结合双随机相位加密和四元数格拉斯曼平均网络的彩色人脸隐私保护识别

徐子涵¹⁾, 邵珠宏^{1)*}, 尚媛园¹⁾, 陈滨²⁾, 毕卉³⁾, 向文涛⁴⁾

¹⁾ (首都师范大学信息工程学院 北京 100048)

²⁾ (嘉兴学院数理与信息工程学院 嘉兴 314001)

³⁾ (常州大学信息科学与工程学院 数理学院 常州 213164)

⁴⁾ (南京医科大学生物医学工程与信息学院 南京 211166)

(zhshao@cnu.edu.cn)

摘要: 为保护彩色人脸图像的隐私并提高识别准确率, 提出一种结合双随机相位加密和四元数格拉斯曼平均网络的彩色人脸隐私保护识别算法. 首先将彩色人脸图像的颜色分量编码为纯四元数矩阵, 使用双随机相位加密和四元数 Gyrator 变换进行加密. 为了隐藏原始彩色人脸图像的内容, 通过随机二值幅度掩模选取部分密文进行解密, 得到不可见的人脸图像, 然后使用四元数格拉斯曼平均网络提取人脸的特征向量和线性支持向量机进行识别. 当人脸特征模板泄露时, 可以重新生成随机二值幅度矩阵并构建新的特征模板替换原始的特征模板, 满足可撤销性, 从而保证原始人脸图像的安全性. 在 Aberdeen, Georgia Tech, Visible Light 和 YouTube Makeup 4 个数据集上与当前 3 种人脸隐私保护识别算法进行比较, 实验结果表明该算法能够有效地提高识别率, 而且对数据集的变化具有较好的鲁棒性.

关键词: 可撤销人脸识别; 双随机相位加密; 四元数 Gyrator 变换; 四元数格拉斯曼平均网络

中图分类号: TP391.41 **DOI:** 10.3724/SP.J.1089.2021.18378

Privacy-Protected Color Face Recognition Using Double Random Phase Encoding and Quaternion Grassmann Average Networks

Xu Zihan¹⁾, Shao Zhuhong^{1)*}, Shang Yuanyuan¹⁾, Chen Bin²⁾, Bi Hui³⁾, and Xiang Wentao⁴⁾

¹⁾ (Information Engineering College, Capital Normal University, Beijing 100048)

²⁾ (College of Mathematics, Physics and Information Engineering, Jiaxing University, Jiaxing 314001)

³⁾ (School of Information Science & Engineering, School of Mathematics & Physics, Changzhou University, Changzhou 213164)

⁴⁾ (School of Biomedical Engineering and Informatics, Nanjing Medical University, Nanjing 211166)

Abstract: To protect the privacy and improve the recognition accuracy, a method of color face privacy protection recognition based on double random phase encoding and quaternion Grassmann average networks is proposed. Firstly, three color components of each color face image are encoded into a pure quaternion matrix. Then the quaternion value matrix is performed double random phase encoding in quaternion gyrator domain. In order to conceal the content of color facial image, only a small part of encrypted data is randomly selected by using random binary amplitude mask and preserved for decryption. For the invisible decrypted face images, quaternion Grassmann average networks is employed to extract features and recognition rate is

收稿日期: 2020-05-10; 修回日期: 2020-07-21. 基金项目: 国家自然科学基金(61876112, 61601311); 北京市优秀人才资助项目(2016000020124G088); 北京市教委科研计划(SQKM201810028018); 江苏省高等学校自然科学研究项目 (19KJB520002); 南京医科大学科技发展基金(NMUB2019030). 徐子涵(1996—), 男, 硕士研究生, 主要研究方向为图像处理; 邵珠宏(1986—), 男, 博士, 副教授, 硕士生导师, CCF 会员, 论文通讯作者, 主要研究方向为多媒体信息安全、计算机视觉; 尚媛园(1977—), 女, 博士, 教授, 主要研究方向为图像处理、计算机视觉、嵌入式系统; 陈滨(1987—), 男, 博士, 讲师, 主要研究方向为图像处理、深度学习; 毕卉(1985—), 女, 博士, 讲师, 主要研究方向为图像处理和分割; 向文涛(1990—), 男, 博士, 讲师, 主要研究方向为脑电信号处理、模式识别.

calculated by linear support vector machine. In case that the face template is leaked, alternative one can be reproduced by new random binary amplitude matrix, which makes face template cancelable and keeps original face images in safe. The four datasets were used including Aberdeen, Georgia Tech, Visible Light and YouTube Makeup and the recognition rates are compared with other three face image privacy protection methods, the experimental results have demonstrated that the proposed method can effectively improve the recognition rates and it shows better robustness to the change of dataset.

