

基于特征距离切尾均值的新颖指纹密钥生成方法

贾忠田^{1,2}, 秦庆龙¹, 马莉³, 彭立志^{1,2}

(1. 济南大学信息科学与工程学院, 山东 济南 250022;

2. 山东省网络环境智能计算技术重点实验室, 山东 济南 250022; 3. 济南大学科技处, 山东 济南 250022)

摘要:近年来,生物特征识别技术在访问控制领域得到了广泛应用,有效解决了身份认证过程中的口令管理问题。但传统的基于生物特征的身份认证方法需要在应用系统中保存用户的生物特征模板,容易造成用户生物特征数据的丢失和泄露。学术上主要采用两种技术路线:一是对提取到的生物特征数据进行处理,使最后正式使用或存储在数据库中的认证信息不包含原始生物特征,二是把生物特征写入智能卡并借助智能卡生成公钥密码体制的私钥。针对如何直接利用指纹特征数据构造公钥密码体制的私钥而不必依赖智能卡的问题,采用指纹细节特征提取分析的方法,对指纹稳定特征点和稳定特征距离进行了详细研究。给出了稳定特征点集合、等长稳定特征点集合、密钥特征点集合以及切尾均值集合的计算方法,提出了基于特征距离切尾均值的新颖指纹密钥生成方法。该方法在不存储指纹数据的条件下通过重新采集指纹即可重构指纹密钥,通过哈希函数加盐的方法实现了指纹密钥的撤销和指纹密钥的更新,解决了从指纹模糊数据到密钥精确数据的转换问题。实验表明,尝试10次重新采集指纹成功重构指纹密钥的概率达到0.7354,尝试60次重新采集指纹成功重构指纹密钥的概率达到0.9806。

关键词:生物特征;指纹特征点;稳定特征点;切尾均值;指纹密钥

中图分类号: TP39

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023073

Novel fingerprint key generation method based on the trimmed mean of feature distance

JIA Zhongtian^{1,2}, QIN Qinglong¹, MA Li³, PENG Lizhi^{1,2}

1. School of Information Science and Engineering, University of Jinan, Jinan 250022, China

2. Shandong Provincial Key Laboratory of Network Based Intelligent Computing, Jinan 250022, China

3. Science and Technology, University of Jinan, Jinan 250022, China

Abstract: In recent years, biometrics has become widely adopted in access control systems, effectively resolving the

收稿日期: 2023-03-23; 修回日期: 2023-08-18

通信作者: 贾忠田, ise_jiazt@ujn.edu.cn

基金项目: 国家自然科学基金(61972176); 山东省自然科学基金(ZR2022MF264); 济南大学科技计划(XKY1931)

Foundation Items: The National Natural Science Foundation of China(61972176), Shandong Natural Science Foundation(ZR2022MF264), Science and Technology Project of University of Jinan(XKY1931)

引用格式: 贾忠田, 秦庆龙, 马莉, 等. 基于特征距离切尾均值的新颖指纹密钥生成方法[J]. 网络与信息安全学报, 2023, 9(5): 178-187.

Citation Format: JIA Z T, QIN Q L, MA L, et al. Novel fingerprint key generation method based on the trimmed mean of feature distance[J]. Chinese Journal of Network and Information Security, 2023, 9(5): 178-187.

challenges associated with password management in identity authentication. However, traditional biometric-based authentication methods often lead to the loss or leakage of users' biometric data, compromising the reliability of biometric authentication. In the literature, two primary technical approaches have been proposed to address these issues. The first approach involves processing the extracted biometric data in a way that the authentication information used in the final stage or stored in the database does not contain the original biometric data. The second approach entails writing the biometric data onto a smart card and utilizing the smart card to generate the private key for public key cryptography. To address the challenge of constructing the private key of a public key cryptosystem based on fingerprint data without relying on a smart card, a detailed study was conducted on the stable feature points and stable feature distances of fingerprints. This study involved the extraction and analysis of fingerprint minutiae. Calculation methods were presented for sets of stable feature points, sets of equidistant stable feature points, sets of key feature points, and sets of truncated means. Based on the feature distance truncated mean, an original fingerprint key generation algorithm and key update strategy were proposed. This scheme enables the reconstruction of the fingerprint key through re-collecting fingerprints, without the need for direct storage of the key. The revocation and update of the fingerprint key were achieved through a salted hash function, which solved the problem of converting ambiguous fingerprint data into precise key data. Experiments prove that the probability of successfully reconstructing the fingerprint key by re-collecting fingerprints ten times is 0.7354, and the probability of reconstructing the fingerprint key by re-collecting fingerprints sixty times is 98.06%.

