doi: 10.3969/j.issn.0490-6756.2019.03.010

一种指纹特征点拓扑结构的加密方法

李 甫[1,2,3], 陈佳宝[2], 胡 娟[4], 吴莉娟[4]
(1. 内江师范学院 四川省高等学校数值仿真重点实验室, 内江 641112;
2. 内江师范学院 数学与信息科学学院 四川省数据恢复重点实验室, 内江 641112;
3. 四川大学计算机学院计算摄像与多维处理实验室, 成都 610065;
4. 四川华雁信息产业股份有限公司, 成都 610065)

摘 要: 提出了一种基于拓扑结构的指纹特征点加密算法. 该加密算法是在无限平面上随机采用三个不属于任何一个指纹特征且互异的点(三个节点构成一个三角形)作为指纹加密的密钥,将特征点到三个采集点的平面距离作为加密值,同样对其余的指纹特征点计算加密值,直至全部特征点加密完成,最后得到密码指纹. 与旧有指纹加密算法相比,该算法优势在于扩大密钥初始值的选择范围,密钥空间增大,使得暴力破解变得更为困难;加密的计算方式简单,算法复杂性低,对大量指纹数据的加密效率有所提升.

关键词: 指纹加密; 加密算法; 拓扑学
中图分类号: TP309.2 **文献标识码**: A **文章编号**: 0490-6756(2019)03-0437-04

An encryption method for topological structure of fingerprint minutiae

LI Fu[1,2,3], *CHEN Jia-Bao*[2], *HU Juan*[4], *WU Li-Juan*[4]
(1. Key Laboratory of Numerical Simulation in the Sichuan Provincial Colleges, Neijiang Normal University, Neijiang 641112, China; 2. Key Laboratory of Data Recovery of Sichuan Province, College of Mathematics and Information Science, Neijiang Normal University, Neijiang 641112, China; 3. Laboratory of Computational Camera and Multidimensional Processing, College of Computer Science, Sichuan University, Chengdu 610065, China; 4. Sichuan Huayan Information Industry Company Limited, Chengdu 610065, China)

Abstract: A novel fingerprint encryption algorithm based on topological structure of fingerprint minutiae is presented in this paper. The encryption algorithm randomly selects three different points on the infinite plan, which form a triangle and do not belong to any fingerprint feature points, as the fingerprint encryption keys. The distance between the fingerprint feature points and the three selected points is taken as encrypted value, which is calculated for every fingerprint feature point until all the feature points are encrypted, and finally the fingerprint encryption value is obtained. Compared with the previous fingerprint encryption algorithms, the advantage of the proposed algorithm is to expand the selection range of the initial value of the key and the key space, which makes the brute force more difficult. The encryption calculation method is simple and its complexity is low, the encryption efficiency for a large amount of fingerprint data is improved.

Keywords: Fingerprint encryption; Encryption algorithm; Topology

收稿日期: 2018-04-03
基金项目: 国家重点研发计划(2016YFB0801101); 国家自然科学基金重点国际合作与交流项目(61860206007)
作者简介: 李甫(1976—), 男, 四川西充人, 硕士, 主要研究人工智能和生物特征识别与模板保护. E-mail: 89199968@qq.com

1 引 言

随着经济和信息技术的不断发展,信息安全成为人们关注的焦点.传统的身份鉴别技术,如智能卡、口令等,由于容易被遗忘,易被盗取或者假冒,而不能满足现代信息安全的需求.近年来,可靠的身份识别与认证需求正在全球范围内稳步增长.由于生物特征(如:人脸,指纹,虹膜,掌纹,手签名,语音等)具有便于携带、难以共享以及难以伪造等特点,生物识别技术越来越被用于医疗卫生、公共安全与银行等敏感行业中[1].

生物识别技术正在增强我们的识别能力.用于身份验证的一些生物识别技术主要是基于是人脸,指纹,虹膜,掌纹,手签名,声音等.在表 1 中,基于各种特征比较了各种生物识别技术.

如表 1 所示,指纹具有唯一性、稳定性和便捷性等综合性能,因此指纹识别技术受到广泛关注.指纹识别原理的关键是借助于指纹在生物识别技术中是人手指上天生的脊(暗线)和山谷(亮区)的图案.除此之外,还有一些细节点(即特征点)——脊结束点或脊分叉点.这些要点可以作为判断一个人身份的有效特征.从技术上讲,指纹是一个人用于识别和验证最可靠的特征之一.

