基于特征点分类的模糊金库方案

孙方圆[1]，郑建德[2]，徐千惠[3]

（1 厦门大学信息科学与技术学院计算机科学系，福建 厦门 361005；
2 厦门大学信息安全实验室， 福建 厦门 361005）

摘要：为解决传统指纹认证方案中指纹模板信息泄露以及指纹和密钥无法融合等问题，本文提出一种基于指纹特征点分类的模糊金库方案——CFM-FV 方案。该方案中，使用指纹奇异点作为辅助数据对指纹图像进行预对齐，将指纹细节点特征应用于模糊金库方案进行密钥绑定。验证时，提取查询指纹奇异点作为辅助数据对指纹预对齐，然后提取指纹细节点特征信息进行多项式的重构。本方案将指纹特征点分类方法与模糊金库方案相结合，一定程度上解决了传统模糊金库方案中无法实现指纹盲对齐带来的影响问题。

关键词：指纹认证；模糊金库方案 2；指纹特征点

中图分类号：TP309.7 **文献标识码：** A

现代数字身份认证手段存在易复制、被盗取等诸多问题。目前，常用的解决方案是采用基于生物特征的身份认证技术[1]。而指纹作为目前最常用的生物特征，具有易采集、难伪造的优点，被广泛应用于现代身份认证中。目前的指纹识别算法过程中都要存储用户指纹模板信息，模板信息泄露问题将是指纹识别算法所面临的最大障碍。指纹和传统密钥相结合的间接指纹认证方法越来越受到重视，指纹密码域技术作为其中一种方法应运而生[2]。其中主要的研究代表有 Juels 等[3,4]人于 1999 年提出一种模糊承诺方案和 Juels 和 Sudan[5,6]在模糊承诺方案的基础上提出了模糊金库方案。基于指纹模糊金库的方案可以实现间接认证的目的，可解决传统认证系统以及基于生物特征单一认证中的很多局限。

模糊金库的方案的安全性是基于多项式重构难点问题。对于杂乱无序的指纹特征点数据来说，特别适用于这种方案。基于模糊金库方案的指纹密码域技术是生物特征认证中的一个新的领域，方案的一个最大优点在于不存储用户生物特征的模板，而只存储辅助数据，这种辅助数据即使在被泄露的情况下也不会泄露指纹模板信息，并且在一定程度上解决了指纹和密钥的有机融合问题。但正是由于这种模糊性（指纹特征集提取的无序性、噪点加入的随机性等因素造成），导致认证过程中 FAR（错误接受率）和 FRR（错误拒绝率）很高，这也将是集成指纹密码域技术面临的重点难题。

1 基于模糊金库算法的指纹密码域技术

1.1 指纹密码域技术

指纹密码域技术从用户的指纹特征数据中提取指纹特征数据，并将该指纹特征数据和传统密钥有机融合，保存部分数据作为辅助数据，不保存用户的指纹特征模板信息。在不同的系统中，用户的注册信息都是不相同的，这点也保证了用户注册身份信息的可更改性。

指纹密码域技术能够有效的保护生物特征模板的安全，系统本身不存储生物模板信息，间接实现指纹特征模板的安全存储、撤销和重新发布，有效的解决了生物模板泄露的问题。但指纹密码域技术中辅助数据是可公开的，所以它其中包含了很少的模板信息，这也为我们重构用户注册信息带来困难。同时，指纹密码域技术在指纹识别率和安全度方面很难做到很好的平衡，这也是一个难点问题。

1.2 模糊金库算法

模糊金库算法的思想是一个用户可以使用一个集合 A 将密钥 s 上锁，形成金库 V；另外一个用户如果想解开这个库，他必须使用和 A 相似的集合 B，也就是说集合 A 和集合 B 在一定程度上必须有足够多的重复元素，B 的用户才能完全解锁金库 V，从而获得密钥 s。算法的突出优势在于，集合 B 与集合 A 可以不相等而只需要在一定程度上相近即可解锁金库获得密钥值。