Keywords: biometric, fingerprint features points, stable features points, trimmed mean, fingerprint key

0 引言

随着网络信息化技术的发展,网络应用系统在各个领域都得到了普遍应用,给人们的生产和生活带来了极大便利。但是,在使用这些网络应用系统时,人们经常被各种账号和口令所困扰。如何在保证用户账号安全的同时,准确且方便地对用户进行身份认证是网络应用系统必须解决的首要问题。传统的认证方法主要是通过账号与口令对用户身份进行验证^[1],但是如果出现口令遗忘、泄露或者被盗等情况,就会带来用户账号丢失、冒用、盗用等诸多网络安全问题。生物特征识别^[2]是近年来迅速发展起来的一种身份认证技术,它利用人与生俱来的生物特征充当身份认证时的信物凭证^[3]。由于人的生物特征具备唯一性、方便性与终身不变性等特点,采用生物特征进行身份认证的方法克服了传统身份认证方案中的系列难题,逐渐成为近年来身份认证领域学术研究的热点问题^[4-5]。但是,传统的基于生物特征识别的身份认证方法需要在应用系统中保存用户的生物特征模板^[6-7],容易造成用户生物特征丢失或泄露。

针对上述问题,本文结合现代密码学的理论

与技术,提出了指纹细节特征生成密钥的新方法。与其他现有相关文献中所提方案不同,本文方法无须在系统后台保存任何指纹模板数据,也无须客户端借助智能卡存储指纹信息,而是通过多次采集指纹并找出指纹共同细节特征的方法,直接构造密码学意义上的密钥。如果把本文提出的利用指纹细节特征生成的密钥作为公钥密码算法的签名私钥,则可以在多种应用场景下非常方便地构建基于数字签名的身份认证方案^[8],而不必担心个人的指纹隐私泄露问题。本文的主要贡献如下。

1) 提出了等长稳定特征点集合、密钥特征点集合以及切尾均值集合的计算方法。

2) 提出了利用切尾均值生成原始指纹密钥的算法。

3) 给出了利用原始指纹密钥及哈希函数生成指纹密钥及密钥更新的方法。

1 生物特征加密技术研究现状

1.1 生物特征识别技术

利用生物特征识别进行身份认证的系统由注册与认证两个过程组成^[3]。在用户注册时,通过传感采集设备采集用户的生物特征,利用特定的提取算法提取出生物特征数据,生成生物特征模

板并保存在模板库中。当用户需要进行身份认证时,系统重新采集用户的生物特征,并且将新提取的生物特征与模板库中的生物特征模板进行对比,根据二者的相似度是否超过系统设置的阈值判断认证是否成功。

1.2 生物特征识别技术的痛点

生物特征识别技术在访问控制和身份认证等领域得到非常广泛的应用,然而生物特征识别技术也暴露出非常严重的安全问题^[9]。首先,人的生物特征资源是非常有限的,如人共有10根手指,即使没有任何指纹信息丢失或者泄露的情况下,最多有10次更新不同手指指纹的机会,无法满足身份认证系统需要定期更新认证凭据的要求。其次,保存在模板数据库中的生物特征模板,极易成为被攻击的目标,任何对生物模板的篡改或者盗窃,都会使采用生物特征识别进行认证的方法失去作用^[10]。

1.3 相关工作

对于上述安全漏洞的学术研究主要集中对生物特征模板数据的保护上,而且多数研究都是根据Tomko^[11]提出的“生物特征加密”技术对生物特征模板数据进行保护。李鹏等^[12]利用UNIX操作系统登录口令加密存储的例子清楚地阐明了这种保护方法的基本原理,但同时指出生物特征不能直接像UNIX操作系统那样直接使用哈希函数进行加密。2004年,Uludag等^[13]总结了几种把密钥与存储在数据库中的生物识别模板进行整体绑定的算法^[14-18],他们认为相关研究应该关注怎样提高单个生物识别匹配器的准确性,以及设计有效的多生物识别策略,保证生物特征的模糊性与密码学的准确性处于相对平衡的状态,这是很多生物特征加密技术研究的重点问题。

随着相关研究在生物特征加密领域不断推进,各式各样的生物特征加密算法不断被提出。文献[19-20]研究了这些加密算法的特点,把它们分成了3类,即生物特征加密系统、可撤销生物特征以及生物特征认证协议。文献[12]通过对各种生物特征加密算法分析研究,归纳出一个较为理想的生物特征加密算法的基本要求,在某种程度上对于生物特征加密算法研究起到了较好的指导作用。

