



JOURNAL OF IMAGE AND GRAPHICS

主办: 中国科学院空天信息创新研究院
中国图象图形学学会
北京应用物理与计算数学研究所

中国图象图形学报

2020
12
VOL.25

ISSN1006-8961
CN11-3758/TB



数字浮雕建模 P2647



第25卷第12期 (总第296期)
2020年12月16日

中国精品科技期刊
中国国际影响力优秀学术期刊
中国科技核心期刊
中文核心期刊

版权声明

凡向《中国图象图形学报》投稿, 均视为同意在本刊网站及CNKI等全文数据库出版, 所刊载论文已获得著作权人的授权。本刊所有图片均为非商业目的使用, 所有内容, 未经许可, 不得转载或以其他方式使用。

Copyright

All rights reserved by Journal of Image and Graphics, Institute of Remote Sensing and Digital Earth, CAS. The content (including but not limited text, photo, etc) published in this journal is for non-commercial use.

主管单位 中国科学院

主办单位 中国科学院空天信息创新研究院

中国图象图形学学会

北京应用物理与计算数学研究所

主 编 吴一戎

编辑出版 《中国图象图形学报》编辑出版委员会

通信地址 北京市海淀区北四环西路19号

邮 编 100190

电子信箱 jig@radi.ac.cn

电 话 010-58887035

网 址 www.cjig.cn

广告发布登记号 京朝工商广登字20170218号

总 发 行 北京报刊发行局

订 购 全国各地邮局

海外发行 中国国际图书贸易集团有限公司

(邮政信箱: 北京399信箱 邮编: 100048)

印刷装订 北京科信印刷有限公司

Journal of Image and Graphics

Title inscription: Song Jian

Monthly, Started in 1996

Superintended by Chinese Academy of Sciences

Sponsored by Aerospace Information Research Institute, CAS

China Society of Image and Graphics

Institute of Applied Physics and Computational Mathematics

Editor-in-Chief Wu Yirong

Editor, Publisher Editorial and Publishing Board of Journal of
Image and Graphics

Address No. 19, North 4th Ring Road West, Haidian District,
Beijing, P. R. China

Zip code 100190

E-mail jig@radi.ac.cn

Telephone 010-58887035

Website www.cjig.cn

Distributed by Beijing Bureau for Distribution of Newspapers and Journals

Domestic All Local Post Offices in China

Overseas China International Book Trading Corporation
(P.O.Box 399, Beijing 100048, P.R.China))

Printed by Beijing Kexin Printing Co., Ltd.

CN 11-3758/TB

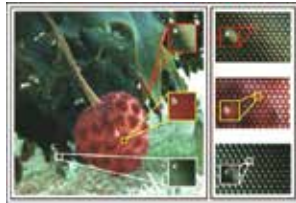
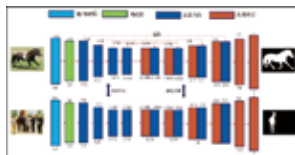
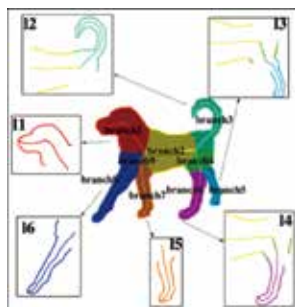
ISSN 1006-8961

CODEN ZTTXFZ

国外发行代号 M1406

国内邮发代号 82-831

国内定价 60.00元

光场显著性检测研究综述
(第2465页)融合注意力机制与知识蒸馏
的孪生网络压缩(第2563页)面向可解释性的物体拓扑结构
骨架表征方法(第2587页)

综述

光场显著性检测研究综述

刘亚美, 张骏, 张旭东, 孙锐, 高隽 2465

图像处理和编码

自适应卷积的残差修正单幅图像去雨

王美华, 何海君, 李超 2484

局部特定空间关系统计特征的RVIN噪声检测器

于海雯, 易昕炜, 徐少平, 林珍玉, 刘蕊蕊 2494

全局与局部属性一致的图像修复模型

孙劲光, 杨忠伟, 黄胜 2505

图像分析和识别

关键语义区域链提取的视频人体行为识别

马淼, 李贻斌, 武宪青, 高金凤, 潘海鹏 2517

针对形变与遮挡问题的行人再识别

史维东, 张云洲, 刘双伟, 朱尚栋, 暴吉宁 2530

多特征融合的行为识别模型

谭等泰, 李世超, 常文文, 李登楼 2541

结构特征下的可撤销人脸识别

孙浩浩, 邵珠宏, 尚媛园, 陈滨, 赵晓旭 2553

融合注意力机制与知识蒸馏的孪生网络压缩

耿增民, 余梦巧, 刘峡壁, 吕超 2563

联合聚焦度和传播机制的光场图像显著性检测

李爽, 邓慧萍, 朱磊, 张龙 2578

图像理解和计算机视觉

面向可解释性的物体拓扑结构骨架表征方法

危辉, 余莉萍 2587

自监督深度残差函数映射网络的3维模型对应关系计算

杨军, 马中昌 2603

融合自编码器和one-class SVM的异常事件检测

胡海洋, 张力, 李忠金 2614

抗高光的光场深度估计方法

王程, 张骏, 高隽 2630

计算机图形学

不同类型高度图控制浅浮雕模型生成方法

尚菁, 余文杰, 王美丽 2647

遥感图像处理

残差密集空间金字塔网络的城市遥感图像分割

韩彬彬, 张月婷, 潘宗序, 台宪青, 李芳芳 2656

结合判别相关分析与特征融合的遥感图像检索

葛芸, 马琳, 储珺 2665

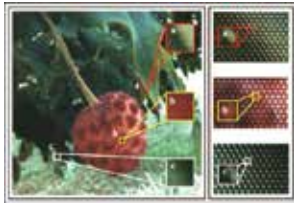
改进卷积网络的高分遥感图像城镇建成区提取

侯博文, 闫冬梅, 郝伟, 黄青青, 苏秀琴, 李青雯 2677

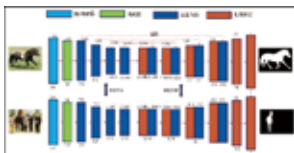
总目次 I

CONTENTS

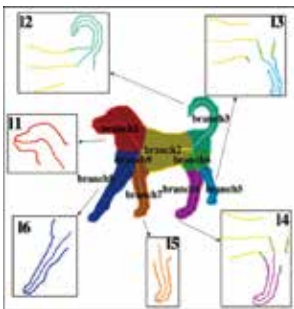
JOURNAL OF IMAGE AND GRAPHICS



Review of saliency detection on light fields(P2465)



Combining attention mechanism and knowledge distillation for Siamese network compression (P2563)



Skeleton characterization of object topology toward explainability (P2587)

Review

Review of saliency detection on light fields

Liu Yamei, Zhang Jun, Zhang Xudong, Sun Rui, Gao Jun 2465

Image Processing and Coding

Single image rain removal based on selective kernel convolution using a residual refine factor

Wang Meihua, He Haijun, Li Chao 2484

Random-valued impulse noise detector using local spatial structure statistics

Yu Haiwen, Yi Xinwei, Xu Shaoping, Lin Zhenyu, Liu Ruirui 2494

Image inpainting model with consistent global and local attributes

Sun Jinguang, Yang Zhongwei, Huang Sheng 2505

Image Analysis and Recognition

Human action recognition in videos utilizing key semantic region extraction and concatenation

