激光与光电子学进展 先进成像

基于双随机相位编码的多特征人脸模板保护方法

张波[1,2*]，佟玉强[1]

[1]沈阳化工大学计算机科学与技术学院，辽宁 沈阳 110142；

[2]辽宁省化工过程工业智能化技术重点实验室，辽宁 沈阳 110142

摘要 针对单一特征模板保护算法效果较差以及存储前对模板保护不足等问题，提出一种多特征融合的人脸模板保护方法。该方法利用两种特征提取算法提取人脸不同的特征，实现多特征的融合保护，并在特征变换阶段将两种特征分别作为两个掩模，使用双随机相位掩模技术对原始图像进行加密。在存储前利用密钥生成思想从图像中直接获取密钥，并结合伴随矩阵性质，设计了一种改进分块幻方变换的置乱算法。为验证算法性能，采用ORL和EYaleB两个人脸数据库分别进行测试。结果表明，置乱算法的置乱度在ORL数据库可以达0.0194，在EYaleB数据库上可达0.0187，所提模板保护方法的识别率可分别达97.12%和96.90%。模板保护的三大特性不可逆性、可撤销性和不可链接性均表现良好。

关键词 模板保护；多特征；双随机相位编码；幻方变换

中图分类号 TP391.41 **文献标志码** A **DOI**：10.3788/LOP202259.1811005

Multifeature Face Template Protection Method Based on Double Random Phase Coding

Zhang Bo[1,2*], Tong Yuqiang[1]

[1]*College of Computer Science and Technology, Shenyang University of Chemical Technology, Shenyang* 110142, *Liaoning, China*;

[2]*Liaoning Key Laboratory of Industrial Intelligence Technology on Chemical Process, Shenyang* 110142, *Liaoning, China*

Abstract Herein, we propose a face template protection method based on multifeature fusion to solve the problems of the poor effect of a single feature template protection algorithm and insufficient template protection before storage. In this method, two feature extraction algorithms were employed to extract different face features to achieve multifeature fusion protection. Furthermore, both features were used as masks in the feature transformation stage. The original image was encrypted using the double random phase mask technology. Before storage, we designed an improved scrambled algorithm based on partitioned magic square transformation to obtain the key from the image using the idea of key generation and properties of the adjoint matrix. To verify the performance of the algorithm, two face databases, ORL and EYaleB, were used. The results show that the scrambling degree of the scrambled algorithm can reach 0.0194 and 0.0187 in the ORL and EYaleB databases, respectively, and the recognition rate of the proposed template protection method reaches 97.12% and 96.90%, respectively. The three characteristics of template protection, namely, irreversibility, revocability, and unlinkability, perform well.

Key words template protection; multi-features; double random phase encoding; magic square transformation

1 引 言

当前，生物特征信息从采集、存储到认证、使用都存在一些漏洞和风险，需要解决。生物特征数据采集的行业准入门槛过低，识别终端的可靠性有待完善，较高的数据存储安全性要求和特征数据使用权限问题等都会成为阻碍生物识别技术发展的障碍。可控的数据采集、优秀的算法、环境适应能力是解决这些问题的可行方案[1-2]。

人脸特征如今受到广泛应用。应用在人脸特征的

收稿日期：2021-08-18；**修回日期**：2021-09-10；**录用日期**：2021-09-24

基金项目：辽宁省教育厅科学研究项目(LJ2020023)、省博士科研启动基金(2019-BS-191)

通信作者：*zber@163.com

模板保护技术有许多方法，大致可分为基于特征变换、基于辅助数据、多特征融合、基于网络安全算法的保护方法4大类。其中，基于特征变换的方法的核心思想是把原始生物特征变换到另一个域中生成安全模板，这类算法的典型代表为生物哈希法[3-5]和不可逆函数变换法[6-7]。但这类方法在降维二值时易造成数据丢失，二值化[4]的阈值选取问题会直接影响整个特征模板的安全性。不可逆变换法是由Ratha等[6]提出的，其核心思想是利用不可逆函数的特性来实现对模板的加密保护。后人利用该思想设计了随机映射[8-9]、随机相位异或[10-11]以及Bloom过滤器[7]等方法。这类方法虽然可以有效抵御交叉攻击，但针对重放攻击表现不佳。基于辅助数据的保护方法以密钥释放、密钥绑定[12-15]和密钥生成[16-18]三类方法为代表。但由于该类方法需要外部密钥作为辅助数据，一旦密钥泄露会对模板安全造成威胁。多特征融合模板保护算法的安全性较单一特征的模板保护算法要高，无论是多模态[19-20]还是多特征[21-22]，攻击者获取多组生物特征中任一组特征也无法完成整个识别认证过程。另外，近几年部分研究者将网络安全领域的蜜罐[23]、同态加密[24]以及差分隐私技术[25]应用于模板保护领域。但这些方法的应用较少，对于能效性、安全性等算法性能测试的实验，论证数据不够充足。

综上所述，针对单一特征模板保护算法效果较差以及存储前对模板保护不足等问题，本文提取人脸的两个特征作为两个相位掩模，通过双随机相位编码技术对原始图像进行加密，并在存储数据库前利用密钥生成算法思想设计了一种改进的分块幻方置乱算法对生成的加密模板进行二次加密。实验结果表明，所提模板保护方法在达到了双重保护作用的同时能够满足人脸认证正确率的要求。