1.3 基于指纹特征的模糊金库方案

Uludag 等人[7]在 fuzzy vault 基础之上提出了基于指纹的模糊金库方案，该方案和模糊金库的基本思想是一致的，但在密钥的处理上有所改进，算法中先将密钥均分为要求的份数，利用 CRC 码进行处理，然后加在密钥的后面，作为最后一项系数，形成多项式 p。比如，算法在运算域 GF（2^{16}）上进行，将长度为 256 位的密钥 k 顺序分割为 16=256/16 个长度为 16 比特位的位串 R：$a_1, a_2, \cdots, a_{16}$，计算 R 的 CRC-16 校验码，记为 a_0。构造出多项式 $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{16} x^{16}$。

指纹库加密过程中，选择 t 个指纹细节特征点（采用横坐标和纵坐标表示一个细节点），构成集合 A，将集合 A 投影到在多项式形 p(x)上构成点对，再加入随机产生的噪点集合，这样就形成了模糊指纹金库 V。具体过程如图 1 所示：

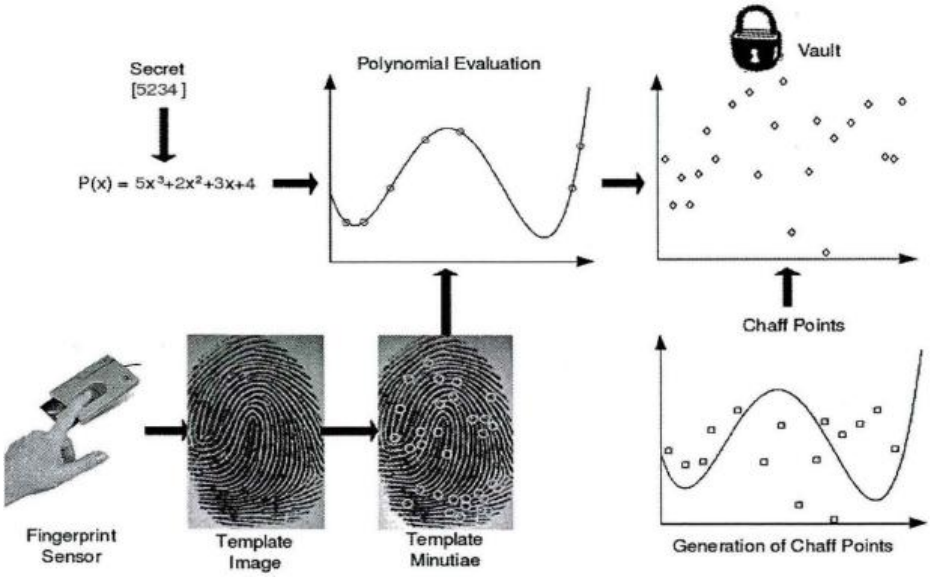


图 1 指纹库加密步骤

Fig.1 Vault encoding

指纹库解密过程中，用户提供指纹细节点特征集合 B（再次提取用户指纹，从指纹图像中获取指纹特征集合）。在模糊指纹金库 V 中选择和集合 B 匹配（两点的距离小于某个阀值）的点，m 为最终匹配点数。如果 m 小于多项式系数，则指纹库解密失败。否则，利用拉格朗日差值法可重构出多项式，并利用 CRC 纠错码进行纠错，就可恢复密钥值 k。具体过程如图 2 所示：

