一种免预对齐的指纹模板隐私加密方法

萧力芮[1] 叶二垒[1] 齐 婧[2] 胡 敏[2]
XIAO Lirui YE Erlei QI Jing HU Min

摘 要 针对指纹模板明文存储所带来的隐私问题，设计了一种基于Fuzzy Vault改进的免对齐指纹模板加密方法。不同于基于特征点坐标的Fuzzy Vault加密方法，所提出的方法通过圆盘结构的设计，更多考虑了特征点间的空间关系。通过引入圆盘结构，可在解密阶段对特征点进行粗细两级筛选，以提高识别效率。实验结果表明，所提出的方法通过结合坐标方向信息与邻域空间关系提高了指纹识别的准确度，通过对特征点数据进行粗筛选，大幅减少了全局几何配准所需计算量。

关键词 指纹；指纹加密；模板保护；隐私保护；Fuzzy Vault

doi：10.3969/j.issn.1672-9528.2024.02.040

0 引言

随着全球信息化的普及，如何有效对个人敏感信息进行保护成为众多学者关注的研究热点之一，在生物特征识别领域，基于指纹特征的识别技术已被应用到社会生活的各个领域，在带来诸多便利的同时，也对的个人隐私带来了很大的威胁。指纹作为身份认证的工具来说，具有唯一性、不可变性、隐私性等特点[1]，指纹自身的这些特点导致一旦指纹信息被丢失或被窃取，永远无法修改，一经丢失则永远丢失，入侵者甚至可以通过指纹信息直接生成出相似的指纹图像。因此，在使用指纹进行身份认证的过程中如何对指纹敏感信息加密，防止敏感信息泄露至关重要。

通常基于密钥的隐私保护加密方法对数据的精确性有很高的要求，即使明文信息只有很小的差异得到的密文也完全不同。而指纹特征具有无序性、不精确性、数量不一性，指纹会因每次采集的角度、姿势、湿度等因素的变化而变化，如特征点坐标位置发生平移旋转、数值上产生误差、数量不同、顺序不同等，因此无法通过常见的加密方法进行加密。如何解决密钥机制精确性与指纹特征模糊性之间的矛盾成为一大难题[2]。

为解决密钥机制精确性与指纹特征模糊性之间的矛盾，Juels等人[3]基于多项式重构的复杂性提出了Fuzzy Vault方案，其加密数据可以是无序的点集，这与指纹特征的无序性、数量不一性正好相匹配，因此Fuzzy Vault成为了指纹特征加密领域中的经典方法之一。但Fuzzy Vault无法解决指纹特征的平移旋转问题，大量的研究都是基于已配准对齐指纹来开展的。

本文基于Fuzzy Vault加密算法，实现了对用户指纹敏感信息的保护。在特征结构方面，结合了平移旋转不变特征与平移旋转敏感特征，以综合考虑指纹图像的模糊性，在加解密方面引入了基于全局域配准的方法进行二次筛选。该方法能够提高指纹识别的准确性，并有效减小了计算量。

1 相关工作

近年来，为解决指纹敏感信息加密问题，许多学者在Fuzzy Vault的方法基础上做出了一定工作。

Clancy等人[4]率先针对指纹的特点，在Fuzzy Vault的基础上加以改进，在智能卡上实现了指纹信息加密，其实验的前提假设是注册指纹集与查询指纹集经过了预对齐。Yang等人[5]提出了一种在加密域进行指纹对齐的方法，该方法使用了一种与距离和方向相关的参考特征点，该方法的前提也假设了注册指纹与查询指纹都能找到该参考点。Uludag等[6]提出了改进的Fuzzy Vault方法，使用Cyclic Redundancy Check（CRC）循环校验方法代替了Fuzzy Vault中的RS Decode方法，该方法也假设指纹进行了预对齐。Nandakumar等人[7]对Fuzzy Vault加以改进的同时，引入了基于方向场信息的高曲率点来辅助指纹对齐。但其算法识别的准确度极大地受限于高曲率点的检测误差，高曲率点检测失败会直接导致指纹识别失败。Kai等人[8]提出了一种基于复合特征结构的层次比对方法，将Fuzzy Vault应用在了指纹匹配算法的中间步骤上。Li等人[9]提出了一种基于两级细节特征点结构的Fuzzy Vault算法，在密钥恢复中使用了双重保护。Li等人[10]将两级保护压缩为一级，利用细节特征点描述来匹配Vault，降低了解