2　基本原理

2.1　双随机相位编码

双随机相位编码是一种光学加密技术，通过在信号上加上两个互不相关的相位掩模获得一个噪声信号，从而实现加密。设计的图像双随机相位编码加密方案为：图像f_1与第一相位掩模h_1相乘后进行快速傅里叶变换（FFT），然后将结果与第二相位掩模h_2相乘，最后对乘积结果再进行FFT得到加密图像f_2。方案的数学表达式为

$$f_2=\mathrm{FFT}\left\{\left[\mathrm{FFT}\left(f_1\times h_1\right)\right]\times h_2\right\},\tag{1}$$

式中：第一相位掩模$h_1=\mathrm{e}^{2\pi\mathrm{i}M_1}$，$M_1$为用户密钥；第二相位掩模$h_2$为图像的另一特征。

2.2　幻方变换

所使用的幻方变换规则[26]是以四阶幻方变换为基础的。四阶幻方变换主要有两种方法，第一种是对两对角线上的数字进行逆序变换，第二种是保持对角线上数字不动对其他数字进行互补交换。

通过上述变换，各个数字的位置发生了变化。因此，在图像处理领域幻方变换可使不同的像素坐标点位置发生变化，从而达到一个置乱的效果。如果图像维度较大，为提高效率，可采用分块变换的方法来达到置乱的目的。

3　所提方法内容

3.1　基于伴随矩阵性质的改进幻方变换置乱算法

通过前文的描述可以发现，原始的幻方变换中只是部分数字的位置发生了变化。如果这种变换规则应用于图像置乱领域，很容易导致图像的像素点的混乱程度较低，且与其他传统图像置乱算法一样具有周期性，经过多次变换才会恢复出原始图像。于是对两种四阶幻方变换方法的规则进行了整合，提出一种适用于本文人脸模板保护方法且置乱度较高的四阶幻方变换规则。表1和图1分别为改进的四阶幻方变换各阶段矩阵相邻位置相关度和在不同变换规则下的置乱度及其图像。先对四阶矩阵采用第二种四阶幻方变换规则（即保持对角线不动，其他数字进行互补交换），然后对四阶矩阵中每个2×2小矩阵进行对角线交换。

在4×4矩阵取得较好置乱效果后，将改进置乱算法引用至图像的置乱。以此为基础，提出的一种图像置乱加密算法具体过程如下。

1）对人脸图像进行分块处理，为节省存储行列式值矩阵的空间大小，先将整个图像分成m个$4n\times n$的小块，记作BLOCK1，对每个BLOCK1小块分别求取逆矩阵$\boldsymbol{A}^{-1}$和行列式值$|\boldsymbol{A}|$。

2）将BLOCK1块的行列式值$|\boldsymbol{A}|$放入到一个$\sqrt{m}\times\sqrt{m}$的二维数组$\boldsymbol{B}$中。将每个逆矩阵小块分成$n\times n$个4×4区域，记作BLOCK2，并使用四阶幻方的变换规则对每个BLOCK2内的元素进行移动；然后对这$n\times n$个BLOCK2整体进行同样变换操作；再对整个图像的m个BLOCK1小块也进行同样的操作，从而得到新的矩阵小块记为$\boldsymbol{A}'$；最后对该二维数组中的数字求取倒数，结果记作$\boldsymbol{B}_1$进行存储，并将其作为置乱图像还原时的密钥。

3）将二维数组$\boldsymbol{B}$中的元素依次与经过变换后的

表1　改进的四阶幻方变换各阶段矩阵相邻位置相关度

Table 1　Matrix adjacent position correlation at each stage of the improved fourth-order magic square transformation

Parameter	Original matrix	Unmodified transformation matrix	Improved transformation matrix
Degree of correlation between adjacent locations	−1.0000	0.3398	0.2653

