文章编号:1671-4598(2023)06-0217-06 DOI:10.16526/j.cnki.11—4762/tp.2023.06.033 中图分类号:TP391.9 文献标识码:A

基于深度学习的人脸图像加密算法研究

鲁 瑞[1],张 南[2],辛君芳[2]
(1.澳大利亚国立大学 计算机与工程学院,堪培拉 2600;
2.北京工商大学 计算机学院,北京 100048)

摘要:图像作为视觉传达的重要信息载体,以一种直观、形象的方式向受众传递信息;但是,图像会在不知不觉中带来个人隐私信息泄露等安全隐患;文章从保护图像中隐私安全角度出发,深度融合人脸检测、人脸对齐方法以及混合混沌序列的图像加解密算法,提出了一种基于深度学习算法的人脸图像信息加密算法,即FIIE算法,用于保护图片中的面部核心部位隐私信息;FIIE算法的具体描述如下:首先,采用WLDER FACE数据集中的人脸图像对MTCNN模型展开训练,并利用训练好的模型根据人脸特征点获取图像中人脸所在的矩形框坐标;然后,通过上述人脸区域坐标生成掩膜,运用生成的掩膜使原图与Logistic混沌序列做位运算,最后,对图像中人脸特定区域的加密;通过实验表明,该算法可以准确识别图像中人脸信息特定区域,实现对图像中面部信息的有效加密,保障用户的隐私安全。

关键词:深度学习;MTCNN模型;混沌加密;人脸检测;图像加密

Research on Face Image Encryption Algorithm Based on Deep Learning

LU Rui[1], ZHANG Nan[2], XIN Junfang[2]
(1. ANU College of Engineering, Computing & Cybernetics, Canberra 2600, Australia;
2. Beijing Technology and Business University, Beijing 100048, China)

Abstract: As an important information carrier of visual communication, images convey information to the audience in an intuitive and visual way. However, images will perhaps bring personal privacy information leakage and other security risks. From the perspective of privacy protection in images, the face detection, face alignment and image encryption and decryption algorithms with chaotic sequences deeply integrated in this paper, a face image information encryption (FIIE) algorithm based on deep learning algorithm is proposed, protecting the privacy information of the core parts of face image. The specific description of FIIE algorithm is as follows: Firstly, the pace image in the WLDER FACE data set is used to train the multitask convolutional neural network (MTCNN) model, and the trained model is used to obtain the rectangular frame coordinates of the face image by the face features. Then, the mask is generated by the coordinates of the face region, and the generated mask is used to perform bit arithmetic between the original image and the Logistic chaotic sequence. Finally, the specific region of the face image is encrypted. Experiments show that this algorithm can accurately identify the specific areas of facial information in images, realizes the effective encryption of facial information in images, and ensures the privacy and security of users.

Keywords: deep learning; MTCNN model; chaotic encryption; face detection; image encryption

0 引言

随着大数据与人工智能时代的悄然到来,人们可以轻松地利用社交平台分享自己的生活。据中国互联网络信息中心发布的《中国互联网络发展状况统计报告》显示,截至2022年6月,我国网民规模为10.51亿,互联网普及率达74.4%。据文献资料统计,约95%左右的网民会将自己的上网时间分配给社交平台[1]。图片作为信息的重要载体,与通过文字表达信息相比更加直观、形象和生动,人们将图片上传到社交平台的现象非十分普遍。但是,这在给人们的生活增加趣味的同时,也带来了隐私信息泄露等安全风险。因此,对图像中关键信息,特别是人脸等隐私部位进行选择性加密非常必要。当前,人们一般通过手动加密或打马赛克的方式对网络上发布的图片区域进行加密,此方法不仅需要花费时间和精力,还很容易被破解。

随着隐私问题越来越被人们重视,图像加密问题受到学术界的广泛关注。通过研究发现,传统密码学对图像数据加密的加密方法在信息量大,像素之间相关性强的图像中效果不好。而基于混沌系统的加密算法具有初值敏感性、不可预测性等特点,使其可以更好地与密码学相适应,在此基础上,其易于实现,因此其被学者们应用于图像加密领域。混沌系统主要包括Logistic映射、Henon映射以及Chen混沌系统[2]。其中,Logistic混沌系统源于人口统计动力学系统,是加密系统中的常用系统。当Loginstic函数的初值与参数满足条件时,Logistic函数工作于无法预测且无

收稿日期:2023-02-15; **修回日期**:2023-02-19。
作者简介:鲁 瑞(1998-),男,山东淄博人,硕士生,主要从事计算机视觉、机器学习等方向的研究。
通讯作者:张 南(1979-),女,辽宁绥中人,博士,副教授,主要从事人工智能、图像处理等方向的研究。
引用格式:鲁 瑞,张 南,辛君芳.基于深度学习的人脸图像加密算法研究[J].计算机测量与控制,2023,31(6):217-222,230.