Key words: cancelable face recognition; double random phase encoding; quaternion Gyrator transform; quaternion Grassmann average networks

人脸识别是生物特征识别中的研究热点之一。得益于人脸识别良好的可接受性、高度的通用性和非接触获取方式,越来越多的生活场景应用了刷脸技术。然而人脸的个性特征是独一无二的,通常不会随着时间的变化而发生明显的改变。由于三维打印等技术不断完善,使用高精度的“非真实”人脸进行盗刷或者解锁近乎可能。一旦攻击者盗取数据库中的人脸,基于该特征注册的其他身份识别系统也将存在安全隐患。其次,面部图像还能反映个人的一些隐私信息,如通过分析人脸图像可以获取个人的年龄、性格、生理和心理的健康状况等信息,而这些信息涉及个人的隐私。近年来,随着基于人脸的身份识别技术被广泛使用,人脸特征模板的安全问题日益凸显^[1-3]。

为了对原始生物特征进行隐私保护, Ratha 等^[4]提出可撤销生物特征的概念。原始生物特征在经过处理后产生无法直接辨认的生物模板,替代原始生物特征保存在数据库中,保证了原始生物特征的安全性。若数据库中的生物模板发生泄漏,则可以通过修改参数生成新的生物模板进行替代,实现了有限生物特征的可替换。Kaur 等^[5]提出使用 log-Gabor 滤波器提取人脸特征的相位与幅值特征,之后使用随机投影法结合用户自定的变量对特征进行不可逆变换,得到具有可撤销性的人脸模板。Kaur 等^[6]提出联合随机距离法的特征构建,该算法将原始人脸特征映射为笛卡儿空间上的点集,通过计算点集与用户指定的随机点间的距离产生具有可撤销性的人脸模板。Kumar 等^[7]使用随机排列法将原始人脸特征中的数据位置置乱,使生成的人脸模板可撤销,然后使用二维主成分分析对人脸模板进行降维,实验结果表明置乱操作没有影响识别精度。Walia 等^[8]提出结合自适应加权图产生可撤销生物特征,该算法提取基于关键图像的一般特征,在降低特征维度的同时实现生物特

征的可撤销,不同形式补充信息的交叉扩散保证了变换的不可逆。Jiang 等^[9]使用 Arnold 变换对人脸表情图像进行置乱,然后使用多图嵌入(many graph embedding, MGE)算法提取置乱图像的特征。章坚武等^[10]同样使用 Arnold 变换对人脸图像的关键区域进行置乱,并使用卷积神经网络(convolutional neural networks, CNN)进行人脸识别。但是,Arnold 变换的周期性导致其安全性有限,攻击者经过多次尝试后可能将置乱的人脸图像还原。Taheri 等^[11]将双随机相位加密(double random phase encoding, DRPE)与光子计数(photo counting, PC)结合,只随机选取小部分的密文进行解密,使人脸模板具有可撤销性。

然而,以上提出的算法使用的都是灰度人脸图像,随着图像采集技术的发展,现在获得的人脸图像大多为彩色图像,同时彩色信息有利于提高身份识别的精度。而传统的彩色人脸图像预处理算法,如灰度化、颜色分量单独或拼接处理,将导致彩色图像颜色分量间内在联系的丢失并影响识别的准确率。四元数作为传统复数的推广,使用其多个分量的表示形式可以对彩色图像的颜色分量进行整体编码。近些年,四元数相关理论被引入彩色图像处理与分析领域。Liu 等^[12]提出四元数最大间距准则的彩色人脸识别算法,该算法将彩色人脸图像的颜色分量编码成四元数向量形式,使用四元数最大间距准则将其映射到低维空间中进行特征降维和最近邻分类器进行识别。Zou 等^[13]将四元数线性回归分类与四元数协同表示的分类器结合为整体,对彩色人脸图像进行分类。Bao 等^[14]提出一种基于四元数的模糊判别分析模型的人脸识别算法,使用改进的模糊四元数判别模型提取彩色人脸特征并进行人脸识别。Zhao 等^[15]提出基于四元数的样本松弛二维主成分分析的人脸识别算法,根据同一标签的训练集彩色人脸图像的方差

生成松弛向量构造协方差矩阵并计算投影矩阵用于降低人脸图像维度, 该算法扩大了全局方差, 取得了良好的识别效果.

