# 基于可撤销人脸的模糊保险箱算法研究与实现

张 波[1,2],贺楚博[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**:针对传统人脸特征识别系统安全性问题,提出了一种可撤销人脸的模糊保险箱算法。解决了由于模糊保险箱方案中存在真实细节点信息,导致人脸特征不安全的问题。在进行特征模板加密过程前,先用正交随机矩阵加密,加密后的模板具有可撤销性,不存储真实细节点信息,增强了系统的安全性。并在解密过程中的解码阶段,用 Berlekamp - Welch 解码算法代替 CRC 解码,该算法在解密阶段仅需根据解码集重构一次多项式,提高了算法的效率。改进后的模糊保险箱算法在生物特征模板受到攻击或者泄露时,能够随时删除并重新产生新的正交随机矩阵,并生成新的生物特征模板,具有可撤销性和安全性。该方案基本流程分为四部分:2DGabor-PCA 特征提取、特征可撤销变换、模板加密、模板解密。在 ORL 人脸库进行测试,最佳识别准确率达到 96%,经过对比实验验证了该方法的有效性,能够满足生物模板保护方案所需的不可逆性和可撤销性。

**关键词**:模板保护;随机矩阵;模糊保险箱;特征提取;多项式;Berlekamp - Welch 解码
**中图分类号**:TP391 **文献标识码**:A **文章编号**:1673-629X(2022)06-0126-05
doi:10.3969/j.issn.1673-629X.2022.06.021

# Research and Implementation of Fuzzy Vault Based on Cancelable Face

ZHANG Bo[1,2], HE Chu-bo[1]
(1. School of Computer Science and Technology, Shenyang University of Chemical Technology, Shenyang 110142, China;
2. Liaoning Key Laboratory of Intelligent Technology for Chemical Process Industry, Shenyang 110142, China)

**Abstract**: Due to the security problem of traditional face recognition system, we propose a fuzzy vault algorithm for cancelable face, which solves the problem that the face features are not safe because of the existence of real minutiae information in the fuzzy vault scheme. Before the process of feature template encryption, orthogonal random matrix is used to encrypt. The encrypted template is revocable and does not store the real node information, which enhances the security of the system. In the decoding stage of the decryption, Berlekamp-Welch decoding algorithm is used to replace CRC decoding. In the decryption, the algorithm only needs to reconstruct the polynomial once according to the decoding set, which improves the efficiency of the algorithm. When the biometric template is attacked or leaked, the improved fuzzy safe algorithm can delete and regenerate a new orthogonal random matrix at any time, and generate a new biometric template, which is revocable and secure. The basic process of the scheme is divided into four parts: 2DGabor-PCA feature extraction, feature revocable transformation, template encryption and template decryption. In ORL face database, the best recognition accuracy is 96%. The experimental results show that the proposed method is effective and can meet the irreversibility and revocability of the biological template protection scheme.

**Key words**: template protection; random matrix; fuzzy vault; feature extraction; polynomial; Berlekamp-Welch decoding

## 0 引 言

随着信息化的快速发展,生物特征识别技术越加普遍,身份认证系统的安全性也随之被重视起来。目前生物特征识别技术包括[1-2]:指纹识别[3]、掌纹与掌形识别、虹膜识别[4]、人脸识别[5]、手指静脉识别、声音识别、签字识别、步态识别、键盘敲击习惯识别甚至

**收稿日期**:2021-07-09 **修回日期**:2021-11-11
**基金项目**:辽宁省教育科学研究项目(LJ2020023);辽宁省博士科研启动基金(2019-BS-191)
**作者简介**:张 波(1979-),女,博士,副教授,研究方向为生物特征识别和计算机视觉检测;贺楚博(1997-),女,硕士研究生,研究方向为生物特征识别。

DNA 识别等等。而其中运用最广泛的还是指纹识别和人脸识别,为保证这些生物特征的安全性,生物特征保护技术应运而生。

目前为止国内外学术领域上出现的比较经典的生物特征模板保护方案可以分为四大类[6],其中可逆变换法和不可逆变化法可以统称为基于特征变换的方法,密钥绑定(密钥再生)法和密钥生成法统称为基于特征加密的方法。