序的混沌状态，可以生成混沌矩阵对原图矩阵进行处理，达到加密目的。Logistic 系统比传统图像加密方法更安全，在图像加密领域具有很好的发展前景[3-5]。因此，本文采用 Logistic 混沌系统进行图像的加密。

值得注意的是，图像加密大多是对整幅图进行加密，但是在军事和医疗等方面的应用中，并不强制加密整个图像。比如，在包含罪犯的图片中只需要将图片中的人脸进行加密，因此针对图像的特定目标部分加密的研究十分重要，有学者指出可以先提取包含主要信息的目标区域，在此基础上对图像的目标区域进行加密工作，从而实现针对目标区域的图像加密[6]。对于图像解密部分，有文献表明，解密结果可以与原始图像有些许差别，因为人类本身对图像具有感知特性，只要图像内容不受影响，解密结果在一定的范围内出现小的失真现象是被允许的，为了实现针对人脸区域的图像选择性加密，需要对人脸进行准确地定位[7]。目前采用的人脸定位方法主要包括基于知识、基于特征与基于表象三类传统人脸定位技术和基于深度学习的人脸定位技术[8-10]。陈小梅[11]等人先对人脸图像进行识别，然后对其进行预处理去除噪音，最后通过灰度投影获得主要特征点为人脸进行定位。有文献指出采用和迭代过程识别图像中可能存在的人脸轮廓区域，之后利用 Snake 算法对可能存在的人脸区域进行精炼细化，以获得最终的目标结果[12]。

深度学习凭借其高准确率、高效率的特性被广泛应用于计算机视觉等各个领域。其中，级联卷积神经网络等网络结构在人脸检测问题上被深入研究与应用，并取得了不错的效果。文献［13］提出级联的 CNN 网络结构进行人脸识别，为了更精准地定位人脸区域此方法设计了一种边界校订网络，并可以进行多分辨率解析，因此成为当时识别效果和速度最好的算法。文献［14］依照实验级联 CNN 模型，提出了 MTCNN 模型，此模型级联的多任务框架，对人脸检测和关键点对其两个认为进行级联。并对三个卷积神经网络 P-Net、R-Net、O-Net 进行串行，从而可以精确的预测人脸的位置坐标和面部特征点坐标。目前，有不少学者提出了通过 haar 级联和神经网络混合的方法构造分类器对人脸区域进行识别[15]。也有一些学者提出不使用级联结构进行人脸检测的深度学习算法。其中，文献［16］采用单个基于深度学习的卷积神经网络模型对多方位的人脸进行检测，该方法使得输入图像的大小不受限制，跟类能力较强，而且不需要对面部姿势等内容进行注释。

通过对上述模型方法的研究，本文研究了一种通过深度学习算法自动检测人脸的关键区域，并对其进行定位和选择性加密的方法。此方法可以有效保护人们的肖像等隐私安全，使得人们可以更放心、安全、自由地享受互联网带来的便捷与快乐。

1 深度学习及图像加密方法介绍

1.1 MTCNN 算法

2016 年，中国科学院深圳研究院提出了用于人脸检测的多任务卷积神经网络（MTCNN，multi-task convolutional neural network）深度学习模型，它是一个多任务人脸检测算法[14]，可以同时进行人脸检测、人脸区域定位和人脸特征点标注三个任务。MTCNN 是一个进行多次单目标检测的多目标检测网络模型，它级联了 3 层卷积神经网络 P-Ne、R-Net、O-Net[17-18]，模型通过上述三层卷积神经网络对人脸图像逐步精化，以得到最终的人脸框坐标和关键的人脸特征点（眼睛、鼻子以及两个嘴角）的坐标。本文试图先得到人脸区域的坐标以方便下一步的加密过程实现，而不需要得到人脸的特征点的坐标。因此，本文的具体实现过程，主要针对网络的人脸检测和人脸定位两个任务进行训练和测试。