为保证人脸图像的安全和识别的精度, 本文提出一种结合 DRPE 和四元数格拉斯曼平均网络 (quaternion Grassmann average networks, QGANet)^[16] 的隐私保护识别算法. 该算法使用四元数矩阵表示彩色人脸图像并进行四元数 Gyrator 变换域的 DRPE, 使用随机二值幅度掩模 (random binary amplitude mask, RBAM) 选择部分密文解密得到视觉上不可见的人脸图像. 然后使用 QGANet 提取特征和线性支持向量机进行识别. 为验证本文算法的有效性, 在多个彩色人脸数据集中进行实验并与其他算法进行对比.

1 相关工作

1.1 四元数与彩色图像表示

四元数包含 1 个实部分量和 3 个虚部分量, 可以表示^[17]为 $q = q_0 + q_1i + q_2j + q_3k$. 其中, $\{q_0, q_1, q_2, q_3\}$ 表示实数; $\{i, j, k\}$ 表示虚数单位且满足关系 $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$. 当实部 $q_0 = 0$ 时, q 简化为纯四元数, q 的共轭与模分别为 $q^* = q_0 - q_1i - q_2j - q_3k$ 和 $\|q\| = \sqrt{q_0^2 + q_1^2 + q_2^2 + q_3^2}$; 当四元数的模值为 1 时, 称之为单位四元数.

以 RGB 彩色图像为例, 使用四元数矩阵的形式可以将其编码为

$$f_q(x, y) = if_R(x, y) + jf_G(x, y) + kf_B(x, y) \quad (1)$$

其中, f_R, f_G, f_B 分别表示彩色图像的红、绿和蓝色分量; (x, y) 表示图像中的坐标位置.

1.2 基于双随机相位和四元数 Gyrator 变换的彩色图像加密

旋转角度为 α 的右边型四元数 Gyrator 变换 (quaternion Gyrator transform, QGT)^[18] 定义为

$$G^\alpha(u, v) = \frac{1}{|\sin \alpha|} \iint f_q(x, y) \exp\left(\mu 2\pi \frac{(uv + xy)(\cos \alpha - 1)}{\sin \alpha}\right) dx dy.$$

其中, $(x, y), (u, v)$ 分别表示空域与频域; μ 表示单位纯四元数. QGT 的逆变换可以通过取旋转角度 $-\alpha$ 实现.

基于双随机相位和 QGT 的彩色图像加密可以表示为 $f_e(x, y) = G^{\alpha_2} \{G^{\alpha_1} \{f_q(x, y) M_1(x, y)\} M_2(\mu, \nu)\}$. 其中, $M_1(x, y)$ 和 $M_2(\mu, \nu)$ 表示 2 个随机相位掩模; α_1 和 α_2 为 2 个旋转角度. 解密过程为其逆变换, 即

$$f_d(x, y) = G^{-\alpha_1} \{G^{-\alpha_2} \{f_e(x, y) M_2^*(\mu, \nu)\} M_1^*(x, y)\}.$$

其中, $*$ 表示四元数共轭运算.

2 本文算法

本文提出的彩色人脸隐私保护识别算法由注册阶段和识别阶段 2 个部分组成. 图 1 所示为算法的具体流程.

2.1 注册阶段

注册阶段主要由彩色人脸图像的 DRPE、稀疏化解密和 QGANet 特征提取组成.

2.1.1 彩色图像加密

令 A, B 为 2 个标准正态分布矩阵, 即

图 1 本文算法流程图

$$\begin{cases} \mathbf{A} = \{a_{i,j} | i = 1, 2, \dots, n; j = 1, 2, \dots, m\} \\ \mathbf{B} = \{b_{i,j} | i = 1, 2, \dots, n; j = 1, 2, \dots, m\} \end{cases}$$

通过 $\mathbf{A}, \mathbf{B}$ 生成随机相位掩模 $P_1(x, y), P_2(x, y)$, 即

$$\begin{cases} P_1(x, y) = \exp(\mu 2\pi A_{i,j}) \\ P_2(x, y) = \exp(\mu 2\pi B_{i,j}) \end{cases}$$

对由式(1)得到的纯四元数矩阵表示的彩色人脸图像 $f_q(x, y)$ 进行加密的过程表示为

$$f_e(x, y) = G^{\alpha_2} \{G^{\alpha_1} \{f_q(x, y) P_1(x, y)\} P_2(x, y)\}.$$

其中, $f_e(x, y)$ 为密文; α_1, α_2 为 QGT 的旋转角度.