2009年,罗成行等^[21]提出了一种基于指纹和

智能卡的密钥封装方案,其基本思想是将指纹特征数据处理后与随机生成的密钥联合编码,再用智能卡存储编码后的结果。因为这种方案不需要存储指纹模板,只需要存储一串具有纠错能力的字符串,所以具有较高的安全性。2010年,陈开志等^[22]提出了一种基于BioHashing和Fuzzy Commitmen 密钥绑定的双重可删除指纹模板(DCFT)方法,使得最后存储在指纹模板数据库中的信息同样不需要原始指纹特征信息。虽然该方案使用Fingercode算法而导致图像识别存在一些缺陷,但是该方案证明这种基于BioHashing和Fuzzy Commitmen 密钥绑定的指纹模板研究方法是可行的。2012年,Sheng等^[23]提出一种通过指纹图像中方向场值生成密钥的方法,虽然该方案不需要保存生物特征模板,但是辅助生成密钥比特的随机序列仍然无法摆脱存储卡或者中心数据库。2015年,张宁等^[20]对目前国际上主流的生物特征加密方法进行了归纳整理,阐述了各种方法的优劣,为该领域的后续研究提供了参考。2016年,高莹等^[24]提出了一种更高效的指纹特征加密方案,该方案从模糊身份加密出发,构造一种新的模糊身份加密算法,在此基础上借助密钥共享算法构造了双阈值的指纹生物特征加密方案。2021年,Wang等^[25]提出了基于特征距离与生成区间的指纹密钥生成算法,该算法基于指纹特征距离,利用生成区间机制以及可变区间编码生成用户指纹密钥,实现了指纹数据的容错性与指纹密钥的可撤销性。此算法不需要存储指纹特征数据、指纹特征点模板,但仍需借助存储介质保存生成区间及其对应码字。2021年,张翔宇等^[26]提出一种基于指纹识别的跨域认证方案,该方案利用区块链的分布式和不易篡改的特性,将辅助恢复值写入全局账本,从而解决了现有跨域认证方案的一些安全和隐私问题。该方案能够有效抵御伪造和字典攻击等安全威胁,同时保护用户的隐私和提供高效的跨域认证服务。虽不需智能卡存储辅助信息,但算法复杂度较高且不具有可再生性。2022年,Elsadai等^[27]未使用传统的Gabor小波和滤波器,而是采用机器学习方法将指纹模板分类为数字特征,将Base 64编码器应用于归一化指纹图像,同时采用内部区块链,以分布式

数据库的形式实现所有安全服务。这种方案侧重于在指纹识别中使用深度学习方法，以及对基于用户数据生成的区块链进行实验，启示了未来研究方向。

综上所述，对于生物模板数据保护的一个有效解决方案是通过各种手段对提取到的生物特征数据进行处理，使得最后正式使用或存储在数据库中的认证信息不包含原始生物特征。这样，即使这些认证信息不慎丢失或泄露也可及时地撤销与更新。

2 新型指纹密钥生成方法

本节详细讨论本文提出的新型指纹密钥生成方法^[28]。为讨论方便，本文用同一个手指的 N 幅指纹图像为例进行论述。

2.1 指纹图像的预处理

用 Aliloup^[29]提出的指纹图像处理方法，对 K 幅指纹图像进行预处理，得到 K 个指纹特征点集合组成的集合 $FM = \{FM_i | i=1,2,\dots,K\}$ ，其中， $FM_i = \{C_i^j = (x_i^j, y_i^j, t_i^j, \theta_i^j) | j=1,2,\dots,K_i\}$ ($i=1,2,\dots,K$) 表示由第 i 个指纹图像得到的特征点集合， K 表示指纹图像的数量， K_i 表示集合 FM_i 所包含的特征点个数，即 $K_i = |FM_i|$ ， x_i^j 、 y_i^j 、 t_i^j 、 θ_i^j 分别表示第 i 幅指纹图像的第 j 个特征点 C_i^j 的横坐标、纵坐标、特征点类型和方向场。

其中，横坐标和纵坐标表示特征点在指纹图像中的像素坐标。特征点类型包括端点、交叉点、中心点等，可作为辅助信息进行指纹匹配。方向场表示特征点周围指纹纹理的走向，可以用于旋转指纹图像，使得特征点方向保持一致，从而提高指纹匹配的准确性。特征点的横坐标、纵坐标、特征类型和方向场共同作为“属性”，来实现指纹图像的匹配和识别。

2.2 确定稳定特征点集合

在得到同一个手指的 K 幅指纹图像的特征点集合 FM_i ($i=1,2,\dots,K$) 之后，需要找出每个特征点集合 FM_i 的最佳中心点，并得到稳定的特征点集合。确定最佳中心点与获得稳定特征点集合的过程包括以下步骤。

步骤 1 任取特征点集合 $FM_r \in FM$ ($1 \leq r \leq K$)，作为参考集合。

步骤 2 用 `match()` 函数计算类型相同的两个特征点 C_r^i ($C_r^i \in FM_r, i=1,2,\dots,K_r$) 与 C_s^j ($C_s^j \in FM_s, j=1,2,\dots,K_s$) 之间的欧几里得距离 Δd_i^j 和方向场之差 $\Delta \theta_i^j$ 。

步骤 3 用 `rotate()` 函数把 FM_s 中的特征点分别按照 Δd_i^j 和 $\Delta \theta_i^j$ 进行平移和旋转，得到 $K_r \times K_s$ 个临时特征点集合 TM_{ij} 。

步骤 4 用 `score()` 函数计算 FM_r 与 TM_{ij} 的匹配度，匹配度计算方法如式(1)所示。

$$q_{ij} = \frac{p_{ij}^2}{K_r \cdot K_s} \quad (1)$$

其中， p_{ij} 为 FM_r 与 TM_{ij} 中匹配成功的特征点的个数，如果特征点 C_r^l ($C_r^l \in FM_r$) 与临时特征点集合 TM_{ij} 中的第 m 个特征点 C_{ij}^m 的特征点之间的欧几里得距离小于阈值 Δd 且方向场小于阈值 $\Delta \theta$ ，则认为这两个特征点匹配成功，给特征点 C_{ij}^m 贴上标签 l ， $\text{label}(C_{ij}^m) = l$ ，表示该特征点与 FM_r 中的第 l 个特征点是同一个特征点。