1.1.1 MTCNN 算法实现过程

将输入图片分割为不同尺寸的图像，将其构造为形如金字塔的结构，称为图像金字塔。将图像金字塔输入 P-Net 以获取含有人脸的候选框，通过 NMS 对候选框进行过滤，去除冗余的候选框得到最终的人脸候选框。然后将所有包含人脸的候选框输入到 R-Net 中，通过更为严格的脸部特征点标准，对候选框进行进一步细化，去掉错误判断，通过 Bounding-Box Regression 和 NMS 对结果进行优化，获得置信度高的人脸候选框。最后，上一步结果输入 O-Net 中，定位最终人脸候选框坐标以及确定 5 个特征点的位置坐标。MTCNN 算法的工作流图如图 1 所示。在本文中，由于没有运用 MTCNN 算法人脸对齐的任务，所以不会做地标标注。

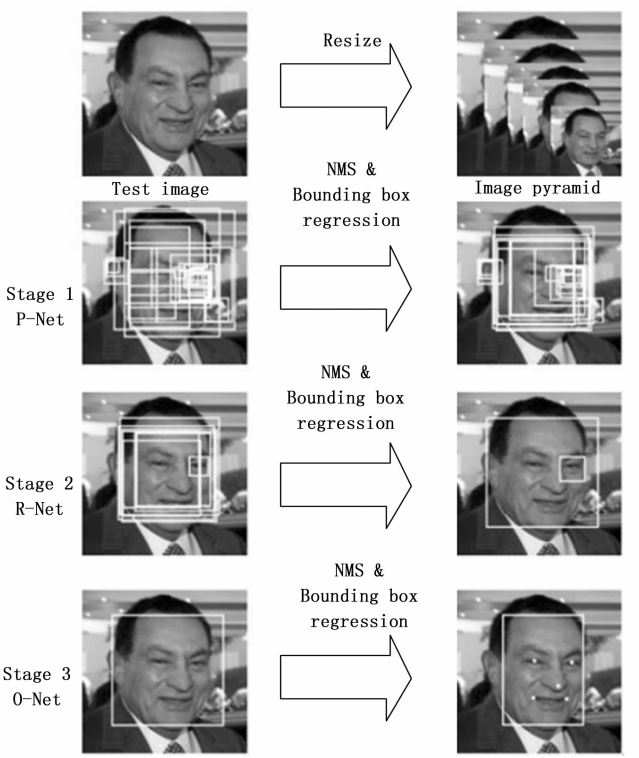

图 1 MTCNN 算法的工作流图[14]

1.1.2　MTCNN 算法的网络结构

P-Net 全称为 Proposal Network，是一个包含 3 个卷积层的卷积网络，他的主要作用就是判断图像中是否包含人脸，并输出人脸候选框和关键点的位置坐标。如图 2 所示，首先，P-Net 对输入图像进行卷积操作的卷积核是一个大小为 3 * 3，步长为 1 的卷积核，在此基础上，对其进行最大池化，其中进行范围为 2 * 2，步长为 2，从而可以得到一个大小为 5 * 5，通道数为 10 的特征图。之后，将上一步得到的特征图继续与一个大小为 3 * 3，步长为 1 的卷积核进行卷积，得到大小为 3 * 3，通道数为 16 的特征图，之后将其再进行上述卷积操作得到一个特征图。最后，将上一步得到的 1 * 1 * 32 的特征图继续进行卷积操作生成最终的特征图并将其用于人脸分类预测、人脸边界框预测与人脸地标预测。

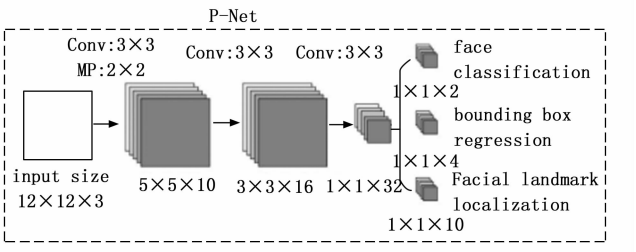

图 2　P-Net 的网络结构图[14]

R-Net 也就是 Refine Network，是一个卷积神经网络，其在 P-Net 的基础上增加了一个全连接层，对上个阶段的输出进行进一步细化。如图 3 所示，它与 P-Net 相比参数不同，而且 R-Net 增加了全连接操作。全连接层允许更精细的处理，消除大量错误的候选区域。R-Net 有规定的输入大小限制，为 24 * 24，它可以在图像经过 P-Net 产生候选框后对其进行筛选、排除，得到更加精确的人脸区域。