2.1.2 稀疏解密

对密文数据 $f_e(x, y)$ 进行解密可以恢复原始彩色人脸图像. 在本文算法中, 使用 RBAM 对密文数据进行稀疏化选取, 使得解密结果无法直接通过视觉辨认, 实现了彩色人脸的隐私保护. 同时相同的稀疏度可以产生不同的稀疏化密文, 使得算法具有可撤销性. 稀疏化密文 $f_e^s(x, y)$ 的生成过程为

$$f_e^s(x, y) = f_e(x, y) M_s(x, y) \quad (2)$$

其中, $M_s(x, y)$ 表示稀疏度为 ρ 的 RBAM; ρ 表示 RBAM 中 1 所占的比例. 图 2 展示了 3 个大小为 64×64 且 $\rho = 20\%$ 的 RBAM.

图 2 $\rho = 20\%$ 的不同 RBAM

然后使用加密阶段的相位掩模 $P_1(x, y), P_2(x, y)$ 和旋转角度 α_1, α_2 对由式(2)得到的稀疏化密文进行逆变换得到解密结果 $f_d(x, y)$, 即

$$f_d(x, y) = G^{-\alpha_1} \{G^{-\alpha_2} \{f_e^s(x, y) P_2^*(x, y)\} P_1^*(x, y)\}.$$

2.1.3 QGANet 特征提取

对稀疏化密文进行解密后, 使用解密结果训练 QGANet 作为特征提取网络提取人脸模板特征. QGANet 构建流程如图 3 所示, 其中, $B_{\text{hist}}(\cdot)$ 表示计算分块直方图统计结果的函数.

设经过部分解密的训练集四元数彩色人脸样本为 $\{X_i \in Q^{n \times m}, i = 1, 2, \dots, N\}$, Q 表示四元数域, 在滤波器构建阶段, 首先使用尺寸为 $h_1 \times h_2$ 的窗口对训练集 X_i 的每个样本进行采样. 对于训练集的第 i 个样本通过采样得到 $(n - h_1 + 1) \times (m - h_2 + 1)$ 幅子图像, 去除每幅子图像的均值并展开成向量形式, 可记为 $\mathbf{x}_i = [\mathbf{x}_{i,1}, \mathbf{x}_{i,2}, \dots, \mathbf{x}_{i,(n-h_1+1) \times (m-h_2+1)}]$; 其中, $\mathbf{x}_i$ 的元素均为 $h_1 \times h_2$ 维列向量. 将所有样本的

图 3 QGANet 构建流程

采样结果进行拼接可以得到 $\mathbf{x}=[\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_N] \in Q^{h_1 \times h_2 \times N \times (n-h_1+1) \times (m-h_2+1)}$. 使用四元数格拉斯曼平均网络算法求解 $\mathbf{x}$ 的前 L_1 个主成分 $\mathbf{q}_i (i=1, 2, \dots, L_1)$, 可求得 QGANet 的 L_1 个滤波器, 即 $\mathbf{W}_i = \text{mat}(\mathbf{q}_i) \in Q^{h_1 \times h_2}$. 其中, $\text{mat}(\cdot)$ 表示将向量 $\mathbf{q} \in Q^{h_1 \times h_2}$ 映射为矩阵 $\mathbf{W} \in Q^{h_1 \times h_2}$ 的函数. 第 i 个滤波器的卷积结果为 $\mathbf{O}_i^h = \mathbf{X}_i * \mathbf{W}_i, i=1, 2, \dots, N$. 其中, $*$ 表示四元数卷积, 每个训练样本可以得到 L_1 幅输出图像.

在二进制哈希编码阶段, 对 $\mathbf{O}_i^h$ 的实部与 3 个虚部分别进行二进制量化得到 $\bar{\mathbf{O}}_i^h$, 使用的示性函数为

$$\chi(x) = \begin{cases} 1, & x > 0 \\ 0, & x \leq 0 \end{cases} \quad (3)$$

将经过式(3)二进制量化得到的 L_1 个滤波器卷积结果转换为一幅四元数图像的过程为

$$\mathbf{T}_i = \sum_{l=1}^{L_1} 2^{l-1} \bar{\mathbf{O}}_i^h = \mathbf{T}_{S,i} + \mathbf{T}_{R,i}i + \mathbf{T}_{G,i}j + \mathbf{T}_{B,i}k, i=1, 2, \dots, N.$$

其中, $\mathbf{T}_{S,i}$ 为 $\mathbf{T}_i$ 的实部; $\mathbf{T}_{R,i}, \mathbf{T}_{G,i}, \mathbf{T}_{B,i}$ 为 $\mathbf{T}_i$ 的 3 个虚部; $\mathbf{T}_i$ 的实部与 3 个虚部中的元素均为 $[0, 2^{L_1-1}]$ 范围内的十进制整数.