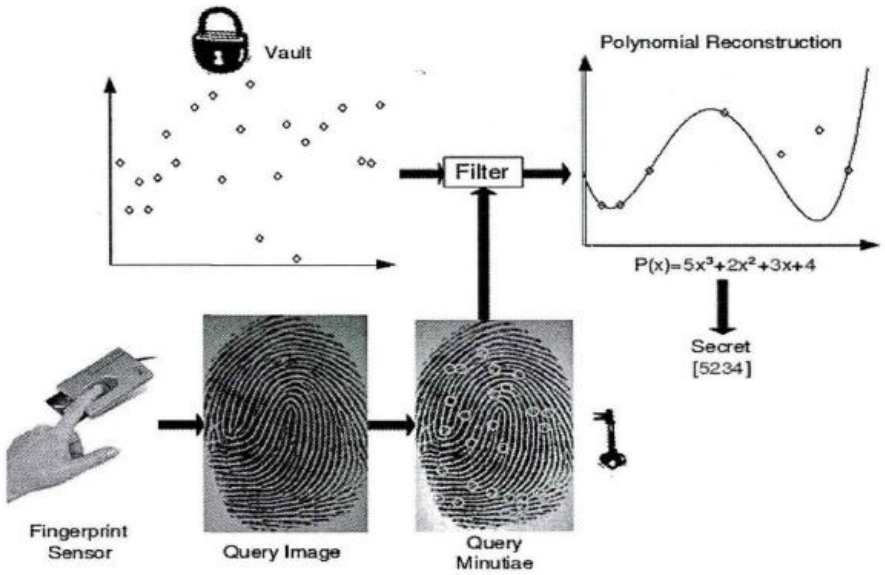


图 2 指纹库解密步骤

Fig.2 Vault decoding

算法通过提取指纹特征点坐标（x,y）作为特征数据。构建指纹金库之前，先要对模板指纹和验证指纹进行校准，目的是要消除由于旋转、扭曲等引起的非线性形变。通过以上分析可得出如下结论：1）该算法是一个可实施的方案，方案简单易行，有较高的指纹识别效率；2）该算法在构建模糊金库之前，都是假设指纹图像是预校准处理后的，这和实际应用不相符。

1.4 现有的指纹模糊金库方案

Clancy 等人[8]在 2003 年首次将指纹应用于模糊金库当中，提出了指纹模糊金库方案。该方案使用指纹细节点的平面坐标进行加锁和解锁，并通过 RS 纠错技术来还原特征点位置，最后再还原多项式。Uludag 等人[9]在 Juels 的模糊金库理论与 Clancy 的指纹模糊金库方案的基础之上提出了一种更加实用化的算法。他们的改进点在于指纹配准算法中，使用指纹细节点代替指纹特征点，算法中计算每两个指纹细节点之间的距离和连线方向来完成指纹的配准操作。算法中对秘密数据 K 使用 CRC 码进行编码之后构造多项式 P，再由指纹特征点的位置信息作为输入，计算点在 P 上面的投影信息，并添加杂凑点共同构成模糊金库。Nandakumar 等人[10]在前人研究的基础之上，引入了特征点的方向信息 θ，使得特征点由原来的(x,y)扩展到(x,y,θ)，这使得杂凑点的选取范围增大。

综上可看出，以上方案仍存在一些缺点：1）使用邻域结构描述特征点加大了模糊金库的存储空间，领域结构也会暴露指纹的局部结构，一定程度上增大了指纹特征点结构泄露的隐患；2）方案中都是假定指纹特征集合和模板集合是预先精确对齐的，这和实际应用不相符；3）由于算法中指纹特征集合是无序集合，加入过多的噪点，使得多项式重构存在误差，这将大大提高 FRR 与 FAR。

2 基于指纹特征点分类的模糊金库方案

本方案对提取的指纹特征进行分类处理，使用指纹奇异点（中心点和三角点）作为辅助数据事先对指纹图像进行预对齐，将指纹细节点特征（端点和分叉点）应用于模糊金库方案进行密钥绑定。验证时，提取查询指纹奇异点作为辅助数据对指纹进行预对齐，然后提取指纹细节点特征信息进行多项式的重构。由于该密钥和指纹特征是相互融合的，为了区分该密

