软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(5):1237−1250 [doi: 10.13328/j.cnki.jos.004594]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

PalmPhasor 算法性能的理论分析*

冷 璐[1,2], 黎 明[1], Andrew Beng Jin TEOH[2], Cheonshik KIM[3]

[1](无损检测技术教育部重点实验室(南昌航空大学),江西 南昌 330063)

[2](School of Electrical and Electronic Engineering, Yonsei University, Seoul 120749, South Korea)

[3](Department of Digital Media Engineering, Anyang University, Seoul 430714, South Korea)

通讯作者: 黎明, E-mail: limingniat@hotmail.com, http://www.nchu.edu.cn

摘 要: 模板的安全性和隐私性是掌纹系统实际应用的关键问题,然而生物特征保护的多项指标通常相互冲突并且难以同时满足.作为解决上述冲突的一种可撤销掌纹编码算法,PalmPhasor 实现了高效、安全的掌纹认证.建立了系统分析 PalmPhasor 性能的完整框架.为了便于具体分析,将情景分为 4 种情况,并且提供了支持相应分析的预备知识,包括辅助定理以及 Gabor 滤波掌纹图像实部和虚部分布特性.在统计学基础上建立的理论分析和实验结果均表明:即使在用户口令被盗的情况下,多方向分数级融合增强的 PalmPhasor 算法也可以同时有效地满足可撤销生物特征的 4 项指标.

关键词: PalmPhasor 算法;理论性能分析;多方向分数级融合;掌纹认证;可撤销生物特征

中图法分类号: TP391

中文引用格式: 冷璐,黎明,Teoh ABJ,Kim C. PalmPhasor 算法性能的理论分析.软件学报,2015,26(5):1237−1250. http://www.jos.org.cn/1000-9825/4594.htm

英文引用格式: Leng L, Li M, Teoh ABJ, Kim C. Theoretical analysis on the performance of PalmPhasor algorithm. Ruan Jian Xue Bao/Journal of Software, 2015,26(5):1237−1250 (in Chinese). http://www.jos.org.cn/1000-9825/4594.htm

Theoretical Analysis on the Performance of PalmPhasor Algorithm

LENG Lu[1,2], LI Ming[1], Andrew Beng Jin TEOH[2], Cheonshik KIM[3]

[1](Key Laboratory of Nondestructive Test of the Ministry of Education (Nanchang Hangkong University), Nanchang 330063, China)

[2](School of Electrical and Electronic Engineering, Yonsei University, Seoul 120749, South Korea)

[3](Department of Digital Media Engineering, Anyang University, Seoul 430714, South Korea)

Abstract: Security and privacy of templates are critical to the practical applications of palmprint systems. However, some objectives of biometric protection are difficult to meet at the same time due to the conflicts among them. As a cancelable palmprint coding algorithm to resolve the aforementioned conflicts, PalmPhasor is efficient and secure for palmprint authentication. In this paper, a complete analytical framework is proposed to systematically analyze the performance of PalmPhasor. The scenarios are categorized into four cases for the convenience of especial analysis. Some preliminaries, including auxiliary theorems, the distribution character of real and imaginary parts of Gabor filtered palmprint images, are provided to support the corresponding analysis. The theoretical analysis based on statistics and experimental results both confirm that PalmPhasor enhanced by multi-orientation score level fusion satisfactorily meets the four objectives of cancelable biometric at the same time even when users' tokens are stolen.

Key words: PalmPhasor algorithm; theoretical performance analysis; multi-orientation score level fusion; palmprint authentication; cancelable biometric

* 基金项目: 国家自然科学基金(61305010, 61262019); 国家研究基金基础科学研究计划(韩国科学、资讯与通信技术暨未来规划部)(2013006574); 国家研究基金基础科学研究计划(韩国教育与科技部)(20120192); 中国博士后科学基金(2013M531554); 江西省博士后日常经费(2013RC20); 江西省远航工程基金(201450); 南昌航空大学博士启动基金(EA201308058)

收稿时间: 2012-06-10; 修改时间: 2014-01-09; 定稿时间: 2014-03-27; jos 在线出版时间: 2014-08-19

CNKI 网络优先出版: 2014-08-19 14:27, http://www.cnki.net/kcms/doi/10.13328/j.cnki.jos.004594.html

由于采集设备低廉、鉴别信息丰富、认证精度高、用户可接受性强等优势,掌纹已发展成一种重要的生物特征身份认证方式[1].用于认证的掌纹特征可大体分为特征点/线特征[2]、统计特征(如各类变换[3−5]、子空间、均值、方差、能量、矩等)和纹理特征.其中,基于纹理特征的编码方法可以在大容量掌纹库上进行高精度认证.根据提出时间先后的顺序和精度的不断提高,掌纹编码包括 Palm Code[6],Fusion Code[7],Competitive Code[8],Ordinal Code[9],Robust Line Orientation Code[10],Binary Orientation Co-occurrence Vector[11]等方案.

但在实际应用中,掌纹也存在着与其他生物特征相同的安全隐患[12]:(1) 特征终生不变,一旦被盗,用户就无法撤销和更新模板;(2) 随着应用领域的扩展,同一用户的相同特征模板可能存储于多个数据库中,一旦其中一个数据库中的模板信息泄露,其他数据库中的相同模板就都不再安全;(3) 原始特征可能泄露用户基因缺陷、疾病等隐私信息.所以,迫切需要掌纹模板安全和隐私保护方案,解决实际应用的瓶颈问题.

理想的生物特征模板保护技术应满足多样性(diversity)、可重用性(reusability) 、不可逆性(non-invertibility)和认证性能(verification performance)这 4 项基本指标要求[13],但这些指标往往因相互冲突而难以同时保证.

中国科学院的李鹏、田捷等学者系统总结了国内外生物特征模板保护技术[14].本文将掌纹模板保护技术分为以下 3 类:

(1) 掌纹密码系统(palmprint cryptosystem)

模糊承诺(fuzzy commitment)[15]和模糊保险箱(fuzzy vault)[16]是两种典型的密钥绑定(key binding)生物特征密码系统.在掌纹密码系统方面,掌纹密钥生成(palmprint key generation)技术要求从掌纹中提取稳定不变的特征作为加密系统的密钥进行认证.Wu 等学者采用两种纠错码技术设计了掌纹加密系统[17,18],但未考虑掌纹模板的多样性和可重用性.Leng 等人在可撤销掌纹模板的基础上提出了双钥(dual-key-binding)绑定方案,赋予了掌纹密钥的多样性和可重用性[19].

(2) 加密掌纹(encrypted palmprint)

此类方法将掌纹模板作为明文进行加密,采用加密后的形式代替原始掌纹特征进行认证[20,21].但此类算法只能对二值的掌纹特征实现加密域的直接认证,否则需要重构和恢复出原始生物特征,从而影响原始模板的安全性.此外,加密过程的异或运算不满足不可逆性.当算法公开时,若密钥和受保护模板同时泄露,则攻击者可以解密出原始掌纹模板.

(3) 单向变换掌纹(one-way transformed palmprint)

此类方法可被认为是典型的可撤销掌纹(cancelable palmprint)方案.可撤销生物特征算法的主要思想是:由用户口令控制某种机制生成一组特定数据,并将这些数据通过单向变换与原始生物特征实现融合.可撤销生物特征方案性能评价必须在最佳和最差两种情况分别讨论,全部用户使用不同口令是最佳情况,全部用户使用相同口令是最差情况.Teoh 等学者提出的 BioHashing 算法融合了用户口令生成的伪随机数和原始生物特征,在最佳情况下得到了理想的认证效果[22,23].但 Kong 等人指出:BioHashing 在口令被盗(stolen-token)时,即最差情况下,性能会严重下降[24].实际上,在最差情况下不进行阈值化的 BioHashing,相当于随机投影(random projection)算法[25],其认证性能与其他子空间算法(如主成分分析、线性鉴别分析等)近似,但难以达到掌纹编码算法的精度.PalmHash 算法是 BioHashing 在掌纹子空间特征上的具体应用[26],因此也难以达到很高的认证精度.Leng 等人通过随机化 Gabor 滤波器参数生成了多样化的随机 Palm Code[27],但此方案的认证性能仅与 Palm Code 近似,难以进一步提高.Leng 等人于 2011 年提出了可撤销掌纹编码方案——PalmPhasor 算法,实现了高效、安全的掌纹认证,并通过多方向分数级融合达到了较高的认证精度[28].然而,PalmPhasor 算法的性能还未经过理论分析加以证实.本文运用统计学原理和相关预备知识,通过系统的理论分析和实验,验证了 PalmPhasor 算法可以同时有效地满足可撤销生物特征的 4 项指标.

1 PalmPhasor 算法

多方向分数级融合增强的 PalmPhasor 算法的流程如下所述:

(a) 从原始掌纹图像中提取尺寸为 128×128 的感兴趣区域(region of interest,简称 ROI),并对 ROI 进行均

值和方差归一化处理.

(b) 生成 Gabor 滤波器 $G(x,y,\theta_\tau,u,\sigma)=\frac{1}{2\pi\sigma^2}\exp\left\{-\frac{x^2+y^2}{2\sigma^2}\right\}\exp\left\{2\pi\sqrt{-1}(ux\cos\theta_\tau+uy\sin\theta_\tau)\right\}$,方向角度为 $\theta_\tau=\frac{(\tau-1)\pi}{L},\tau=1,2,...,L$.$L$ 和τ分别表示融合方向个数和第τ个方向.为了避免光照干扰,将滤波器直流分量调整为 0,$\overline{G}(x,y,\theta_\tau,u,\sigma)=G(x,y,\theta_\tau,u,\sigma)-\frac{\sum_{i=-n}^{n}\sum_{j=-n}^{n}G(x,y,\theta_\tau,u,\sigma)}{(2M+1)^2}$,$(2M+1)^2$ 为滤波器尺寸.