模糊保险箱算法属于密钥绑定法,是生物特征加密领域中经典的实用化方案之一[7],此方案包括加密和解密两个部分。此算法是由 Juels A 等人[8]首次提出来的,克服了模糊承诺方案中对特征向量要求有序的缺点。李芬等人[9]将私钥存储于用户智能卡中,再用模糊保险箱算法保护智能卡 PIN,双重保护了数字身份,对模糊保险箱算法的安全性进行了提高。张淑苗等人[10]用随机点和用户特征结合改进了多项式构造过程,提高了安全性并节约了存储空间。袁立等人将人脸和人耳特征进行融合,优化了单独人脸和人耳的识别率和误识率。王科俊等人[11]成功将模糊保险箱算法用到了指静脉上,取得了较好的准确度。Sujitha, V 等人[12]将指纹特征和掌纹特征进行融合并应用到模糊保险箱中,证明了多重生物识别系统的性能优于单一特征识别。Yang 等人[13]将带有拓扑代码的 Delaunay 四边形系统对指纹进行配准,获得更好的性能和安全性。Peng Li 等人[14]用哈夫曼编码技术对细节点的储存容量进行压缩,可以避免模糊保险箱方案的对准过程,提高了性能和安全性。张璐等人[15]改进了算法基点距离选取规则和细节点的提取范围,降低了算法的拒真率和认假率,具有实用性。人脸特征作为最广泛应用的生物特征之一[6],具有很强的应用性,使用起来更加的方便,所以对人脸特征的隐私和安全的保护也变得十分重要。虽然模糊保险箱算法非常流行,但其存在一些局限性:模糊保险箱不能保证算法的可撤销性,一旦遭到破坏,容易受到交叉匹配攻击。模糊保险箱算法的真实点在匹配阶段会暴露,攻击者容易恢复这些点。Clancy 等人[16]分析表明,对解锁点的编号进行统计分析的暴力攻击,很容易破坏保险箱的安全性。

为了解决上述问题,该文提出了一种改进的模糊保险箱算法,与原本的模糊保险箱算法相比,提高了算法的安全性和准确性。在该算法中,首先利用正交随机矩阵与人脸特征做置乱操作,将人脸特征进行可撤销变换加密。然后再把加密后的特征模板与混杂的干扰数据融合形成保险箱。这样攻击者很难从保险箱中获取真实的细节点,起到了加密作用,提高了算法的安全性。另外,在解码时用 Berlekamp – Welch 解码算法代替 16 位 CRC 解码[17],使算法更有效率。并且只有与之匹配的特征人脸才能成功解密,释放密钥。

## 1　算法基本原理

### 1.1　对人脸特征进行可撤销变换的基本原理

具体过程是先生成正交随机矩阵:

$$\boldsymbol{s}=\begin{bmatrix} s_{11} & s_{12} & \cdots & s_{1n} \\ s_{21} & s_{22} & \cdots & s_{2n} \\ \vdots & \vdots & & \vdots \\ s_{n1} & s_{n2} & \cdots & s_{nn} \end{bmatrix} \tag{1}$$

然后将人脸特征向量 $\boldsymbol{k}=[k_1,k_2,\cdots,k_n]$ 与正交随机矩阵的每一列分别做内积运算,进行置乱操作,生成加密后的人脸特征序列:

$$\text{imface}=[\text{face}_1,\text{face}_2,\cdots,\text{face}_n] \tag{2}$$

其中,

$$\text{face}_i=\sum_{j=1}^{n} s_{ji}k_j \tag{3}$$

最后将人脸特征序列做归一化处理,方便进行特征比对。人脸模糊保险箱算法是在模糊保险箱算法上实现的更实用化的一种算法[18]。该算法是通过人脸图像信息达到了密钥信息和个人身份特征相互绑定的目的。基本原理是先将生物特征数据和随机密钥进行结合,经过一系列的变换存入数据库中,待认证模板经过反变换与数据库进行比对,比对成功则释放密钥。