1. 中国电子科技集团公司第三十研究所 四川成都 610041
2. 中国人民解放军 61660 部队 北京 100089

密的时间复杂度。Seira 等人[11]提出了一种新的加密模板存储方案，在文章中评估了各种存储方案的安全性。Zhang 等人[12]提出了一种改进的 Fuzzy Vault 方法，该方法有着更少的占用的内存空间和更小的解密损失。Qiong 等人[13]指出了 Fuzzy Vault 在解锁阶段中使用 Reed-Solomon 算法存在的问题，并提出了新的解锁算法。

在指纹自动对齐方面，Moon 等人[14]提出了指纹的自动对齐技术，能够在 Fuzzy Vault 加密域上进行自动对齐，但其需要遍历包括杂凑点在内的所有点。Chung 等人[15]提出了使用几何哈希技术来解决 Fuzzy Vault 中的对齐问题，这种技术提前计算了所有可能的对齐参数，节约了一定的认证时间。Jason 等人[16]提出了一种对齐方法使用指纹特征点集中的内在属性，在该方法中使用了五个最近邻特征点、Voronoi 最近邻、三角结构来进行对齐。Baghel 等人[17]提出在 Fuzzy Vault 中使用主成分分析技术来对齐指纹。Alam 等人[18]设计了一种基于极坐标系的三元特征组的免对齐 Fuzzy Vault，同时引入了离散傅里叶变换和随机投影以实现模板的可撤销性。

2 相关方法

Fuzzy Vault 是一种由 Fuzzy Commitment[19]改进而来的隐私加密方法，其在 Fuzzy Commitment 的基础上采用了模糊匹配的方法。Fuzzy Vault 将待保护的密钥信息 K 使用真实点数据集 A 进行编码，然后将点数据集 A 隐藏在一堆杂乱干扰点数据集 C 中，攻击者很难从这些数据中分离出真实点，密钥可看作是被真实数据加锁了。若要解开密钥，必须提供与真实点集数据 A 相似的点集数据 B。

具体地，Fuzzy Vault 算法可分为加锁和解锁两个阶段。在算法的加锁阶段，首先通过密钥信息 K 去构造一个多项式 $P(x)$，然后将真实点数据集转换为数值形式并映射到多项式 $P(x)$ 上，得到一组多项式 $P(x)$ 上的坐标集合，最后添加大量不在多项式 $P(x)$ 上的杂乱干扰坐标，真实的坐标集合与杂乱干扰坐标集取并集就可得到加锁后的数据 V。在解锁阶段，需要输入一个新的点数据集，使用该数据集与加锁阶段得到的数据 V 进行匹配，然后使用匹配到的信息尝试对多项式 $P(x)$ 进行重构，只要能够匹配到足够多的数据就能够重构出 $P(x)$，进而得到其对应的密钥 K。

3 方法实现

3.1 指纹特征描述

指纹特征具有模糊性，在采集时会随着按压姿势、力度、湿度等的变化而变化，具体反映在其特征点的坐标会产生平移旋转、数值会产生误差扰动，但不同特征点间的相对位置关系是基本固定的，因此只要对特征点间的相对属性进行描述就可得到平移旋转不变的特征。基于这一认识，本文提出的指纹特征描述方法融合了平移旋转不变特征与平移旋转敏感特征，将每个特征点分为两部分来进行描述。其中，一部分用于表征指纹特征点自身的属性，主要包括特征点的坐标与方向信息；另一部分则是局部圆盘结构编码，用于刻画指纹特征点固定半径邻域内的空间关系，从而实现对特征点间相对位置关系的描述。

令 $T=\{m_1, m_2, \ldots, m_n\}$ 为指纹采集图像上符合 ISO/IEC 19794-2 的指纹细节特征点，每个细节特征点 m_i 是一个三元向量 $m_i=\{x_i, y_i, \theta_i\}$，其中 x_i 和 y_i 是细节特征点在笛卡尔坐标系下的坐标，θ_i 为其方向。每一细节特征点 m_1 对应的局部圆盘结构由 L 个半径为 r_l，圆心为 (x_m, y_m) 的同心圆组成 $(1 \le l \le L)$，不同半径同心圆中间围成的区域又可从 θ_m 所指角度开始均匀的划分为 k_l 个区域。