Ma Miao, Li Yibin, Wu Xianqing, Gao Jinfeng, Pan Haipeng 2517

Person re-identification based on deformation and occlusion mechanisms

Shi Weidong, Zhang Yunzhou, Liu Shuangwei, Zhu Shangdong, Bao Jining 2530

Multi-feature fusion behavior recognition model

Tan Dengtai, Li Shichao, Chang Wenwen, Li Denglou 2541

Cancelable face recognition with fusion of structural features

Sun Haohao, Shao Zhuhong, Shang Yuanyuan, Chen Bin, Zhao Xiaoxu 2553

Combining attention mechanism and knowledge distillation for Siamese network compression

Geng Zengmin, Yu Mengqiao, Liu Xiabi, Lyu Chao 2563

Saliency detection on a light field via the focusness and propagation mechanism

Li Shuang, Deng Huiping, Zhu Lei, Zhang Long 2578

Image Understanding and Computer Vision

Skeleton characterization of object topology toward explainability

Wei Hui, Yu Liping 2587

Correspondence Calculation of 3D Models by a Self-Supervised Deep Residual Functional Maps Network

Yang Jun, Ma Zhongchang 2603

Anomaly detection with autoencoder and one-class SVM

Hu Haiyang, Zhang Li, Li Zhongjin 2614

Anti-specular light-field depth estimation algorithm

Wang Cheng, Zhang Jun, Gao Jun 2630

Computer Graphics

Bas-relief generation controlled by different height maps

Shang Jing, Yu Wenjie, Wang Meili 2647

Remote Sensing Image Processing

Residual dense spatial pyramid network for urbanremote sensing image segmentation

Han Binbin, Zhang Yueting, Pan Zongxu, Tai Xianqing, Li Fangfang 2656

Remote sensing image retrieval combining discriminant correlation analysis and feature fusion

Ge Yun, Ma Lin, Chu Jun 2665

Urban built-up area extraction using high-resolution remote sensing images with an improved convolutional neural network

Hou Bowen, Yan Dongmei, Hao Wei, Huang Qingqing, Su Xiuqin, Li Qingwen 2677

中图分类号: TP391.4 文献标识码: A 文章编号: 1006-8961(2020)12-2553-10

论文引用格式: Sun H H, Shao Z H, Shang Y Y, Chen B and Zhao X X. 2020. Cancelable face recognition with fusion of structural features. *Journal of Image and Graphics*, 25(12): 2553-2562 (孙浩浩, 邵珠宏, 尚媛园, 陈滨, 赵晓旭. 2020. 结构特征下的可撤销人脸识别. *中国图象图形学报*, 25(12): 2553-2562) [DOI:10.11834/jig.190439]

结构特征下的可撤销人脸识别

孙浩浩¹, 邵珠宏¹, 尚媛园¹, 陈滨², 赵晓旭¹

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

摘要: 目的 相对于其他生物特征识别技术, 人脸识别具有非接触、不易察觉和易于推广等特点, 在公共安全和日常生活中得到广泛应用。在移动互联网时代, 云端人脸识别可以有效地提高识别精度, 但是需要将大量的人脸数据上传到第三方服务器。由于人的面部特征是唯一的, 一旦数据库泄露就会面临模板攻击和假冒攻击等安全威胁。为了保证人脸识别系统的安全性并提高其识别率, 本文提出一种融合人脸结构特征的可撤销人脸识别算法。方法 首先, 对原始人脸图像提取结构特征作为虚部分量, 与原始人脸图像联合构建复数矩阵并通过随机二值矩阵进行置乱操作。然后, 使用2维主成分分析方法将置乱的复数矩阵映射到新的特征空间。最后, 采用基于曼哈顿距离的最近邻分类器计算识别率。结果 在4个不同人脸数据库上的实验结果表明, 原始人脸图像和结构特征图像经过随机二值矩阵置乱后, 人眼无法察觉出有用的信息且可以重新生成, 而且融合方差特征后, 在GT(Georgia Tech)、NIR(Near Infrared)、VIS(Visible Light)和YMU(YouTube Makeup)人脸数据库上, 平均人脸识别率分别提高了4.9%、2.25%、2.25%和1.98%, 且平均测试时间均在1.0 ms之内, 表明该算法实时性强, 能够满足实际应用场的需求。结论 本文算法可在不影响识别率的情况下保证系统的安全性, 满足可撤销性。同时, 融合结构特征丰富了人脸信息的表征, 提高了人脸识别系统的识别率。

关键词: 可撤销人脸识别; 随机二值矩阵; 2维主成分分析; 人脸结构特征; 复数矩阵

Cancelable face recognition with fusion of structural features

Sun Haohao¹, Shao Zhuhong¹, Shang Yuanyuan¹, Chen Bin², Zhao Xiaoxu¹

1. College of Information Engineering, Capital Normal University, Beijing 100048, China;

2. College of Mathematics Physics and Information Engineering, Jiaxing 314001, China

Abstract: Objective Along with the wide usage of various digital image processing hardware and software and the continuous advancements in the field of computer vision, biometric recognition has been introduced to solve identification problems in people's daily lives and has been applied in the fields of finance, education, healthcare, and social security, among others. Compared with iris, palm print, and other biometric recognition technologies, face recognition has received the most attention due to its special characteristics (e.g., on-contact, imperceptible, and easy to promote). Given the wide usage of mobile Internet, cloud face recognition can achieve high recognition accuracy requires a large amount of face data to be uploaded to a third-party server. On the one hand, face images may reflect one's private information, such as gender, age, and health status. On the other hand, given that each person has unique facial features, hacking into face image databases

收稿日期: 2020-02-19; 修回日期: 2020-03-03; 预印本日期: 2020-03-10

基金项目: 国家自然科学基金项目(61876112, 61601311); 北京市优秀人才资助项目(2016000020124G088); 北京市教委科研计划项目(SQKM201810028018, KM201910028018)

Supported by: National Natural Science Foundation of China(61876112, 61601311)