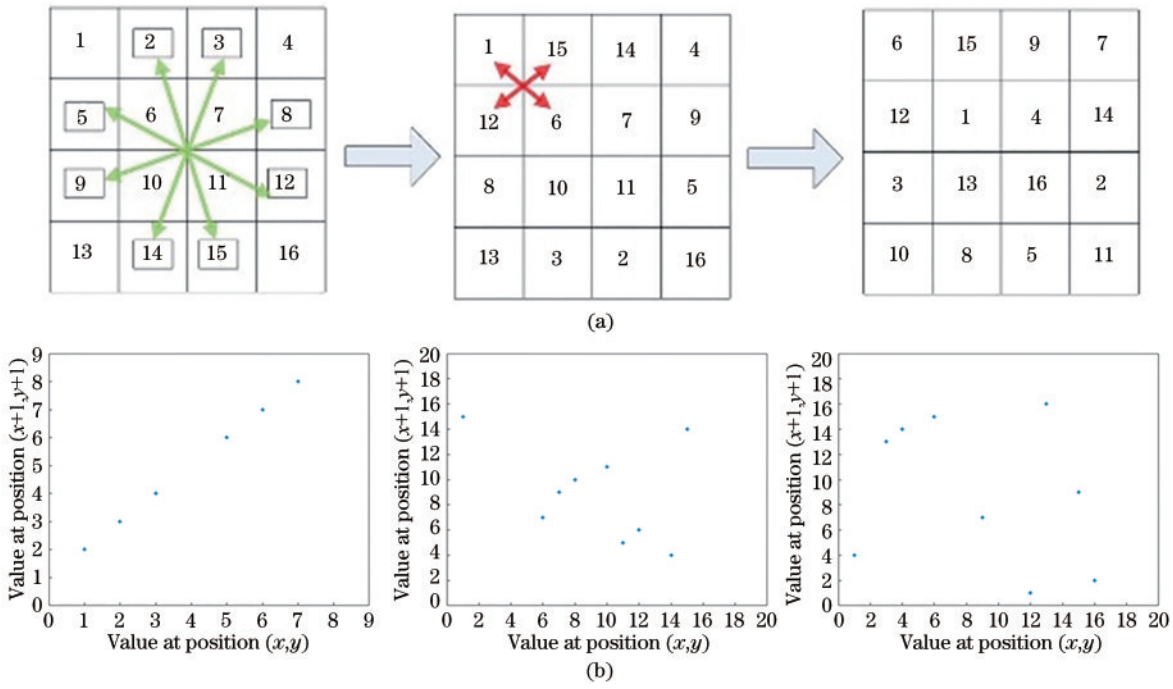

图 1　改进四阶幻方算法示意图及置乱图像。(a)改进的四阶幻方变换规则示意图;(b)改进的四阶幻方变换各阶段的置乱度图像

Fig.1　Schematic of improved fourth-order magic square algorithm and scrambled images. (a) Diagram of the improved fourth-order magic square transformation rules; (b) scramble degree images at each stage of the improved fourth-order magic square transformation

图像逆矩阵小块$\boldsymbol{A}'$相乘,得到加密的小块$\boldsymbol{C}$,例如$\boldsymbol{C}_1=\boldsymbol{A}_1'\times\boldsymbol{B}_{(1,1)}$,$\boldsymbol{C}_2=\boldsymbol{A}_2'\times\boldsymbol{B}_{(1,2)}$,$\boldsymbol{C}_3=\boldsymbol{A}_3'\times\boldsymbol{B}_{(1,3)}$,…,$\boldsymbol{C}_k=\boldsymbol{A}_k'\times\boldsymbol{B}_{(i,j)}$,以此类推。将得到的所有加密小块$\boldsymbol{C}$按分块时的顺序整合,就得到了最后的置乱加密图像。

在还原阶段,对每个做完变换的小块进行矩阵的逆运算后将各个小块整合,即得到了原始的图像。

3.2　所提方法流程

所提人脸模板保护方法利用局部二值模式(LBP)和方向梯度直方图(HOG)特征提取算法提取不同的特征,从而实现一个针对原始图像的多特征保护方案,并在存储数据库之前使用基于伴随矩阵性质的改进幻方变换置乱算法进行置乱,从而达到一个双重加密的作用。加密注册方案的具体流程如下。

首先,对人脸图像进行预处理,将图像维度调整为128×128,并对图像使用LBP算法和HOG算法分别提取特征。

然后,分别将提取的LBP特征和HOG特征记为$L(x,y)$和$H(x,y)$,并进行傅里叶变换(FT)部分调整整幅图像,将零频点移到频谱的中间;对LBP特征进行FFT后与第一相位掩模相乘,再进行FT;将结果与第二相位掩模(变换后的HOG特征)相乘,再进行FFT,得到最后的对原始图像的加密模板。该过程简单表示为

$$L'=L^{\mathrm{FT}}(x,y),H'=H^{\mathrm{FT}}(x,y),\tag{2}$$

$$Q(x,y)=\{[L'\times \mathrm{e}^{2\pi\mathrm{i}M(x,y)}]^{\mathrm{FFT}}\times H'\}^{\mathrm{FFT}},\tag{3}$$

式中:$M(x,y)$为用户设定的密钥;$Q(x,y)$为经过双随机相位编码后得到的加密模板。

最后,在存储数据库之前使用设计的基于伴随矩阵性质的改进幻方变换置乱算法对模板进行置乱加密。

认证阶段,首先采集用户的人脸信息并提取对应的算法;然后用户调取加密阶段存储的置乱密钥,将置乱模板还原,得到经过双随机相位编码后的模板;最后将该模板作傅里叶逆变换和去除相位操作后与待测图像模板进行比较,得出结果。

4　实验结果与分析

为检测所提方法的性能,采用ORL人脸图像数据库和EYaleB人脸图像数据库进行验证。ORL图库共有40个人脸,每人采集10张,共计400张人脸图像,数据库图像均为经过归一化处理的灰度图像,像素大小均为92×112,图像背景为黑色。EYaleB图库共有38个人脸,每人采集64张,像素大小均为168×192,图像均为黑色背景的灰度图像;根据人脸与摄像机的方向角(12°,25°,50°,77°,90°),将每人的64张照片分为5个部分,每人每个部分均为不同光照下的人脸图像,数目分别为7,12,12,14,19。在实验论证过程中,实验平台采用MATLAB R2016a和PyCharm。

4.1　置乱算法流程及性能分析

4.1.1　置乱算法性能分析

为分析置乱算法的性能,设计了三个实验来论证算法的可行性、稳定性及无周期性。

为测试所提置乱算法的可行性，分别在ORL人脸数据库和EYaleB人脸数据库中随机抽取一张人脸图像进行置乱还原实验，测试原始图像、置乱图像以及还原图像相邻像素点位置的相关性。相邻像素点以坐标为(x,y)和$(x-1,y-1)$的两点为标准，讨论位置的相关性，相关性的定义式为

$$\rho_{(x,y)}=\frac{\mathrm{cov}(x,y)}{\sqrt{d(x)}\times\sqrt{d(y)}},\tag{4}$$

其中：

$$\mathrm{cov}(x,y)=e(x)\times e(y)-e(xy),\tag{5}$$

$$d(x)=e^2(x)-e(x)\times e(x),\tag{6}$$

$$\begin{cases}e(x)=\dfrac{1}{N}\displaystyle\sum_{i=1}^{N}x(i)\\ e(xy)=\dfrac{1}{N}\displaystyle\sum_{i=1}^{N}[x(i)\cdot y(i)]\end{cases}。\tag{7}$$