步骤 5 计算最大匹配度 q_{uv} ，即比较步骤 4 中得到的 $K_r \times K_s$ 个 q_{ij} 并把数值最大的一个记为 q_{uv} 。

步骤 6 把步骤 5 中计算得到的 q_{uv} 对应的临时特征点集合中所有匹配成功的特征点选出来组成新特征点集合，称为稳定特征点集合，记作 FM'_s ，记 $N_s = |FM'_s|$ ，把特征点 C_s^v 作为稳定特征点集合 FM'_s 的最佳中心点。确定稳定特征点集合的过程如算法 1 所示。

算法 1 确定稳定特征点集合

输入 指纹特征点集合 FM

输出 $S[K]$ //最佳中心点

$FM' = \{FM'_s | s=1,2,\dots,K-1\}$

//任取集合 FM 中的一个特征点集合 $\forall FM_r \in FM$

//把 FM_r 中的每一个特征点与其他 $K-1$ 个特

//征点集合中的特征点逐个进行匹配

For FM_s in FM / FM_r {

For C_r^i in FM_r {

For C_s^j in FM_s {

If($t_r^i == t_s^j$) {

//计算欧几里得距离与方向场差

```

match( $C_r^i, C_s^j, \Delta d_{ij}, \Delta \theta_{ij}$ );
}
//把  $FM_s$  逐点平移旋转并存入  $TM_{ij}$ 
rotate( $FM_s, \Delta d_{ij}, \Delta \theta_{ij}, TM_{ij}$ );
}
}
 $q_{uv} = \max(\text{score}(FM_r, TM));$ 
 $FM'_s = \text{select}(TM_{uv});$ 
 $S[s] = C_s^v;$ 
}

```

2.3 构造密钥特征点集合

通过算法 1, 得到稳定特征点集合 FM' , 即 $FM' = \{FM'_s \mid s=1, 2, \dots, K-1, N_s \neq FM'_s\}$ 。在此基础上构造密钥特征点集合, 该过程包括以下步骤。

步骤 1 按照标签值是否相同依次检查稳定特征点集合 FM'_s ($s=1, 2, \dots, K-1$) 中的特征点是否也存在其他稳定特征点集合 $FM' \setminus FM'_s$ 中(即判断两个特征点的标签值是否相等), 若存在, 则把当前特征点按顺序放入等长稳定特征点集合 FM''_s 中 ($s=1, 2, \dots, K-1$), 令 $FM'' = \{FM''_s \mid s=1, 2, \dots, K-1\}$, 其中每一个 FM''_s ($s=1, 2, \dots, K-1$) 都具有相同的元素个数, 记 $|FM''_s| = N$, 具体过程如算法 2 所示。

步骤 2 从 FM'' 中任取 m_1 个等长稳定特征点集合, 随机取 m_2 次, 得到 $m_1 m_2$ 个等长稳定特征点集合, 这 $m_1 m_2$ 个等长稳定特征点集合称作密钥特征点集合。

步骤 3 令 $M = m_1 m_2$, 则这 M 个密钥生成特征点集合可以表示为 $SM_k = \{\alpha_k^1, \alpha_k^2, \dots, \alpha_k^N \mid N \neq FM''_s, s=1, 2, \dots, K-1, k=1, \dots, M\}$ 。

经过以上步骤得到的密钥特征点集合具有相同的元素个数, 即每个密钥特征点集合包含相同数量的特征点, 特征点在集合中按照标签值从小到大的顺序排列, 而且包含一个特殊的特征点, 即最佳中心点。

算法 2 等长稳定特征点集合构造

输入: 稳定特征点集合 FM'

输出: 等长稳定特征点集合 FM''

For FM'_s in FM' {

```

For  $FM'_t$  in  $FM' \setminus FM'_s$  {
  For( $i=0; i \leq N_s-1; i++$ ) {
    For( $j=0; j \leq N_t-1; j++$ ) {
      If( $\text{label}(FM'_s[i]) = \text{label}(FM'_t[j])$ )
         $FM''_s[i] = FM'_s[i];$ 
    }
  }
}
 $FM'' = \{FM''_s \mid s=1, 2, \dots, K-1\}$ 

```

2.4 特征距离计算

在获得密钥特征点集合 SM_k ($k=1, \dots, M$) 后, 按照算法 1 确定最佳中心点 $\alpha_k^o = (x_k^o, y_k^o, t_k^o, \theta_k^o)$, 计算其与本集合其余特征点 $\alpha_k^j = (x_k^j, y_k^j, t_k^j, \theta_k^j)$ 之间的欧几里得距离 d_k^j , $o \in \{1, 2, \dots, N\}$, $j=1, 2, \dots, o-1, o+1, \dots, N$ 。