据文献[2]报告:2016 年全球指纹模组市场规模 362 亿元,出货量达到 6.78 亿颗,预计 2020 年市场规模达到 600 亿元,出货量 15 亿颗,出货量年复合增长率约 22%.2016 年中国指纹模组市场规模 323 亿元,出货量 5.5 亿颗,预计 2020 年将达到 511 亿元,出货量将超过 12 亿颗,出货量年复合增长率约 21%.可见指纹识别市场需求潜力巨大,对互联网用户生活的渗透率也越来越高.

此外,指纹识别的应用场景也日渐广阔,对指纹识别加密的需求,如出境认证,犯罪和预防犯罪,司法调查和取证,考勤,支付系统,访问控制等在日益增加.

指纹识别对我国社会国民与企业的生产生活的巨大推进作用.然而随着指纹识别技术应用的愈加深入,隐私性与安全性等方面的问题也逐渐显露[3-7].因此,解决指纹识别技术在安全性和隐私性方面存在的问题已迫在眉睫.

表 1 生物识别标识符性能比对

Tab. 1 Comparison of biometric identifier performance

识别标识符	普遍性 (universality)	区分性 (Distinct)	持久性 (Permanence)	可采集性 (Collect ability)	性能 (Performance)	可攻击性 (Attack)	防御性 (Circumvention)
人脸	高	低	中	高	低	高	高
指纹	中	高	高	中	高	中	中
手掌	中	中	中	高	中	中	中
虹膜	高	高	高	中	高	低	低
按键	低	低	低	中	低	中	中
笔迹	低	低	低	中	低	高	高
声纹	中	低	低	中	低	高	高

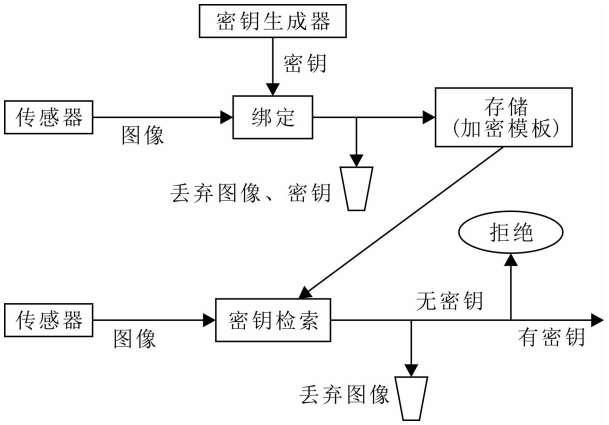

图 1 指纹加密过程示意图

Fig. 1 Diagram of fingerprint encryption process

指纹特征加密技术可以将指纹数据重新编码为 PIN,密码或字母数字字符串,应用于多种场景,例如:银行 ATM,楼宇访问和计算机终端访问.值得强调的是,数据库只需要存储生物信息测量加密的 PIN 或密码,而不存储个人指纹的敏感信息,在图 1 中显示指纹加密的过程.

指纹特征加密技术实际是将指纹识别技术与密码学理论的结合.近年来,指纹特征加密技术受到国内外学者的广泛关注[8-16].现有指纹加密算法主要利用极坐标变换、笛卡尔坐标变换、高斯核函数、哈希函数等方法建立指纹模板保护的不可逆变化.然而这些方法存在的问题都是密钥空间都停留

在二维空间上，从而容易被高性能计算机暴力破解或预测密钥.

基于上述指纹加密算法的不足，本文提出了一种基于拓扑结构的指纹特征点加密算法. 指纹加密过程主要包括：首先在平面上任意找到一个三角形，以此三角形的三个顶点的二维坐标作为密钥；然后分别计算各个指纹特征点到这个三角形的三个顶点的距离作为加密值，从而构造了一个从二维到三维的不可逆变换. 该算法的优点在于两个方面：一方面，把特征点的密钥从二维映射到三维空间，密钥空间维数的增加，显著加大了暴力破解的难度，有效提高了指纹模板的安全性；另一方面，加密本身的算法简单，提高了指纹数据加密效率.