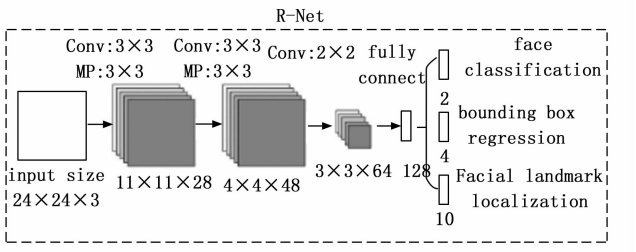

图 3　R-Net 的网络结构图[14]

O-Net 全称 Output Network，如图 4 所示，它也是一个卷积神经网络而且比 R-Net 更复杂，它又比 R-Net 多一个卷积层。O-Net 的输入大小为 48 * 48，它可以对经过 R-Net 人脸区域进一步过滤，得到最终的输出结果。

通过对上述三个卷积网络的了解可以看到 MTCNN 级联的三个网络的结构都比较简单，训练起来比较容易，通过对这三个网络逐步精化，了以得到较为准确的检测结果。因此，MTCNN 在检测速度和检测率上表现都比较好。

MTCNN 算法模型包括交并比和非极大值抑制两种工具，用其判断候选区域和加块区域识别速度。交并比实际表示两个识别框之间交集和并集的比值，它用于表示两个识别框之间的相似程度。除此之外，在生成训练数据时，交并比可以判断样本属于正样本、负样本还是部分样本，或者在非极大值抑制过滤候选框时，判断去除与其余候选框相似度高的候选区域。非极大值抑制用于抑制不是极大值的元素，并搜索此区域内的极大值。非极大值抑制以得到的候选框的置信度（为人脸区域的概率）为标准进行排序。检测每个网络时，可以通过非极大值抑制去掉置信度较低且与其他候选框区域交并比较大的候选框区域。通过非极大值抑制对候选框进行筛选，可以将效果较好的人脸候选区域进行筛选，从而减少下一个网络中输入的候选框数目，以此来提高 人脸区域的检测速度。

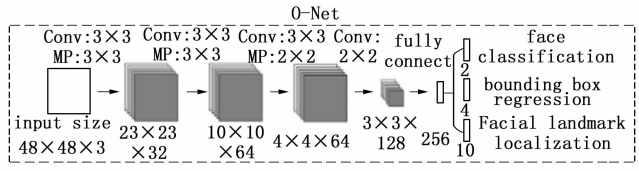

图 4　O-Net 的网络结构图[14]

1.2　Logistic 图像混沌置乱加密算法

混沌是指确定性动力学系统表现出的看似随机、却无法预测的运动[19]。混沌系统凭借其初值敏感性、随机性等良好的混沌特性，可以很好地提高图像加密的效果。Logistic 系统是一种经典的混沌系统，在图像加密领域得到广泛应用。Logistic 映射的系统方程如式（5）所示：

$$X_{n+1} = UX_n(1-X_n) \quad n = 0,1,2,3 \qquad (1)$$

式中，X_n 为迭代结果，X_0 为初值，$X_n \in (0, 1)$；U 为参数，$U \in (0, 4]$。当 $X_0 \in (0, 1)$，当 $U \in (3.569, 4]$ 时，Logistic 映射工作处于混沌状态。如图 5 所示，当参数满足设定的条件时，对初值进行迭代获得的序列是没有周期性的，即使参数发生微小改变，迭代的结果也会发生巨大变化。

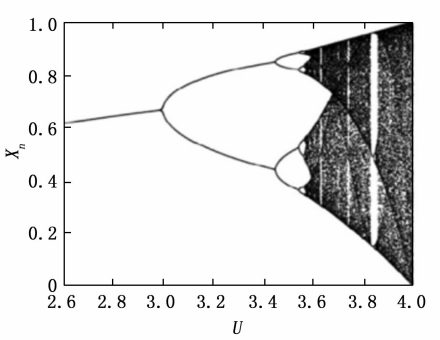

图 5　Logistic 映射迭代图[20]