经过计算, 得到指纹特征点特征距离集合, 记作 $D_k = \{d_k^j \mid j=1, 2, \dots, o-1, o+1, \dots, N\}$, $k=1, 2, \dots, M$ 。

定义最佳中心点 α_k^o ($o \in \{1, 2, \dots, N\}$) 与其他特征点 α_k^j ($j=1, 2, \dots, o-1, o+1, \dots, N$) 之间的切尾均值, 如式(2)所示。

$$d_j = \frac{d_{j,\text{sum}} - d_{j,\text{min}} - d_{j,\text{max}}}{M-2} \quad (2)$$

切尾均值生成如图 1 所示, $d_{j,\text{sum}} = \text{sum}(d_1^j, d_2^j, \dots, d_M^j)$, $d_{j,\text{min}} = \min(d_1^j, d_2^j, \dots, d_M^j)$, $d_{j,\text{max}} = \max(d_1^j, d_2^j, \dots, d_M^j)$, 得到切尾均值集合 $FD = \{d_j \mid j=1, 2, \dots, N-1\}$ 。

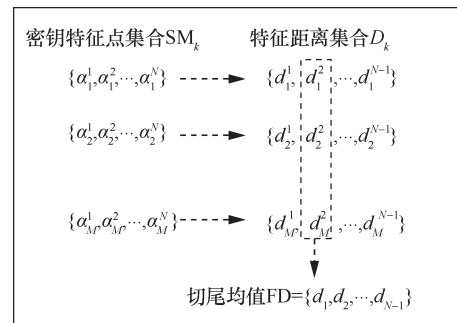


图 1 切尾均值生成

Figure 1 Trim mean generation

2.5 原始指纹密钥生成

原始指纹密钥生成算法如算法 3 所示, 包括

以下步骤。

步骤 1 调用 round() 函数, 从切尾均值小数点后最后一位小数开始往前依次进行四舍五入, 直到个位上的数完成四舍五入。处理后的切尾均值全部成为个位数为零的整数。

步骤 2 将个位数为零的切尾均值分别除以 10, 得到只保留 10 进位以上的整数。

步骤 3 将每个十进制数依次转化为二进制数。

步骤 4 截取二进制数据右边的 L bit, 不足 L bit 的, 在左边用 “0” 补齐。

步骤 5 将 $N-1$ 个 L bit 的二进制比特串依次连接形成 $L(N-1)$ bit 的原始指纹密钥 BK。

算法 3 原始指纹密钥生成算法

输入 最终特征距离集合 FD

输出 原始指纹密钥 BK

For($j=0; j \leq N-2; j++$) {

For($i=-4; i \leq 1; i++$) {

FD[j] = round(FD[j], i) }

}

FD[j] = rtim(dec2bin(FD[j]/10), L);

BK=BK || FD[j];

}

2.6 安全性分析

为防止出现指纹密钥丢失与泄露的情况, 可按照式(3)在原始指纹密钥 BK 后添加特定字符串进行加盐处理, 然后利用单向 Hash 函数进行消息摘要计算, 最后将摘要值 HK 作为该组指纹图像的指纹密钥。

$$HK = \text{Hash}(BK || \text{Salt}) \quad (3)$$

该指纹密钥 HK 可以用作对称密码体制的加密密钥实现对数据的加密, 但该指纹密钥 HK 更重要的价值在于用作公钥密码体制的私钥。在公钥密码体制中, 私钥的安全管理是整个密码系统成功运行的关键, 也是影响公钥密码方案用户体验水平的重要因素。只有私钥得到安全有效的管理, 确保私钥只掌握在用户自己手中, 才能真正实现数字签名的认证功能和不可否认性。但在实际应用中, 公钥密码体制的私钥总是借助硬件存储介质进行存储的, 如 U 盘或智能卡。当用户需要使用私钥时, 必须接入私钥的存储介质, 让计

算机从存储介质中读取用户的私钥。这种借助存储介质的私钥管理方法不仅降低了用户的体验水平, 而且导致私钥容易丢失和损坏。本文所提的指纹密钥生成算法无须存储任何指纹数据, 在每次需要密钥时, 可随时采集指纹图像并利用本文方法生成指纹密钥。这种指纹密钥的生成方法极大地保证了指纹数据的安全性, 提升了用户体验值。在正式使用中, 对于指纹密钥的更新可通过修改输入的特定字符串 Salt 的方法轻松得到。若指纹密钥在使用中存在安全隐患, 也可通过更换特定字符串的方式生成新的指纹密钥。

另外, 指纹密钥的长度由摘要值计算函数决定。通常使用 256 bit 的 Hash 算法, 摘要值长度为 256 bit, 直接暴力破解需要执行 2^{256} 次计算, 能够满足绝大多数系统的安全需要, 有效解决公钥密码体制的私钥管理问题。