钥和普通口令密钥等的区别，本文称该密钥为身份密钥。

2.1 辅助数据概念

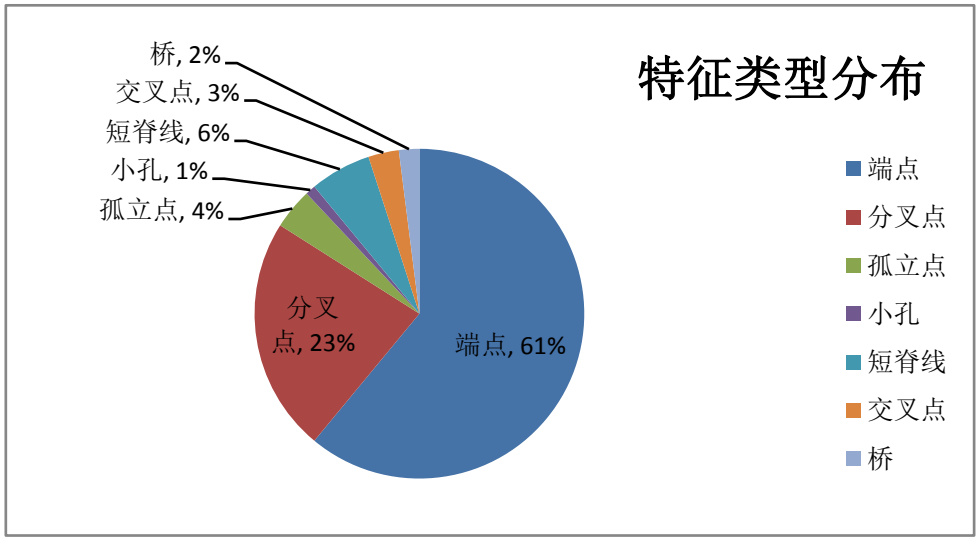
模糊金库方案中需要对指纹图像进行指纹预对齐操作，库中需要存储一种辅助数据用来指纹的预对齐。该辅助数据需存储为一种公开信息，这种公开信息不能泄露太多的指纹模板特征点的信息。同时，辅助数据也要包含足够的信息用来进行指纹预对齐。

指纹的奇异点占指纹特征点的很少一部分（见图 3），它包含了指纹特征的很少信息，基于奇异点的配准匹配方法[11,12]往往具有很高的配准速度和识别率，所以本文将使用指纹的奇异点作为指纹预对齐的辅助数据。

图 3 特征类型分布

Fig.3 Type of characteristics

2.2 基于指纹奇异点的预对齐算法



针对指纹奇异点的配准算法，本文采用传统的指纹特征点配准操作，逐步进行局部配准和全局配配准。由于篇幅原因，指纹预对齐前的指纹图像处理工作暂不多做介绍，而指纹奇异点的提取采用传统的基于 POINCARE 指数[13]的检测算法进行过滤得到。通过选择参考点配准的方法，来完成指纹查询集合 Q 和指纹模板集合 T 的配准操作。

1）选取指纹奇异点对：从集合 Q 和集合 T 中各选取一个点作为参考点，若两点落在可变限界盒中，计算出两图的位移量（transx,transy)和旋转量 rotation。

$transx$：$\Delta x = x_i - x_j^{'}$

$transy$：$\Delta y = y_i - y_j^{'}$

$rotation$：$\Delta\theta = \theta_i - \theta_j$

2）整体对齐指纹奇异点对：根据以上三个公式中得到的水平和垂直位移量以及旋转量，将指纹查询集合 Q 进行旋转和平移。计算出落在可变限界盒中的点，落在其中的点认为是匹配的点。最后，统计匹配的点到集合 M 用来以后的多项式还原操作。