图2和图3为所提置乱算法对从ORL数据库随机抽取的人脸图像的处理效果图及坐标点图像；图4和图5为所提置乱算法对从EYaleB数据库随机抽取的人脸图像的处理效果图及坐标点图像。

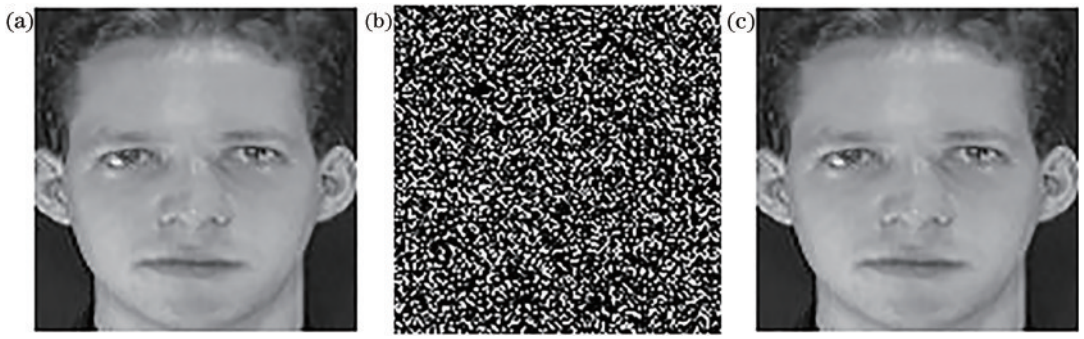

图2　ORL数据库置乱还原情况。(a)原始图像；(b)所提置乱算法置乱后的图像；(c)复原后的图像

Fig. 2　Scrambling restoration of ORL database. (a) Original image; (b) image scrambled by the proposed scrambling algorithm; (c) restored image

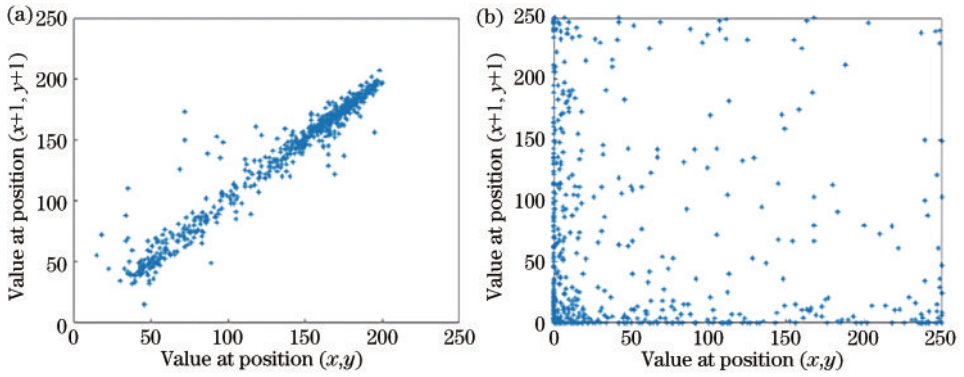

图3　ORL数据库像素点坐标图。(a)原始图像相邻位置点分布图；(b)置乱图像相邻位置点分布图

Fig. 3　Pixel point coordinate map in ORL database. (a) Distribution map of adjacent position points of the original image; (b) distribution map of adjacent position points of the scrambled image

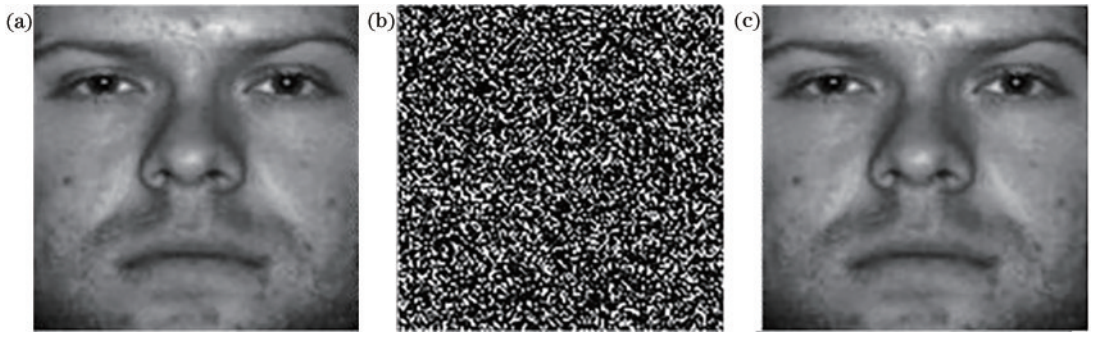

图4　EYaleB数据库置乱还原情况。(a)原始图像；(b)所提置乱算法置乱后的图像；(c)复原后的图像

Fig. 4　Scrambling restoration of EYaleB database. (a) Original image; (b) image scrambled by the proposed scrambling algorithm; (c) restored image