### 1.2　Berlekamp–Welch 解码

Reed–Solomon 编码简称 RS 编码,是一种最大距离可分码[19]。其中,消息组向量记为 $\boldsymbol{m}$ :

$$\boldsymbol{m}=[x_1,x_2,\cdots,x_k],x_i\in f(p),i=1,2,\cdots,k \tag{4}$$

用定义在 $f(p)$ 上的多项式来表示这个消息组,即:

$$P(t)=\sum_{i=1}^{k} x_i t^{i-1} \tag{5}$$

由于 RS 解码的复杂度过于高,从一组多项式中能解码出一组系数,所以一共有 $C_n^k$ 种可能。CRC 解码方法由于其必须在拉格朗日插值中测试不同的可能子集[20],具有较高的计算成本。

所以使用 Berlekamp – Welch 算法进行解码,算法时间复杂度为 $o(n^2)$ ,此方法仅基于一个解码集,并且引入了一个队列,把当前步不确定是否要计算的步交给下一步,省去了不必要的计算。Berlekamp–Welch 可以高效地解码 BCH 码与 RS 码,该算法通常用来解码 RS 码。Nandakumark 等人评估了 33 个候选多项式,这些多项式在 Matlab 中运行需要大约 8 秒的计算时间。而 Berlekamp–Welch 算法基于一个解码集,只需要计算一个多项式即可。

Berlekamp–Welch 算法的关键方程组可表示为:

$$P(t)=\frac{N(t)}{E(t)} \tag{6}$$

其中，$P(t)$ 为已知的校验位多项式，$N(t)$ 为与错误大小相关的多项式，$E(t)$ 为错误辨认多项式。错误辨认多项式可以定义为：

$$E(t)=\prod_{j=1}^{l}(t-i_j) \tag{7}$$

其中，$i_j=1,2,\cdots,n$ 代表出错的符号的位置。设接收端收到的码为 $R$，对于所有的 i 来讲，$R_iE(i)=E(i)P(i)$。因为当 $R_i$ 为正确的码时，$R_i=P(i)$，当 $R_i$ 为错误的码时，$E(i)=0$ 等式依旧成立。

## 2 改进的人脸模板保护方法

改进后的人脸模糊保险箱算法流程分为特征加密和特征解密两个阶段。

### 2.1 加密过程

在特征提取阶段后，所有的特征 imface 都被用于构造模糊保险箱。加密过程时将密钥编码生成多项式。将特征提取后的人脸特征进行可撤销变换，方法是生成随机矩阵，将随机矩阵和人脸特征做置乱操作，最后把可撤销变换后的人脸特征在[-1,1]的范围内做归一化处理，将处理后的数据在多项式上进行投影，最后在保险箱中加入杂凑点生成保险箱。

具体步骤是在构造保险箱阶段，先随机生成密钥，将密钥分成 $d+1$ 个相等的分段，并对其编码生成多项式 $P$。其中，$d$ 为多项式 $P$ 的次数。将经过预处理后的人脸特征进行可撤销变换，先生成一个正交随机矩阵，再将经过 2 维 Gabor 小波和主成分分析后的人脸特征向量内积进行置乱操作，生成可撤销变换后的人脸特征模板。将人脸特征模板在 $P$ 上进行投影得到特征点集：

$$U=\{(d_i,P(d_i))\mid i=1,2,\cdots,N\} \tag{8}$$

其中，$N$ 为特征点的个数。

使用随机数生成器生成杂凑点，在模糊保险箱中加入杂凑点（$v_j$，$w_j$），杂凑点不能落在多项式上，且与真实点有一定的距离。将杂凑点和真实点无序地混合在一起形成了模糊保险箱，杂凑点个数要远远大于真实点个数，这样才能使模糊保险箱的安全性更高。

### 2.2 解密过程

解密过程是根据待认证的特征模板，如果待认证特征模板与注册模板大多数点重合，使用 Berlekamp-Welch 解码能成功获得密钥。

具体步骤是从待认证模板中提取细节点集 $C$，将待认证模板与保险箱中点集进行比对，从点集中选取一定数目的点，找出待解密的候选点集 $D$。候选点集的选取需要先设定一个阈值，对比保险箱中点集与待认证模板点集的最小欧氏距离，将距离小于设定阈值的点放入待解密的候选点集 $D$ 中，大于阈值的点看作是杂凑点进行删除，将所有数据过滤一遍最后得到候选点集 $D$。用 Berlekamp-Welch 解码对候选点集 $C$ 进行解码，解码成功串联获得密钥，解码失败证明该人脸模板和模糊保险箱中储存的人脸模板不匹配。