(c) 掌纹 ROI 进行 Gabor 滤波后,对结果的实部和虚部下采样,得到尺寸为 $m\times 2m$ 的矩阵 $\boldsymbol{A}$,m=32.$\boldsymbol{A}$ 的左半部分和右半部分分别对应实部和虚部的下采样结果.

(d) 由口令控制生成服从标准正态分布的非 0 伪随机数(pseudo-random number,简称 PRN),PRN 为 0 的概率很小,若 PRN=0,则舍弃并重新生成新的 PRN.由生成的 PRN 组成向量$\{\boldsymbol{r}_j\in\mathbb{R}^{2m}|j=1,2,\ldots,m\}$.

(e) 将 $\boldsymbol{A}$ 第 i 行的行向量 $\boldsymbol{a}_i$ 和 $\boldsymbol{r}_j$ 组合成复数向量$\left\{\boldsymbol{z}_{ij}=\boldsymbol{r}_j+\boldsymbol{a}_i\sqrt{-1}\in\mathbb{C}^{2m}\mid i=1,2,...,m,j=1,2,...,m\right\}$.

(f) 计算复数向量的反正切主值向量$\{\boldsymbol{\varphi}_{ij}=\arctan(\boldsymbol{z}_{ij})=\arctan(\boldsymbol{a}_i/\boldsymbol{r}_j)\in\mathbb{R}^{2m}|i=1,2,\ldots,m,j=1,2,\ldots,m\}$.

(g) 计算反正切主值向量的平均值$\left\{\overline{\varphi}_{ij}=\frac{1}{2m}\sum_{k=1}^{2m}\varphi_{ijk}\mid i=1,2,...,m,j=1,2,...,m\right\}$,$\varphi_{ijk}$是$\boldsymbol{\varphi}_{ij}$的第 k 个元素.

(h) 通过二值化得到 PalmPhasor 结果为 $b_{ij}=\begin{cases}0, & \text{if } 0<\overline{\varphi}_{ij}<\pi/2\\ 1, & \text{if } -\pi/2<\overline{\varphi}_{ij}\leqslant 0\end{cases},i=1,2,...,m,j=1,2,...,m.$

(i) 计算θ_τ方向上两个 PalmPhasor 模板的匹配分数(此处的匹配分数为归一化海明距离):

$$H^\tau(\boldsymbol{P}^\tau,\boldsymbol{Q}^\tau)=\frac{\sum_{i=1}^{m}\sum_{j=1}^{m}P_{ij}^\tau\oplus Q_{ij}^\tau}{m\times m},$$

$\boldsymbol{P}^\tau$,$\boldsymbol{Q}^\tau$分别为第τ个方向的两个 PalmPhasor 模板,P_{ij}^τ 和 Q_{ij}^τ 分别为 $\boldsymbol{P}^\tau$,$\boldsymbol{Q}^\tau$中的元素,⊕为“位异或”符号.

(j) 采用多方向分数级融合进一步提高性能,对 L 个方向的匹配分数采用均值准则融合.融合后,匹配分数为 $H_n(\boldsymbol{P}^\tau,\boldsymbol{Q}^\tau)=\frac{\sum_{\tau=1}^{L}H^\tau(\boldsymbol{P}^\tau,\boldsymbol{Q}^\tau)}{L}$.

2 预备知识

本节对 PalmPhasor 算法性能理论分析涉及的预备知识进行介绍,包括分析情景的情况分类、Gabor 滤波掌纹图像实部和虚部的分布特性以及相关的辅助定理.

2.1 情况分类

为了便于分析,根据样本是否来自相同个体和用户口令是否相同,将情景分为如表 1 所示的 4 种情况类别.

- 第 1 种情况:相同个体、相同口令.其中,对同一用户多次采集的生物特征样本由于各种干扰,存在类内差异,并非完全一致.
- 第 2 种情况:相同个体、不同口令.即,用户通过修改口令产生更新的可撤销模板,废除原先模板.更新模板和废除的模板必须有较大的差异,以保证多样性和可重用性.
- 第 3 种情况:不同个体、相同口令.要求口令相同、个体不同时,可撤销生物特征仍能保证类间鉴别性.
- 第 4 种情况:不同个体、不同口令.由于每个用户口令不同,使此时的可撤销模板通常比原始模板具有更高的类间鉴别性.

在上述 4 种情况中:第 1 种情况和第 4 种情况是系统正常运行中最常见的状态;第 2 种情况对应的是用户更新模板的情形;第 3 种情况对应的是用户口令被盗的情形,即,攻击者用非法的生物特征和合法的口令生成可

撤销模板,用于冒充真实用户.

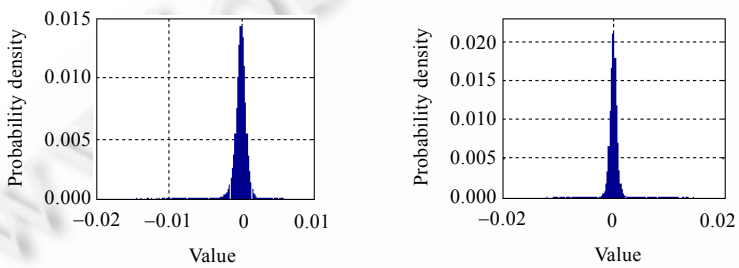
Table 1 Scenario categories of analysis

表 1 分析的情景类别

	样本来自相同个体	样本来自不同个体
用户口令相同	最佳情况/最差情况的类内匹配	最差情况的类间匹配
用户口令不同	多样性,可重用性	最佳情况的类间匹配

2.2 Gabor滤波掌纹图像分布特性

实验在香港理工大学掌纹数据库(http://www4.comp.polyu.edu.hk/~biometrics/)第 2 版(Version 2)上测试,数据库包含了 193 个人的 386 个掌纹,共 7 752 张掌纹图片.PalmPhasor 算法步骤(c)对每个掌纹 ROI 滤波和下采样后,实部和虚部分别得到 32×32 个数据.图 1 为水平方向 Gabor 滤波掌纹图像实部和虚部的概率密度直方图,实部和虚部分别统计了 32×32×7752=7938048 个数值.通过统计分析,验证了 Gabor 滤波掌纹图像实部和虚部的以下统计特性:(1) 其他各个方向的 Gabor 滤波掌纹图像实部和虚部的概率密度直方图均与水平方向有类似的分布特性;(2) 实部和虚部的数值较小,通常在 10^{-3} 数量级;(3) 实部和虚部的概率密度分布函数为偶函数.



(a) 实部 (b) 虚部

Fig.1 Histogram of the values of Gabor-filtered palmprint images along horizon orientation

图 1 水平方向 Gabor 滤波掌纹图像数值概率密度直方图

2.3 辅助定理

定理 1. 设 X 为一随机变量,其概率密度函数为偶函数,即 $f_X(x)=f_X(-x)$.当 $X\neq 0$ 时,$Y=1/X$,则 Y 的概率密度函数也为偶函数,即 $f_Y(y)=f_Y(-y)$.

定理 2. 设 X,Y 为两个独立的随机变量,X 的概率密度函数为偶函数,例如 $f_X(x)=f_X(-x)$.$Z=XY$,则 Z 的概率密度函数也为偶函数,即 $f_Z(z)=f_Z(-z)$.根据 X,Y 的对称性,当 Y 的概率密度函数为偶函数时,也有相同结论.

定理 3. 设 X,Y 为两个独立的随机变量,其概率密度函数均为偶函数,即 $f_X(x)=f_X(-x)$,$f_Y(y)=f_Y(-y)$.$Z=X+Y$,则 Z 的概率密度函数也为偶函数,即 $f_Z(z)=f_Z(-z)$.

3 PalmPhasor 性能理论分析

本节在 4 种情况下分别对 PalmPhasor 算法的性能进行理论分析,并给出多方向分数级融合的理论分析.为了简化分析中的符号定义,省略了上标 τ,但分析过程适用于各个 θ_τ 方向.首先给出以下定义:

定义 1(“位异或”的数学期望). 假设 $x'=\begin{cases}1, & \text{if } x\geqslant 0\\ 0, & \text{if } x<0\end{cases}$,$y'=\begin{cases}1, & \text{if } y\geqslant 0\\ 0, & \text{if } y<0\end{cases}$,则 $x'\oplus y'$ 的数学期望定义为

$$E(x'\oplus y')=1\cdot\Pr(x'\oplus y'=1)+0\cdot\Pr(x'\oplus y'=0)=1\cdot\Pr(xy<0)+0\cdot\Pr(xy\geqslant 0)=\Pr(xy<0).$$

若 x,y 相互独立,则

$$E(x'\oplus y')=\Pr(xy<0)=\Pr(x>0)\Pr(y<0)+\Pr(x<0)\Pr(y>0).$$

定义 2. 实数向量 $\boldsymbol{x}=[x_1,x_2,..,x_d]$和 $\boldsymbol{y}=[y_1,y_2,..,y_d]$, $\boldsymbol{x}\otimes\boldsymbol{y}=\frac{1}{d}\sum_{i=1}^{d}\arctan\left(\frac{x_i}{y_i}\right)$.