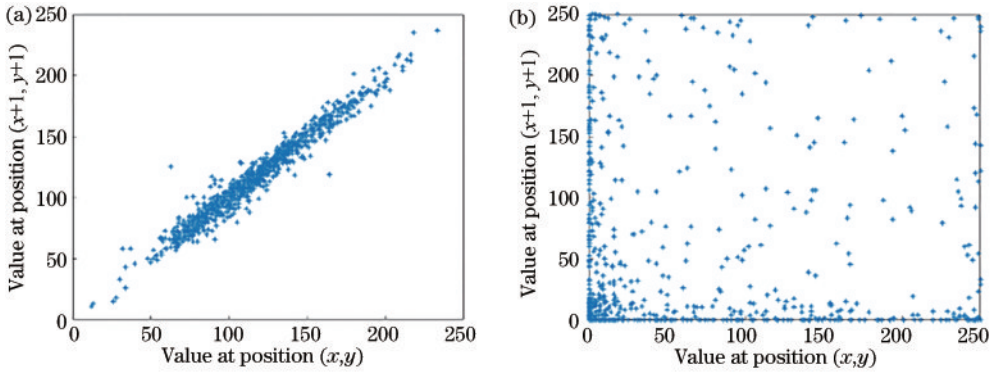

图 5　EYaleB 数据库像素点坐标图。(a)原始图像相邻位置点分布图;(b)置乱图像相邻位置点分布图

Fig. 5　Pixel point coordinate map in EYaleB database. (a) Distribution map of adjacent position points of the original image; (b) distribution map of adjacent position points of the scrambled image

为了测试所提置乱算法的稳定性,对两个人脸图像数据库中的人脸图像(共计 2843 张图像)进行置乱测试。为方便统计,对人脸图像得到的置乱均进行取绝对值处理,最终测试结果如图 6 所示,所提置乱算法稳定性良好。

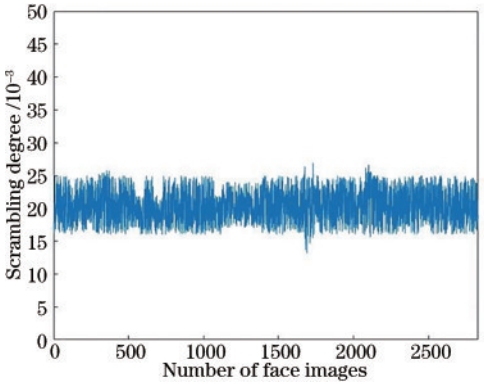

图 6　置乱度稳定图

Fig. 6　Scrambling stability map

为证明所提置乱算法的无周期性,设计了下列实验来进行辅助证明。

设

$$\boldsymbol{A}=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix},\ n\geqslant 2,\ n\in\mathbf{N}^{*},\ k\in\mathbf{N}^{*},$$

令 $\boldsymbol{B}_0=|\boldsymbol{A}|*\boldsymbol{A}^{-1}$, $\boldsymbol{B}_k=|\boldsymbol{A}|*\left(\boldsymbol{B}_{k-1}\right)^{-1}$, 若 $\boldsymbol{B}_k=\boldsymbol{A}$, 则该过程有周期性且周期为 k。

结合所提置乱算法,令 $n=4$,结果如表 2 所示,在实验中多次输入 k 值后,结果表明,$|\boldsymbol{A}|\boldsymbol{A}^{-1}$ 过程经过多次循环也无法得到原始矩阵。所以,推广证明到所提置乱算法可知,即使幻方变换算法具有周期性,但经过改进后的算法无法得到原始图像,不再具有周期性。

4.1.2　置乱算法比较分析

为了进一步证明所提置乱算法的有效性,对所提置乱算法、文献[27]中的算法、文献[28]中的算法、Arnold、Barker 以及原始幻方变换置乱算法在人脸图像数据库上进行置乱度对比。

表 2　周期性实验论证结果

Table 2　Periodic experimental demonstration result

k	Is it periodic
10	No
50	No
100	No
1000	No
2000	No

文献[27]中的算法和文献[28]中的算法是比较经典的将一维置乱算法应用于二维图像的方法。文献[27]中的算法的核心思想是利用 Logistic 混沌序列顺序改变图像中像素点的灰度值,从而实现图像置乱。文献[28]设计了两种洗牌置乱方案,一种是对行列坐标分别使用洗牌算法排序,另一种是直接洗牌置乱明文序列,并实验论证了后者的置乱度要好于前者。故本文将后者算法分别应用于 ORL 和 EYaleB 人脸数据库中进行测试,并与所提置乱算法进行对比。

对比实验的结果如表 3 所示。由对比结果可知:所

表 3　不同算法的对比结果

Table 3　Comparison result of different algorithms

Algorithm	Degree of correlation between adjacent locations
Original image (ORL)	0.9817
Original image (EYaleB)	−0.9822
Proposed algorithm (ORL)	0.0194
Proposed algorithm (EYaleB)	0.0187
Original magic square (ORL)	−0.3048
Original magic square (EYaleB)	0.1907
Barker (ORL)	−0.3310
Barker (EYaleB)	0.1729
Arnold (ORL)	0.2539
Arnold (EYaleB)	0.1221
Algorithm in Ref. [27]	0.0379
Algorithm in Ref. [28]	0.0183

提置乱算法的置乱程度相对较好，但与文献[28]中的算法相比置乱度有所下降；文献[28]中使用的基于洗牌思想的置乱算法需要使用外部序列以密钥形式作为变换规则，所提置乱算法采用密钥生成思想从图像中直接获得密钥，以极小的置乱度代价换取较高的安全度。