用 Berlekamp-Welch 解码[20]时，若 $(d+2e)<N'$，可以最多修正 e 个误差。所以在解码阶段需要备选 $N'\gg d$ 个点，使用 Berlekamp-Welch 算法重建多项式恢复密钥来进行解码，若至少有 $(N'+d)/2$ 个真实点，则解码成功，成功获取密钥。否则，解码失败。使用 Berlekamp - Welch 解码算法而不是用 CRC 解码方法是由于 CRC 解码方法具有较高的计算成本，CRC 解码需要在一定范围的备选点中选出 $d+1$ 个点用拉格朗日插值法构造多项式，构造多项式失败时需要在排除上一个点集，重新选取 $d+1$ 个点进行多项式重构，需要很高的时间成本。而 Berlekamp - Welch 解码算法只需在备选点中直接重构一次多项式，大大降低了时间成本。并且在构造模糊保险箱时，杂凑点和真实点不重合并有一定的距离，这使得在匹配过程中可以快速过滤大部分的杂凑点，提高了算法的正确接受率（GAR）并降低了算法的错误接受率（FAR）。并且可撤销模板的添加使得算法的安全性更高。

## 3 实验结果分析与讨论

### 3.1 图库选取

该算法是建立在 ORL[21]人脸库上进行的。ORL（Olivetti research laboratory）是英国剑桥大学 Olivetti 研究所制作的人脸数据库，如图 1 所示。

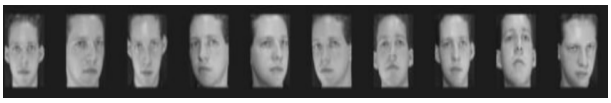

图 1 ORL 人脸图像库

该数据库共 400 幅人脸图像，其中包括每个人 10 幅图像，共 40 个人。每幅原始图像为 256 个灰度级，分辨率为 92 * 112。ORL 人脸图像是在不同时间、不同表情、各种视角和各种脸部细节的条件下拍摄的。该文选取此图库每个人的前 5 幅图像做训练样本。

### 3.2 人脸图像特征提取

模糊保险箱涉及真实点和杂凑点，真实点的横坐标代表生物特征模板。为了增加模糊保险箱的安全性，防止模糊保险箱泄露时泄露真实特征点，将二维 Gabor 小波后的特征进行 PCA 并将其转换为可撤销的特征点。

原始人脸图像能表达的信息有限，为了使人脸信息更加丰富，使用二维 Gabor 小波对人脸不同尺度和方向进行特征提取，二维 Gabor 小波变换对表情、曝光

度以及角度变换具有鲁棒性。图 2 所示为一幅人脸图像在 5 个尺度、8 个方向上的 40 个幅值图像。但是使用二维 Gabor 小波算法会造成维度过高的问题,为解决此问题还需对特征提取后的图像进行 PCA 降维,通过计算数据的均方差大小来获取高维数据的主要特征信息,去除冗余信息。

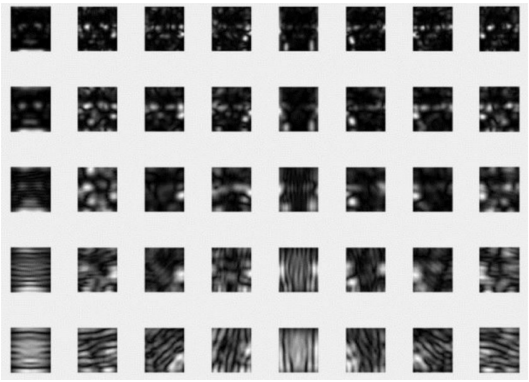

图 2　经过二维 Gabor 小波的人脸图像

将去除冗余后的特征模板先进行可撤销变换加密,对特征模板利用单向变换随机矩阵的每一列分别做内积,变换矩阵满足不可逆性、局部平滑等特征。加密后的人脸特征序列记为 imface,即 imface = $s \cdot k$,若特征模板 $k$ 被破坏,可利用随机生成的新的正交矩阵做变换生成新的可撤销特征模板,即 imface$'$ = $s' \cdot k$。由于 $s$ 的随机性,特征向量 imface 的特征点是独立的,所以暴力攻击变得十分困难。