在分块直方图统计阶段, 将 $\mathbf{T}_i$ 的实部分量 $\mathbf{T}_{S,i}$ 分割成大小相同的 B 幅图像, 计算每幅子图像的直方图分布, 再将所有结果依次拼接成向量得到 $\mathbf{T}_{S,i}$ 的分块直方图统计结果 $B_{\text{hist}}(\mathbf{T}_{S,i}) \in \mathbb{R}^{2^{L_1} \times B}$. 同样求出虚部分量 $\mathbf{T}_{R,i}, \mathbf{T}_{G,i}, \mathbf{T}_{B,i}$ 的分块直方图统计结果后进行拼接, 得到 $\mathbf{T}_i$ 的特征向量

$$\mathbf{f}_{t,i} = [B_{\text{hist}}(\mathbf{T}_{S,i}), B_{\text{hist}}(\mathbf{T}_{R,i}), B_{\text{hist}}(\mathbf{T}_{G,i}), B_{\text{hist}}(\mathbf{T}_{B,i})] \in \mathbb{R}^{4 \times 2^{L_1} \times B}.$$

其中, $i=1, 2, \dots, N$.

2.2 识别阶段

识别阶段使用线性支持向量机作为分类器, 令 $y_{t,i} (i=1, 2, \dots, N)$ 为 $\mathbf{f}_{t,i}$ 对应的类别, 训练线性支持向量机的过程即为求解无约束优化问题

$$\min f(\mathbf{w}) = \frac{1}{2} \mathbf{w}^T \mathbf{w} + \sum_{i=1}^1 (\max(0, 1 - y_{t,i} \mathbf{w}^T \mathbf{f}_{t,i}))^2.$$

测试集图像同样经过加密与稀疏解密, 然后使用 QGANet 提取测试集图像特征向量 $\mathbf{f}_{v,j} (j=$

$1, 2, \dots, M)$, 将 $\mathbf{f}_{v,j}$ 输入训练好的线性支持向量机进行识别.

3 实验结果

本文选取 4 个彩色人脸数据集进行实验, 设备的配置为 2.50 GHz Intel^(R) CoreTM i5-4200M CPU, 4 GB 内存, Windows 8.1 操作系统. Aberdeen^①人脸数据集由 29 个人的 377 幅彩色人脸图像组成, 其中每个人包含 13 幅不同光照、表情的正面人脸图像. GT (Georgia Tech)^②人脸数据集包含 50 个人的 750 幅彩色人脸图像, 其中每个人包含 15 幅不同光照、表情的正面或不同程度倾斜的人脸图像. VIS (Visible Light)^③人脸数据集包含 100 个人的 400 幅彩色人脸图像, 每个人包含 4 幅不同光照的正面人脸图像, 其中有部分人脸图像被眼镜遮挡. YMU (YouTube Makeup)^[19]人脸数据集的图像来自 YouTube 的化妆教程, 包含 151 个人的 604 幅彩色人脸图像, 其中每个人包含 4 幅不同表情、姿态和化妆程度的正面人脸图像. 图 4 展示了部分彩色人脸示例.

图 4 部分彩色人脸示例

实验使用的人脸图像根据眼睛的位置进行裁剪并调整为 64×64 像素, 对于 Aberdeen 人脸数据集和 GT 人脸数据集每个类别分别随机选取 9 幅与

① http://pics.stir.ac.uk/2D_face_sets.htm

② http://www.anefian.com/research/face_reco.htm

③ <http://biometrics.idealtest.org/>

10 幅人脸图像作为训练图像进行多次实验; 对于 VIS 人脸数据集和 YMU 人脸数据集, 由于每个类别样本数量较少, 使用留一法进行实验. 在实验中, 单位纯四元数的选取为 $\mu = (i + j + k)/\sqrt{3}$, QGT 的旋转角度选取为 $\alpha_1 = 0.7$, $\alpha_2 = -1.2$. 首先讨论部分参数的选取对识别效果的影响, 然后将本文算法的识别效果与其他算法进行对比.

