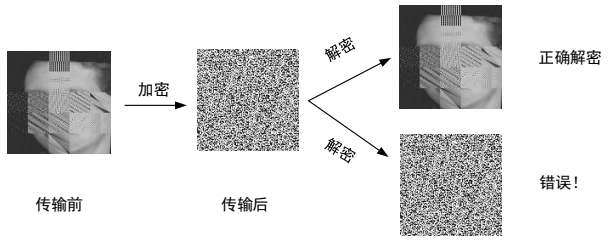
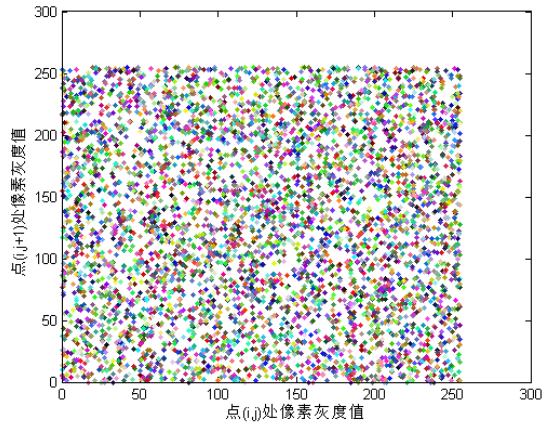
数构造 Arnold，如果需要对图像进行还原，必须要知道这 3 个参数。因此，使用本文的 Arnold 变换的方法可以增大破解置乱图片的难度。但同时为了通过深度神经网络进行识别，仍需要保留一定的相关性，若为如图 7（b）所示的相邻像素相关性，则很难从中提取到有效特征用于识别。

利用本文所提出的分块随机置乱可以取得较高的识别率，进一步考虑到安全性问题，在传输或存放到服务器上之前，对分块随机置乱后的图像进行二次加密并将密钥保存。如图 8（a）所示。图 8（b）是本文使用混沌加密后得到的相邻像素相关性图，由像素点之间的表现可知相关性得到进一步降低。但实验结果表明二次加密后很难从中提取到有效特征用于分类识别，识别率仅约为 20%。因此在允许牺牲少量安全性的前提下，本文方法具有很好的运用空间。



（a）二次加密示意图



（b）二次加密后相邻像素相关性图

图 8 二次加密示意及其相邻像素相关性图

Fig.8 Secondary encryption and its adjacent pixel correlation map. ((a) Secondary encryption diagram; (b) Adjacent pixel correlation after secondary encryption)

3 结　论

本文提出了一种基于分块随机置乱的深度神经网络模型，并结合加密技术应用于人脸隐私保护问题。实验表明，本文提出的方法不仅在特征提取和降维操作复杂度上优先传统人脸识别算法，且在训练样本少的情况下，仍能保持高识别率。其次，在进行分块置乱后，相邻像素点之间的相关性明显降低，由此达到隐私保护的目的。在未来的研究中，将进一步对 Arnold 算法进行深入研究，以期获得更大范围和更低相关度的隐私保护，同时进一步提高识别率。

参考文献(References)

[1] Chen W C. The research of biometric template protection based on chaotic encryption [D]. Beijing：Beijing Jiaotong University, 2014. [程维春. 基于混沌加密的生物特征模板保护研究[D]. 北京: 北京交通大学, 2014.]

[2] Jiang G H. The research of biometric encryption method based on fingerprint [D]. Xian：Xidian University, 2017. [蒋广涵. 基于指纹的生物特征加密技术研究[D]. 西安: 西安电子科技大学, 2017.]