### 3.3　安全性分析

将 ORL 人脸库中每人 5 幅共 200 幅人脸图像作为训练库进行加密分别保存到保险箱中,每人后 5 幅共 200 幅人脸图像作为验证库用于解密。理论上来说模糊保险箱的杂凑点( $v_j$ , $w_j$ )数目越多,模糊保险箱的安全性越高,因为杂凑点多的时候攻击者需要尝试的次数越多。但由于平面直角坐标的区域有限,杂凑点与真实点之间需要保持一定的距离,所以限制了杂凑点( $v_j$ , $w_j$ )的个数。实验得出结论杂凑点个数在 200 至 500 间实验效果最佳。

### 3.4　实验结果分析与讨论

为了全面评估该算法的准确性,选取了 3 种不同多项式长度和 3 种不同杂凑点分别进行了实验。实验结果分析用正确接受率(genuine accept rate,GAR)和错误接受率(false accept rate,FAR)来评价。

该文测试了在不同多项式长度和不同杂凑点个数下算法的安全性和准确性。如表 1 所示,当多项式阶数为 7( $d$ =7)杂凑点 200 到 300 时,算法的准确性最高,在增加杂凑点的同时,算法的安全性也会提高,但是算法的准确性会降低。如表 2 所示,当多项式阶数增加到 11 时,GAR 大幅下降。实验结果表明,当 $d$ 增大时,杂凑点个数增多时,GAR 减小。

表 1　不同多项式时算法的安全性和准确性

| $d$ | 杂凑点 | GAR/% |
|---|---|---|
| 7 | 200 | 96 |
| 7 | 300 | 96 |
| 7 | 400 | 94 |
| 9 | 200 | 90 |
| 9 | 300 | 90 |
| 9 | 400 | 86 |
| 11 | 200 | 77 |
| 11 | 300 | 77 |
| 11 | 400 | 66 |

在杂凑点为 300 时,分别计算三种不同多项式的错误接受率。其中 $d$ =11 时错误接受率最低,这是因为在 $d$ =7 时,入侵者会更容易找到模糊保险箱解码阶段恢复密钥所需的 8 个真实的点。在 $d$ 增加到 11 时,入侵者和用户本身都很难检索到 12 个真实的点去解锁模糊保险箱。所以 $d$ 值的增加会降低 GAR 和 FAR。

表 2　杂凑点为 300 时的算法准确率

| 杂凑点 | $d$ | GAR/% | FAR/% |
|---|---|---|---|
| 300 | 7 | 96 | 15 |
| 300 | 9 | 90 | 6 |
| 300 | 11 | 77 | 1 |

M. A. Dabbah 等人[22]提出的将原始生物特征被多项式并转换到安全域的可撤销模板保护算法中,其最佳结果达到96%的识别率。Hooda R 等人[18]提出了一种新的杂凑点生成方法,使用 20 个细节点,与 Clancy[16]的模糊保险箱算法识别率比较没有变化,GAR 为 90%,FRR 为 10%,FAR 为 9%。但是运行速度比传统的 Clancy 算法快,以 300 杂凑点为基础对比,Hooda R 等人提出的算法生成杂凑点方式需要 7.2 毫秒,传统方法需要 10.5 毫秒。文中算法在杂凑点生成方式上与传统方法比没有明显变化,但在解密过程中,由于 Berlekamp – Welch 解码算法在解码时仅根据一个解码集进行重构,大大降低了解密过程的运行时间。以 $d$ =7 时的两种方法执行时间做比较,传统方法需要 1 120 毫秒,文中算法需要 940 毫秒。并且由于可撤销模板的引进,文中算法的正确接受率与 Hooda R 等人提出的算法相比也有了明显的提升,最佳结果达到 96%(见表 3)。

表 3　不同加密算法准确率对比

| 文献 | 生物特征 | GAR/% | 时间/毫秒 |
|---|---|---|---|
| 文献[16] | 指纹 | 90 | |
| 文献[18] | 指纹 | 90 | |

续表 3

| 文献 | 生物特征 | GAR/% | 时间/毫秒 |
|---|---|---|---|
| 文献[22] | 人脸 | 96 | 1 120 |
| 文献[23] | 人脸 | 91 | |
| 该文 | 人脸 | 96 | 940 |