3）匹配分数计算：计算集合 M 的个数，通过计算匹配分数来决定配准的准确度。根据多次匹配，给出一个阀值作为参考值，当匹配分数超过阀值时就认为该次匹配是成功的，否则是失败的，返回步骤 1）重新开始选择参考点。当所有的参考点都配准失败，就认为这两个指纹不是来自同一个手指，直接返回指纹配准失败，以后的操作无需进行。

2.3 基于指纹特征点分类的模糊金库方案

基于 Fuzzy Vault 的实现方案包括两个步骤：指纹金库加密（Vault Encoding）和指纹金库解密（Vault Decoding）。

在指纹金库加密阶段（如图 4 所示）：

1）从用户输入的指纹图像中提取奇异点集 HD 作为辅助数据，以及指纹细节点（端点和分叉点），每个特征点拥有 x、y 坐标，A 代表细节点点集：

$A=\{(x_i,y_i)\,|\,i=1,2,.....n\}$，n 代表特征点的总数目。

2）用户首先计算密钥 Key 的纠错码(CRC 校验码)，并将计算得到的 CRC 校验值 a_0 与密钥 Key 连接，得到 S，然后基于 S 构造一个关于 x 的多项式 p（阶数为 k），并计算 S 的散列值 hash(S)：

$$p(x)=a_0+a_1x+a_2x^2+\cdots+a_kx^k$$

$$S=a_0\|a_1\cdots\|a_k,\ a_i\in GF(p^2)$$

K = hash(S)

3）将特征点集 A 中的元素映射到 GF（p^2)上，得到结果集 R_A：

$$R_A=\{(r_i,v_i)\,|\,i=1,2....n\},r_i=(x_i,y_i)$$

$$v_i=p(Z_i)+b_i,\ Z_i=x_i\oplus y_i\in GF(p^2),\ i=1,2\cdots n,\ b_i\text{为随机数}$$