may expose people to threats, including template and fake attacks. Therefore, how to boost the privacy and security of face images has become a core issue in the field of biometric recognition. Among the available biometric template protection methods, the transform-based method can simultaneously satisfy multiple criteria of biometric template protection and is presently considered the most typical cancelable biometric algorithm. The protected biometric template is obtained via an invertible transformation of the original biometric that is saved in a database. When this biometric template is attacked or threatened, a new feature template can be reissued to replace the previous template by modifying the external factors. To guarantee the security of the face recognition system and improve its recognition rate, this paper investigates a cancelable face recognition algorithm that integrates the structural features of the human face. **Method** First, structural features are extracted from the original face image by using its gradient, local binary pattern, and local variance. By taking the original face images as real components and the extracted structural features as imaginary components, a complex matrix is built to represent the face image. To render the original face images and contour of their structural features invisible, the complex matrix is permuted by multiplying it by a random binary matrix. Afterward, complex 2D principal component analysis (C2DPCA) is performed to project a random permuted complex matrix into a new feature space. The 2DPCA result for the scrambled complex face matrix is theoretically deduced and verified to be the result of original complex face matrix 2DPCA multiplied by a random binary matrix. The resulting value does not change after scrambling given that only the row of the original 2DPCA is scrambled in the process. The nearest neighbor classifier based on Manhattan distance is then employed to calculate the recognition rate, that is, the distance between the tested face images and all training samples, and the training sample category that corresponds to the minimum distance is taken as the category. **Result** The experimental results obtained for the four face databases reveal that after scrambling the original face and structural feature images by using a random binary matrix, the human eye cannot detect useful information, and the scrambled results can be regenerated. Therefore, scrambling the random binary matrix can ensure the security of the proposed algorithm. Compared with three other algorithms, the fusion of a structural feature can effectively improve the recognition rate. Among the three structural features considered in this work, the variance feature obtains the highest recognition rate, which has increased by 4.9% on the Georgia Tech (GT) database, 2.25% on the Near Infrared (NIR) database, 2.25% on the Visible Light (VIS) database, and 1.98% on the YouTube Makeup YMU database. The employed random binary matrix does not affect the recognition rate, that is, the recognition rates of each database are the same before and after random scrambling. Given that the introduced random matrix is binary, the values do not change after random scrambling. The average testing time for the four face databases is within 1 millisecond. **Conclusion** A combination of the original face image with the structural features of the human face enriches the representation ability of face image information and helps improve facial recognition rate. A random permutation operation can also protect the privacy of the original face image. When the biometric template is leaked, resetting position 1 in the random binary matrix will re-scramble the complex face matrix and generate a new biometric template. The proposed algorithm also shows an excellent real-time performance and can meet the demands of practical application scenarios.

Key words: cancelable face recognition; random binary matrix; two-dimensional principal component analysis (2DPCA); face structural feature; complex matrix

0 引言

与其他生物特征识别技术相比,人脸识别因具有方便操作、非接触和接受度高等特点,已在公共安全领域和日常生活中得到广泛应用(Cai, 2018; Dantcheva 等, 2016)。每个人的脸图像具有唯一性,正是这种唯一性让大家认为人脸识别是安全的。在云计算和大数据时代,进行人脸识别时,需要将人脸图像上传到第三方服务器。这些人脸图像一旦泄

露,就不可避免地会面临模板攻击、假冒攻击等安全威胁。同时,无法更新和修改的人脸图像将不适合再在人脸识别系统中应用,由此造成的人脸生物特征损失很难弥补。因此,如何有效保护人脸图像的隐私和安全,已成为生物特征识别领域的重要问题之一(Barni 等, 2015; Natgunanathan 等, 2018)。

为保护生物特征数据,Ratha 等人(2001)提出可撤销生物特征概念,将原始生物特征数据加密,作为生物特征模板放在数据库中。一旦生物特征模板受到攻击或者威胁,可通过修改外界因素重新发布

新的特征模板替换之前的生物特征模板。Soliman 等人(2018a)提出双随机相位加密用于可撤销虹膜认证方法,通过对眼睛的特征向量进行分数阶傅里叶变换,构建可撤销的生物特征模板。Jiang 等人(2016,2017)提出使用 Arnold 变换对人脸图像预处理,进行可撤销变换,但是 Arnold 变换具有周期性,这种方法的安全性有限。Rahulamathavan 等人(2012)提出在加密域进行局部 Fisher 判别分析的可撤销人脸识别方法,对人脸图像进行同态加密,用局部 Fisher 判别分析对加密人脸进行识别。但是同态加密运算复杂、抗噪声能力弱,不适合实际应用。Kaur 和 Khanna(2017)提出 log-Gabor 滤波器的可撤销人脸识别方法,基于 log-Gabor 相位和幅值模式生成可撤销二进制特征,利用用户特定的标记变量对生物特征数据进行变形,对原始人脸图像进行保护。Teoh 等人(2018)提出使用随机置乱 Maxout 变换构建可撤销人脸识别方法,首先利用随机二值矩阵将原始人脸图像置乱,然后用 Maxout 变换离散人脸特征,该方法能够保证人脸图像置乱前后识别率不变并对人脸图像加以保护。Kumar 等人(2018a)提出随机置乱 2 维主成分分析(random permutation two-dimensional principal component analysis, RP2DPCA)方法,将原始人脸图像经过随机二值矩阵进行置乱,然后用 2 维主成分分析进行人脸识别。此外, Kumar 和 Rawat(2020)提出随机置乱局部保留投影(random permutation locality preserving projection, RP-LPP)可撤销人脸识别方法。Kaur 和 Khanna(2019)提出随机斜率法生成可撤销生物特征模板,将生物特征和一些随机的用户特定数据映射为笛卡尔空间的点。通过计算通过这些特征点和随机点的直线的斜率和截距生成变换后的特征,从而对原始生物特征加以保护。Soliman 等人(2018b)提出基于双随机相位加密的可撤销人脸识别方法,首先对原始人脸图像进行尺度不变特征变换(scale-invariant feature transform, SIFT),对特征矩阵进行双随机相位加密,然后与原始人脸图像卷积,实现可撤销人脸识别。Taheri 等人(2015)提出基于光学图像加密和滤波器的方法,实现可撤销人脸识别。首先用双随机相位编码对人脸图像加密,然后采用光子分布掩模对加密图像进行信息约简,最后使用无约束最小平均相关能量滤波器(unconstrained minimum average correlation energy filter, UMACE)对解密人脸图

像进行识别。但是该方法随机丢失部分人脸图像信息,识别率受到很大影响。

随着深度学习的发展,国内外学者提出了与深度学习结合的可撤销人脸识别方法。Han 等人(2018)提出基于循环神经网络(recurrent neural network, RNN)的自联想记忆可撤销人脸识别方法,首先提取人脸特征进行训练,然后输入到自动联想记忆模型中生成参数作为生物特征模板代替原始人脸图像。Kumar 等人(2018b)提出一种基于深度卷积神经网络的可撤销人脸识别方法,首先给每个用户随机生成一串固定长度的二进制码,用 VGG (Visual Geometry Group)-Face CNN (convolutional neural networks)网络训练图像映射到生成的二进制代码。然后以分配给每个用户的二进制码作为输入,使用安全 Hash 算法生成 512 位的二进制码作为生物特征模板。章竖武等人(2019)提出卷积神经网络的人脸隐私保护识别方法,对人脸图像进行分块 Arnold 变换,然后用基于分块随机加扰的卷积神经网络模型直接对置乱后的人脸图像进行识别。该方法虽然减少了手工特征的提取量,且具有高识别率,但是存在需要较大的样本和训练时间长等不足。

上述算法主要是基于人脸图像的灰度值进行识别。通常,人眼在快速理解图像时对其结构特征更为敏感。为了保护人脸图像的隐私和安全,同时获得较高的识别率,本文提出一种融合结构特征的可撤销人脸识别算法。

1 本文算法

本文提出的融合结构特征的可撤销人脸识别算法包括 3 个步骤:1)对人脸图像提取结构特征并作为虚部分量,联合原始人脸图像构建复数矩阵。2)通过随机二值矩阵对复数矩阵进行置乱,对生物特征模板进行复数 2 维主成分分析提取特征向量。3)采用最近邻分类器计算识别率。如果生物特征模板受到攻击或者威胁,则可以重新生成随机二值矩阵得到新的生物特征模板,替换受到攻击或者威胁的生物特征模板,赋予人脸图像重新发布的能力。本文算法流程如图 1 所示。