[3] Gomez-Barrero M, Fierrez J, Galbally J, et al. Implementation of fixed-length template protection based on homomorphic encryption with application to signature biometrics[C]// 2016 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). Las Vegas, NV, USA: IEEE, 2016:259-266. [DOI: 10.1109/CVPRW.2016.39]

[4] Ngo D C L, Teoh A B J, Goh A. Biometric hash: high-confidence face recognition[J]. IEEE Transactions on Circuits & Systems for Video Technology, 2006, 16(6):771-775. [DOI: 10.1109/TCSVT.2006.873780]

[5] Teoh A B J, Goh A, Ngo D C L. Random

multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs[J]. IEEE Transactions on Pattern Analysis & Machine Intelligence, 2006, 28(12):1892-901. [DOI: 10.1109/TPAMI.2006.250]

[6] Juarez-Sandoval O, Fragoso-Navarro E, Cedillo-Hernandez M, et al. Improved unseen-visible watermarking for copyrigth protection of digital image[C] // 2017 5th International Workshop on Biometrics and Forensics (IWBF). Coventry, UK: IEEE, 2017:1-5. [DOI: 10.1109/IWBF.2017.7935084]

[7] Chen Z. Analysis and control of chaotic systems and their application in image encryption [D]. Changsha：Hunan University, 2018. [陈中. 混沌系统分析与控制若干问题及其图像加密的应用研究[D]. 长沙: 湖南大学, 2018.]

[8] Zhao Z H, Chen L. A context-aware recommendation method with multi-feature fusion based on fisher linear discriminant analysis [J]. Journal of Xian Jiaotong University, 2017, 51(8):40-46. [赵志华,陈莉.融合 Fisher 线性判别分析的多维特征融合情景感知推荐方法[J].西安交通大学学报,2017,51(08):40-46.] [DOI:10.7652/xjtuxb201708007]

[9] Xu J M, Li L. A face recognition algorithm based on sparse representation and support vector machine[J]. Computer Technology and Development, 2018, 28(02):59-63. [徐静妹, 李雷. 基于稀疏表示和支持向量机的人脸识别算法[J]. 计算机技术与发展, 2018, 28(02):59-63.] [DOI:10.3969/j.issn.1673-629X.2018.02.014]

[10] https://github.com/RiweiChen/FaceTools

[11] Sun N, Gu Z D, Liu J X. End-to-end trainable deep fusion network for facial age estimation [J]. Journal of Image and Graphics, 2018, 23(01): 133-143. [孙宁, 顾正东, 刘佶鑫,等. 面向人脸年龄估计的深度融合神经网络[J]. 中国图象图形学报, 2018, 23(01): 133-143.] [DOI:10.11834 / jig. 170305]

[12] Zou J C, Tie X Y. Arnold transformation of digital image with two dimensions and its periodicity [J]. Journal of North China University of Technology, 2000(01): 10-14. [邹建成, 铁小匀. 数字图像的二维 Arnold 变换及其周期性[J]. 北方工业大学学报, 2000(01):10-14.]

[13] Huang L Y, Xiao D G. The best image scrambling degree of binary image based on arnold transform [J]. Journal of Computer Applications, 2009, 29(2): 474-476, 483. [黄良永, 肖德贵. 二值图像 Arnold 变换的最佳置乱度[J]. 计算机应用, 2009, 29(2): 474-476, 483.]

[14] Xu Z, Feng C H. Modified convolutional neural network for small scale traffic image recognition [J]. Journal of Computer Applications, 2018, (3): 671-676. [徐喆, 冯长华. 用于小尺度交通图像识别的卷积神经网络改进[J]. 计算机应用, 2018, (3): 671-676.] [DOI:10.11772/j/issn.1001-9081.2017082054]

第一作者简介：

章坚武(1961-)，男，教授，博导。1999年7月获浙江大学通信与信息系统专业工学博士学位，主要研究方向为移动互联网、多媒体通信技术、网络安全等，主要研究成果获省部级科技进步二等奖二项。E-mail：jwzhang@hdu.edu.cn。

通讯作者：

沈炜，男，硕士研究生。主要研究方向为图象处理和模式识别，
E-mail：shenweiluck@126.com。

其他作者：

第三作者：

吴震东，男，副教授，主要研究方向信息安全，wzd@hdu.edu.cn。