定义 3. 二值向量 $\boldsymbol{x}'=[x_1',x_2',...,x_d']$ 和 $\boldsymbol{y}'=[y_1',y_2',...,y_d']$,$\boldsymbol{x}'$和 $\boldsymbol{y}'$的海明距离为 $H(\boldsymbol{x}',\boldsymbol{y}')=\sum_{i=1}^{d}(x_i'\oplus y_i')$.

定义 4. 二值向量 $\boldsymbol{x}'=[x_1',x_2',...,x_d']$ 和 $\boldsymbol{y}'=[y_1',y_2',...,y_d']$,$\boldsymbol{x}'$和 $\boldsymbol{y}'$的归一化海明距离为 $H_n(\boldsymbol{x}',\boldsymbol{y}')=\frac{H(\boldsymbol{x}',\boldsymbol{y}')}{d}$.

定义 5. $E(x)$表示随机变量 x 的数学期望.

定义 6. $D(x)$表示随机变量 x 的方差.

3.1 相同个体、相同口令

在第 1 种情况下,来自同一个体的多个掌纹样本用相同口令生成对应的 PalmPhasor 模板.通过分析,用掌纹特征中元素数学期望和方差表达了 PalmPhasor 对应元素相等概率的解析式,并给出了此概率的下限值.

设同一个体两次采集和提取的 d 维 Gabor 滤波掌纹图像的实部和虚部元素组成掌纹特征向量$\boldsymbol{\alpha}=[\alpha_1,\alpha_2,\ldots,\alpha_d]$和$\boldsymbol{\beta}=[\beta_1,\beta_2,\ldots,\beta_d]$.由于两个掌纹特征向量分两次采集和提取,因此是独立的.又因为来自同一个体,因此分布相同.$E(x)$和 $D(x)$分别表示随机变量 x 的数学期望和方差.假设 $E(\alpha_i)=E(\beta_i)=\mu_i$,$D(\alpha_i)=D(\beta_i)=\sigma_i^2$.方差表明:由于各类干扰和条件差异,同一个体多次采集和提取的掌纹特征样本存在类内差异,并非完全相同.

由口令作为种子控制生成 $PRN,r_{ij}\sim N(0,1)$并且 $r_{ij}\neq 0$,组成尺寸为 $d\times k$ 的矩阵 $\boldsymbol{R}$.当用户口令不变时,$\boldsymbol{R}$ 不变,被看作常数矩阵.

$$f(\boldsymbol{\alpha})=d[\boldsymbol{\alpha}\otimes\boldsymbol{r}_1,\boldsymbol{\alpha}\otimes\boldsymbol{r}_2,\ldots,\boldsymbol{\alpha}\otimes\boldsymbol{r}_k]=\boldsymbol{P}=[P_1,P_2,\ldots,P_k],\ f(\boldsymbol{\beta})=d[\boldsymbol{\beta}\otimes\boldsymbol{r}_1,\boldsymbol{\beta}\otimes\boldsymbol{r}_2,\ldots,\boldsymbol{\beta}\otimes\boldsymbol{r}_k]=\boldsymbol{Q}=[Q_1,Q_2,\ldots,Q_k],$$

得到两个新的向量 $\boldsymbol{P}$ 和 $\boldsymbol{Q}$,$\boldsymbol{r}_j$ 表示 $\boldsymbol{R}$ 的第 j 列的列向量.

其中, $P_j=\sum_{i=1}^{d}\arctan\left(\frac{\alpha_i}{r_{ij}}\right),Q_j=\sum_{i=1}^{d}\arctan\left(\frac{\beta_i}{r_{ij}}\right)$, r_{ij} 是 $\boldsymbol{r}_j$ 的第 i 个元素.

此处,$f(\boldsymbol{\alpha})$和 $f(\boldsymbol{\beta})$的计算公式前加入了比例因子 d.由于比例因子不影响最终阈值化的结果,因此这一修改在不影响分析结果的同时,避免了分析过程中每项前面 $1/d$ 系数的繁琐表达.

根据洛必达(L' Hospital)法则, $\lim_{x\to 0}\frac{x}{\arctan x}=\lim_{x\to 0}\frac{x'}{(\arctan x)'}=\lim_{x\to 0}\frac{1}{\frac{1}{(1+x^2)}}=\lim_{x\to 0}(1+x^2)=1$.

因为 $\lim_{x\to 0}\arctan x\approx x$,Gabor 滤波掌纹图像实部和虚部数值较小,通常为 10^{-3} 的数量级,

所以, $P_j=\sum_{i=1}^{d}\arctan\left(\frac{\alpha_i}{r_{ij}}\right)\approx\sum_{i=1}^{d}\frac{\alpha_i}{r_{ij}},Q_j=\sum_{i=1}^{d}\arctan\left(\frac{\beta_i}{r_{ij}}\right)\approx\sum_{i=1}^{d}\frac{\beta_i}{r_{ij}}$.

$$E(P_jQ_j)=E\left(\sum_{l=1}^{d}\arctan\left(\frac{\alpha_l}{r_{lj}}\right)\cdot\sum_{m=1}^{d}\arctan\left(\frac{\beta_m}{r_{mj}}\right)\right)\approx E\left(\sum_{l=1}^{d}\sum_{m=1}^{d}\frac{\alpha_l}{r_{lj}}\frac{\beta_m}{r_{mj}}\right)=\sum_{l=1}^{d}\sum_{m=1}^{d}\frac{\mu_l}{r_{lj}}\frac{\mu_m}{r_{mj}},$$

$$E((P_jQ_j)^2)=E\left(\left(\sum_{i=1}^{d}\arctan\left(\frac{\alpha_i}{r_{ij}}\right)\cdot\sum_{i=1}^{d}\arctan\left(\frac{\beta_i}{r_{ij}}\right)\right)^2\right)\approx E\left(\left(\sum_{i=1}^{d}\frac{\alpha_i}{r_{ij}}\cdot\sum_{i=1}^{d}\frac{\beta_i}{r_{ij}}\right)^2\right)=E\left(\sum_{l=1}^{d}\sum_{m=1}^{d}\sum_{p=1}^{d}\sum_{q=1}^{d}\frac{\alpha_l}{r_{lj}}\frac{\alpha_m}{r_{mj}}\frac{\beta_p}{r_{pj}}\frac{\beta_q}{r_{qj}}\right),$$

$$D(P_jQ_j)=E((P_jQ_j)^2)-E(P_jQ_j)^2\approx E\left(\left(\sum_{l=1}^{d}\sum_{m=1}^{d}\frac{\alpha_l}{r_{lj}}\frac{\beta_m}{r_{mj}}\right)^2\right)-\left(\sum_{l=1}^{d}\sum_{m=1}^{d}\frac{\mu_l}{r_{lj}}\frac{\mu_m}{r_{mj}}\right)^2=$$

$$E\left(\sum_{l=1}^{d}\sum_{m=1}^{d}\sum_{p=1}^{d}\sum_{q=1}^{d}\frac{\alpha_l\beta_m\alpha_p\beta_q}{r_{lj}r_{mj}r_{pj}r_{qj}}\right)-\left(\sum_{l=1}^{d}\sum_{m=1}^{d}\frac{\mu_l\mu_m}{r_{lj}r_{mj}}\right)^2.$$

上式推导结果中的第 1 项为

$$E\left(\sum_{l=1}^{d}\sum_{m=1}^{d}\sum_{p=1}^{d}\sum_{q=1}^{d}\frac{\alpha_l\beta_m\alpha_p\beta_q}{r_{lj}r_{mj}r_{pj}r_{qj}}\right)=$$

$$E\left(\underbrace{\sum_{l=1}^{d}\sum_{m=1}^{d}\sum_{p=1}^{d}\sum_{q=1}^{d}\frac{\alpha_l\beta_m\alpha_p\beta_q}{r_{lj}r_{mj}r_{pj}r_{qj}}}_{l\neq p \text{ and } m\neq q}+\underbrace{\sum_{l=1}^{d}\sum_{m=1}^{d}\sum_{p=1}^{d}\sum_{q=1}^{d}\frac{\alpha_l\beta_m\alpha_p\beta_q}{r_{lj}r_{mj}r_{pj}r_{qj}}}_{l=p \text{ and } m\neq q}+\underbrace{\sum_{l=1}^{d}\sum_{m=1}^{d}\sum_{p=1}^{d}\sum_{q=1}^{d}\frac{\alpha_l\beta_m\alpha_p\beta_q}{r_{lj}r_{mj}r_{pj}r_{qj}}}_{l\neq p \text{ and } m=q}+\underbrace{\sum_{l=1}^{d}\sum_{m=1}^{d}\sum_{p=1}^{d}\sum_{q=1}^{d}\frac{\alpha_l\beta_m\alpha_p\beta_q}{r_{lj}r_{mj}r_{pj}r_{qj}}}_{l=p \text{ and } m=q}\right)=$$

$$E\left(\underbrace{\sum_{l=1}^{d}\sum_{m=1}^{d}\sum_{p=1}^{d}\sum_{q=1}^{d}\frac{\alpha_l\beta_m\alpha_p\beta_q}{r_{lj}r_{mj}r_{pj}r_{qj}}}_{l\neq p \text{ and } m\neq q}+\underbrace{\sum_{l=1}^{d}\sum_{m=1}^{d}\sum_{p=1}^{d}\sum_{q=1}^{d}\frac{\alpha_l^2\beta_m\beta_q}{r_{lj}^2r_{mj}r_{qj}}}_{l=p \text{ and } m\neq q}+\underbrace{\sum_{l=1}^{d}\sum_{m=1}^{d}\sum_{p=1}^{d}\sum_{q=1}^{d}\frac{\beta_m^2\alpha_l\alpha_p}{r_{mj}^2r_{lj}r_{pj}}}_{l\neq p \text{ and } m=q}+\underbrace{\sum_{l=1}^{d}\sum_{m=1}^{d}\sum_{p=1}^{d}\sum_{q=1}^{d}\frac{\alpha_l^2\beta_m^2}{r_{lj}^2r_{mj}^2}}_{l=p \text{ and } m=q}\right)=$$