4.2　人脸模板保护方法流程及性能分析

4.2.1　模板保护方法识别性能测试及分析

为了提高所提方法的识别效率，结合测试图库的数据量、加密算法本身特性及时间效率等多方面因素设计了一个简化的深度学习 AlexNet 模型。该模型使用了一个卷积层和一个池化层，卷积核为 11×11，步长为 4。对两个人脸数据库得到的融合模板均按照 7∶3 分配训练集和测试集，并通过正确识别率（GAR）和等错误率（EER）两大指标对所提方法与其他方法进行比较。图 7 为两个数据库学习迭代次数与识别率的关系曲线。

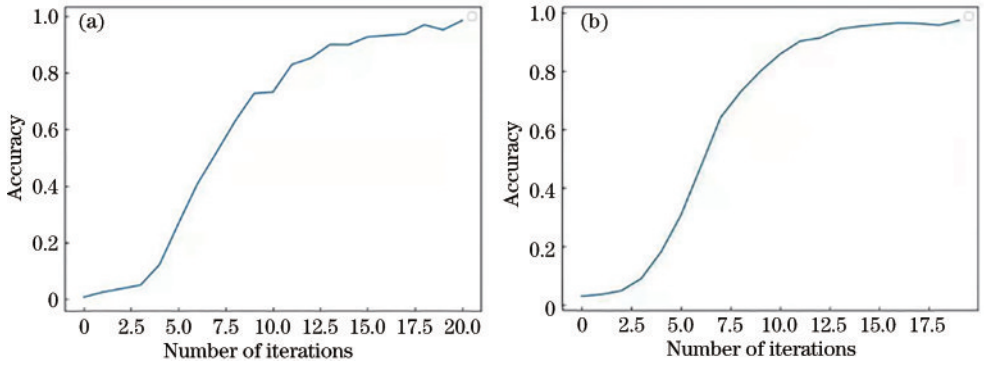

图 7　学习迭代次数与识别率的关系。(a) ORL 数据库；(b) EYaleB 数据库

Fig. 7　Relationship between number of iterations and recognition rate. (a) ORL database; (b) EYaleB database

表 4 和表 5 分别为不同方法的正确识别率和等错误率。与文献[29]中的方法和文献[30]中的方法这两个未进行模板加密的方法相比，所提方法在 ORL 人脸数据库上的识别率不相上下；与文献[21]中提到的单一人脸特征在不同辨别点个数的平均等错误率和文献[31]中的人脸不可逆变换保护算法的等错误率相比，所提方法均有明显减小；相比文献[21]中的方法需要采集人脸和人耳两个生物特征，所提方法使用人脸一个生物特征就实现多特征保护，可在信息采集阶段提升便利性。另外，在 EYaleB 人脸数据库上对所提方法进行验证过程中发现，较正常状态下采集的数据库（ORL 数据库），所提方法在 EYaleB 数据库上的识别率有所降低，但降低幅度仅为 0.22 个百分点。由于 EYaleB 人脸数据库是在不同角度和光照下采集的，说明所提方法的效率依然能够满足人脸识别的基本要求。

表 4　不同方法的识别率比较

Table 4　Comparison of recognition rate of different methods

Parameter	Method in Ref. [29]	Method in Ref. [30]	Proposed method (ORL)	Proposed method (EYaleB)
GAR /%	96.00	96.37	97.12	96.90

表 5　不同方法的等错误率比较

Table 5　EER comparison of different methods

Parameter	Method in Ref. [21]	Method in Ref. [31]	Proposed method (ORL)	Proposed method (EYaleB)
EER /%	11.85	14.53	10.97	11.02

4.2.2　模板保护方法安全性分析

目前公认的安全的模板保护方法需要具备三大特性，即不可逆性、可撤销性和不可链接性。

1）不可逆性要求从原始模板到加密模板的转换是不可逆的。所提模板保护方法的不可逆性可以从双随机相位编码和置乱算法两个方面讨论。首先，所提置乱算法较传统置乱算法的优势之一就是没有周期性，即在没有得到密钥的前提下，无法从置乱后的模板得到置乱前的模板。另外，在双随机相位编码的逆过程中，想要得到原始图像模板 f_1 必须同时得到两相位掩模 h_1 和 h_2，在缺乏求解参数的情况下，只能采取穷举法获得原始数据。由于密钥在 $[0, 2\pi]$ 上均匀分布，参与测试的图像经过处理后维度为 128×128，故利用穷举法得到原始图像数据的概率极小，仅为 $\left(314^{128\times128}\right)^{-1}$。综上所述，所提模板保护方法满足生物特征模板保护的不可逆性要求。

2）可撤销性要求当加密模板受损或者遭到泄露时可以撤销，然后新的模板可以重新发布。在所提模板保护方法中，当用户的模板遭到泄露时，存储人脸模板的数据库服务器可以删除泄露的模板。当模板泄露的用户重新注册模板时，两个相位掩模以及置乱算法

生成的密钥均会发生变化，从而生成新的模板。因此，所提模板保护方法满足生物特征模板保护的可撤销性要求。

3）不可链接性要求攻击者无法确定来自不同应用程序的两个模板是否对应于同一用户。为验证所提模板保护方法的不可链接性，对两个图库所有人脸图像均在不同密钥下进行变换并以巴氏系数（Bhattacharyya coefficient）为指标检测变换后两个模板的相似度，结果如图 8 所示。在两个模板上使用的随机生成的密钥分别为 0.816 和 0.543 时，EYaleB 人脸数据库生成的模板相似度均在 60% 以下，其中一半模板的相似度在 10% 以下，ORL 人脸数据库生成的模板相似度均在 50% 以下。故由此说明，所提模板保护方法符合模板保护算法的不可链接性。