4) 随机生成干扰点集 C，保证该点集不在 p(x)上：

$$C=\{(c_i,v_i)\mid i=n+1,n+2\cdots,n+r\},c_i=(x_i,y_i)$$

$$v_i=p(Z_i)+b_i,\ Z_i=x_i\oplus y_i\in GF(p^2),\ i=n+1,n+2\cdots,n+r$$

5）由干扰集 C 和结果集 R_A 生成并集 R，这样指纹金库 V 就形成了。

$R=\{(r_i,v_i)\,|\,i=1,2,\cdots n+r\},r_i=(x_i,y_i)$。

$V=(R,HD,K,k)$

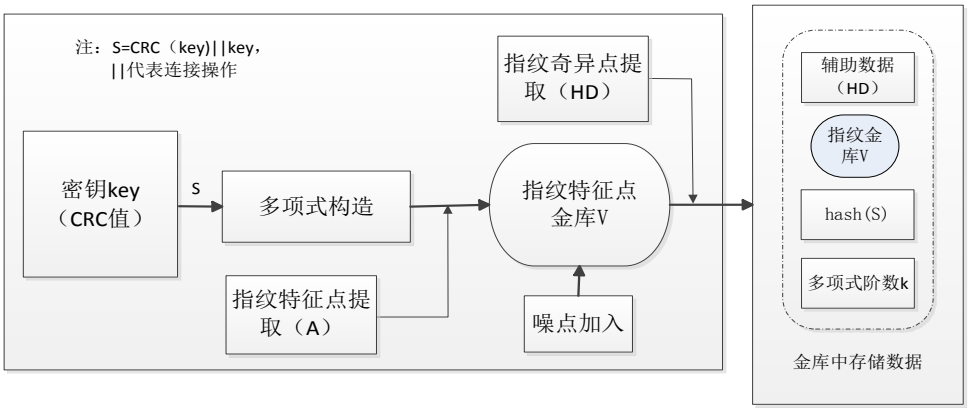


图 4 指纹金库加密步骤

Fig.4Vault encoding

指纹金库解密阶段（如图 5 所示）：

1）当验证用户身份的时候，通过指纹仪提取用户指纹特征，并将其分类处理。通过指纹奇异点完成指纹图像的预对齐，平移和旋转后得到查询图像中的指纹细节点集合 U：

$\mathrm{U}=\{(x_i^{'},y_i^{'})\,|\,i=1,2\cdots,m\}$，m 代表特征点的数目

2）将集合 U 和在库加密步骤中生成的指纹金库 V 进行比较，用 M 表示集合 U 和集合 R 中，由任意两点差值落在可变限界盒内形成的点集，r 表示配准数：

$$\mathrm{M}=\{(m_i,v_i)\,|\,i=1,2\cdots t\},m_i=(x_i,y_i),\mathrm{M}\in\mathrm{R},t\le r$$

3）将 M 和 k 作为牛顿多项式插值法的参数，解开金库中的 k 阶多项式 $\mathrm{p}^{'}(x)$，由多项式 $\mathrm{p}^{'}(x)$ 便可以得到多项式的每位参数项系数 $\mathrm{a}_0^{'},a_1^{'}\cdots,a_k^{'}$，由此可得到每项参数连接后的哈希值 $\mathrm{K}^{'}$：

$$\mathrm{p}^{'}(x)=\mathrm{RS}（\mathrm{k},M)=\mathrm{a}_0^{'}+a_1^{'}\mathrm{x}\cdots,a_k^{'}x^k$$

$$\mathrm{K}^{'}=\mathrm{hash}(\mathrm{a}_0^{'}\|a_1^{'}\|\cdots\|a_k^{'})$$

4）此时，如果 $\mathrm{K}^{'}$ 和 K 是一致的，则用户身份验证成功，并可还原用户密钥，否则失败。如果集合 M 包含 k+1 个真的指纹特征点，那么模糊金库算法就可重构出同一个多项式。

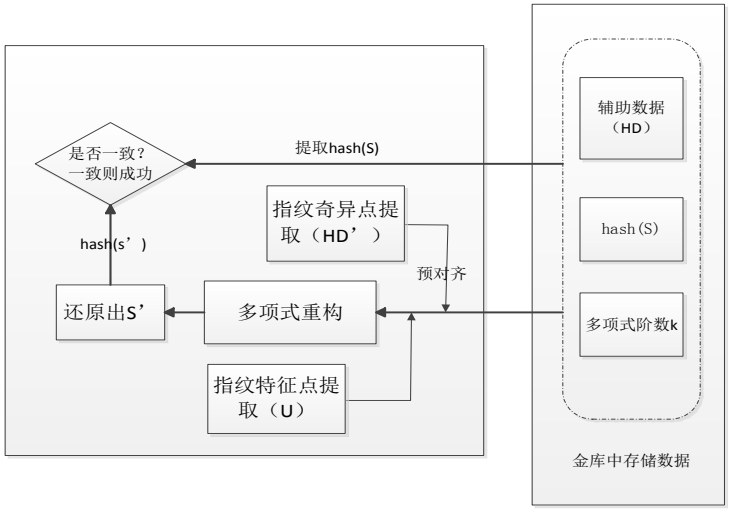


图 5 指纹库解密步骤

Fig.5 Vault decoding

3. 实验结果分析

为了验证基本方案的性能，我们使用 FVC2002 的 DB2 指纹库，并应用 VS2008 编程工具做了仿真实验与前人的研究进行比较。FVC2002 的 DB2 指纹数据库是由 10 个手指，每个手指采集 8 个指纹组成，总共有 80 个指纹。实验中，先后使用了本方案与 ASFV[14]方案，MFVC[15]方案及 Nagar.2008[16]方案进行指纹对比和解锁操作。错误拒绝率（FRR）通过同一指纹与相同指纹的其他 7 个指纹进行比较，总共进行了 7*8*10=560 次比较，统计得到结果。错误接收率（FAR）通过一个指纹与其他不同指纹的 70 个指纹进行比较，比较次数为 80*70=5600 次。