将参数 U 设定在指定区间，使 Logisic 函数工作于混沌状态，对其进行若干次迭代，便可获得一组混沌序列。在计算机中图像通过矩阵形式进行存储与处理，因此可以将图像的矩阵表达形式与生成的混沌序列进行运算对图像进

行加密，由于图像像素值处于 0～255 之间而生成混沌序列值位于 0～1 之间，因此对混沌序列按照 0～255 的范围进行归一化处理从而得到新的混沌序列。在此之后，将新序列转化为二维矩阵，与原图进行异或操作，得到加密后的图像，以上便是图像的 Logistic 混沌置乱加密流程，设定的参数 U 和初值 X_0 即为秘钥。

2 FIIE 算法

本文提出了 FIIE 算法模型对人脸图像进行识别和加密，该模型首先对输入数据进行分类，识别出目标图片是否包含人脸以及识别出的区域是否是人脸区域，然后对人脸所在区域进行预测，识别出人脸预测框并计算其与真实数据之间的偏移量，以确定人脸边界框的最终范围，最后，通过 Logistic 加密算法对上述结果进行加密，完成目标图片的最终加密结果。FIIE（face image information encryption）算法实现过程如图 6 所示。

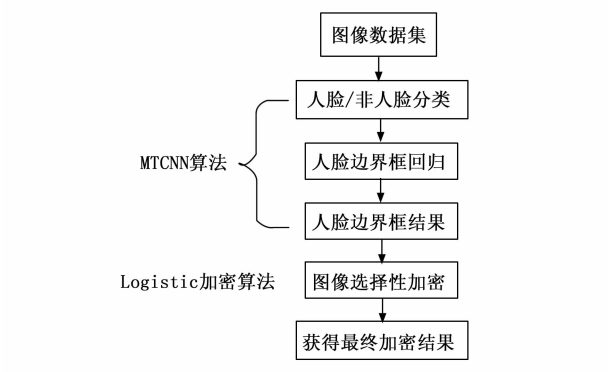

图 6 FIIE 算法结构图

FIIE 算法融合了 MTCNN 网络模型的重要部分及 Logistic 加密算法思想，运用人脸/非人脸分类、人脸边界框回归、人脸边界框检测结果可确定识别人脸标记框，再通过图像选择性加密算法实现对标记框中的人脸进行准确、安全加密。

2.1 增强人脸边界精确表示

MTCNN 网络模型可以进行人脸/非人脸分类、人脸边界框回归和人脸关键点定位三个任务的训练，本文则提出采用增强人脸边界精确表示算法，只需对人脸进行识别并通过边界框标记，无需对人脸关键点进行标记，因此本文只加强了前两个任务的训练。

2.1.1 人脸/非人脸分类任务

该任务的学习目标是一个二分类问题，以此来解决人脸和非人脸区域的问题，此问题用交叉熵损失函数：

$$L_i^{\det} = -(y_i^{\det}\log(p_i) + (1-y_i^{det})(1-\log(p_i))) \quad (2)$$

式（1）中，p_i 为网络模型输出候选样本是人脸的概率；$y_i^{\det}$ 表示样本的真实标签，其取值为 0 或 1。

2.1.2 人脸边界框回归任务

MTCNN 网络将其视为一个回归问题，将上面人脸非人脸区域的分类结果进行标出，得到一个人脸候选框，此问题采用均方误差损失函数：

$$L_i^{\text{box}} = \left\| \hat{y}_i^{\text{box}} - y_i^{\text{box}} \right\|_2^2 \quad (3)$$

式（2）中，$\hat{y}_i^{\text{box}}$ 为网络预测的候选框坐标；y_i^{box} 为与候选框最近的真实框的坐标，包括左上角点的横纵坐标与高度、宽度。

2.1.3 多任务训练

综合上述两个任务的损失函数为：

$$min \sum_{i=1}^{N} \sum_{j \in \{\det,\text{box}\}} \alpha_j \beta_i^j L_i^j \quad (4)$$

式（3）中，N 为训练样本数目；α_j 为权重值，表示每个任务的重要性，其中，分类任务的权重 $\alpha_{\det}$ 为 1，边界框回归任务的权重 α_{box} 为 0.5；L_i^j 为上述的损失函数；β_i^j 为样本类型，其值为 0 或 1。