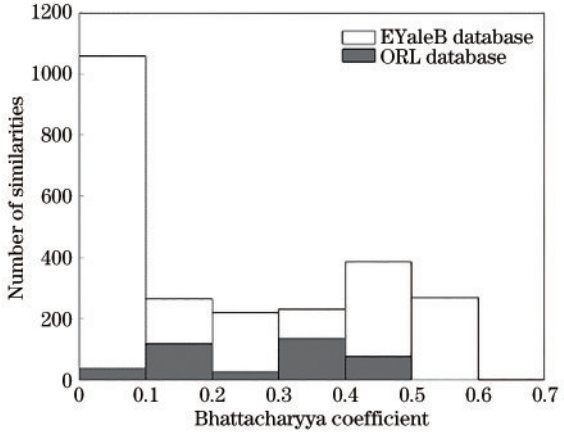

图 8　不同密钥下生成的两模板相似度个数分布图

Fig. 8　Similarity number distribution graph of two templates generated with different keys

5　结　　论

为解决人脸单一特征模板保护效果差以及模板存储前缺乏保护等问题，设计了一种双重人脸加密保护方法。首先对原始图像提取 LBP 和 HOG 两大特征，然后通过双随机相位编码对两特征进行加密，最后在存储数据库之前，使用一种基于伴随矩阵性质的置乱算法进行置乱加密。所提方法对人脸特征模板起到了双重加密保护的作用。经过实验证明，所提方法在 ORL 数据库上的识别率可达 97.12%，在 EYaleB 数据库上的识别率可达 96.90%，满足生物特征模板保护的三大特性，不可逆性、可撤销性和不可链接性，在实现模板保护的同时满足识别性能的需求。

但设计的方法依然存在两个缺陷，后续研究者可以此为方向继续研究：包括本文在内的大部分人脸模板算法处理的图像都是灰度图像，目前针对人脸的彩色模板保护算法研究还比较少；由于所提置乱算法中使用的伴随矩阵性质要求处理的矩阵必须为 $N\times N$ 维（其中 N 为 2^k）的方阵，这就需要对图像维度进行预处理，这就对算法的适应范围和时间效率造成影响。

参　考　文　献

[1] 毋立芳，马玉琨，周鹏，等. 生物特征模板保护综述[J]. 仪器仪表学报，2016，37(11)：2407-2420.
Wu L F，Ma Y K，Zhou P，et al. Review of biometric template protection[J]. Chinese Journal of Scientific Instrument，2016，37(11)：2407-2420.

[2] 王会勇，唐士杰，丁勇，等. 生物特征识别模板保护综述[J]. 计算机研究与发展，2020，57(5)：1003-1021.
Wang H Y，Tang S J，Ding Y，et al. Survey on biometrics template protection[J]. Journal of Computer Research and Development，2020，57(5)：1003-1021.

[3] Wang Y，Huang Y B，Zhang R，et al. Multi-format speech BioHashing based on energy to zero ratio and improved LP-MMSE parameter fusion[J]. Multimedia Tools and Applications，2021，80(7)：10013-10036.

[4] 王慧珊，张雪锋. 基于 BioHashing 的指纹模板保护算法[J]. 自动化学报，2018，44(4)：760-768.
Wang H S，Zhang X F. Improved BioHashing fingerprint template protection algorithms[J]. Acta Automatica Sinica，2018，44(4)：760-768.

[5] 许秋旺，张雪锋. 改进的 BioHashing 指纹模板保护算法[J]. 计算机应用与软件，2017，34(2)：256-261，303.
Xu Q W，Zhang X F. Improved BioHashing fingerprint template protection algorithm[J]. Computer Applications and Software，2017，34(2)：256-261，303.

[6] Ratha N K，Chikkerur S，Connell J H，et al. Generating cancelable fingerprint templates[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence，2007，29(4)：561-572.

[7] Rathgeb C，Breitinger F，Busch C. Alignment-free cancelable iris biometric templates based on adaptive bloom filters[C]//2013 International Conference on Biometrics (ICB)，June 4-7，2013，Madrid，Spain. New York：IEEE Press，2013.

[8] 丁勇，李佳慧，唐士杰，等. 基于随机映射技术的声纹识别模板保护[J]. 计算机研究与发展，2020，57(10)：2201-2208.
Ding Y，Li J H，Tang S J，et al. Template protection of speaker recognition based on random mapping technology[J]. Journal of Computer Research and Development，2020，57(10)：2201-2208.

[9] Rajasekar V，Premalatha J，Sathya K. Cancelable iris template for secure authentication based on random projection and double random phase encoding[J]. Peer-to-Peer Networking and Applications，2021，14(2)：747-762.

[10] 黄林茎，刘会，王志颖，等. 结合混沌映射与 DNA 计算的自适应图像加密算法[J]. 小型微型计算机系统，2020，41(9)：1959-1965.
Huang L Q，Liu H，Wang Z Y，et al. Self-adaptive image encryption algorithm combining chaotic map with DNA computing[J]. Journal of Chinese Computer Systems，2020，41(9)：1959-1965.

[11] Zhao D D，Fang S，Xiang J W，et al. Iris template protection based on local ranking[J]. Security and

Communication Networks, 2018, 2018: 4519548.

[12] Uludag U, Pankanti S, Jain A K. Fuzzy vault for fingerprints[M]//Kanade T, Jain A, Ratha N K. Audio- and video-based biometric person authentication. Lecture notes in computer science. Heidelberg: Springer, 2005, 3546: 310-319.