3.1 稀疏度选取

稀疏度的选取影响人脸图像的安全性和人脸识别的精度, 较高的稀疏度使得解密图像更容易辨认, 人脸识别率高但保护人脸图像的能力降低, 较低的稀疏度可以隐藏人脸图像的内容, 但可能对识别率造成影响, 因此需要选取合适的稀疏度以兼顾识别精度与安全性. 本文通过非线性四元数相关(nonlinear quaternion correlation, NQC)^[20]和峰相关能量(peak-to-correlation energy, PCE)对稀疏度进行选取. NQC 定义为

$$\text{NQC}(x, y) = F^{-1} \left\{ \left| F[f_q(x, y)] F^*[f_d(x, y)] \right|^{\lambda-1} \right. \\ \left. F[f_q(x, y)] F^*[f_d(x, y)] \right\} \quad (4)$$

其中, $F[\cdot]$ 与 $F^{-1}[\cdot]$ 分别表示四元数傅里叶变换与四元数傅里叶逆变换. 由式(4)可计算 PCE 为

$$\text{PCE} = \frac{\max \left[\left| \text{NQC}(f_q(x, y), f_d(x, y)) \right|^2 \right]}{\sum \left| \text{NQC}(f_q(x, y), f_d(x, y)) \right|^2}.$$

其中, $f_q(x, y)$ 和 $f_d(x, y)$ 分别表示编码为四元数矩阵的原始彩色人脸图像与解密后的图像. PCE 越大, 识别效果越好. 本文选取 $\lambda = 0.3$ 进行 PCE 计算, 结果如图 5 所示.

图 6 所示为不同稀疏度下的解密图像. 从图中可以看到, 当 $\rho = 100\%$ 时, 解密图像清晰可见, 无法对人脸图像进行有效的保护. 随着稀疏度降低, 人脸图像的细节变得无法直接辨认, 人脸图像的内容得到有效的隐藏. 为兼顾安全性与识别效果, 本文选取 $\rho = 20\%$ 进行后续实验.

3.2 QGANet 参数选取

本文算法使用的 QGANet 需要设定的参数有滤波器尺寸、滤波器个数、分块直方图子图像尺寸以及分块直方图子图像重叠率. 下面讨论 4 个参数对识别率的影响因素.

3.2.1 滤波器尺寸选取

为了分析滤波器尺寸对识别率的影响, 对于 Aberdeen, VIS 和 YMU 人脸数据集 QGANet 的滤

图 5 不同人脸数据集的 PCE

图 6 不同稀疏度下的人脸图像解密结果

波器个数、分块直方图子图像尺寸以及分块直方图子图像重叠率取 8, 10×10 和 0.5; 对于 GT 人脸数据集取 8, 8×8 和 0, 分别计算在 3×3, 5×5, 7×7 和 9×9 大小的滤波器下得到的人脸识别率, 实验结果如图 7 所示. 实验结果表明, 识别率的高低与滤波器尺寸没有线性关系, 在 Aberdeen, VIS 和 YMU 人脸数据集中, 当滤波器尺寸增大到 7×7 后识别率不再提高; 在 GT 人脸数据集中, 当滤波器尺寸超过 3×3 时识别率反而有所降低.

图 7 不同滤波器尺寸下的人脸识别率

3.2.2 滤波器个数选取

为了分析滤波器个数对识别率的影响, 对于 Aberdeen, VIS 和 YMU 人脸数据集 QGANet 的滤波器尺寸、分块直方图子图像尺寸以及分块直方图子图像重叠率取 7×7, 10×10 和 0.5; 对于 GT 人脸

数据集取 3×3, 8×8 和 0, 分别计算在 3~9 个滤波器下得到的人脸识别率, 实验结果如图 8 所示. 在 4 个人脸数据集中, 当滤波器个数增加到 8 时, 识别率达到最大值; 当滤波器数量超过 8 后, 识别率并没有提高, 反而会增大 QGANet 的参数数量, 导致训练速度降低.

图 8 不同滤波器个数下的人脸识别率

3.2.3 分块直方图子图像尺寸选取

为了分析分块直方图子图像尺寸对识别率的影响, 对于 Aberdeen, VIS 和 YMU 人脸数据集 QGANet 的滤波器尺寸、滤波器个数以及分块直方图子图像重叠率取 7×7, 8 和 0.5; 对于 GT 人脸数据集取 3×3, 8 和 0, 分别计算在不同分块直方图子图像尺寸下得到的人脸识别率, 实验结果如图 9 所示. 在 Aberdeen, VIS 和 YMU 人脸数据集中, 当分

块直方图子图像尺寸增大到 10×10 时, 人脸识别率达到最高, 尺寸继续增大后识别率有所降低. 在 GT 人脸数据集中, 当分块直方图子图像尺寸增大到 8×8 时, 人脸识别率达到最高.