2.2 Logistic 混沌加密算法

现有对图像加密的研究主要是使用 Logistic 混沌加密算法对整幅图进行加密，本文为了达到对区域进行选择性加密的目的，对此算法进行了改进，在图像不失真的情况下大大增强图像加密的安全性。不同于传统算法中将由混沌序列生成的图像二维矩阵与需要加密的图像进行异或操作从而得到加密图像，本文先利用前一步骤得到的人脸区域坐标生成所需掩码，通过掩码过滤掉图像中与人脸不相关的区域，使其不参与运算，从而减少运算成本，之后将其与混沌序列生成的二维矩阵以及需要加密的图像进行异或操作，完成对图像的人脸区域进行加密的任务。具体操作过程如图 7 所示。

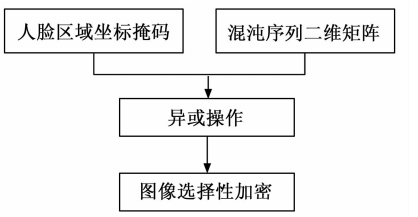

图 7 Logistic 加密过程图

3 实验

3.1 数据集准备及数据预处理

本文使用了 WIDER FACE 数据集在对 MTCNN 模型进行训练。WIDER FACE 数据集包含 32 203 张图片，一共包含了 393 703 个人脸数据，如图 8 所示，根据这些图片场景的不同，改数据集又分为了 Parade、Handshaking、Rescue、Ceremony 等 61 个类，并将每个类别以 4：1：5 的比例划分为训练集、验证集和测试集。在实验中，本文从训练集中随机选取了中的 3 069 张图片对模型进行训练。

官网中的关于图像标注的文件有 MATLAB 存储格式和文本格式两种，本文主要采用文本格式的标注文件。如图 9 所示，在图像标注文件中，第一行代表每个图片的名称，第二行表示此图片中标注的人脸个数，接下来的每一行依次表示图片中标注的边界框的左上角点 x、y 坐标、边界框的宽、高、人脸的模糊程度、做出表情的程度等 10 个详细信息。本文主要利用与人脸边界框位置相关的 4 个信息。

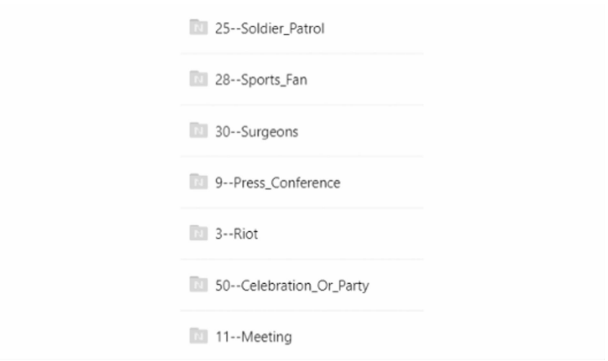

图 8　WLDERFACE 数据集

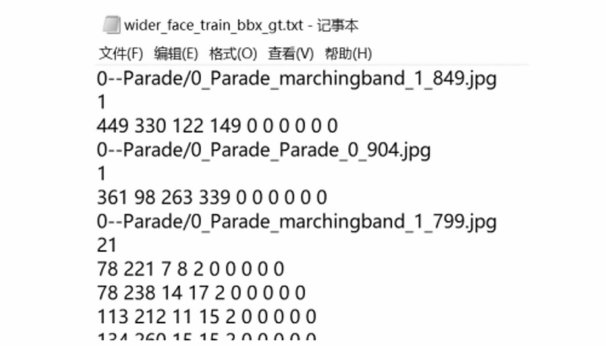

图 9　标注文件格式

为了简便后续实验操作，本文对原始的标注文件内容进行了修改，如图 10 所示，修改后的标注文件一行代表一张图片，每张图片的信息以图片为首，除此之外的其他数据每四个为一组来表示此图片中所有标注过人脸的边界框的左上角点以及右下角的点 x、y 坐标。修改后的标注文件就可以直接用于 MTCNN 模型进行训练。