[13] 袁立, 李文明. 基于模糊保险箱的人脸: 人耳融合模板保护[J]. 工程科学学报, 2015, 37(9): 1225-1229.
Yuan L, Li W M. Face and ear fusion template protection based on fuzzy vaults[J]. Chinese Journal of Engineering, 2015, 37(9): 1225-1229.

[14] Liao Y F. Template calibration parameter optimization of fuzzy vault method[J]. International Journal of Pattern Recognition and Artificial Intelligence, 2020, 34(7): 2059020.

[15] Ferhaoui Cherifi C, Deriche M, Hidouci K W. An improved revocable fuzzy vault scheme for face recognition under unconstrained illumination conditions[J]. Arabian Journal for Science and Engineering, 2019, 44(8): 7203-7217.

[16] Mahendran R K, Velusamy P. A secure fuzzy extractor based biometric key authentication scheme for body sensor network in Internet of Medical Things[J]. Computer Communications, 2020, 153: 545-552.

[17] 李亚楠, 张雪锋. 基于安全概略的可撤销掌纹模板生成算法[J]. 计算机工程与应用, 2018, 54(18): 115-120.
Li Y N, Zhang X F. Cancelable palmprint template method based on secure sketch[J]. Computer Engineering and Applications, 2018, 54(18): 115-120.

[18] Li Y N, Zhang X F. Generation algorithm of revocable palmprint template based on safety profile[J]. Computer Engineering and Applications, 2018, 54(18) :115-120.

[19] 杨雪鹤, 刘欢喜, 肖建力. 多模态生物特征提取及相关性评价综述[J]. 中国图象图形学报, 2020, 25(8): 1529-1538.
Yang X H, Liu H X, Xiao J L. Extraction and relevance evaluation for multimodal biometric features[J]. Journal of Image and Graphics, 2020, 25(8): 1529-1538.

[20] 彭加亮. 基于手指多模态生物特征的身份认证关键问题研究[D]. 哈尔滨: 哈尔滨工业大学, 2014.
Peng J L. Research on key issues of multi-modal biometric verification based on finger[D]. Harbin: Harbin Institute of Technology, 2014.

[21] 袁立, 李文明, 穆志纯. 人脸人耳多模态生物特征模板保护方法研究[J]. 仪器仪表学报, 2012, 33(12): 2767-2773.
Yuan L, Li W M, Mu Z C. Face and ear multimodal biometric template protection[J]. Chinese Journal of Scientific Instrument, 2012, 33(12): 2767-2773.

[22] 曹洁, 赵修龙, 王进花. 融合改进指尖点和Hu矩的手势识别[J]. 计算机工程与应用, 2017, 53(21): 138-143, 194.
Cao J, Zhao X L, Wang J H. Gesture recognition method based on improved finger tip and Hu moments[J]. Computer Engineering and Applications, 2017, 53(21): 138-143, 194.

[23] Yang B, Martiri E. Using honey templates to augment hash based biometric template protection[C]//2015 IEEE 39th Annual Computer Software and Applications Conference, July 1-5, 2015, Taichung, Taiwan, China. New York: IEEE Press, 2015: 312-316.

[24] Yasuda M. Secure Hamming distance computation for biometrics using ideal-lattice and ring-LWE homomorphic encryption[J]. Information Security Journal: A Global Perspective, 2017, 26(2): 85-103.

[25] Arif M, Chen J E, Wang G J, et al. Privacy preserving and data publication for vehicular trajectories with differential privacy[J]. Measurement, 2021, 173: 108675.

[26] 胡克亚, 王君, 王莹. 基于分块压缩感知和改进幻方变换的图像加密[J]. 激光技术, 2019, 43(4): 96-102.
Hu K Y, Wang J, Wang Y. Image encryption based on block compression sensing and the improved magic square transformation[J]. Laser Technology, 2019, 43(4): 96-102.

[27] 李凯, 张婷. Logistic映射在数字图像加密算法中的应用[J]. 信息通信, 2017, 30(1): 139-140.
Li K, Zhang T. Application of logistic mapping in digital image encryption algorithm[J]. Information & Communications, 2017, 30(1): 139-140.

[28] 赵尹. 基于洗牌算法的混沌系统图像加密[D]. 淮南: 安徽理工大学, 2019.
Zhao Y. Image encryption of chaotic system based on shuffle algorithm[D]. Huainan: Anhui University of Science & Technology, 2019.

[29] 姚立平, 潘中良. 基于改进的HOG和LBP算法的人脸识别方法研究[J]. 光电子技术, 2020, 40(2): 114-118, 124.
Yao L P, Pan Z L. Research on face recognition method based on improved HOG and LBP algorithms[J]. Optoelectronic Technology, 2020, 40(2): 114-118, 124.

[30] 王燕, 李鑫. 基于LDP特征和贝叶斯模型的人脸识别[J]. 计算机科学, 2017, 44(12): 283-286, 291.
Wang Y, Li X. Face recognition based on LDP feature and Bayesian model[J]. Computer Science, 2017, 44(12): 283-286, 291.

[31] 毋立芳, 江思源, 肖鹏, 等. 基于人脸模板保护的不可逆变换方法[J]. 信号处理, 2012, 28(7): 1006-1013.
Wu L F, Jiang S Y, Xiao P, et al. Noninvertible transformation schemes for face template protection[J]. Signal Processing, 2012, 28(7): 1006-1013.