3 实验

3.1 实验方案

假设每个参与测试的志愿者都采集了同一手指的 8 幅指纹图像, 指纹密钥生成实验方案如下。

步骤 1 通过 “Import” 功能按钮导入同一手指的 $K(K=8)$ 幅指纹图像, 处理得到每幅图像中各个特征点 $\alpha_k^j = (x_k^j, y_k^j, t_k^j, \theta_k^j)$ 信息, 生成 $K(K=8)$ 个指纹特征点集合, 如图 2 生成指纹密钥中的第 1 个表单所示。

步骤 2 按照 2.2 节给出的方法, 平移旋转得到 $8(K-1)$ 个稳定特征点集合。

步骤 3 按照 2.3 节讨论的方法, 生成 $M = m_1 m_2$ ($m_1 = 5, m_2 = 4$) 个密钥特征点集合。

步骤 4 按照 2.4 节阐述的方法计算每个密钥特征点集合最佳中心点与其他特征点的欧几里得距离, 前 5 个集合的计算结果如图 2 中的第 3 个表单所示。

步骤 5 按照式(2)计算得到切尾均值结合 FD, 如图 2 中第 4 个表单所示。

步骤 6 再按照算法 3 计算得到原始密钥 BK, 如图 2 中的第 5 个表单所示。

步骤 7 按照式(3)生成指纹密钥 HK, 如图 2 中的第 7 个表单所示。

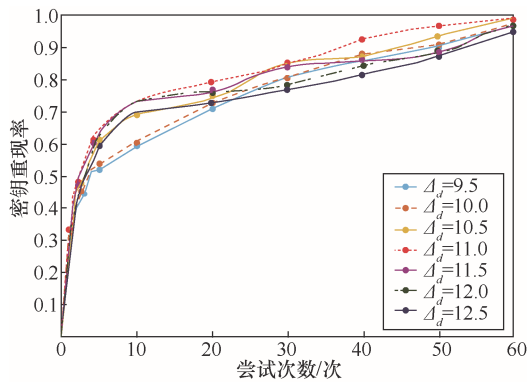


图3 参数阈值 Δ_d 对密钥重现率的影响
Figure 3 The impact of parameter threshold Δ_d on the reconstruction rate of the key

其次, 令欧几里得距离的阈值 $\Delta_d=11$, 观察不同的方向场参数阈值 Δ_θ 对密钥重现率的影响。如图4所示, 其影响情况基本上与特征距离的阈值 Δ_d 对指纹密钥重现率的影响类似。由图4可以看出, 方向场阈值 Δ_θ 在 13.5~14.5 时, 能够获得最优的指纹密钥重现效果, 实验尝试 10 次时指纹密钥重现的概率已经超过 70%, 因此, 本文采用方向场阈值 $\Delta_\theta=14$ 作为最优参数值。

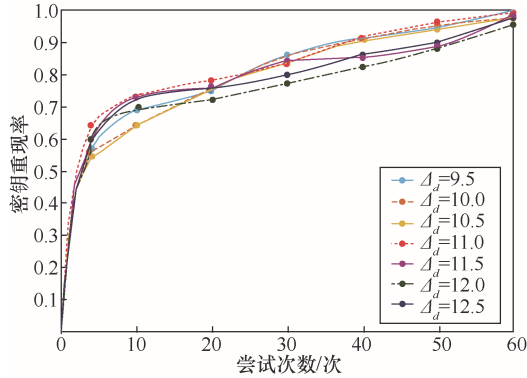


图4 参数阈值 Δ_θ 对密钥重现率的影响
Figure 4 The impact of parameter threshold Δ_θ on the reconstruction rate of the key

再次, 讨论重复选取次数参数阈值 m , 由于每次选取 5 个稳定特征点集合的事件都是独立的, 为了保证多次选取的稳定特征点集合尽可能覆盖全部的稳定特征点集合, 这里的重复选取次数参数阈值 m 不应太小, 但是考虑到系统的执行效率, 该参数也不宜过大。图5展示了参数阈值 m 对密钥重现率的影响, 从图5可以看出, 当重复选取次数参数阈值 $m=4$ 时能够获得最优实验效果。

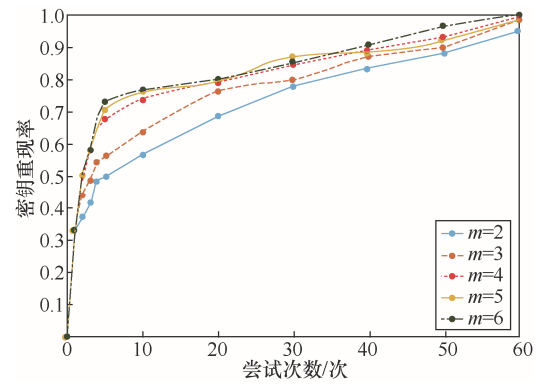


图5 参数阈值 m 对密钥重现率的影响
Figure 5 The impact of parameter threshold m on the reconstruction rate of the key