$$\underbrace{\sum_{l=1}^{d}\sum_{m=1}^{d}\sum_{p=1}^{d}\sum_{q=1}^{d}\frac{\mu_l\mu_m\mu_p\mu_q}{r_{lj}r_{mj}r_{pj}r_{qj}}}_{l\neq p \text{ and } m\neq q}+\underbrace{\sum_{l=1}^{d}\sum_{m=1}^{d}\sum_{p=1}^{d}\sum_{q=1}^{d}\frac{(\sigma_l^2+\mu_l^2)\mu_m\mu_q}{r_{lj}^2r_{mj}r_{qj}}}_{l=p \text{ and } m\neq q}+\underbrace{\sum_{l=1}^{d}\sum_{m=1}^{d}\sum_{p=1}^{d}\sum_{q=1}^{d}\frac{(\sigma_m^2+\mu_m^2)\mu_l\mu_p}{r_{mj}^2r_{lj}r_{pj}}}_{l\neq p \text{ and } m=q}+\underbrace{\sum_{l=1}^{d}\sum_{m=1}^{d}\sum_{p=1}^{d}\sum_{q=1}^{d}\frac{(\sigma_l^2+\mu_l^2)(\sigma_m^2+\mu_m^2)}{r_{lj}^2r_{mj}^2}}_{l=p \text{ and } m=q}.$$

因此,

$$D(P_jQ_j)=E((P_jQ_j)^2)-E(P_jQ_j)^2=\underbrace{\sum_{l=1}^{d}\sum_{m=1}^{d}\sum_{q=1}^{d}\frac{\sigma_l^2\mu_m\mu_q}{r_{lj}^2r_{mj}r_{qj}}}_{m\neq q}+\underbrace{\sum_{l=1}^{d}\sum_{m=1}^{d}\sum_{p=1}^{d}\frac{\sigma_m^2\mu_l\mu_p}{r_{mj}^2r_{lj}r_{pj}}}_{l\neq p}+\sum_{l=1}^{d}\sum_{m=1}^{d}\frac{\sigma_l^2\sigma_m^2}{r_{lj}^2r_{mj}^2}.$$

由切比雪夫(Chebyshev)不等式,得:

$$\Pr(|P_jQ_j-E(P_jQ_j)|<\varepsilon)\geqslant 1-\frac{D(P_jQ_j)}{\varepsilon^2}.$$

当$\varepsilon=E(P_jQ_j)$时, $\Pr(0<P_jQ_j<2E(P_jQ_j))\geqslant 1-\dfrac{D(P_jQ_j)}{E(P_jQ_j)^2}$.

因为 $\Pr(P_jQ_j>0)=\Pr(0<P_jQ_j<2E(P_jQ_j))+\Pr(P_jQ_j\geqslant 2E(P_jQ_j))$,

所以, $\Pr(P_jQ_j>0)\geqslant 1-\dfrac{D(P_jQ_j)}{E(P_jQ_j)^2}$.

其中,$E(P_jQ_j)$和 $D(P_jQ_j)$均已求得.

因为 $E(P_jQ_j)\approx\sum_{l=1}^{d}\sum_{m=1}^{d}\dfrac{\mu_l}{r_{lj}}\dfrac{\mu_m}{r_{mj}}$,当$\mu_i\to\infty$时, $\dfrac{1}{E(P_jQ_j)^2}$ 是 $\dfrac{1}{D(P_jQ_j)}$ 的高阶无穷小,

所以, $\lim\limits_{\mu_i\to\infty}\Pr(P_jQ_j>0)=\lim\limits_{\mu_i\to\infty}\dfrac{D(P_jQ_j)}{E(P_jQ_j)^2}=\lim\limits_{\mu_i\to\infty}1-\dfrac{\dfrac{1}{E(P_jQ_j)^2}}{\dfrac{1}{D(P_jQ_j)}}=1-0=1.$

可见,在掌纹特征中元素的数学期望无穷大和方差为 0 的两种极限情况下,两个 PalmPhasor 对应元素的数值必定相等.

对向量 $\boldsymbol{P}$ 和 $\boldsymbol{Q}$ 中的元素二值化: $P_j'=\begin{cases}1, & \text{if } P_j\geqslant 0\\ 0, & \text{if } P_j<0\end{cases}$, $Q_j'=\begin{cases}1, & \text{if } Q_j\geqslant 0\\ 0, & \text{if } Q_j<0\end{cases}$,

得到对应的二值向量: $\boldsymbol{P}'=[p_1',p_2',...,p_d']$, $\boldsymbol{Q}'=[q_1',q_2',...,q_d']$.

设 $\Pr(P_jQ_j>0)=1-p>1-\dfrac{D(P_jQ_j)}{E(P_jQ_j)^2}$, $1-p$ 是两个 PalmPhasor 第 j 个元素相同的概率,其下限为 $1-\dfrac{D(P_jQ_j)}{E(P_jQ_j)^2}$, 则两个 PalmPhasor 第 j 个元素不同的概率为 p,其上限为 $\dfrac{D(P_jQ_j)}{E(P_jQ_j)^2}$.

于是,$H(\boldsymbol{P}',\boldsymbol{Q}')$是服从参数为 k,p 的二项分布,$H(\boldsymbol{P}',\boldsymbol{Q}')\sim b(k,p)$.

$$E(H(\boldsymbol{P}',\boldsymbol{Q}'))=E\left(\sum_{j=1}^{k}(P_j'\oplus Q_j')\right)=\sum_{j=1}^{k}E(P_j'\oplus Q_j')=\sum_{j=1}^{k}\Pr(P_jQ_j<0)=\sum_{j=1}^{k}p=kp,$$

$$\Pr(H(\boldsymbol{P}',\boldsymbol{Q}')=n)=\binom{k}{n}p^n(1-p)^{k-n},n=0,1,...,k,$$

$$E(H_n(\boldsymbol{P}',\boldsymbol{Q}'))=E\left(\frac{H(\boldsymbol{P}',\boldsymbol{Q}')}{k}\right)=\frac{E\left(\sum_{j=1}^{k}(P_j'\oplus Q_j')\right)}{k}=\frac{\sum_{j=1}^{k}(P_j'\oplus Q_j')}{k}=\frac{kp}{k}=p.$$

证毕. □

从 p 的上限式可知,p 与掌纹特征中元素的数学期望的绝对值负相关,与其方差正相关.当掌纹特征中元素的数学期望的绝对值足够大、方差足够小时,第 1 种情况下的两个 PalmPhasor 对应元素将以高概率相等.

3.2 相同个体、不同口令

第 2 种情况时,来自同一个体的掌纹样本用不同口令生成对应的 PalmPhasor 模板,相当于用户更新口令的情景.此时须证明的是,同一个体的掌纹样本用不同口令生成的 PalmPhasor 之间的海明距离足够大.

向量$\boldsymbol{\alpha}$和$\boldsymbol{\beta}$的定义与第 1 种情况相同.

用户采用两个不同口令分别生成两组 PRN: $r_{ij}^{\alpha}\sim N(0,1)$并且 $r_{ij}^{\alpha}\neq 0$,$r_{ij}^{\beta}\sim N(0,1)$并且 $r_{ij}^{\beta}\neq 0$,并且组成矩阵 $\boldsymbol{R}^{\alpha}$ 和 $\boldsymbol{R}^{\beta}$.

$$f(\boldsymbol{\alpha})=d[\boldsymbol{\alpha}\otimes\boldsymbol{r}_1^{\alpha},\boldsymbol{\alpha}\otimes\boldsymbol{r}_2^{\alpha},...,\boldsymbol{\alpha}\otimes\boldsymbol{r}_k^{\alpha}]=\boldsymbol{P}=[P_1,P_2,...,P_k],f(\boldsymbol{\beta})=d[\boldsymbol{\beta}\otimes\boldsymbol{r}_1^{\beta},\boldsymbol{\beta}\otimes\boldsymbol{r}_2^{\beta},...,\boldsymbol{\beta}\otimes\boldsymbol{r}_k^{\beta}]=\boldsymbol{Q}=[Q_1,Q_2,...,Q_k],$$

得到两个新的向量 $\boldsymbol{P}$ 和 $\boldsymbol{Q}$,$\boldsymbol{r}_j^{\alpha}$ 和 $\boldsymbol{r}_j^{\beta}$ 分别表示 $\boldsymbol{R}^{\alpha}$和 $\boldsymbol{R}^{\beta}$的第 j 列的列向量.

其中,$P_j=\sum_{i=1}^{d}\arctan\left(\frac{\alpha_i}{r_{ij}^{\alpha}}\right),Q_j=\sum_{i=1}^{d}\arctan\left(\frac{\beta_i}{r_{ij}^{\beta}}\right)$,$r_{ij}^{\alpha}$ 和 r_{ij}^{β} 分别是 $\boldsymbol{r}_j^{\alpha}$ 和 $\boldsymbol{r}_j^{\beta}$ 的第 i 个元素.

