^n - 1)^2}{MSE}\right) \quad (5)$$

PSRN 的值越大,去除遮蔽后的图像质量越高。经过计算,上述 3 个例子中的 $PSNR = +\infty$。该结果证明,恢复遮蔽后的图像质量与原始图像质量相同,满足物联网相机中图像加密算法的图像质量要求。

3.4　*NPCR* 和 *UACI*

像素数变化率(*NPCR*)表示不同加密图像在

同一位置不同灰度值的比率,计算公式如式(6)所示。统一平均变化强度(*UACI*)表示不同加密图像之间的平均变化密度,计算公式如式(7)所示。使用这2个参数来验证本文提出的图像遮蔽操作对抗差分攻击的强度。表4给出了实验图的*PSNR*和*UACI*值。

$$NPCR(I_1,I_2) = \frac{1}{W \times H}\sum_{i=1}^{W}\sum_{j=1}^{H} D(i,j) \quad (6)$$

$$UACI = \frac{1}{W \times H}\sum_{i=1}^{W}\sum_{j=1}^{H} \frac{|I_1(i,j) - I_2(i,j)|}{255}$$

$$\text{where } D(i,j) = \begin{cases} 0, & \text{if } I_1(i,j) = I_2(i,j) \\ 1, & \text{if } I_1(i,j) \neq I_2(i,j) \end{cases} \quad (7)$$

表4 原图与去掉遮蔽后图像的*NPCR*与*UACI*值

Table 4 *NPCR* and *UACI* values between original image and masking recovery image

Image	*NPCR*	*UACI*
Barbara	0.996 1	0.334 6
AL	0.996 0	0.334 4
Lena	0.150 3	0.050 2

4 结 论

在智慧家居环境中,为了防止图像在上传至云服务器时泄露用户的隐私信息,本文提出了一种图像隐私保护模型。该模型分为图像采集及预处理部分以及遮蔽算法部分。在图像采集及预处理部分,用户可以根据自身的隐私需要设置图像中的隐私标签;在遮蔽算法部分,笔者在智能摄像头上部署了YOLO v5算法,通过用户预先设定的隐私标签,YOLO v5算法可以识别图像中的隐私区域,并将该区域的坐标信息反馈给云服务器,云服务器利用Logistic映射算法发送给智能摄像头,最终,智能摄像头通过VHE算法及DNA加密技术实现图像中隐私区域的遮蔽,从而保护了用户的隐私。该模型充分考虑了智慧家居环境中智能摄像头计算资源受限的特点,所采用的加密算法均为轻量级的加密算法,由于利用云进行辅助加密计算,减少了本地的资源消耗,并且云无法恢复原始的图片文件;该模型充分考虑了用户在不同场景下的隐私服务,并向用户提供了一种可定制化的图像隐私保护方案,在保护用户隐私的同时提高了数据的可用性;本文在实际的智慧家居环境中进行了充分的实验,实验表明,所提出的算法在安全性等多个方面可以满足实际中图像隐私保护的需求。

参考文献:

[1] Kumar P, Braeken A, Gurtov A, et al. Anonymous secure framework in connected smart home environments[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(4):968-979.

[2] Poh G S, Gope P, Ning J. PrivHome: Privacy-preserving authenticated communication in smart home environment[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(3): 1095-1107.

[3] 杨利平, 龚卫国, 李伟红, 等. 基于网络技术的远程智能家居系统[J]. 仪器仪表学报, 2004, 25: 308-311.

[4] Chang H H, Chiu W Y, Sun H, et al. User-centric multiobjective approach to privacy preservation and energy cost minimization in smart home[J]. IEEE Systems Journal, 2019, 13(1):1030-1041.

[5] Kaur A, Singh G. A random selective block encryption technique for secure image cryptography using blowfish algorithm [C]//2018 Second International Conference on Inventive Communication and Computational Technologies(ICICCT). Piscataway: IEEE, 2018:1290-1293.

[6] Mahajan P, Sachdeva A. A study of encryption algorithms AES, DES and RSA for security[J/OL]. Global Journal of Computer Science and Technology, 2013, 13(15):14-22[2021-09-12]. https://computerresearch.org/index.php/computer/article/view/272.

[7] Wang X, Ma J, Liu X, et al. Search in my way: Practical outsourced image retrieval framework supporting unshared key [C]//IEEE INFOCOM 2019-IEEE Conference on Computer. Piscataway: IEEE, 2019: 2485-2493.

[8] Lorenz E N. Deterministic nonperiodic flow[J]. Journal of Atmospheric Sciences, 1963, 20:130-141.

[9] Lu J H, Chen G R. A new chaotic attractor coined[J]. International Journal of Bifurcation & Chaos in Applied Sciences & Engineering, 2002, 12:659-661.

[10] Henon M. A two-dimensional mapping with a strange attractor[J]. Communications in Mathematical Physics, 1976, 50: 69-77.

(下转第93页)