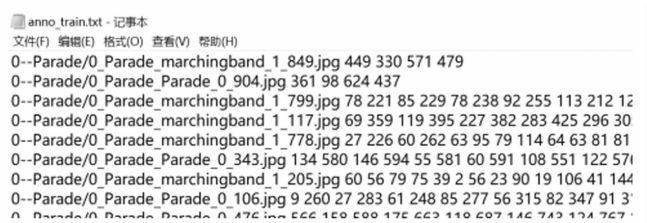

图 10　修改后的数据集标注文件格式

3.2　训练数据准备

在对 MTCNN 网络模型进行训练时，需要分阶段依次对 P-Net、R-Net 和 O-Net 网络进行数据准备。

在准备 P-Net 的数据时，需要对训练集的图片进行截取，将截取的正方形区域与标注文件中的人脸边界框进行 IOU 的计算，根据得到的结果对截取的区域进行分类。当 IOU 小于 0.3 时，则表明此区域没有人脸的图像，将其分类到负样本中；如果 IOU 大于等于 0.4 但小于 0.65，则表明此区域含有局部人脸图像，属于部分样本；如果 IOU 大于等于 0.65，表明此区域含有一张完整人脸，分类为正样本。在训练 P-Net 时，其输入都是 $12 * 12 * 3$ 的图像，所以要将这些样本调整大小为 $12 * 12$，之后分别保存到如图 11 所示的 negative、part、positive 文件夹下。

图 11　P-Net 训练数据的目录

通过上述操作可以得到本实验的训练样本，在此之后制作这些样本的标注文件。如图 12～14 所示，用代码 0 表示负样本的标签样本类型；用代码 1 表示正样本的标签样本类型，其中正样本标签中包含图片对于真实人脸边界框的偏移量，偏移量是通过真实框左上角点和右下角点的坐标值与建议框对应的坐标值相减并除以建议框的尺寸所得到的；部分样本的标签用类型代码－1 表示，其也包含它对于真实人脸边界框的偏移量。将这三个标注文件完成后，将其整合到一个文本文件中，便于后续训练网络使用。

图 12　负样本的标注文件

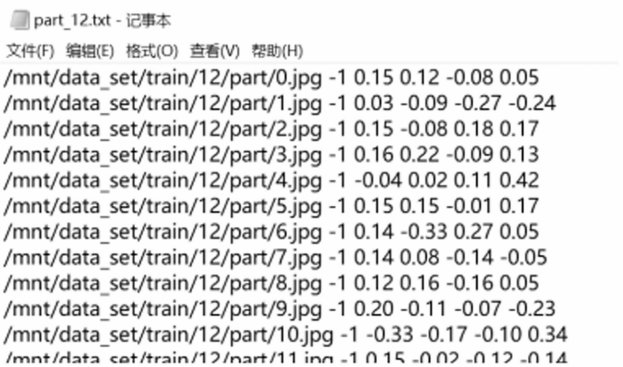

图 13　部分样本的标注文件

正样本和负样本用来训练人脸分类任务，正样本和部分样本用于训练人脸边框回归任务。

R-Net 的训练样本需要用 P-Net 训练好的网络来生成，并将生成的样本调整大小为 $24 * 24$。生成样本之后，对样本的分类方法和标注文件的格式与 P-Net 都相同。同理，