1.1 人脸图像预处理

原始人脸图像中所表达的信息是有限的,为了提高人脸信息的表征能力。本文算法将人脸图像的

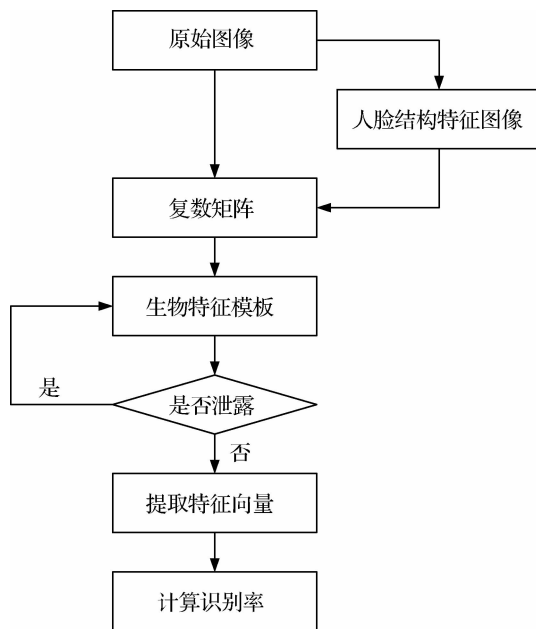


图1 算法流程图

Fig. 1 Flowchart of the proposed algorithm

结构特征与原始人脸图像结合构建新的人脸图像信息矩阵。该方法首先对人脸图像提取结构特征并作为虚部分量,然后以原始人脸图像为实部分量,结合成复数矩阵,其数学表达式为

$$\mathbf{F} = \mathbf{F}_y + \mathbf{F}_t i \quad (1)$$

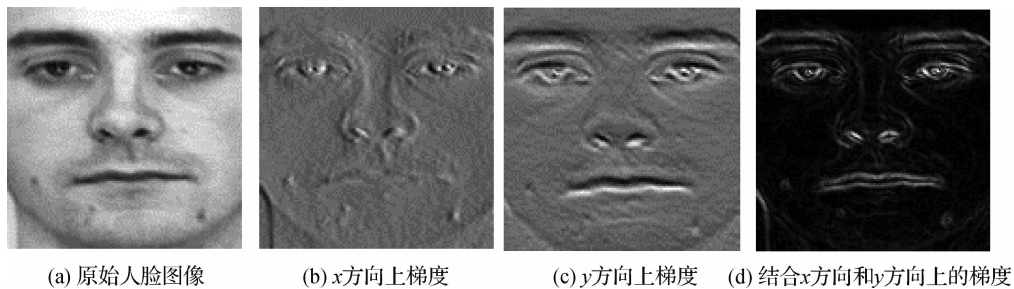


图2 人脸图像梯度

Fig. 2 Gradient of face image ((a) original face image;

(b) gradient in the x direction; (c) gradient in the y direction; (d) combining the x and y directions)

1.1.2 局部二值模式

在计算局部二值模式 (LBP) 时,使用尺寸为 3×3 的算子,以中心像素点的像素为阈值,然后将中心像素点与相邻的其他 8 个像素点按顺序进行比较,得到一组二进制码,然后转成十进制代替中心像素点的值来反映该区域的纹理信息。

LBP 在 3×3 图像块中心点的值计算为

$$f_{\text{LBP}} = \sum_{n=0}^7 h(x_n - x_c) 2^n, h(t) = \begin{cases} 1 & t \geq 0 \\ 0 & t < 0 \end{cases} \quad (5)$$

式中, $\mathbf{F}$ 表示复数人脸矩阵, $\mathbf{F}_y$ 表示原始人脸图像, $\mathbf{F}_t$ 表示结构特征图像, i 表示虚部单位。本文算法提取了人脸图像的梯度、局部二值模式 (local binary pattern, LBP) 和局部方差。

1.1.1 图像梯度

对于一幅 2 维灰度人脸图像 $f(x, y)$, 像素点 (x, y) 处的梯度表示在位置 (x, y) 处 f 的最大变化率方向,具体定义为

$$\nabla f = \frac{\partial f}{\partial x} \hat{i} + \frac{\partial f}{\partial y} \hat{j} \quad (2)$$

式中, $\hat{i}$ 和 $\hat{j}$ 分别表示该像素点在 x 和 y 方向上的梯度,向量 ∇f 的幅度值表示为 $M(x, y)$,即

$$M(x, y) = \sqrt{g_x^2 + g_y^2} \quad (3)$$

$$g_x = \frac{\partial f}{\partial x}$$

$$g_y = \frac{\partial f}{\partial y}$$

式中, g_x 是人脸图像 x 方向上梯度, g_y 是人脸图像 y 方向上梯度。 $M(x, y)$ 是与原始人脸图像尺寸相同的图像,它是梯度向量方向变化率在 (x, y) 处的值,称为图像梯度,图 2 给出了不同方向的人脸图像梯度。本文算法中,使用绝对值运算计算人脸图像梯度,即

$$M(x, y) \approx |g_x| + |g_y| \quad (4)$$

式中, x_n 和 x_c 分别表示周围像素和中心像素。LBP 示意图和人脸图像的 LBP 分别如图 3 和图 4 所示。

1.1.3 图像局部方差

对于灰度人脸图像,对应的局部方差为

$$V(I_{m,m}) = \frac{1}{m \times m} \sum_{p=1}^{m \times m} \left(v_p - \frac{1}{m \times m} \sum_{p=1}^{m \times m} v_p \right)^2 \quad (6)$$

式中, $m \times m$ 表示图像中每一像素点邻域尺寸, $I_{m,m}$ 表示分块尺寸, p 表示该分块中第 p 个像素点, v_p 表示该像素点的像素值。图 5 给出了不同邻域尺

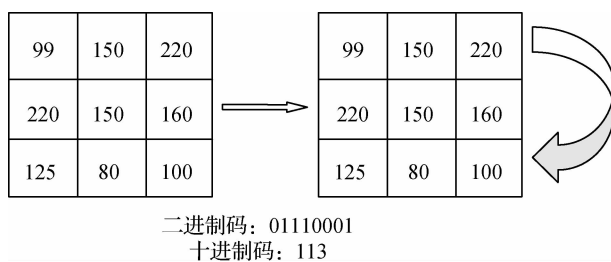


图3 LBP 示意图

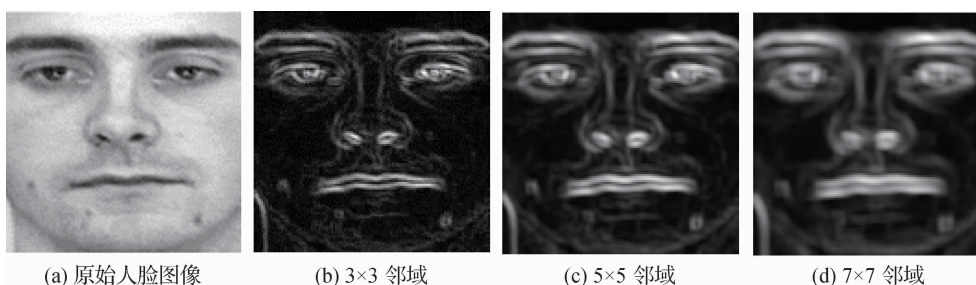
Fig.3 LBP schematic



(a) 原始人脸图像 (b) LBP

图4 人脸图像 LBP

Fig.4 LBP of face image((a) original face image; (b) LBP)