对向量 $\boldsymbol{P}$ 和 $\boldsymbol{Q}$ 中的元素二值化: $P_j'=\begin{cases}1, & \text{if } P_j\geqslant 0\\ 0, & \text{if } P_j<0\end{cases}$,$Q_j'=\begin{cases}1, & \text{if } Q_j\geqslant 0\\ 0, & \text{if } Q_j<0\end{cases}$,

得到对应的二值向量: $\boldsymbol{P}'=[p_1',p_2',...,p_d'],\boldsymbol{Q}'=[q_1',q_2',...,q_d']$.

$$E(H(\boldsymbol{P}',\boldsymbol{Q}'))=E\left(\sum_{j=1}^{k}(P_j'\oplus Q_j')\right)=\sum_{j=1}^{k}E(P_j'\oplus Q_j')=\sum_{j=1}^{k}\Pr(P_jQ_j<0),$$

$$E(P_jQ_j)=E\left(\sum_{l=1}^{d}\arctan\left(\frac{\alpha_l}{r_{lj}^{\alpha}}\right)\sum_{m=1}^{d}\arctan\left(\frac{\beta_m}{r_{mj}^{\beta}}\right)\right)\approx E\left(\sum_{l=1}^{d}\frac{\alpha_l}{r_{lj}^{\alpha}}\sum_{m=1}^{d}\frac{\beta_m}{r_{mj}^{\beta}}\right)=\sum_{l=1}^{d}E\left(\frac{\alpha_l}{r_{lj}^{\alpha}}\right)\sum_{m=1}^{d}E\left(\frac{\beta_m}{r_{mj}^{\beta}}\right).$$

因为 $r_{ij}^{\alpha}\sim N(0,1)$并且 $r_{ij}^{\alpha}\neq 0$,$r_{ij}^{\beta}\sim N(0,1)$并且 $r_{ij}^{\beta}\neq 0$,

所以,r_{lj}^{α} 和 r_{mj}^{β} 的概率密度函数均为偶函数.

因为 $\boldsymbol{R}^{\alpha}$,$\boldsymbol{R}^{\beta}$,$\boldsymbol{\alpha}$和$\boldsymbol{\beta}$中的元素相互独立,

所以,根据定理 1,$1/r_{ij}^{\alpha}$ 和 $1/r_{mj}^{\beta}$ 的概率密度函数也均为偶函数.

所以,根据定理 2,α_l/r_{ij}^{α} 和β_m/r_{mj}^{β} 的概率密度函数也均为偶函数.

所以,$E\left(\frac{\alpha_l}{r_{lj}^{\alpha}}\right)=0,E\left(\frac{\beta_m}{r_{mj}^{\beta}}\right)=0$,因此 $E(P_jQ_j)=0$.

设 $Z=P_jQ_j$,根据定理 2 和定理 3,得 $f_Z(z)=f_Z(-z)$.所以,$\int_0^{\infty}f_Z(z)\mathrm{d}z=\int_{-\infty}^{0}f_Z(z)\mathrm{d}x$.

又因为 $\int_0^{\infty}f_Z(z)\mathrm{d}z+\int_{-\infty}^{0}f_Z(z)\mathrm{d}x=1$,所以,$\int_0^{\infty}f_Z(z)\mathrm{d}z=\int_{-\infty}^{0}f_Z(z)\mathrm{d}x=0.5$.

则 $\Pr(P_jQ_j\geqslant 0)=\Pr(Z\geqslant 0)=0.5,\Pr(P_jQ_j<0)=\Pr(Z<0)=0.5$,

则 $H(\boldsymbol{P}',\boldsymbol{Q}')$是服从参数为 k,0.5 的二项分布,$H(\boldsymbol{P}',\boldsymbol{Q}')\sim b(k,0.5)$.

$$E(H(\boldsymbol{P}',\boldsymbol{Q}'))=E\left(\sum_{j=1}^{k}(P_j'\oplus Q_j')\right)=\sum_{j=1}^{k}E(P_j'\oplus Q_j')=\sum_{j=1}^{k}\Pr(P_jQ_j<0)=\sum_{j=1}^{k}0.5=0.5k,$$

$$\Pr(H(\boldsymbol{P}',\boldsymbol{Q}')=n)=\binom{k}{n}0.5^n(1-0.5)^{k-n},n=0,1,...,k,$$

$$E(H_n(\boldsymbol{P}',\boldsymbol{Q}'))=E\left(\frac{H(\boldsymbol{P}',\boldsymbol{Q}')}{k}\right)=\frac{E\left(\sum_{j=1}^{k}(P_j'\oplus Q_j')\right)}{k}=\frac{\sum_{j=1}^{k}E(P_j'\oplus Q_j')}{k}=\frac{0.5k}{k}=0.5.$$

证毕. □

可见,来自相同个体的掌纹样本用不同口令生成的 PalmPhasor 之间的归一化海明距离为 0.5,足以保证 PalmPhasor 的多样性、可重用性.

3.3 不同个体、相同口令

在第 3 种情况下,全部用户使用相同口令,须验证口令被盗情况下算法仍保证足够的类间鉴别性,从而保持认证精度.因此,需要证明口令被盗情况下,不同用户用相同口令生成的 PalmPhasor 之间的海明距离足够大.

设来自任意两个不同个体的 d 维 Gabor 滤波掌纹图像的实部和虚部元素组成掌纹特征向量$\boldsymbol{\alpha}=[\alpha_1,\alpha_2,\ldots,\alpha_d]$和$\boldsymbol{\beta}=[\beta_1,\beta_2,\ldots,\beta_d]$,两个向量元素相互独立.根据预备知识中 Gabor 滤波掌纹图像统计分布特性,实部和虚部的概率密度函数均为偶函数.

两个个体用相同口令作为种子控制生成矩阵 $\boldsymbol{R},\boldsymbol{R}$ 的定义与第 1 种情况相同.

$f(\boldsymbol{\alpha})=d[\boldsymbol{\alpha}\otimes\boldsymbol{r}_1,\boldsymbol{\alpha}\otimes\boldsymbol{r}_2,\ldots,\boldsymbol{\alpha}\otimes\boldsymbol{r}_k]=\boldsymbol{P}=[P_1,P_2,\ldots,P_k]$,$f(\boldsymbol{\beta})=d[\boldsymbol{\beta}\otimes\boldsymbol{r}_1,\boldsymbol{\beta}\otimes\boldsymbol{r}_2,\ldots,\boldsymbol{\beta}\otimes\boldsymbol{r}_k]=\boldsymbol{Q}=[Q_1,Q_2,\ldots,Q_k]$,

得到两个新的向量 $\boldsymbol{P}$ 和 $\boldsymbol{Q}$,$\boldsymbol{r}_j$ 表示 $\boldsymbol{R}$ 的第 j 列的列向量.

其中, $P_j=\sum_{i=1}^{d}\arctan\left(\frac{\alpha_i}{r_{ij}}\right),Q_j=\sum_{i=1}^{d}\arctan\left(\frac{\beta_i}{r_{ij}}\right)$, r_{ij} 是 $\boldsymbol{r}_j$ 的第 i 个元素.

对向量 $\boldsymbol{P}$ 和 $\boldsymbol{Q}$ 中的元素二值化: $P_j'=\begin{cases}1, & \text{if } P_j\geqslant 0\\ 0, & \text{if } P_j<0\end{cases}$,$Q_j'=\begin{cases}1, & \text{if } Q_j\geqslant 0\\ 0, & \text{if } Q_j<0\end{cases}$,

得到对应的二值向量: $\boldsymbol{P}'=[p_1',p_2',...,p_d']$,$\boldsymbol{Q}'=[q_1',q_2',...,q_d']$.

$$E(H(\boldsymbol{P}',\boldsymbol{Q}'))=E\left(\sum_{j=1}^{k}(P_j'\oplus Q_j')\right)=\sum_{j=1}^{k}E(P_j'\oplus Q_j')=\sum_{j=1}^{k}\Pr(P_jQ_j<0),$$

$$E(P_jQ_j)=E\left(\sum_{l=1}^{d}\arctan\left(\frac{\alpha_l}{r_{lj}}\right)\sum_{m=1}^{d}\arctan\left(\frac{\beta_m}{r_{mj}}\right)\right)\approx E\left(\sum_{l=1}^{d}\frac{\alpha_l}{r_{lj}}\sum_{m=1}^{d}\frac{\beta_m}{r_{mj}}\right)=E\left(\sum_{l=1}^{d}\frac{\alpha_l}{r_{lj}}\right)E\left(\sum_{m=1}^{d}\frac{\beta_m}{r_{mj}}\right).$$

因为$\boldsymbol{\alpha}$和$\boldsymbol{\beta}$中的元素相互独立,并且其概率密度函数均为偶函数,

所以,α_l/r_{lj} 和 β_m/r_{mj} 的概率密度函数也均为偶函数.

所以, $E\left(\frac{\alpha_l}{r_{lj}}\right)=0,E\left(\frac{\beta_m}{r_{mj}}\right)=0,$

所以,$E(P_jQ_j)=0$.

设 $Z=P_jQ_j$,根据定理 2 和定理 3,得 $f_Z(z)=f_Z(-z)$.

所以, $\int_0^{\infty}f_Z(z)\mathrm{d}z=\int_{-\infty}^{0}f_Z(z)\mathrm{d}x$.