2　基于拓扑结构的算法设计

2.1　算法思想

计算机随机选取平面上构成某一三角形的三个点(不属于任何一个指纹特征点)作为算法密钥，将指纹特征点到三个有序点的距离进行不同的运算处理，得到三个不同有序加密值，增加加密复杂度，通过这样的处理把指纹特征点从二维映射到三维，同时所得到的映射是不可逆的，增加了破解难度. 这种加密算法设计简单，计算量小，加密效率更高.[17]

2.2　算法步骤

第 1 步　确定本枚指纹的密钥；

在平面上任意选取三个有序点，记为(A，B，C)，A、B 和 C 三点能够构成一个三角形，且不属于任何一个指纹特征点，以这三个有序点(A，B，C)的坐标作为本枚指纹的密钥，如图 2 所示.

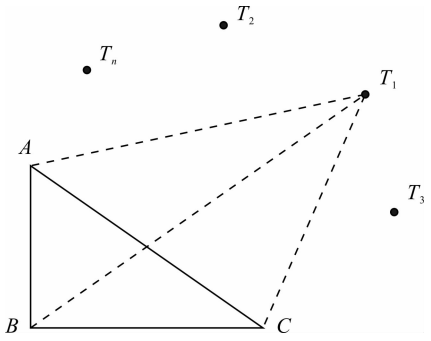

图 2　算法示意图
Fig. 2　Diagram of algorithm

第 2 步　任选一个指纹特征点，并计算该特征点的加密值；

在所有的指纹特征点中任意选取一个特征点，例如 T_1，计算出该特征点到三个有序顶点(A，B，C)的距离，形成一个有序三数组(X_1，Y_1，Z_1)作为特征点 T_1 的加密值；

为了增加破解难度，还可以对该特征点到三个有序顶点(A，B，C)的距离形成的有序三数组(X_1，Y_1，Z_1)进行运算处理，得到新的有序三数组(a_1，b_1，c_1)作为特征点 T_1 的加密值，具体运算方法如下.

$$a_1 = X_1 - \mathrm{int}[(A_x + A_y)/10]$$
$$b_1 = Y_1 - \mathrm{int}[(B_x + B_y)/10]$$
$$c_1 = Z_1 - \mathrm{int}[(C_x + C_y)/10]$$

其中，ing 为取整函数，A_x、A_y 分别表示 A 点的横、纵坐标；B_x、B_y 分别表示 B 的横、纵坐标；C_x、C_y 分别表示 C 点的横、纵坐标.

第 3 步　计算指纹特征点 T_i($i=2,3,\cdots,n$，其中 n 为特征点的个数)的加密值：

在未加密的指纹特征点中随机选取一个特征点 T_i($i=2,3,\cdots,n$)；其中 n 为特征点的个数，计算 T_i 到三个顶点(A，B，C)的距离，形成一个有序数组(X_i，Y_i，Z_i)，作为特征点 T_i 的加密值；

同样，为了增加破解难度，还可以对(X_i，Y_i，Z_i)进行运算处理，得到新的有序三数组(a_i，b_i，c_i)作为特征点 T_i 的加密值，具体运算处理方法如下：

$$a_i = X_i - \mathrm{int}[(A_x + A_y)/10]$$
$$b_i = Y_i - \mathrm{int}[(B_x + B_y)/10]$$
$$c_i = Z_i - \mathrm{int}[(C_x + C_y)/10]$$

第 4 步　重复第 3 步，直到所有的指纹特征点的坐标都加密完成.

2.3　算法流程图

根据设计的算法思想和步骤，算法流程图如下.

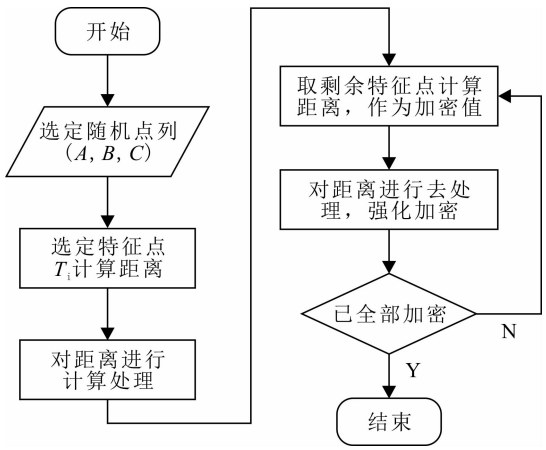

图 3　算法流程图
Fig. 3　Diagram of the algorithm flow

2.4 算法优势分析

1) 该加密算法思路新颖,原理简单,计算量小,而且便于计算机编程实现其加解密,加解密复杂度低,提高了加解密效率.