对于每组指纹模板生成的模糊金库，由真实点和随机生成的 300 个噪点共同组成，若成功解锁金库就可获得密钥，若不成功则得不到密钥。应用实验数据库中的指纹重复上锁与解锁实验，并统计实验结果得到相应的错误接受率(FAR)和错误拒绝率(FRR)。

实验中指纹金库加密和解密步骤使用的相关参数如下，如表 1 所示：

表 1 实验中指纹金库相关参数

Tab.1The involved parameters of the experiment

指纹金库相关参数名称	参数值
POINCARE 值	-1 代表中心点，1 代表三角点
可变限界盒	水平、垂直距离、角度差值均小于 10
接受相似度	>50
接受配准数(aligned points)	>9
噪点数（noise points）	300 个
可接受奇异点数	<30
多项式的阶	10

本文方案与前人的基于模糊金库方案的实验结果对比，如表 2 所示：

表 3.2 实验结果对比

Tab2.Comparison of experimental result

方案名称	数据库	是否预对齐	时间（s）	FAR（%）	FRR（%）
ＡＳＦＶ	FVC2004	是	0.546	0.0047	0.2645
ＭＦＶＣ	FVC2004	是	0.945	0.001	0.2532
Nagar.2008	FVC2002	是	3	0.001	6
本方案	FVC2002	是	0.371	0.0001	0.3263

从实验结果的对比中可以看出，本文方案的 FAR 小于 0.0001%是比较低的，在这方面可看出，基于指纹分类的模糊金库方案的性能是优于前人方案的。由于每次加入的噪声点的随机性以及标准库中指纹质量问题，这导致了 FRR 的结果稍微比较高（实验证明，如果进行同个人的不同指纹的两次查询，FRR 就可降低到 0.03%左右），但从指纹金库解锁耗时的角度，这种结果是可以接受的。而基于自动配准的方案（ASFV，MFVC）仅仅使用细节点创建模糊金库，这样有可能造成细节点泄露，从而泄露指纹模板。而本文采用指纹奇异点作为辅助数据，能够加强多指纹模板的安全保护。同时，由于奇异点的高配准率的性质，使得配准时间缩短。多重控制指纹模糊方案（ASFV）采用了多个指纹给秘密信息加锁，这种方法虽然能更有效地保证安全性，但同时也会提高错误拒绝率，增加了验证时间，造成一些不必要的麻烦。

此外，通过实验表明，当两个方案的 FAR 相同时，本文方案的 GAR（GAR 为真实接收率，GAR=1-FAR）大于其他糊金库方案的 GAR；当 GAR 相同时，本文方案的误识率相对较小。

该方案可有效解决由于单一生物特征认证过程中生物特征模板泄露问题、存储空间大小限制问题、指纹和传统密钥无法有机融合等问题。而模糊金库的安全性由模糊金库的模糊性和多项式重构难题保证，如果暴力破解金库，取每个指纹对应的多项式阶次均为 10，平均每个模板包含细节点数为 40,干扰点个数为 300。采用文献[17]中的安全性分析方法，从所有点（包括干扰点和真实点）中获取 11 个点，即可得到总秘密信息。复杂度为 C(11，340)/C(11，40)，约为 85 亿次。

4. 总结

本文通过指纹特征点分类的方法，将指纹奇异点的高配准率的性质应用到指纹的预对齐方案中，利用模糊金库的特点，通过筛选出的指纹特征点还原出原有密钥，实现指纹和密钥的有机融合。但由于库中随机加入的噪点（增大了模糊性），这将影响算法性能的稳定性。如何在满足一定模糊性的情况下，保持高配准率，减少对多项式重构带来的影响，将是本文以后需要深入研究的地方。

参考文献：

[1] 郑智强. 指纹匹配算法及集成方案的研究[D]. 厦门: 厦门大学, 2013.