综上, 为实现最佳效果, 上述参数的最优取值应是 $\Delta_d=11$ 、 $\Delta_\theta=14$ 、 $m=4$ 。如图6所示, 在 155 组 $\times$ 100 次共计 15 500 次实验尝试中, 尝试次数少于 10 次能成功重现指纹密钥的概率为 0.735 4, 尝试次数多于 60 次仍未成功的比例为 0.019 4, 即尝试 60 次能实现指纹密钥重现率为 0.980 6。因此, 实验证明本文所提指纹密钥生成算法能够提供一个好的指纹密钥重现率。

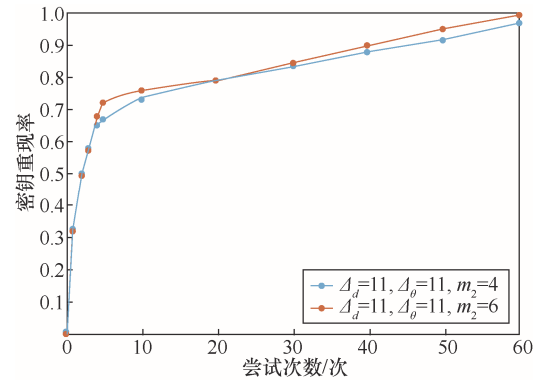


图6 尝试次数及所占比例
Figure 6 Number and percentage of attempts

4 结束语

本文提出了一种全新的指纹密钥生成方法, 该方法只需通过重新采集指纹即可重构指纹密钥, 有效地解决了指纹密钥生成无法脱离预存指纹特征数据的热点问题。另外, 通过加盐的方法可以实现指纹密钥的撤销和指纹密钥的更新。实验表明, 本文提出的指纹密钥生成方法在 10 次尝试生成密钥的条件下, 指纹密钥的成功重现率达到 0.73 以上, 尝试 60 次能实现指纹密钥重现率

达到 0.980 6。基于存储介质的密钥生成方法比较如表 1 所示, 本文提出的密钥生成方法具有更低的 FAR (false acceptance rate)、较低的 FRR (false rejection rate) 和密钥长度仅依赖于哈希值等优势。

表 1 基于存储介质的密钥生成方法比较
Table 1 Comparisons with other key generation methods based on storage media

方法	FAR/FRR	SMD	R-New	Size
本文方法	0/26.46% (尝试次数=10) 0/1.940% (尝试次数=60)	No	Yes	Hash's size
文献[25]方法	2.58%/7.08%	Yes	Yes	120~168
文献[22]方法	5.33%/4.81%	Yes	Yes	Hash's size
文献[24]方法	0/7.6%	Yes	—	80

本文实验过程中用到的指纹图像在采集时, 对于指纹质量具有较高要求(使用 ZKTecoLive20R 光学指纹采集器), 实际应用时需要改进指纹的采集方法, 进一步提高指纹图像的质量。由于本文采用了全新的密钥生成方法, 与目前广泛使用的生物特征密钥绑定机制相比, 本文方法在单次密钥生成的重现率、拒识率等指标上存在不小的差距, 在实际应用中借助多次重复尝试的方式进行。但是随着指纹采集技术的不断进步, 特别是 3D 指纹识别技术研究发展, 本文提出的从模糊指纹数据到精确密钥数据研究方法, 能够为生物特征密钥的研究提供一个新思路。未来研究重点是探索 3D 指纹的密钥生成方法, 降低密钥重现所需要的重复次数。

参考文献:

- [1] LAMPORT L. Password authentication with insecure communication[J]. Communications of the ACM, 1981, 24(11): 770-772.
- [2] JAIN A, ROSS A, PRABHAKAR S. An introduction to biometric recognition[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2004, 14(1): 4-20.
- [3] JAIN A, HONG L, PANKANTI S. Biometric identification[J]. Communications of the ACM, 2000, 43(2): 90-98.
- [4] RUI Z, YAN Z. A survey on biometric authentication: toward secure and privacy-preserving identification[J]. IEEE Access, 2018, 7: 5994-6009.
- [5] SABHANAYAGAM T, VENKATESAN V P, SENTHAMARAK. A comprehensive survey on various biometric systems[J]. International Journal of Applied Engineering Research, 2018, 13(5): 2276-2297.
- [6] RIAZ N, RIAZ A, KHAN S A. Biometric template security: an overview[J]. Sensor Review, 2017, 38(1): 120-127.
- [7] SARKAR A, SINGH B K. A review on performance, security and various biometric template protection schemes for biometric authentication systems[J]. Multimedia Tools and Applications, 2020, 79(37): 27721-27776.
- [8] KHOLMATOV A, YANIKOGLU B. Identity authentication using improved online signature verification method[J]. Pattern Recognition Letters, 2005, 26(15): 2400-2408.
- [9] PRABHAKAR S, PANKANTI S, JAIN A. Biometric recognition: security and privacy concerns[J]. IEEE Security & Privacy, 2003, 1(2): 33-42.
- [10] RATHA NK, CONNELL J, BOLLE R. An analysis of minutiae matching strength[C]//International Conference on Audio and Video-Based Biometric Person Authentication. 2001: 223-228.
- [11] TOMKO G, SOUTAR C, SCHMIDT G. Fingerprint controlled public key cryptographic system[P]. US5541994, 1996-7-30.
- [12] 李鹏, 田捷, 杨鑫, 等. 生物特征模板保护[J]. 软件学报, 2009, 20(6): 1553-1573.
- [13] LI P, TIAN J, YANG X, et al. Biometric Template protection[J]. Journal of Software, 2009, 20(6): 1553-1573.
- [14] ULUDAG U, PANKANTI S, PRABHAKAR S, et al. Biometric cryptosystems: issues and challenges[J]. Proceedings of the IEEE, 2004, 92(6): 948-960.
- [15] DAVIDA G, FRANKEL Y, MATT B. On enabling secure applications through off-line biometric identification[C]//IEEE Symposium on Security and Privacy. 1998: 148-157.
- [16] JUELS A, SUDAN M. A fuzzy vault scheme[J]. Designs, Codes and Cryptography, 2006, 38(2): 237-257.
- [17] JUELS A, WATTENBERG M. A fuzzy commitment scheme[C]//The 6th ACM conference on Computer and Communications Security. 1999: 28-36.
- [18] SOUTAR C, ROBERGE D, STOIANOV A, et al. Biometric encryption using image processing[J]. Optical Security and Counterfeit Deterrence Techniques II, 1998, 3314: 178-188.
- [19] VERBITSKIY E, TUYLS P, DENTENEER D, et al. Reliable biometric authentication with privacy protection[C]//Proc 24th Benelux Symposium on Information Theory. 2003: 19.
- [20] RATHGEB C, UHL A. A survey on biometric cryptosystems and cancelable biometrics[J]. EURASIP Journal on Information Security, 2011, 2011(1): 1-25.
- [21] 张宁, 臧亚丽, 田捷. 生物特征与密码技术的融合——一种新的安全身份认证方案[J]. 密码学报, 2015, 2(2): 159-176.
- [22] ZHANG N, ZANG Y L, TIAN J. The integration of biometrics and cryptography—a new solution for secure identity authentication[J]. Journal of Cryptologic Research, 2015, 2(2): 159-176.
- [23] 罗成行, 杨得新, 杨波. 一个基于指纹和智能卡的密钥封装方案[J]. 信息安全与通信保密, 2009 (8): 338-340.
- [24] LUO X C, YANG D X, YANG B. A key encapsulation scheme based on fingerprint and smartcard[J]. Information Security and

Communication Privacy, 2009 (8): 338-340.

- [22] 陈开志, 胡爱群, 宋宇波, 等. 基于 BioHashing 和密钥绑定的双重可删除指纹模板方法[J]. 高技术通讯, 2010, 20(11): 1115-1120.
CHEN K Z, HU A Q, SONG Y B, et al. A dual cancellable fingerprint template method for securing the original finger print biometric in formation based on BioHashing and key bindings[J]. High Technology Letters, 2010, 20(11): 1115-1120.
- [23] SHENG W, HOWELLS G, FAIRHURST M, et al. Reliable and secure encryption key generation from fingerprints[J]. Information Management & Computer Security, 2012, 20(3): 207-221.
- [24] 高莹, 郑长春, 张凯, 等. 更高效的指纹生物特征加密[J]. 密码学报, 2016, 3(2): 157-170.
GAO Y, ZHENG C C, ZHANG K, et al. More efficient fingerprint biometric encryption. Journal of Cryptologic Research. 2016, 3(2): 157-170.
- [25] WANG P, YOU L, HU G, et al. Biometric key generation based on generated intervals and two-layer error correcting technique[J]. Pattern Recognition, 2021, 111: 107733.
- [26] 张翔宇. 基于指纹识别的认证方法研究[D]. 北京: 北京邮电大学, 2021.
ZHANG X. Research on authentication method on fingerprint recognition[D]. Beijing: Beijing University of Posts and Telecommunications, 2021.
- [27] ELSADAI A, ADAMOVIĆ S, ŠARAC M, et al. New approach for fingerprint recognition based on stylometric features with block-chain and cancellable biometric aspects[J]. Multimedia Tools and Applications, 2022, 81(25): 36715-36733.
- [28] 贾忠田, 马莉, 秦庆龙, 等. 一种指纹密钥生成方法、系统、介质及设备[P]. 山东省: CN115720170A, 2023-02-28.
JIA Z, MA L, QIN Q. A method, system, medium and device for fingerprint key generation[P]. Shandong Province: CN115720170A, 2023-02-28.
- [29] ALILOU V. Fingerprint matching: a simple approach[EB].

[作者简介]



贾忠田（1972—），男，山东聊城人，济南大学副教授，主要研究方向为密码学与网络安全。



秦庆龙（2001—），男，山东德州人，主要研究方向为生物特征识别与信息安全。



马莉（1979—），女，山东乳山人，济南大学讲师，主要研究方向为数据挖掘与信息安全。



彭立志（1975—），男，湖南永州人，济南大学教授，主要研究方向为人工智能与网络安全。