## 4 结束语

提出了在人脸模糊保险箱加密和解密过程中,将人脸特征先进行可撤销变换,提高保险箱的安全性,弥补了传统模糊保险箱的不足。在待识别人脸特征泄露时,攻击者也无法窃取或重构出原始人脸特征信息,并且可以随时删除并重新产生正交随机矩阵,生成新的待识别人脸特征模板。实验表明用正交随机矩阵进行置乱后的特征与原始特征相比有更好的正确接受率。在解码阶段用 Berlekamp – Welch 解码算法代替 CRC 解码算法,大大提高了算法的运行时间,并且与现有的缩短运行时间的算法相比,有着更高的准确率。

**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.

[2] 刘 畅. 加密人脸图像识别鲁棒算法研究[D]. 海口:海南大学,2018.

[3] PERALTA D,TRIGUERO I,SANCHEZ-REILLO R,et al. Fast fingerprint identification for large databases[J]. Pattern Recognition,2014,47(2):588-602.

[4] 刘笑楠,张文云,高艳娜. 局部置乱结合双随机相位编码的双虹膜身份模板保护方法[J]. 仪器仪表学报,2020,41(6):233-239.

[5] 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.

[6] 马玉琨. 基于人脸的安全身份认证关键技术研究[D]. 北京:北京工业大学,2018.

[7] 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.

[8] JUELS A,SUDAN M. A fuzzy vault scheme[J]. Des Codes Crypt,2006,38:237-257.

[9] 李 芬,刘 泉,庞辽军,等. 基于 Fuzzy Vault 的身份认证[J]. 武汉理工大学学报,2011,33(3):161-164.

[10] 张淑苗,张书晔,冯 全,等. 模糊保险箱的多项式表示方法[J]. 计算机工程,2011,37(23):147-148.

[11] 王科俊,曹 逸,姜博威,等. 基于纠错码的指静脉加密算法[J]. 智能系统学报,2017,12(1):55-59.

[12] SUJITHA V,CHITRA D. A novel technique for multi biometric cryptosystem using fuzzy vault[J]. Journal of Medical Systems,2019,43(5):112.

[13] YANG Wencheng, HU Jiankun, WANG Song. A delaunay quadrangle-based fingerprint authentication system with template protection using topology code for local registration and security enhancement[J]. IEEE Trans. Information Forensics and Security,2014,9(7):1179-1192.

[14] LI Peng,YANG Xin,CAO Kai,et al. An alignment-free fingerprint cryptosystem based on fuzzy vault scheme[J]. Journal of Network and Computer Applications,2010,33(3):207-220.

[15] 张 璐,王金海,崔 军,等. 模糊保险箱算法的模板校准参数优化研究[J]. 计算机科学与探索,2017,11(9):1451-1460.

[16] CLANCY T C,KIYAVASH N,LIN D J. Secure smartcard based fingerprint authentication[C]//Proceedings of the 2003 ACM SIGMM workshop on biometrics methods and applications. [s. l. ]:ACM,2003:45-52.

[17] NANDAKUMAR K,JAIN A K,PANKANTI S. Fingerprint-based fuzzy vault: implementation and performance[J]. IEEE Transactions on Information Forensics and Security,2007,2(4):744-757.

[18] HOODA R,KAUR M. Novel chaff generation for fingerprint fuzzy vault[J]. British Journal of Mathematics & Computer Science,2015,10(3):1-9.

[19] 任 可. 针对 REED-SOLOMON 码的快速 CHASE 解码算法的研究[D]. 哈尔滨:哈尔滨工业大学,2008.

[20] CHERIFIC F,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.

[21] 杜海顺,李 昉,张 帆,等. 一种模糊双向最大间距准则人脸识别方法[J]. 仪器仪表学报,2011,32(5):1077-1082.

[22] DABBAH M A,WOO W L,DLAY S S. Appearance-based biometric recognition:secure authentication and cancellability[C]//2007 15th international conference on digital signal processing. Cardiff,UK:IEEE,2007:479-482.

[23] SAPKAL S,SHRISHRIMAL P,DESHMUKH R R. Face verification using scale invariant feature transform with template security[C]//2017 IEEE international conference on fuzzy systems (FUZZ-IEEE). Naples,Italy:IEEE,2017:1-5.