构建出每一特征点 m_i 所对应的局部圆盘结构后，其相邻细节特征点就可被映射到圆盘结构中的每一个小段中，若该小段中含有细节特征点则置该小格为 1，否则为 0。从 θ_m 正方向沿逆时针方向从内侧到外侧依次展开，则可得到该局部圆盘结构的比特编码信息 B_i。将坐标信息与圆盘结构的比特编码结合起来就得到了本文所用的指纹特征结构 $F_i=(m_i, B_i)$，其中圆盘结构的比特编码信息的相似度可由以下公式计算。

$$S(a,b)=1-\frac{\|a \oplus b\|}{\|a\|+\|b\|} \tag{1}$$

3.2 加密算法

如图 1 所示，假设加密密钥 K 的长度为 128 位，本算法的加密流程如下。

（1）需要根据密钥 K 构造多项式 $P(x)$，将密钥 K 按顺序分成 8 段，每段 16 bit，即 $K=k_8k_7k_6k_5k_4k_3k_2k_1$，然后计算出 K 的 CRC-16 值并记为 k_0，将 k_8、k_7、k_6、k_5、k_4、k_3、k_2、k_1、k_0 分别作为多项式 $P(x)$ 的系数，得到：

$$P(x)=k_8x^8+k_7x^7+k_6x^6+k_5x^5+k_4x^4+k_3x^3+k_2x^2+k_1x^1+k_0 \tag{2}$$

（2）把注册指纹的 n 个特征点 $T=\{m_1, m_2, \ldots, m_n\}$ 转换为前文所述指纹特征结构，得到 $T'=\{(m_1, B_1), \ldots, (m_n, B_n)\}$，将 B_i 通过多项式 $P(x)$ 进行映射得到 $Y_i=P(B_i)$，所有特征点都完成映射后，就可得到真实点集合：

$$G=\{((m_1,B_1),Y_1),\ldots,((m_n,B_n),Y_n)\} \tag{3}$$

（3）随机生成 k 个杂凑干扰点集合 $C=\{((w_1,e_1),r_1),\ldots,((w_k,e_k),r_k)\}$，其中集合 C 中元素需满足 $r_i \neq P(e_i)$，$(w_j,e_j) \notin T'$，且 k 要大于 n 以保证数据的安全性。将真实点集合 G 与杂凑干扰点集合 C 取并集得到：