(a) 原始人脸图像 (b) 3×3 邻域 (c) 5×5 邻域 (d) 7×7 邻域

图5 人脸图像局部方差

Fig.5 Local variance of face image

((a) original face image; (b) 3 × 3 neighborhood; (c) 5 × 5 neighborhood; (d) 7 × 7 neighborhood)

寸的图像局部方差。

1.2 可撤销特征构建

对复数人脸矩阵进行复数2维主成分分析(complex two-dimensional principal component analysis, C2DPCA)。C2DPCA 的准则为 $J(W) = W^H S W$ (Yang 等, 2004), H 代表复数矩阵的转置, W 是 C2DPCA 的特征向量矩阵, S 为 C2DPCA 协方差矩阵。假设 A_i 代表复数人脸矩阵, 经过 C2DPCA 后的结果为

$$Y_i = A_i W \quad (7)$$

为使得人脸图像在视觉上不可见, 首先对复数人脸矩阵进行随机置乱, 即通过左乘、右乘每行每列有且只有一个1的随机二值矩阵。一旦生物特征模板泄露, 则可重新置乱随机二值矩阵中1的位置, 再次对复数人脸矩阵进行置乱, 生成新的生物特征模板。令 N 代表复数人脸矩阵的数量, 两个随机二值矩阵用 Q 和 R 表示。则置乱后的复数人脸矩阵可以表示为

$$A'_i = Q A_i R \quad (8)$$

置乱后复数人脸矩阵的平均值定义为

$$\begin{aligned} \bar{A}' &= \frac{1}{N} \sum_{i=1}^N A'_i = \frac{1}{N} \sum_{i=1}^N Q A_i R = \\ Q \left(\frac{1}{N} \sum_{i=1}^N A_i \right) R &= Q \bar{A} R \end{aligned} \quad (9)$$

式中, $\bar{A}$ 和 $\bar{A}'$ 分别表示置乱前后复数人脸矩阵的平均值。

协方差矩阵为

$$S' = \frac{1}{N} \sum_{i=1}^N (A'_i - \bar{A}')^H (A'_i - \bar{A}') \quad (10)$$

根据式(9)和式(10), 得

$$\begin{aligned} S' &= \frac{1}{N} \sum_{i=1}^N (Q A_i R - Q \bar{A} R)^H (Q A_i R - Q \bar{A} R) = \\ \frac{1}{N} \sum_{i=1}^N (Q (A_i - \bar{A}) R)^H (Q (A_i - \bar{A}) R) &= \\ \frac{1}{N} \sum_{i=1}^N R^T (A_i - \bar{A})^H Q^T Q (A_i - \bar{A}) R &= \\ R^T \left(\frac{1}{N} \sum_{i=1}^N (A_i - \bar{A})^H (A_i - \bar{A}) \right) R &= \end{aligned} \quad (11)$$

由此可得

$$S' = R^T S R \quad (12)$$

结合判决准则 $J(W) = W^H S W$, 则

$$J(W') = (W')^H S' W' = (R W')^H S R W' \quad (13)$$

因此可得

$$W' = R^T W \quad (14)$$

经过随机二值矩阵置乱后的复数人脸矩阵再进行 C2DPCA 的计算结果为

$$Y'_i = A'_i W' = Q A_i R R^T W = Q A_i W \quad (15)$$

分析式 (15) 可知, 置乱后复数人脸矩阵的 C2DPCA 的结果为原始复数人脸矩阵 C2DPCA 的结果左乘随机二值矩阵 Q 。由于矩阵 Q 的二值性, 得到的结果数值并没有改变, 只是原复数人脸矩阵 C2DPCA 结果的行置乱。

1.3 计算识别率

在计算识别率时, 采用基于曼哈顿距离的最近邻分类器对代表复数人脸矩阵的特征矩阵进行分类。两个尺寸均为 $m \times n$ 的特征矩阵 c_1 和 c_2 的曼哈顿距离定义为

$$d = \sum_{i=1}^m \sum_{j=1}^n |c_1(i, j) - c_2(i, j)| \quad (16)$$

对于待测的人脸图像, 分别计算其与所有训练样本之间的距离, 将最小距离对应的训练样本类别作为其类别。

2 实验结果与分析

2.1 数据库

为了验证本文算法的有效性和可行性, 使用 GT (Georgia Tech) (http://www.anefian.com/research/face_reco.htm)、NIR (Near Infrared)、VIS (Visible Light) (<http://biometrics.idealtest.org/>) 和 YMU (YouTube Makeup) (Dantcheva 等, 2012; Chen 等, 2013) (<http://www.antitza.com/makeup-datasets.html>) 4 个人脸数据库进行实验, 如表 1 所示。其中, GT 人脸数据库共 750 幅图像, 包含 50 个人, 每个人包含 15 幅不同表情、姿态下的彩色图像。NIR 人脸数据库共 400 幅图像, 包含 100 个人, 每个人包含 4 幅正面灰度图像; VIS 人脸数据库共计 400 幅图像, 包

含 100 个人, 每个人包含 4 幅正面彩色图像; YMU 人脸数据库是从 YouTube 化妆教程收集的图像, 共计 604 幅图像, 包含 151 个人, 每个人包含 4 幅图像, 化妆前 2 幅图像和化妆后 2 幅图像, 化妆程度不等并包含一些表情和姿势变化的彩色图像。实验中将所有人脸图像进行灰度化并根据眼睛位置裁剪为 64×64 像素, 70% 的人脸图像用来进行训练。

表 1 实验数据库

Table 1 Experimental databases

数据库	人数	总图像/幅	训练图像/幅	测试图像/幅
GT	50	15	10	5
NIR	100	4	3	1
VIS	100	4	3	1
YMU	151	4	3	1

2.2 可撤销性分析

通过实验分析随机置乱复数 2 维主成分分析 (random-permutation complex two-dimensional principal component analysis, RP-C2DPCA) 的识别率, 并与 C2DPCA 的结果进行比较。实验中, 对 4 个人脸数据库分别提取图像梯度、局部二值模式和局部方差, 计算图像局部方差的邻域尺寸为 3×3 。随机置乱结果如图 6 所示, 图 6(a) 和图 6(b) 分别为原始人脸图像和从原始人脸图像提取的 3×3 邻域局部方差, 图 6(c) 和图 6(d) 分别是经过随机二值矩阵置乱后的人脸图像和局部方差图像。显然, 原始图像和局部方差图像经过随机二值矩阵置乱后变得杂乱无章, 人眼无法察觉出任何相关的信息。

使用复数 2 维主成分分析和随机置乱复数 2 维主成分分析进行识别的结果如图 7 所示, 不同数据

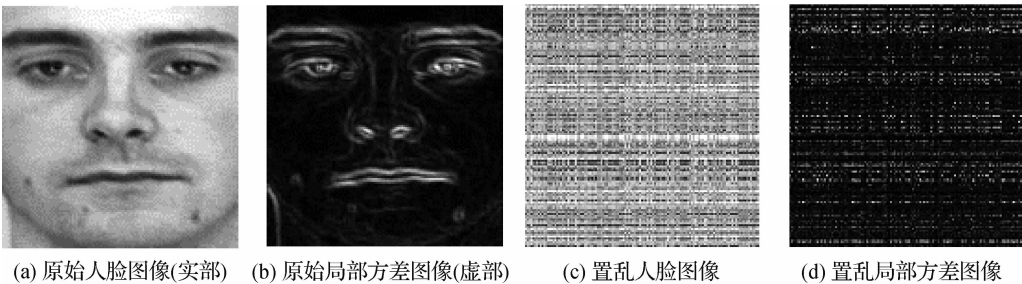


图 6 随机置乱结果

Fig. 6 The random permutation results ((a) original face image (real part); (b) original local variance image (imaginary part); (c) random permutation face image; (d) random permutation local variance image)