又因为 $\int_0^{\infty}f_Z(z)\mathrm{d}z+\int_{-\infty}^{0}f_Z(z)\mathrm{d}x=1,$

所以, $\int_0^{\infty}f_Z(z)\mathrm{d}z=\int_{-\infty}^{0}f_Z(z)\mathrm{d}x=0.5.$

则 $\Pr(P_jQ_j\geqslant 0)=\Pr(Z\geqslant 0)=0.5,\Pr(P_jQ_j<0)=\Pr(Z<0)=0.5,$

则 $H(\boldsymbol{P}',\boldsymbol{Q}')$是服从参数为 k,0.5 的二项分布,$H(\boldsymbol{P}',\boldsymbol{Q}')\sim b(k,0.5)$.

$$E(H(\boldsymbol{P}',\boldsymbol{Q}'))=E\left(\sum_{j=1}^{k}(P_j'\oplus Q_j')\right)=\sum_{j=1}^{k}E(P_j'\oplus Q_j')=\sum_{j=1}^{k}\Pr(P_jQ_j<0)=\sum_{j=1}^{k}0.5=0.5k,$$

$$\Pr(H(\boldsymbol{P}',\boldsymbol{Q}')=n)=\binom{k}{n}0.5^n(1-0.5)^{k-n},n=0,1,...,k,$$

$$E(H_n(\boldsymbol{P}',\boldsymbol{Q}'))=E\left(\frac{H(\boldsymbol{P}',\boldsymbol{Q}')}{k}\right)=\frac{E\left(\sum_{j=1}^{k}(P_j'\oplus Q_j')\right)}{k}=\frac{\sum_{j=1}^{k}E(P_j'\oplus Q_j')}{k}=\frac{0.5k}{k}=0.5.$$

证毕. □

理论上,$\Pr(P_jQ_j<0)=0.5$,但由于掌纹特征的分布有一定的规律性,在单个掌纹的少量数据中,并非完全呈现出与概率密度函数完全一致的随机性分布,导致实际上 $\Pr(P_jQ_j<0)$略小于 0.5.即,不同用户用相同口令生成的 PalmPhasor 之间的归一化海明距离略低于 0.5.因此,口令被盗情况下的认证性能低于未被盗情况下的性能.但口令被盗时,通过多方向分数级融合的方法仍可以使 PalmPhasor 达到较高的精度.

3.4 不同个体、不同口令

第 4 种情况是正常使用的情景,相当于全部用户使用不同口令和各自的掌纹样本生成各自的 PalmPhasor.须证明全部用户使用不同口令生成各自的 PalmPhasor 之间的海明距离足够大,以保证类间的鉴别性.

向量$\boldsymbol{\alpha}$和$\boldsymbol{\beta}$的定义与第 3 种情况相同.矩阵 $\boldsymbol{R}^{\alpha}$和 $\boldsymbol{R}^{\beta}$的定义与第 2 种情况相同.

$$f(\boldsymbol{\alpha})=d[\boldsymbol{\alpha}\otimes\boldsymbol{r}_1^{\alpha},\boldsymbol{\alpha}\otimes\boldsymbol{r}_2^{\alpha},...,\boldsymbol{\alpha}\otimes\boldsymbol{r}_k^{\alpha}]=\boldsymbol{P}=[P_1,P_2,...,P_k],f(\boldsymbol{\beta})=d[\boldsymbol{\beta}\otimes\boldsymbol{r}_1^{\beta},\boldsymbol{\beta}\otimes\boldsymbol{r}_2^{\beta},...,\boldsymbol{\beta}\otimes\boldsymbol{r}_k^{\beta}]=\boldsymbol{Q}=[Q_1,Q_2,...,Q_k],$$

得到两个新的向量 $\boldsymbol{P}$ 和 $\boldsymbol{Q}$,$\boldsymbol{r}_j^{\alpha}$ 和 $\boldsymbol{r}_j^{\beta}$ 分别表示 $\boldsymbol{R}^{\alpha}$和 $\boldsymbol{R}^{\beta}$的第 j 列的列向量.

其中,$P_j=\sum_{i=1}^{d}\arctan\left(\frac{\alpha_i}{r_{ij}^{\alpha}}\right),Q_j=\sum_{i=1}^{d}\arctan\left(\frac{\beta_i}{r_{ij}^{\beta}}\right)$,$r_{ij}^{\alpha}$ 和 r_{ij}^{β} 分别是 $\boldsymbol{r}_j^{\alpha}$ 和 $\boldsymbol{r}_j^{\beta}$ 的第 i 个元素.

对向量 $\boldsymbol{P}$ 和 $\boldsymbol{Q}$ 中的元素二值化:$P_j'=\begin{cases}1, & \text{if } P_j\geqslant 0\\ 0, & \text{if } P_j<0\end{cases},Q_j'=\begin{cases}1, & \text{if } Q_j\geqslant 0\\ 0, & \text{if } Q_j<0\end{cases}$.

得到对应的二值向量:$\boldsymbol{P}'=[p_1',p_2',...,p_d'],\boldsymbol{Q}'=[q_1',q_2',...,q_d']$.

$$E(H(\boldsymbol{P}',\boldsymbol{Q}'))=E\left(\sum_{j=1}^{k}(P_j'\oplus Q_j')\right)=\sum_{j=1}^{k}E(P_j'\oplus Q_j')=\sum_{j=1}^{k}\Pr(P_jQ_j<0),$$

$$E(P_jQ_j)=E\left(\sum_{l=1}^{d}\arctan\left(\frac{\alpha_l}{r_{lj}^{\alpha}}\right)\sum_{m=1}^{d}\arctan\left(\frac{\beta_m}{r_{mj}^{\beta}}\right)\right)\approx E\left(\sum_{l=1}^{d}\frac{\alpha_l}{r_{lj}^{\alpha}}\sum_{m=1}^{d}\frac{\beta_m}{r_{mj}^{\beta}}\right)=\sum_{l=1}^{d}\sum_{m=1}^{d}E\left(\frac{\alpha_l}{r_{lj}^{\alpha}}\right)E\left(\frac{\beta_m}{r_{mj}^{\beta}}\right).$$

因为 $r_{ij}^{\alpha}\sim N(0,1)$并且 $r_{ij}^{\alpha}\neq 0,r_{ij}^{\beta}\sim N(0,1)$并且 $r_{ij}^{\beta}\neq 0$,所以,r_{lj}^{α} 和 r_{mj}^{β} 的概率密度函数均为偶函数.

因为 $\boldsymbol{R}^{\alpha},\boldsymbol{R}^{\beta},\boldsymbol{\alpha}$和$\boldsymbol{\beta}$中的元素相互独立,

所以,根据定理 1,$1/r_{lj}^{\alpha}$ 和 $1/r_{mj}^{\beta}$ 的概率密度函数也均为偶函数.

所以,根据定理 2,α_l/r_{ij}^{α} 和β_m/r_{mj}^{β} 的概率密度函数也均为偶函数.

所以,$E\left(\frac{\alpha_l}{r_{lj}^{\alpha}}\right)=0,E\left(\frac{\beta_m}{r_{mj}^{\beta}}\right)=0$,因此,$E(P_jQ_j)=0$.

设 $Z=P_jQ_j$,根据定理 2 和定理 3,得 $f_Z(z)=f_Z(-z)$.所以,$\int_0^{\infty}f_Z(z)\mathrm{d}z=\int_{-\infty}^{0}f_Z(z)\mathrm{d}x$.

又因为 $\int_0^{\infty}f_Z(z)\mathrm{d}z+\int_{-\infty}^{0}f_Z(z)\mathrm{d}x=1$,所以,$\int_0^{\infty}f_Z(z)\mathrm{d}z=\int_{-\infty}^{0}f_Z(z)\mathrm{d}x=0.5$,

则 $\Pr(P_jQ_j\geqslant 0)=\Pr(Z\geqslant 0)=0.5,\Pr(P_jQ_j<0)=\Pr(Z<0)=0.5$,

则 $H(\boldsymbol{P}',\boldsymbol{Q}')$是服从参数为 k,0.5 的二项分布,$H(\boldsymbol{P}',\boldsymbol{Q}')\sim b(k,0.5)$.

$$E(H(\boldsymbol{P}',\boldsymbol{Q}'))=E\left(\sum_{j=1}^{k}(P_j'\oplus Q_j')\right)=\sum_{j=1}^{k}E(P_j'\oplus Q_j')=\sum_{j=1}^{k}\Pr(P_jQ_j<0)=\sum_{j=1}^{k}0.5=0.5k,$$

$$\Pr(H(\boldsymbol{P}',\boldsymbol{Q}')=n)=\binom{k}{n}0.5^n(1-0.5)^{k-n},n=0,1,...,k,$$

$$E(H_n(\boldsymbol{P}',\boldsymbol{Q}'))=E\left(\frac{H(\boldsymbol{P}',\boldsymbol{Q}')}{k}\right)=\frac{E\left(\sum_{j=1}^{k}(P_j'\oplus Q_j')\right)}{k}=\frac{\sum_{j=1}^{k}E(P_j'\oplus Q_j')}{k}=\frac{0.5k}{k}=0.5.$$

证毕. □

不同用户用不同口令生成各自的PalmPhasor之间的归一化海明距离为0.5,保证了足够的类间差异性,使第4种情况下PalmPhasor达到了很高的认证性能.

4种情况分析的结论见表2.