图9 不同分块直方图子图像尺寸下的人脸识别率

3.2.4 分块直方图子图像重叠率选取

为了分析分块直方图子图像重叠率对识别率的影响, 对于 Aberdeen, VIS 和 YMU 人脸数据集 QGANet 的滤波器尺寸、滤波器个数以及分块直方图子图像尺寸取 $7 \times 7, 8$ 和 10×10 ; 对于 GT 人脸数据集取 $3 \times 3, 8$ 和 8×8 , 分别计算在不同分块直方图子图像重叠率下得到的人脸识别率, 实验结果如图 10 所示. 在 Aberdeen, VIS 和 YMU 人脸数据集中,

当分块直方图子图像重叠率增大到 0.5 时, 人脸识别率达到最高, 重叠率继续增加后, 识别率有所下降, QGANet 的参数量加大. 在 GT 人脸数据集中, 分块直方图子图像无重叠时人脸识别率最高.

图10 不同分块直方图子图像重叠率下的人脸识别率

3.3 识别率与运行时间比较

为了客观评估本文算法的性能, 将本文算法与 MGE 算法^[9], Arnold-CNN 算法^[10]和 PC-DRPE 算法^[11]进行比较. 在 Aberdeen, VIS 和 YMU 人脸数据集中, 本文算法的滤波器尺寸、滤波器个数、分块直方图子图像尺寸和分块直方图子图像重叠率的选取分别为 $7 \times 7, 8, 10 \times 10$ 和 0.5, 在 GT 人脸数据集中分别为 $3 \times 3, 8, 8 \times 8$ 和 0, 其他 3 种算法的参数根据文献中的描述设置. 实验中 Arnold-

CNN 算法的迭代次数为 300 次。

表 1 列出了以上 4 种算法在 4 个彩色人脸数据集的平均识别率和标准差。可以看出, 本文提出的彩色人脸隐私保护算法在不同的人脸数据集都得到了最高识别率, 表明本文算法的有效性。

表 1 不同算法识别率比较 %

数据集	MGE ^[9]	Arnold-CNN ^[10]	PC-DRPE ^[11]	本文
Aberdeen	98.84±0.93	97.63±1.91	91.81±4.37	99.14±1.73
GT	85.30±1.83	87.90±0.89	71.80±1.15	92.50±0.50
VIS	97.50±1.73	90.00±4.40	93.50±3.87	97.75±0.96
YMU	75.67±5.00	76.88±4.16	74.67±3.68	91.72±3.60

图 11 展示了本文算法解密图像生成过程中各步骤的用时情况, 其中彩色图像加密过程用时最长, 占总时长的 43%, 而稀疏化密文解密过程用时较短, 只占总时长的 9%。

图 11 本文算法解密图像生成过程用时分析

表 2 列出了以上 4 种算法在 4 个彩色人脸数据集的运行时间, 本文算法相比 Arnold-CNN 算法运行时间更短, 但本文算法使用的 QGANet 是一种深度学习算法, 因此相比 MGE 算法和 PC-DRPE 算法耗时更长。

表 2 不同算法运行时间比较 s

数据集	MGE ^[9]	Arnold-CNN ^[10]	PC-DRPE ^[11]	本文
Aberdeen	4.44	2 802.79	6.31	300.52
GT	10.38	5 296.54	12.72	148.92
VIS	8.48	3 099.78	10.08	329.32
YMU	9.61	4 399.93	16.48	408.35

4 结 语

针对彩色人脸图像隐私信息的安全保护, 本文提出一种结合 DRPE 与 QGANet 的识别算法。在

注册阶段, 首先对训练集中的彩色人脸图像进行基于双随机相位和 QGT 的加密操作得到密文。为了实现彩色人脸图像的隐私保护, 通过 RBAM 选取部分密文进行解密。然后使用 QGANet 对解密结果提取人脸模板特征。在识别阶段, 使用与注册阶段相同的密钥对人脸图像进行预处理, 得到隐藏了原始人脸图像内容的解密结果, 同样通过 QGANet 提取特征。最后使用线性支持向量机进行判别。如果人脸模板发生泄漏, 则可以更改稀疏矩阵生成新的人脸模板进行替换, 实现人脸模板的重新发布。实验结果表明, 本文算法在保护彩色人脸隐私的同时取得了较好的识别效果。