库的识别率在随机置乱前后一样。这是由于引入的随机矩阵具有二值性,随机置乱后数值并没有改变,只是原始复数人脸矩阵 C2DPCA 结果的行置乱。而且在进行人脸识别时使用相同的随机二值矩阵并不影响识别率。同时随机二值矩阵的置乱也说明了本文算法的安全性,原始人脸图像经随机二值矩阵置乱后变得杂乱无章,保护了原始人脸图像的隐私。以 64×64 像素的人脸图像为例,生成的随机二值

矩阵尺寸为 64×64 ,则原始人脸图像经过两个随机二值矩阵置乱以后共有 $64! \times 64!$ 种可能。在不知道随机二值矩阵的情况下,蛮力破解原始人脸图像则需要迭代 $64! \times 64!$ 次。此外,如果放在数据库中的生物特征模板不慎泄露,可以随时重新产生随机二值矩阵生成新的生物特征模板进行替代。因此,通过引入随机二值矩阵能够在不影响识别率的情况下,保护人脸图像信息的安全和具备可撤销性。

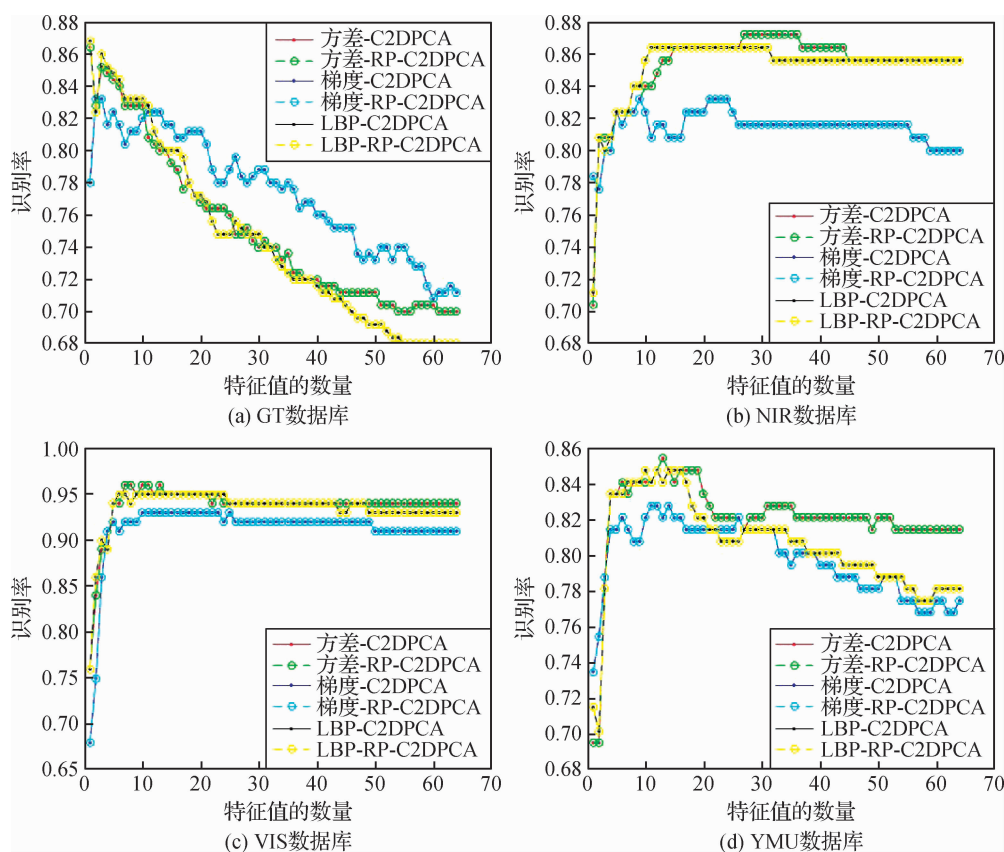


图7 RP-C2DPCA 和 C2DPCA 识别率比较

Fig. 7 Comparison of recognition rate between RP-C2DPCA and C2DPCA

((a) GT; (b) NIR; (c) VIS; (d) YMU)

2.3 局部方差邻域尺寸选择

为了分析邻域尺寸对识别率的影响,对4个人脸数据库使用不同尺寸的邻域计算局部方差并统计识别率,实验结果如图8所示。可以看出,对于同一人脸数据库,使用不同的邻域尺寸提取图像局部方差时得到的识别率不同;对于不同人脸数据库,最高识别率对应的邻域尺寸也不一样。因此,人脸图像局部方差邻域尺寸对识别率有一定影响,而且无法使用统一邻域尺寸计算图像局部方差,在实验时需要根据图像库的不同特点选择不同的邻域尺寸。本

文算法中,GT 数据库使用的邻域尺寸为 9×9 ,NIR 和 VIS 数据库使用的邻域尺寸为 7×7 ,YMU 数据库使用的邻域尺寸为 5×5 。

2.4 识别率比较

对使用不同结构特征的识别率进行分析并与基于随机置乱2维主成分分析(RP-2DPCA)算法(Kumar等,2018)、基于随机置乱局部保留投影(RP-LPP)算法(Kumar和Rawat,2020)和基于无约束最小平均相关能量滤波器(UMACE)算法(Taheri等,2015)的结果进行比较。图9给出了使用不同数量