$$V=\{((m_i,B_i),Y_i),((w_j,e_j),r_j) \mid i \in [1,n]; j \in [1,k]\} \tag{4}$$

（4）随机打乱集合 V 的顺序就得到了加密数据 V'。

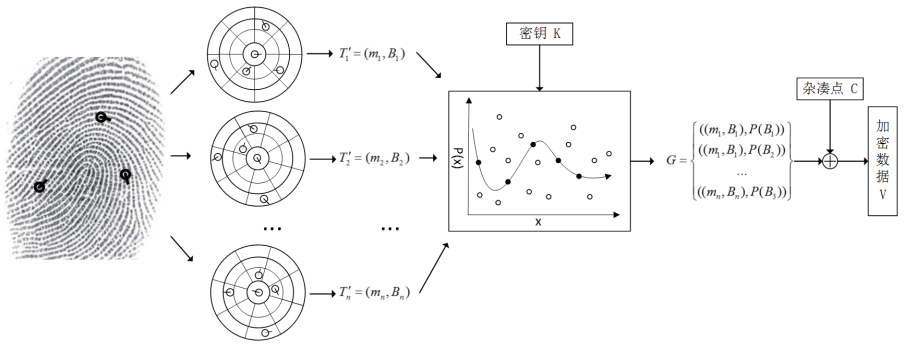

图 1 加密流程示意图

3.3 匹配算法

在匹配时，需要根据待查询指纹与加密模板 V 筛选出候选数据，然后根据坐标信息对候选数据进行筛选，最后通过筛选后的数据进行多项式重构，具体流程如下。

（1）将待查询指纹特征点集 Q 中 n 个特征点转换为本文所述指纹特征结构，得到 $Q'=\{(m_1,B_1),\ldots,(m_n,B_n)\}$。遍历 Q' 与 V' 中所有的圆盘结构编码并计算其相似度，若 Q' 中第 i 个元素与 V' 中第 j 个元素相似度大于阈值 t，则将查询指纹特征点的圆盘编码 B_i、加密数据中相似点的多项式映射值 γ_j、查询指纹特征点的方向与坐标信息 m_i、加密数据中相似点的方向与坐标 m_j 放在一起组成一个候选数据。

（2）在候选数据集中任选一个元素，计算查询指纹特征点与其对应加密数据中相似点的平移旋转偏移量。根据该偏移量对所有候选元素进行变换，若变换后两点的坐标偏差在一定界限盒内则认为这两点经过变换后相匹配。遍历所有的候选数据进行变换并统计每个变换下的匹配特征个数。若所有的变换下匹配数都小于阈值，则解密失败。否则取匹配数最多的一组变换，将不匹配的元素从候选数据中删除。

（3）从筛选后的候选数据中任选大于多项式阶数个元素，根据候选元素的圆盘编码 B_i 与多项式映射值 γ_j 使用拉格朗日插值法对多项式进行重构，得到：

$$P'(x)=k_8'x^8+k_7'x^7+k_6'x^6+k_5'x^5+k_4'x^4+k_3'x^3+k_2'x^2+k_1'x^1+k_0' \quad (5)$$

（4）连接多项式的所有系数得到 $R'=[k_8'|k_7'|\ldots|k_1']$，计算 R' 的 CRC-16 纠错码，若其与 k_0' 相等，则认为指纹匹配成功，R' 就是加密前的密钥，否则重复步骤（3）～（4），直到遍历完所有数据。

4 实验与结果分析

4.1 数据来源及预处理

本研究所使用的实验数据集来源于本单位自主采集的指纹图像。该数据集中对 538 名受试者分别进行了 10 次指纹采集，共得到 5380 张指纹图像。在实验过程中，首先对数据库中的所有指纹图像进行了去噪和增强处理，以减少图像中的干扰和噪声，并突出指纹纹理的特征。然后通过计算指纹脊线的平均周期，并利用 Gabor 滤波技术提取出指纹纹线图，以便捕获指纹图像中的主要纹线结构信息。最后，对提取得到的指纹纹线图进行细化处理，并进一步提取出细节特征点。整个处理流程如图 2 所示。

图 2 指纹特征点提取主要流程示意图

4.2 实验结果

为验证本文所提出方法，在自采数据集上进行了实验，对于同一手指采集到的 10 张指纹图像，选择细节特征点个数最多的那一枚作为注册指纹，其余指纹图像作为现场采集的指纹。参照文献 [4] 所设实验参数，实验所设置密钥长度为 128 bit，对应多项式的阶为 8，至少需匹配 9 个坐标点才能重构该多项式。

如表 1 所示，本文所提出方法的拒真率与文献 [4] 方法拒真率 23.2% 相比，有一定提高，这主要是由于本文方法结合了细节特征点邻域关系信息与特征点方向信息进行匹配。

表 1 128 bit 密钥下实验结果

方法	拒真率
本文方法	11.4%
文献 [4] 方法	23.2%

在计算量方面，如表 2 所示，得益于对特征点所进行的粗筛选，本文方法大幅减少了全局几何配准所需变换的次数。

表 2 全局几何配准所需变换次数

方法	平均变换次数
对特征点粗筛选	349
未对特征点粗筛选	1291

5 结语

本文提出了一种改进的免对齐 Fuzzy Vault 指纹模板保护方案，提高了指纹特征模板加密的安全性和性能。在特征描述方面，本方案通过特征点圆盘结构的设计，在传统基于坐标信息的 Fuzzy Vault 基础上引入了特征点空域关系与方向

信息，提高了指纹匹配的准确度。在加密匹配方面本方案结合特征点筛选策略设计了自动对齐方法，提高了 Fuzzy Vault 方案的可用性。然而，本方案并未解决指纹模板保护中的可撤销性，为了克服该限制，后续还需将加盐模板保护方案与 Fuzzy Vault 方案结合起来，设计出具有可撤销功能的 Fuzzy Vault 以提高整体安全性。

参考文献：

[1] HAN F,HU J,HE L,et al.Generation of reliable pins from fingerprints. security symposium[C]//IEEE International Conference on Communication (ICC).Piscataway: IEEE, 2007: 24-28.