参考文献(References):

- [1] Ma Z, Liu Y, Liu X M, *et al.* Lightweight privacy-preserving ensemble classification for face recognition[J]. IEEE Internet of Things Journal, 2019, 6(3): 5778-5790
- [2] Akhtar Z, Hadid A, Nixon M S, *et al.* Biometrics: in search of identity and security (Q & A)[J]. IEEE MultiMedia, 2018, 25(3): 22-35
- [3] Yang W C, Wang S, Hu J K, *et al.* Securing mobile healthcare data: a smart card based cancelable finger-vein bio-crypto-system[J]. IEEE Access, 2018, 6: 36939-36947
- [4] Ratha N K, Connell J H, Bolle R M. Enhancing security and privacy in biometrics-based authentication systems[J]. IBM Systems Journal, 2001, 40(3): 614-634
- [5] Kaur H, Khanna P. Cancelable features using log-Gabor filters for biometric authentication[J]. Multimedia Tools and Applications, 2017, 76(4): 4673-4694
- [6] Kaur H, Khanna P. Random distance method for generating unimodal and multimodal cancelable biometric features[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(3): 709-719
- [7] Kumar N, Singh S, Kumar A. Random permutation principal component analysis for cancelable biometric recognition[J]. Applied Intelligence, 2018, 48(9): 2824-2836
- [8] Walia G S, Jain G, Bansal N, *et al.* Adaptive weighted graph approach to generate multimodal cancelable biometric templates[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 1945-1958
- [9] Jiang R, Ho A T S, Cheheb I, *et al.* Emotion recognition from scrambled facial images via many graph embedding[J]. Pattern Recognition, 2017, 67: 245-251
- [10] Zhang Jianwu, Shen Wei, Wu Zhendong. Recognition of face privacy protection using convolutional neural networks[J]. Journal of Image and Graphics, 2019, 24(5): 744-752(in Chinese) (章坚武, 沈伟, 吴震东. 卷积神经网络的人脸隐私保护识别[J]. 中国图象图形学报, 2019, 24(5): 744-752)
- [11] Taheri M, Mozaffari S, Keshavarzi P. Cancelable face verification using optical encryption and authentication[J]. Journal of the Optical Society of America, 2015, 32(10): 1772-1779
- [12] Liu Z H, Qiu Y, Peng Y L, *et al.* Quaternion based maximum

- margin criterion method for color face recognition[J]. *Neural Processing Letters*, 2017, 45(3): 913-923
- [13] Zou C M, Kou K I, Dong L, *et al.* From grayscale to color: quaternion linear regression for color face recognition[J]. *IEEE Access*, 2019, 7: 154131-154140
- [14] Bao S Z, Song X N, Hu G S, *et al.* Colour face recognition using fuzzy quaternion-based discriminant analysis[J]. *International Journal of Machine Learning and Cybernetics*, 2019, 10(2): 385-395
- [15] Zhao M X, Jia Z G, Gong D W. Sample-relaxed two-dimensional color principal component analysis for face recognition and image reconstruction[OL]. [2020-05-10]. <https://arxiv.org/abs/1803.03837>
- [16] Shi J, Zheng X, Wu J J, *et al.* Quaternion Grassmann average network for learning representation of histopathological image[J]. *Pattern Recognition*, 2019, 89: 67-76
- [17] Hamilton W R. *Elements of quaternions*[M]. London: Longmans, Green and Co, 1866
- [18] Shao Z H, Wu J S, Coatrieux J L, *et al.* Quaternion gyrator transform and its application to color image encryption[C] // *Proceedings of the IEEE International Conference on Image Processing*. Los Alamitos: IEEE Computer Society Press, 2013: 4579-4582
- [19] Dantcheva A, Chen C J, Ross A. Can facial cosmetics affect the matching accuracy of face recognition systems?[C] // *Proceedings of the 5th IEEE International Conference on Biometrics: Theory, Applications and Systems*. Los Alamitos: IEEE Computer Society Press, 2012: 391-398
- [20] Shao Z H, Shang Y Y, Tong Q B, *et al.* Multiple color image encryption and authentication based on phase retrieval and partial decryption in quaternion gyrator domain[J]. *Multimedia Tools and Applications*, 2018, 77(19): 25821-25840