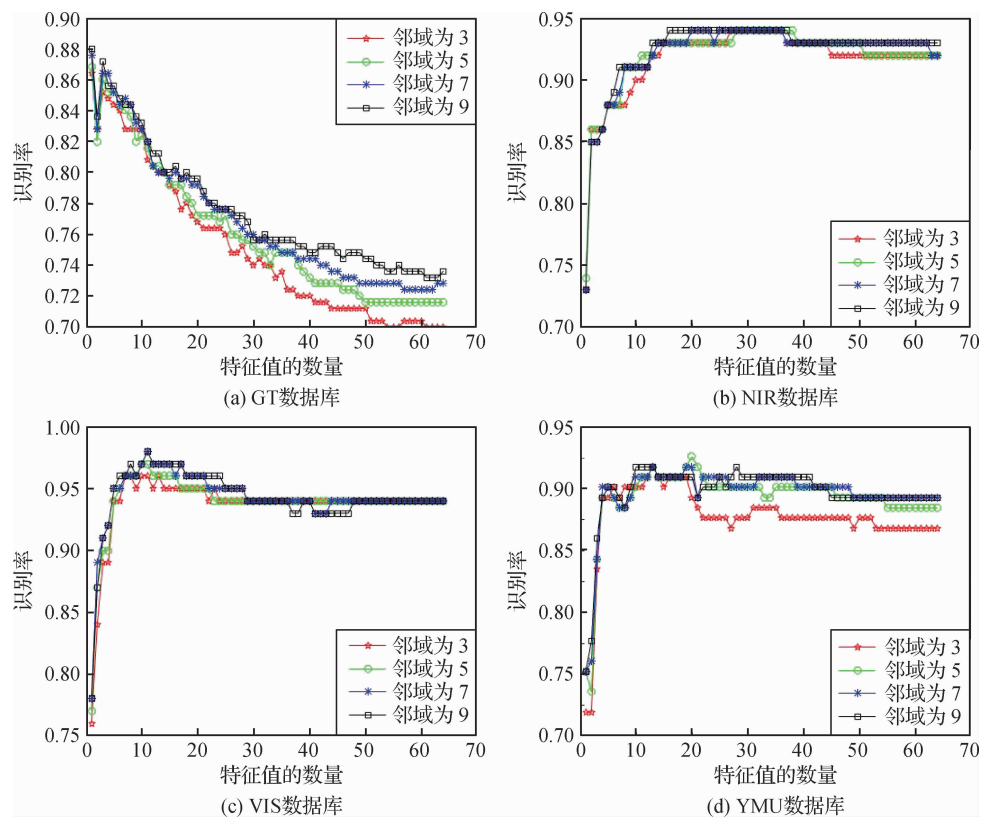


图8 不同图像局部方差识别率比较

Fig. 8 Comparison of recognition rate by using different local variance ((a) GT; (b) NIR; (c) VIS; (d) YMU)

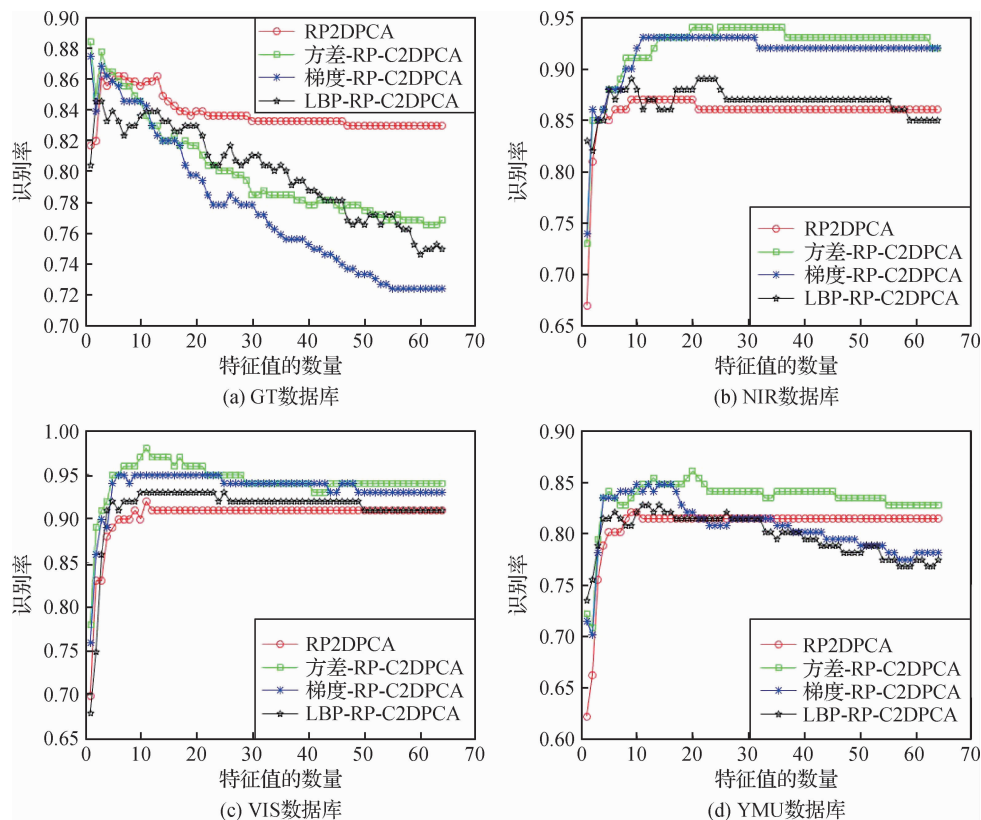


图9 不同方法识别率比较

Fig. 9 Comparison of recognition rate by using different methods ((a) GT; (b) NIR; (c) VIS; (d) YMU)

的特征值时,本文算法和基于随机置乱2维主成分分析(RP-2DPCA)算法的识别率变化,表2统计了不同方法的平均识别率。实验结果表明,与其他3种算法相比,本文算法在不同人脸数据库得到的识别率均为最高,在分别使用图像梯度、局部LBP和局部方差作为人脸图像的结构特征中,使用图像局部方差作为人脸图像的结构特征得到的识别率最高。

表2 平均识别率比较

Table 2 Comparison of average recognition rate

算法	数据库			
	GT	NIR	VIS	YMU
RP-2DPCA	85.80	95.75	94.25	85.93
RP-LPP	69.00	90.50	95.00	76.33
UMACE	67.80	91.25	91.75	78.14
梯度-RP-C2DPCA	88.90	97.75	95.00	87.09
LBP-RP-C2DPCA	87.60	96.00	96.50	87.58
方差-RP-C2DPCA	90.70	98.00	96.50	87.91

注:加粗字体表示各列最优结果。

2.5 算法时间统计

表3给出了使用图像局部方差作为人脸结构特征进行识别的运行时间,其中,训练时间为每个人脸数据库取得最高识别率对应的特征值数量,GT、NIR、VIS和YMU数据库的取值分别为1、20、11和20,共进行100次训练。GT、NIR、VIS和YMU数据库的局部方差的邻域尺寸分别为 9×9 、 7×7 、 7×7 和 5×5 。每个数据库测试时间的分别取与训练对应的特征值数量及方差邻域尺寸,共进行100次测试。分析NIR和YMU数据库的时间结果可知,在图像尺寸与所取特征值数量相同的情况下,训练时间和测试时间随着图像数量的增加而增加。通过

表3 算法时间统计

Table 3 Algorithm time statistics

数据库	/s			
	训练时间	平均训练时间	测试时间	平均测试时间
GT	477.944 5	4.779 445	5.420 175	0.000 217
NIR	248.757 9	2.487 579	5.714 996	0.000 571
VIS	245.166 7	2.451 667	4.923 348	0.000 492
YMU	399.804 8	3.998 048	11.832 180	0.000 784

NIR和VIS数据库的时间结果可以得到,在图像尺寸和数量相同的情况下,训练时间和测试时间随着特征值数量的增加而增加。实验中,4个人脸数据库的平均测试时间均在1.0 ms之内,表明该算法实时性强,能够满足实际应用场景的需求。

3 结论

本文提出一种融合结构特征的可撤销人脸识别算法,在实现人脸图像特征模板安全保护的同时提高了人脸识别率。根据原始人脸图像分别提取相应的梯度、局部二值模式和局部方差,并分别与原始图像融合为复数矩阵作为人脸图像的描述。同时,使用随机二值矩阵对复数人脸矩阵进行置乱。通过复数2维主成分分析表明,复数人脸矩阵置乱后的2维主成分分析结果等于原始复数人脸矩阵相应的结果左乘随机二值矩阵。换言之,置乱前后的数值并没有改变。如果生物特征模板受到攻击或者威胁,能够随时删除并重新产生随机二值矩阵生成新的生物特征模板。在不同人脸数据库上的实验结果表明,使用复数矩阵作为人脸图像的表征丰富了图像的信息,有利于提高人脸识别的精度。置乱后的人脸图像特征在视觉上无法察觉,起到保护人脸图像隐私和安全的作用,而且置乱前后的人脸识别率保持不变。其中,使用图像局部方差作为人脸图像的结构特征能够得到最高的识别率。另外,本文算法在4个人脸数据库的平均测试时间表明该算法实时性强,可以满足实际应用场景的需求。