[2] SoutarC, Roberge D, Stoianov A, et al. Biometric encryption. ICSAGuidetoCryptography, McGraw-Hill, 1999, http://www.bioscrypt.com/assets/BiometricEncryption.pdf.

[3] Juels A, Wattenberg M. A fuzzy commitment scheme[C]. ACM, 1999.

[4] Juels A, Wattenberg M. A fuzzy commitment scheme. In: Proc. of the 6th ACM Conf. Computer and Comm.Security(CCCS). NewYork: ACM. 1999. 28—36.

[5] Juels A, Sudan M. A fuzzy vault scheme [J]. Designs, Codes and Cryptography. 2006, 38(2): 237-257.

[6] Juels A, Sudan M. A fuzzy vault scheme. In: Lapidoth A, Teletar E, eds. Proc. IEEE Int'l Symp. on Information Theory. Institute of Electrical and Electronics Engineers, Inc., 2002. 408.

[7] Uludag U, Pankanti S, Jain A K. Fuzzy vault for fingerprints[C]. Springer, 2005.

[8] Clancy T C, Kiyavash N, Lin D J. Secure smartcard based fingerprint authentication[C]. ACM, 2003.

[9] Uludag U, Jain A. Securing fingerprint template: Fuzzy vault with helper data[C]. IEEE,2006.

[10] Jeffers J, Arakala A. Fingerprint Alignment for a Minutiae-based Fuzzy Vault[C]. Biometrics Symposium,2007:1-6.

[11] Chen Y, Dass S C, Jain A K. Fingerprint quality indices for predicting authentication performance[C]. Springer, 2005.

[12] Karu K, Jain A K. Fingerprint classification [J]. Pattern recognition. 1996, 29(3): 389-404.

[13] 谭台哲，宁新宝，尹义龙，詹小四，陈蕴．一种指纹图像奇异点检测的方法[J]．软件学报.2003:1082-1088.

[14] Fang E, Han C, Liu J. Auto-aligned sharing fuzzy fingerprint vault[J]. Communications China, 2013, 10(10):145 - 154.

[15] 姚旭，刘嘉勇，韩彩芸,等. 基于指纹自动配准的多重控制模糊金库方案[J]. 四川大学学报：自然科学版, 2014, 51(6). DOI:10.3969/j.issn.0490-6756.2014.06.017.

[16] Nagar A, Nandakumar K, Jain A K. Securing fingerprint template: Fuzzy vault with minutiae descriptors[J]. Internat.conf.for Pattern Recognition, 2008:1 - 4.

[17] Boles W, Boyd C, Hirschbichler M. A multiple-control fuzzy vault[J]. Proceedings of Sixth Annual Conference on Privacy Security & Trust, 2008:36-47.

Fuzzy Vault Scheme Based on Classification of Fingerprint Features Scheme

SUN Fang-yuan,XU Qian-hui, ZHENGJian-de

(1 Computer Dept., School of Information Science and Technology, Xiamen University;
2 Information Security Lab, Xiamen University 361005, China)

Abstract: In order to solve the problems that fingerprint template leakage problem and the unable combination of fingerprint and the traditional key in the traditional fingerprintidentification, Fuzzy Vault Scheme Based on Classification of Fingerprint Features Scheme -----CFM-FV is proposed in this paper. In our scheme, the singularities will be as helper data for pre-align the fingerprint. While the minutia features will be used to encoding the vault in this scheme. In the stage of verification, the singularities will be extracted as helper data for fingerprint pre-aligned, then the extracted minutia features will be used to reconstruct the polynomial. In this scheme, the problem that the traditional scheme cannot align the fingerprint blind will be solved to some extent by combining classification method of fingerprint features with fuzzy vault scheme.

Keywords: Fingerprint Authentication;Fuzzy Vault Scheme; Fingerprint Features