Table 2 Conclusions of the analysis in four scenarios

表2 4种情况分析的结论

情况	结论
第1种情况	归一化海明距离与掌纹特征元素的数学期望绝对值负相关,与其方差正相关
第2种情况	归一化海明距离保证了可重用性和多样性
第3种情况	归一化海明距离保证了最差情况下的类间鉴别性
第4种情况	归一化海明距离了最佳情况下的类间鉴别性

3.5 多方向分数级融合

采用均值策略进行多方向匹配分数融合提高性能的主要机制,依赖于对匹配分数方差的抑制作用.L 个方向匹配分数 d^τ进行分数级融合,则融合匹配分数的方差为

$$D\left(\frac{1}{L}\sum_{\tau=1}^{L}d^\tau\right)=\left(\frac{1}{L}\right)^2\left[\sum_{\tau=1}^{L}D(d^\tau)+\sum_{\tau1\neq\tau2}\mathrm{cov}(d^{\tau1},d^{\tau2})\right].$$

证明:

因为 $D\left(\frac{1}{L}\sum_{\tau=1}^{L}d^\tau\right)=\left(\frac{1}{L}\right)^2D\left(\sum_{\tau=1}^{L}d^\tau\right)$,

所以,问题转化为求证:

$$D\left(\sum_{\tau=1}^{L}d^\tau\right)=\left[\sum_{\tau=1}^{L}D(d^\tau)+\sum_{\tau1\neq\tau2}\mathrm{cov}(d^{\tau1},d^{\tau2})\right].$$

采用数学归纳法证明.

首先证明 L=2 的情况,即,$1\leqslant\tau1,\tau2\leqslant2$:

$$\begin{aligned}D(d^1+d^2)&=E[(d^1+d^2)-E(d^1+d^2)^2]\\&=E\{[(d^1-E(d^1))+(d^2-E(d^2))]^2\}\\&=E\{[d^1-E(d^1)]^2\}+E\{[d^2-E(d^2)]^2\}+2E\{[d^1-E(d^1)][d^2-E(d^2)]\}\\&=D(d^1)+D(d^2)+2\mathrm{cov}(d^1,d^2)\\&=D(d^1)+D(d^2)+\sum_{\tau1\neq\tau2}\mathrm{cov}(d^{\tau1},d^{\tau2}).\end{aligned}$$

若 L–1 个方向匹配分数融合的方差满足:

$$D\left(\sum_{\tau=1}^{L-1}d^\tau\right)=\left[\sum_{\tau=1}^{L-1}D(d^\tau)+2\sum_{\tau1\neq\tau2}\mathrm{cov}(d^{\tau1},d^{\tau2})\right],1\leqslant\tau1,\tau2\leqslant L-1,$$

则 L 个方向匹配分数融合的方差满足:

$$
\begin{aligned}
D\left(\sum_{\tau=1}^{L} d^{\tau}\right) &= D\left(\sum_{\tau=1}^{L-1} d^{\tau} + d^{L}\right) \\
&= D\left(\sum_{\tau=1}^{L-1} d^{\tau}\right) + D(d^{L}) + 2\operatorname{cov}\left(\sum_{\tau=1}^{L-1} d^{\tau}, d^{L}\right) \\
&= \left[\sum_{\tau=1}^{L-1} D(d^{\tau}) + \sum_{\tau 1 \neq \tau 2} \operatorname{cov}(d^{\tau 1}, d^{\tau 2})\right] + D(d^{\tau}) + 2\operatorname{cov}\left(\sum_{\tau=1}^{L-1} d^{\tau}, d^{L}\right) \\
&= \left[\sum_{\tau=1}^{L-1} D(d^{\tau}) + D(d^{L})\right] + \left[\sum_{\tau 1 \neq \tau 2} \operatorname{cov}(d^{\tau 1}, d^{\tau 2}) + 2\operatorname{cov}\left(\sum_{\tau=1}^{L-1} d^{\tau}, d^{L}\right)\right] \\
&= \left[\sum_{\tau=1}^{L} D(d^{\tau}) + \sum_{\tau 1 \neq \tau 2} \operatorname{cov}(d^{\tau 1}, d^{\tau 2})\right].
\end{aligned}
$$

所以, $D\left(\frac{1}{L}\sum_{\tau=1}^{L} d^{\tau}\right) = \left(\frac{1}{L}\right)^{2}\left[\sum_{\tau=1}^{L} D(d^{\tau}) + \sum_{\tau 1 \neq \tau 2} \operatorname{cov}(d^{\tau 1}, d^{\tau 2})\right]$.

证毕. □

分数级融合后匹配分数的方差是各匹配分数方差和各协方差的平均值,由于 $\operatorname{cov}(d^{\tau 1}, d^{\tau 2}) < D(d^{\tau})$,分数级融合后的方差比各匹配分数的方差小,从而有效地降低了融合后的方差,提高了匹配分数分布的聚合性.

但随着方向个数 L 的增加,各个方向匹配分数的协方差 $\operatorname{cov}(d^{\tau 1}, d^{\tau 2})$会增加,因此随着 L 的增加,不仅计算量会增加,多方向分数级融合对性能的提高效果也会减弱.第 4.1 节将对 L 的取值做进一步的探讨和实验验证.

4 实验结果

本文实验在香港理工大学掌纹数据库(http://www4.comp.polyu.edu.hk/~biometrics/)上测试,数据库包含了 193 个人的 386 个掌纹,每个掌纹分两个时间段采集约 20 张图片,共 7 752 张掌纹图片.

4.1 多样性与可重用性

多样性和可重用性在数学意义上是等价的.为了考核多样性和可重用性,给出新的评判指标,将同类生物特征与不同口令生成的可撤销生物特征模板之间的匹配定义为“伪类间”匹配.第 2 种情况的理论分析已证明:PalmPhasor 随着口令的改变,更新的模板和原先的模板之间的归一化海明距离足够大,即,伪类间匹配的归一化海明距离足够大,以保证成功更新模板.

传统的认证 ROC(receiver operating characteristic)曲线的横、纵坐标分别为错误接受率(false accept rate,简称 FAR)和正确接受率(genuine accept rate,简称 GAR).将类内距离和伪类间距离比较,可以绘制新型的更新 ROC 曲线,横、纵坐标分别为错误更新率(false update rate,简称 FUR)和 GAR.FUR 表示在某一阈值下模板不能成功更新的概率.图 2 是 4 个方向 PalmPhasor 及其多方向分数级融合的更新 ROC 曲线.多方向分数级融合后的更新性能比单方向的更新性能有明显的提高,满足常用系统的更新率指标要求.

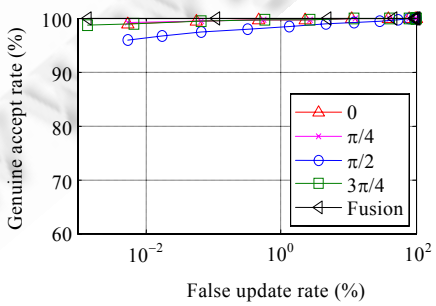


Fig.2 Update ROCs of PalmPhasors along four orientations and their multi-orientation score level fusion

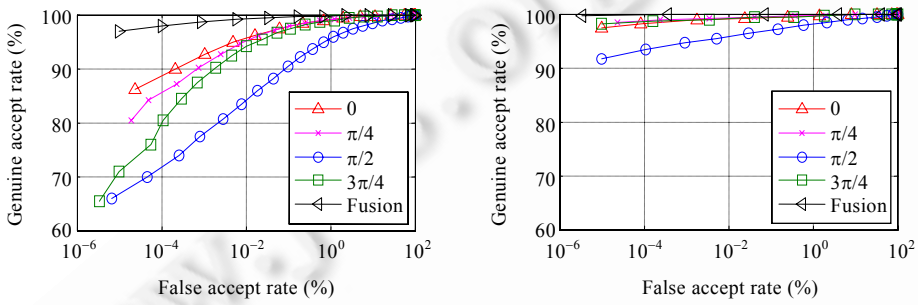
图 2 4 个方向 PalmPhasor 及其多方向分数级融合的更新 ROC 曲线

4.2 不可逆性

PalmPhasor 算法的不可逆性依赖于以下 3 个单向变换策略:(1) 方程系统存在 m 个方程和 $2m$ 个未知数,$m<2m$,属于欠定方程,有无数个解,无法重构和恢复出原始的掌纹特征;(2) 数据经过阈值化操作转化为二值化数据,不可逆量化过程进一步提高了掌纹模板的安全性和隐私性;(3) 当对应的掌纹特征与随机数的商值足够大时,非线性方程也增强了系统的安全性.

4.3 认证性能

图 3 是最差和最佳两种情况下,4 个方向 PalmPhasor 及其多方向分数级融合的认证 ROC 曲线.多方向分数级融合的认证性能比单方向的认证性能有明显的提高,最佳情况下的认证精度高于最差情况;但在最差情况下,多方向分数级融合的 PalmPhasor 仍然可以达到较高的精度.

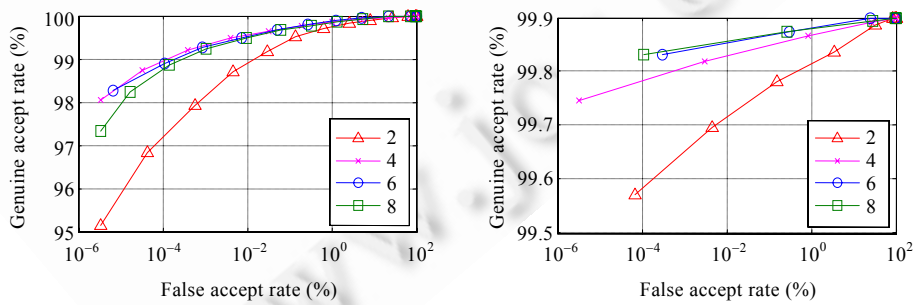


(a) 最差情况 (b) 最佳情况

Fig.3 Verification ROCs of PalmPhasors along four orientations and their multi-orientation score level fusion

图 3 4 个方向 PalmPhasor 及其多方向分数级融合的认证 ROC 曲线

图 4 是最差和最佳两种情况下取不同方向个数进行多方向分数级融合的认证 ROC 曲线.最差情况下,4 个、6 个和 8 个方向融合的精度较为接近,并且优于两个方向融合;最佳情况下,6 个和 8 个方向融合的精度较为接近,并且优于两个和 4 个方向融合.融合方向个数越多,计算复杂度越高.当融合方向个数多于 6 个时,精度没有明显提高,因此选取 6 个方向融合较为合适.在精度要求满足的条件下,权衡计算效率,也可选择 4 个方向融合.