pos_12.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
/mnt/data_set/train/12/positive/0.jpg 1 -0.08 -0.02 -0.23 0.01
/mnt/data_set/train/12/positive/1.jpg 1 0.03 0.11 -0.21 0.03
/mnt/data_set/train/12/positive/2.jpg 1 0.03 -0.11 0.01 0.08
/mnt/data_set/train/12/positive/3.jpg 1 -0.02 -0.36 0.08 -0.01
/mnt/data_set/train/12/positive/4.jpg 1 0.15 0.11 -0.06 0.07
/mnt/data_set/train/12/positive/5.jpg 1 -0.07 -0.05 -0.25 -0.04
/mnt/data_set/train/12/positive/6.jpg 1 -0.01 -0.09 -0.20 -0.10
/mnt/data_set/train/12/positive/7.jpg 1 0.04 -0.04 -0.17 -0.07
/mnt/data_set/train/12/positive/8.jpg 1 -0.06 -0.04 -0.06 0.25
/mnt/data_set/train/12/positive/9.jpg 1 0.21 0.05 -0.04 0.02
```

图 14 正样本的标注文件

O-Net 的训练样本需要 R-Net 训练好的模型来生成，此部分大小需调整为 48 * 48。

将网络训练好之后，对训练好的网络进行测试，测试结果如图 15 所示。

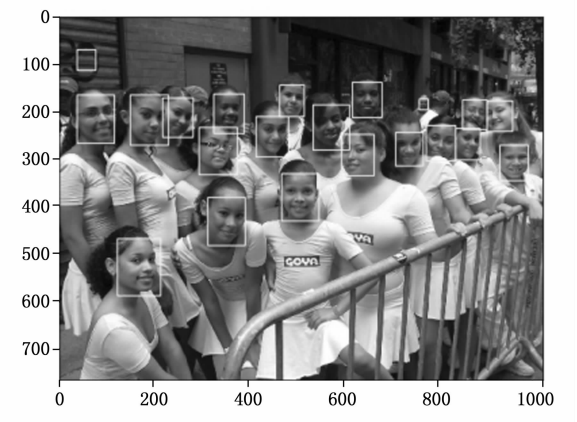

图 15 测试结果

通过实验发现，即使实验图片中包含较多的人脸数目时，MTCNN 算法也能有效地检测并定位人脸位置，并且该算法可以识别拥有较多人脸信息的侧脸。不过，对于一些面部大量被遮挡的图片信息以及与人脸十分相似的图片信息，MTCNN 网络模型在检测过程中也会出现检测不出或者过度检测的情况。但是，对于大多数的图片结果，此算法模型还是可以输出较好的检测和定位结果。

通过对 Logistic 加密算法的创新，得到如图 16 所示的加密结果。

图 16 图像部分加密结果

由图 16 可以看出本文使用的加密方法对加密图片中部分区域有比较不错的实现效果，由此可见，通过创新后的 Logistic 混沌置乱加密可以解决保护图像中面部区域隐私问题。

4 结束语

本文研究了一种针对图像的面部区域进行选择性解密的算法模型，实现对图片中的人脸隐私部位的有效保护。该方法融合了人脸检测算法、人脸对齐方法及图像加密算法，对图像中的人脸信息进行加密保护。通过对 WLDER FACE 数据集的标注数据进行修改，并用此数据集以及修改后的标注文件对 MTCNN 模型进行训练。此外 MTCNN 网络模型级联了 P-Net、R-Net、O-Net 三层卷积神经网络，并对上述三个网络分别依次进行训练。将三个网络模型训练好后，通过训练好的模型对图片数据集进行人脸检测和定位，便可得到图片中人脸区域标记的矩形框的坐标。通过得到的矩形框坐标可以生成掩码，利用掩码对 Logistic 混沌序列和原图片进行 OpenCV 位运算，然后对得到的区域进行加密从而获得加密后的图像。后续将在检测速度或较多遮挡情况下的人脸隐私等方面展开进一步的研究。

参考文献：

[1] CNNIC 发布第 49 次《中国互联网络发展状况统计报告》[J]. 新闻潮，2022 (2)：3.

[2] 石金晶，陈 添，陈淑慧，等. 基于 Arnold 变换的量子图像混沌加密方法 [J]. 电子与信息学报，2022，44 (12)：4284 - 4293.

[3] 何 灏，张海民. 基于混沌 Logistic 加密算法的图像加密技术应用研究 [J]. 网络安全技术与应用，2022 (1)：34 - 35.

[4] 韩雪娟，李国东，王思秀. 基于 Logistic 和超混沌结合的加密算法 [J]. 计算机科学，2019，46 (S2)：477 - 482.

[5] 李春彪，赵云楠，李雅宁，等. 基于正弦反馈 Logistic 混沌映射的图像加密算法及其 FPGA 实现 [J]. 电子与信息学报，2021，43 (12)：3766 - 3774.

[6] 陈景柱，鲍玉斌. 图像处理中基于改进 YOLO 的 ROI 提取算法研究 [J]. 数学的实践与认识，2020，50 (22)：179 - 185.

[7] KRISHNAMOORTHI R，MALARCHELVI P. Selective combinational encryption of gray scale images using orthogonal polynomials based transformation [J]. International Journal of Computer Science and Network Security，2008，8 (5)：195 - 204.

[8] 游清清，谌海云，骆 俊，等. 人脸检测技术综述 [J]. 无线互联科技，2017 (10)：137 - 140.

[9] 梁路宏，艾海舟，徐光祐，等. 人脸检测研究综述 [J]. 计算机学报，2002 (5)：449 - 458.

[10] 范小九，彭 强，CHEN J X，等. 一种改进的 AAM 人脸特征点快速定位方法 [J]. 电子与信息学报，2009，31 (6)：1354 - 1358.

[11] 陈小梅. 基于灰度积分投影的人脸区域定位 [J]. 福建电脑，2017，33 (12)：122 - 123，168.

(下转第 230 页)