[2] 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.

[3] JUELS A, SUDAN M. A fuzzy vault scheme[J].Designs, codes and cryptography,2002,38:237-257.

[4] CLANCY T,LIN D,KIYAVASH N. Secure smartcard-based fingerprint authentication[C]//Proceedings of the 2003 ACM SIGMM Workshop on Biometrics Methods and Applications. New York: ACM, 2003:45-52.

[5] YANG S,VERBAUWHEDE I. Automatic secure fingerprint verification system based on fuzzy vault scheme[C]//In Proc. of IEEE International Conference on Acoustics.Piscataway: IEEE, 2005:609-612.

[6] ULUDAG U, PANKANTI S, JAIN A K, et al. Fuzzy vault for fingerprints[C]// In Proc. of Audio- and Video-based Biometric Person Authentication. Berlin: Springer,2005:310-319.

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

[8] XI K,HU J. Biometric mobile template protection: a composite feature based fingerprint fuzzy vault[C]// International Conference on Communications IEEE. Piscataway: IEEE, 2009:829-833.

[9] LI C,HU J.A security-enhanced alignment-free fuzzy vault-based fingerprint cryptosystem using pair-polar minutiae structures[J].IEEE Trans. Inf. Forensics Secur, 2016, 11(3): 543–555.

[10] LI X M, DING N, LU H, et al. A modified fuzzy fingerprint vault based on pair-polar minutiae structures[C]//Information Security and Cryptology: 13th International Conference. Berlin:Springer International Publishing, 2018:482-499.

[11] SEIRA H,TETSUSHI O,NAOHISA K,et al.On biometric encryprtion using fingerprint and its secirity evaluation[C]// In 10th International Conference on Control, Automation and Robotics and Vision. Piscataway:IEEE, 2008:950-956.

[12] ZHANG X ,SHI R,RITCEY J.On the implementation of modified fuzzy vault for biometric encryption[C]//In Information Theory and Applications Workshop (ITA). Piscataway:IEEE,2012:56-61.

[13] LI Q, LIU Z, NIU X. Analysis and problems of fuzzy vault scheme[C]//In proceedings of IEEE.Piscataway: IEEE, 2006:244-250.

[14] MOON D, LEE S, CHUNG Y, et al.Implementation of automatic fuzzy fingerprint vault[J].Seventh international conference on machine learning and cybernetics,2008(7):3781-3786.

[15] CHUNG Y,MOON D,LEE S,et al.Automatic alignment of fingerprint features for fuzzy fingerprint vault[J].LNCS, 2005, 3822: 358-369.

[16] JASON J,ARATHI A.Fingerprint alignment for a minutiae-based fuzzy vault[C]//In Biometric Symposium IEEE. Piscataway:IEEE,2007:1-6.

[17] VIVEK SINGH B, PRAKASH S, AGRAWAL I. An enhanced fuzzy vault to secure the fingerprint templates[J]. Multimedia tools and applications,2021,80(21):33055-33073.

[18] ALAM B, JIN Z,YAP W S,et al. An alignment-free cancelable fingerprint template for bio-cryptosystems[J]. Journal of network and computer applications,2018,115(1): 20-32.

[19] JUELS A, WATTENBERG M. A fuzzy commitment scheme[C]//In: Proceedings of the sixth ACM conference computer community security. New York: ACM Press; 1999:28–36.

【作者简介】

萧力芮（1994—），男，四川遂宁人，硕士，研究方向：指纹识别、深度学习。

叶二垒（1992—），男，河南商丘人，本科，研究方向：密码保密。

齐婧（1981—），女，甘肃庆阳人，硕士，研究方向：网络安全、数据保护。

胡敏（1978—），女，河南长葛人，硕士，研究方向：网络安全、数据处理。

（收稿日期：2023-11-27）