(a) 最差情况 (b) 最佳情况

Fig.4 Verification ROCs of multi-orientation score level fusion with different numbers of orientation

图 4 不同方向个数多方向分数级融合的认证 ROC 曲线

5 结论与展望

已有可撤销生物特征方案难以同时满足多项性能指标要求.PalmPhasor 算法是用于掌纹模板保护的一种高效而安全的可撤销掌纹编码方案,此方案同时满足了可撤销生物特征的多项指标.即使在最差情况下,

PalmPhasor 也可以达到实用化的精度要求.本文建立了用于系统分析 PalmPhasor 性能的完整框架.在相关辅助定理以及 Gabor 滤波掌纹图像实部和虚部分布特性的预备知识基础上,分 4 种情况分别进行了具体的理论分析和证明.理论分析和实验结果均证实了多方向分数级融合增强的 PalmPhasor 算法的有效性.

致谢 感谢评审专家在本文修改和完善过程中提出的宝贵建议.感谢香港理工大学人体生物特征识别研究中心的张大鹏教授课题组为本文的研究和测试提供了掌纹数据库.

References:

[1] Kong A, Zhang D, Kamel M. A survey of palmprint recognition. Pattern Recognition, 2009,42(7):1408−1418. [doi: 10.1016/j.patcog.2009.01.018]

[2] Wu XQ, Wang KQ, Zhang D. An approach to line feature representation and matching for palmprint recognition. Ruan Jian Xue Bao/Journal of Software, 2004,15(6):869−880 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/15/869.htm

[3] Li WX, Zhang D, Xu ZQ. Palmprint recognition based on Fourier transform. Ruan Jian Xue Bao/Journal of Software, 2002,13(5):879−886 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/13/879.htm

[4] Leng L, Zhang JS, Khan MK, Chen X, Alghathbar K. Dynamic weighted discrimination power analysis: A novel approach for face and palmprint recognition in DCT domain. Int'l Journal of the Physical Sciences, 2010,5(17):2543−2554.

[5] Leng L, Zhang JS, Xu J, Khan MK, Alghathbar K. Dynamic weighted discrimination power analysis in DCT domain for face and palmprint recognition. In: Proc. of Int'l Conf. on Information and Communication Technology Convergence. Washington: IEEE Computer Society, 2010. 467−471. [doi: 10.1109/ICTC.2010.5674791]

[6] Zhang D, Kong WK, You J, Wong M. On-Line palmprint identification. IEEE Trans. on Pattern Analysis and Machine Intelligence, 2003,25(9):1041−1050. [doi: 10.1109/TPAMI.2003.1227981]

[7] Kong A, Zhang D, Kamel M. Palmprint identification using feature-level fusion. Pattern Recognition, 2006,39(3):478−487. [doi: 10.1016/j.patcog.2005.08.014]

[8] Kong A, Zhang D. Competitive coding scheme for palmprint verification. In: Proc. of the 17th Int'l Conf. on Pattern Recognition. Washington: IEEE Computer Society, 2004. 520−523. [doi: 10.1109/ICPR.2004.1334184]

[9] Sun Z, Tan T, Wang Y, L SZ. Ordinal palmprint representation for personal identification. In: Proc. of the IEEE Int'l Conf. on Computer Vision and Pattern Recognition. Washington: IEEE Computer Society, 2005. 279−284. [doi: 10.1109/CVPR.2005.267]

[10] Jiaa W, Huang DS, Zhang D. Palmprint verification based on robust line orientation code. Pattern Recognition, 2008,41(5):1504−1513. [doi: 10.1016/j.patcog.2007.10.011]

[11] Guo ZH, Zhang D, Zhang L, Zuo WM. Palmprint verification using binary orientation co-occurrence vector. Pattern Recognition Letters, 2009,30(13):1219−1227. [doi: 10.1016/j.patrec.2009.05.010]

[12] Jain AK, Nandakumar K, Nagar A. Biometric template security. EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics, 2008. 1−20. [doi: 10.1155/2008/579416]

[13] Ratha N, Connell J, Bolle R. Enhancing security and privacy in biometrics-based authentication systems. IBM System Journal, 2001,40(3):614−634. [doi: 10.1147/sj.403.0614]

[14] Li P, Tian J, Yang X, Shi P, Zhang YY. Biometric template protection. Ruan Jian Xue Bao/Journal of Software, 2009,20(6):1553−1573 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3528.htm [doi: 10.3724/SP.J.1001.2009.03528]

[15] Juels A, Wattenberg M. A fuzzy commitment scheme. In: Proc. of the 6th ACM Conf. on Computer and Communication Security. New York: ACM Press, 2009. 28−36. [doi: 10.1145/319709.319714]

[16] Juels A, Sudan M. A fuzzy vault scheme. Designs, Codes and Cryptography, 2006,38(2):237−257. [doi: 10.1007/s10623-005-6343-z]

[17] Wu XQ, Zhang D, Wang KQ. A palmprint cryptosystem. In: Lee SW, Li SZ, eds. Proc. of the Int'l Conf. on Biometrics, Vol.4642. Berlin: Springer-Verlag, 2007. 1035−1042. [doi: 10.1007/978-3-540-74549-5_108]

[18] Wu XQ, Zhang D, Wang KQ. A cryptosystem based on palmprint feature. In: Proc. of the 19th Int'l Conf. on Pattern Recognition. Washington: IEEE Computer Society, 2008. 1−4. [doi: 10.1109/ICPR.2008.4761117]

[19] Leng L, Zhang JS. Dual-Key-Binding cancelable palmprint cryptosystem for palmprint protection and information security. Journal of Network and Computer Applications, 2011,34(6):1979−1989. [doi: 10.1016/j.jnca.2011.07.003]

[20] Li HJ, Zhang JS, Zhang ZT. Generating cancelable palmprint templates via coupled nonlinear dynamic filters and multiple orientation palmcodes. Information Sciences, 2010,180(20):3876−3893. [doi: 10.1016/j.ins.2010.06.040]

[21] Li HJ, Zhang JS. A novel chaotic stream cipher and its application to palmprint template protection. Chinese Physics B, 2010,19(4): 040505_1−040505_10. [doi: 10.1088/1674-1056/19/4/040505]

[22] Teoh ABJ, Ngo DCL, Goh A. BioHashing: Two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognition, 2004,37(11):2245−2255. [doi: 10.1016/j.patcog.2004.04.011]

[23] Teoh ABJ, Ngo DCL. Cancellable biometrics featuring with tokenised random number. Pattern Recognition Letters, 2005,26(10): 1454−1460. [doi: 10.1016/j.patrec.2004.11.021]

[24] Kong A, Cheung KH, Zhang D, Kamel M, You J. An analysis of BioHashing and its variants. Pattern Recognition, 2006,39(7): 1359−1368. [doi: 10.1016/j.patcog.2005.10.025]

[25] Johnson W, Linderstrauss J. Extensions of lipshitz mapping into hilbert space. Contemporary Mathematics, 1984,26:189−206. [doi: 10.1090/conm/026/737400]

[26] Connie T, Teoh ABJ, Goh M, Ngo D. PalmHashing: A novel approach for cancelable biometrics. Information Processing Letters, 2005,93(1):1−5. [doi: 10.1016/j.ipl.2004.09.014]

[27] Leng L, Zhang JS, Khan MK, Chen X, Ji M, Alghathbar K. Cancelable PalmCode generated from randomized Gabor filters for palmprint template protection. Scientific Research and Essays, 2011,6(4):784−792.

[28] Leng L, Zhang JS, Chen G, Khan MK, Bai P. Two dimensional PalmPhasor enhanced by multi-orientation score level fusion. In: Proc. of the 8th FTRA Int'l Conf. on Secure and Trust Computing, Data Management, and Applications. Berlin: Springer-Verlag, 2011. 122−129. [doi: 10.1007/978-3-642-22339-6_15]

附中文参考文献:

[2] 邬向前,王宽全,张大鹏.一种用于掌纹识别的线特征表示和匹配方法.软件学报,2004,15(6):869−880. http://www.jos.org.cn/1000-9825/15/869.htm

[3] 李文新,张大鹏,许卓群.基于傅立叶变换的掌纹识别方法.软件学报,2002,13(5):879−886. http://www.jos.org.cn/1000-9825/13/879.htm

[14] 李鹏,田捷,杨鑫,时鹏,张阳阳.生物特征模板保护.软件学报,2009,20(6):1553−1573. http://www.jos.org.cn/1000-9825/3528.htm [doi: 10.3724/SP.J.1001.2009.03528]

冷璐(1982−),男,山东青岛人,博士,讲师,CCF 学生会员,主要研究领域为生物特征模板保护,生物特征识别与身份认证,图像处理,信息安全.

黎明(1965−),男,博士,教授,博士生导师,主要研究领域为图像处理与模式识别,智能计算.

Andrew Beng Jin TEOH(1975−),男,博士,副教授,主要研究领域为生物特征安全,模式识别,机器学习.

Cheonshik KIM(1966−),男,博士,教授,主要研究领域为多媒体系统,数据隐藏,水印.