2) 密钥空间大. 在暴力破解方法中,如果加密方法的密钥空间不够大则很容易借助高性能计算机暴力破解. 该加密方法扩大密钥初始值的选择范围,密钥空间增大,极大增加暴力破解方法的难度,有效地保护指纹模板的安全性.

3) 指纹特征点从二维映射为三维,并且该映射不可逆,通过前后加密值的叠加混淆,进一步增加了破解难度,提高指纹模板的安全性.

3 结 论

为了增强指纹加密/解密算法的安全性,本文提出了一种基于拓扑结构的指纹特征点加密方案. 在数字指纹加密中在满足安全性的同时,增加了密钥生成的空间,降低了加密和解密的复杂度,使得暴力破解变得更为困难和提高了加密解密的效率. 该算法理论分析和实验结果都证明该算法是有利的.

参考文献:

[1] Cavoukian A, Stoianov A. Biometric encryption: a positive-sum technology that achieves strong authentication, security and privacy [M]. USA, Ontario: Information and Privacy Commissioner, 2007.

[2] 智研咨询集团. 2019~2025 年中国指纹识别系统行业市场需求预测及投资未来发展趋势报告 [R]. R679923. 北京: 智研咨询集团, 2018.

[3] 张宁, 臧亚丽, 田捷. 生物特征与秘密技术的融合——一种新的安全身份认证方案 [J]. 密码学报, 2015, 2: 159.

[4] 李鹏, 田捷, 杨鑫, 等. 生物特征模板保护[J]. 软件学报, 2009, 20: 1553.

[5] 申飞, 黄承杰, 吴仲城. 生物特征加密技术现状与发展趋势 [C]//全国计算机安全学术交流会. 合肥: 中国科学技术大学出版社, 2008.

[6] 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: 157.

[7] 刘辉元, 马金辉, 黄琼. 基于改进克里金插值的室内定位位置指纹库构建方法 [J]. 重庆邮电大学学报: 自然科学版, 2017, 29: 751.

[8] Katha N K, Chikkerur S. Generating cancelable fingerprint templates [J]. IEEE Trans Pattern Anal, 2007, 29: 561.

[9] Munmar G, Tulyakov S, Govindaraju V. Combination of symmetric hash functions for secure fingerprint matching [C]//Proceedingsof the 20th International Conference on Pattern Recognition. [S. l.]: IEEE, 2010.

[10] Cappelli R, Ferrara M, Maltoni D. Minutia cylinder-code: a new representation and mat-ching technique for fingerprint recognition [J]. IEEE Trans Pattern Anal, 2010, 32: 2128.

[11] Mujahdi C B, Bebis G, Ghouzali S, *et al*. Fingerprint shell: secure representation of fingerprint template [J]. Pattern Recognition Letters, 2014, 45: 1242.

[12] Ahmad T, Hu J K, Wang S. String-based cancelable fingerprint templates. [C]//Procee-dings of 2011 6th IEEE Conference on Industri-al Electronics and ApplicationsBeijing. [S. l.]: IEEE, 2011.

[13] Christian R, Andreas U. A survey on biometric cryptosystems and cancelable biometrics [J]. J Inform Secur, 2011, 3: 1.

[14] 茹宇, 刘嘉勇, 汤殿华. 基于三角拓扑结构的指纹加密方案 [J]. 通信技术, 2015, 46: 362.

[15] 喻建平, 张鹏, 王瑶, 等. 安全高效的可撤销指纹模板构造 [J]. 中国图象图形学报, 2013, 18: 36.

[16] 姚旭, 于璐, 刘嘉勇, 等. 一种基于指纹特征比特串的可撤销指纹加密方案 [J]. 四川大学学报: 自然科学版, 2017, 54: 747.

[17] 李甫, 余文春, 傅荣会. 一种指纹特征点拓扑结构的加密方法: 中国, CN201410549340. X [P]. 2015-01-21.

引用本文格式:

中 文: 李甫, 陈佳宝, 胡娟, 等. 一种指纹特征点拓扑结构的加密方法 [J]. 四川大学学报: 自然科学版, 2019, 56: 437.

英 文: Li F, Chen J B, Hu J, *et al*. An encryption method for topological structure of fingerprint minutiae [J]. J Sichuan Univ: Nat Sci Ed, 2019, 56: 437.