然而,由于不同的人脸数据库存在光照、表情、姿态和化妆等因素的干扰,在提取人脸图像的局部方差特征时需要手动选取最佳的邻域尺寸和特征的数量。在今后的研究工作中,本文将考虑使用复数域的卷积神经网络,进一步提高算法的鲁棒性和识别率。

参考文献 (References)

- Barni M, Droandi G and Lazzeretti R. 2015. Privacy protection in biometric-based recognition systems: a marriage between cryptography and signal processing. *IEEE Signal Processing Magazine*, 32(5): 66-76 [DOI: 10.1109/MSP.2015.2438131]
- Cai R. 2018. Application of face recognition technology based on CA algorithm in intelligent residential property management. *Journal of Intelligent and Fuzzy Systems*, 35(3): 2909-2919 [DOI: 10.

- 3233/JIFS-169646]
- Chen C J, Dantcheva A and Ross A. 2013. Automatic facial makeup detection with application in face recognition//Proceedings of 2013 International Conference on Biometrics. Madrid, Spain: IEEE: 1-8 [DOI: 10.1109/ICB.2013.6612994]
- Dantcheva A, Chen C J and Ross A. 2012. Can facial cosmetics affect the matching accuracy of face recognition systems? //Proceedings of the 5th IEEE International Conference on Biometrics: Theory, Applications, and Systems, USA. Arlington: IEEE: 391-398 [DOI: 10.1109/BTAS.2012.6374605]
- Dantcheva A, Elia P and Ross A. 2016. What else does your biometric data reveal? A survey on soft biometrics. IEEE Transactions on Information Forensics and Security, 11(3): 441-467 [DOI: 10.1109/TIFS.2015.2480381]
- Han Q, Wu Z Y, Deng S Q, Qiao Z Q, Huang J J, Zhou J J and Liu J. 2018. Research on face recognition method by autoassociative memory based on RNNs. Complexity, 2018: #8524825 [DOI: 10.1155/2018/8524825]
- Jiang R, Bouridane A, Crookes D, Celebi M E and Wei H L. 2016. Privacy-protected facial biometric verification using fuzzy forest learning. IEEE Transactions on Fuzzy Systems, 24(4): 779-790 [DOI: 10.1109/TFUZZ.2015.2486803]
- Jiang R, Ho A T S, Cheheb I, Al-Maadeed N, Al-Maadeed S and Bouridane A. 2017. Emotion recognition from scrambled facial images via many graph embedding. Pattern Recognition, 67: 245-251 [DOI: 10.1016/j.patcog.2017.02.003]
- Kumar J A, Chalamala S and Kumar J S. 2018b. Face template protection using deep convolutional neural network//Proceedings of 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops. Salt Lake City, USA: IEEE: 462-470 [DOI: 10.1109/cvprw.2018.00087]
- Kaur H and Khanna P. 2017. Cancelable features using log-Gabor filters for biometric authentication. Multimedia Tools and Applications, 76(4): 4673-4694 [DOI: 10.1007/s11042-016-3652-3]
- Kaur H and Khanna P. 2019. Random Slope method for generation of cancelable biometric features. Pattern Recognition Letters, 126: 31-40 [DOI: 10.1016/j.patrec.2018.02.016]
- Kumar N and Rawat M. 2020. RP-LPP: a random permutation based locality preserving projection for cancelable biometric recognition. Multimedia Tools and Applications, 79(3): 2363-2381 [DOI: 10.1007/s11042-019-08228-2]
- Kumar N, Singh S and Kumar A. 2018a. Random permutation principal component analysis for cancelable biometric recognition. Applied Intelligence, 48(9): 2824-2836 [DOI: 10.1007/s10489-017-1117-7]
- Natgunanathan I, Mehmood A, Xiang Y, Hua G, Li G and Bangay S. 2018. An overview of protection of privacy in multibiometrics. Multimedia Tools and Applications, 77(6): 6753-6773 [DOI: 10.1007/s11042-017-4596-y]
- Rahulamathavan Y, Phan R C W, Chambers J A and Parish D J. 2012. Facial expression recognition in the encrypted domain based on local fisher discriminant analysis. IEEE Transactions on Affective Computing, 4(1): 83-92 [DOI: 10.1109/T-AFFC.2012.33]
- Ratha N K, Connell J H and Bolle R M. 2001. Enhancing security and privacy in biometrics-based authentication system. IBM Systems Journal, 40(3): 614-634 [DOI: 10.1147/sj.403.0614]
- Soliman R F, Amin M and El-Samie F E A. 2018a. A double random phase encoding approach for cancelable iris recognition. Optical and Quantum Electronics, 50(8): #326 [DOI: 10.1007/s11082-018-1591-0]
- Soliman R F, El Banby G M, Algarni A D, Elsheikh M, Soliman N F, Amin M and Abd El-Samie F E. 2018b. Double random phase encoding for cancelable face and iris recognition. Applied Optics, 57(35): 10305-10316 [DOI: 10.1364/AO.57.010305]
- Taheri M, Mozaffari S and Keshavarzi P. 2015. Cancelable face verification using optical encryption and authentication. Journal of the Optical Society of America A, 32(10): 1772-1779 [DOI: 10.1364/JOSAA.32.001772]
- Teoh A B J, Cho S and Kim J. 2018. Random permutation Maxout transform for cancellable facial template protection. Multimedia Tools and Applications, 77(21): 27733-27759 [DOI: 10.1007/s11042-018-5956-y]
- Yang J, Zhang D, Frangi A F and Yang J Y. 2004. Two-dimensional PCA: a new approach to appearance-based face representation and recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence, 26(1): 131-137 [DOI: 10.1109/TPAMI.2004.1261097]
- Zhang J W, Shen W and Wu Z D. 2019. Recognition of face privacy protection using convolutional neural networks. Journal of Image and Graphics, 24(5): 744-752 (章坚武, 沈炜, 吴震东. 2019. 卷积神经网络的人脸隐私保护识别. 中国图象图形学报, 24(5): 744-752) [DOI: 10.11834/jig.180444]

作者简介



孙浩浩, 1996年生, 男, 硕士研究生, 主要研究方向为计算机视觉。

E-mail: 2181002010@cnu.edu.cn



邵珠宏, 通信作者, 男, 副教授, 硕士生导师, 主要研究方向为多媒体信息安全与计算机视觉。

E-mail: zhshao@cnu.edu.cn

尚媛园, 女, 教授, 主要研究方向为图像处理和计算机视觉。

E-mail: sy@bao.ac.cn

陈滨, 男, 博士, 主要研究方向为图像处理、深度学习。

E-mail: chenbin@zjxu.edu.cn

赵晓旭, 女, 讲师, 主要研究方向为信号与图像处理。

E-mail: zhaoxiaoxu@cnu.edu.cn