doi: 10.3969/j.issn.0490-6756.2017.04.014

一种基于指纹特征比特串的可撤销指纹加密方案

姚　旭[1,2], 于　璐[1], 刘嘉勇[1], 汤殿华[2]
(1. 四川大学电子信息学院, 成都 610064; 2. 保密通信重点实验室, 成都 610041)

摘　要: 本文以指纹作为生物识别的研究对象,在保护指纹隐私安全的前提下,研究基于模糊提取的可撤销指纹加密方案. 首先,在注册阶段,通过检测指纹奇异点并以指纹奇异点为基础,从指纹图片中提取二进制串序列作为指纹特征信息,再将二进制串结合 BCH 纠错编码和模糊提取技术生成指纹密钥和辅助数据. 最后只要待鉴别指纹为同源指纹,同时结合辅助数据,便可恢复出指纹密钥,通过身份鉴别. 实验结果表明,方案具有较高的鉴别性能. 安全性分析表明,该方案具有较高的安全性,可以满足现有需求.

关键词: 指纹; 指纹二进制串; 纠错编码; 生物特征加密; 模糊提取
中图分类号: TP309.2　　**文献标识码**: A　　**文章编号**: 0490-6756(2017)04-0747-06

A cancellable fingerprint bio-cryptosystem based on fingerprint binary string

YAO Xu[1,2], *YU Lu*[1], *LIU Jia-Yong*[1], *TANG Dian-Hua*[2]
(1. College of Electronics and Information Engineering, Sichuan University, Chengdu 610064, China;
2. Science and Technology on Communication Security Laboratory, Chengdu 610041, China)

Abstract: The cancellable fingerprint bio-cryptosystems based on the fingerprint binary string is study under the premise of protecting the security of fingerprint privacy. During the registration, first detect the fingerprint singular point as the base point, and extract the binary string from the fingerprint as the fingerprint feature, then generate the fingerprint key and auxiliary information by combining the error-correct code and fuzzy scheme. Finally, during the authentication, the fingerprint key could be recovered by auxiliary information and homology fingerprint. Experiments demonstrate that the proposed biometric cryptosystem has good recognition performance. And security analysis indicates that the security strength of the proposed biometric cryptosystem can satisfy the need of current security circumstances.
Keywords: Fingerprint; Fuzzy schemes; Fingerprint binary strings; Error-correcting code; Biometric encryption

1　引　言

传统的身份鉴别技术,如利用口令、智能卡等方式,因其易遗忘,易盗取和易假冒等弊端,已经越来越难满足人们的需求了. 而生物特征以其独有的唯一性、不可替代性、便捷性在身份鉴别领域得到了广泛的应用. 人们熟知的生物特征主要分为个人固有的物理特征,如指纹、掌纹、视网膜、虹膜、静脉、脸型及 DNA 等,和行为特征,如步态、声音、按键力度及笔迹等[1]. 虽然利用生物特征进行用户身份鉴别可以带来很大的便捷性,但是一旦这些生物特征信息泄露将永远无法恢复,给个人隐私安全带来巨大的威胁,所以生物模板保护和加密技术便应运而生.

收稿日期: 2016-06-09
基金项目: 保密通信重点实验室基金(9140C110401140C11053)
作者简介: 姚旭(1991－), 女, 硕士生, 研究方向为信息安全与生物特征模板保护.
通讯作者: 刘嘉勇. E-mail: ljy@scu.edu.cn

2 相关研究工作

本文以指纹为生物特征主要研究对象. 文献[2]提出了三种用于指纹模板保护的不可逆变换方式,分别是极坐标变换、笛卡尔坐标变换和函数变换,其安全性在于通过不可逆的变换方式,无法恢复出原始指纹特征信息. 还有一些学者提出利用哈希函数来进行不可逆变换[3]. 文献[4]则提出了一种细节点柱形编码 Minutia Cylinder-Code(MCC)的指纹保护方法,此方法利用每个细节点的局部特征信息(距离,方向)构造一个三维圆柱体的方式来编码指纹细节点描述符. Clouaib Moujahdi 等人提出的一种指纹模板保护的变换方式是根据指纹细节点之间的相对不变量构造了一种指纹螺旋线[5].

Chulhan Lee 等人提出了一种基于指纹细节点比特串的模板保护方案[6]. 其基本思想是将指纹细节点信息进行安全域转换,提取特征比特串,然后通过计算指纹模板和活体样板对应的比特串的相似度来判断指纹是否同源. 此方案的优点是在实现了一种可撤销的模板保护方案的同时不泄露指纹的原始信息,并且还能够实现指纹的自动配准[7]. 但是此方案仍有以下不足.

(1) 采用几何哈希技术[7],从每一幅指纹图片中提取到的指纹比特串数量平均较多,通常在 40 以上,与指纹细节点数量相同,需要较大的计算和存储代价,匹配效率较低,不适于模糊提取技术.

(2) 生成的指纹二进制串的扰乱性和鲁棒性不好. 由于指纹二进制串中"1"表示了指纹细节点所在的单元格,"0"表示了没有指纹细节点的单元格,可能泄露指纹细节点的位置信息.

(3) 只是将指纹细节点信息转换为了二进制串表示形式,没有与传统密码学结合,也没有解决生物加密技术的难题,即无法平衡生物特征的模糊性与传统密码学的精确性之间的差异.

本文在上述研究工作基础上,提出了一种基于指纹奇异点的特征比特串的密钥生成方案. 首先对指纹信息进行特征二进制串提取[8],然后用混沌序列对指纹二进制串加密生成可撤销指纹模板,最后结合模糊提取和 *BCH* 纠错编码,提出一种指纹加密方案. 这样的改进具有以下优势.

(1) 提出一种基于指纹奇异点的特征二进制串提取的方法,在提取二进制串之前先进行指纹奇异点的检测,然后提取指纹二进制串,可降低在提取指纹比特串时计算代价较大的问题.

(2) 引入混沌序列加密指纹二进制串,生成可撤销指纹模板. 这样以用户口令构造的混沌加密变换可使变换域的指纹模板具有可撤销性;而且用混沌密码加密后的可撤销指纹模板可以隐藏指纹细节点的位置信息,使得可撤销指纹模板中"1"不再代表指纹细节点的位置信息,增强了指纹模板安全性.

(3) 将可撤销指纹模板引入到模糊提取算法中,从原始生物信息中直接取出指纹密钥,用于加密秘密消息,由此将生物特征与传统密码学有机结合,利用 BCH 编码的纠错特性使得系统中不再需要存储原始指纹模板,因而实现了生物特征的"零存储",降低了指纹隐私泄露的概率[9].

3 基于指纹奇异点的二进制串提取

从指纹图像信息中提取指纹二进制串是整个生物特征密钥提取方案的重要环节. 本文在 Lee 等人提出的指纹比特串生成方案的基础上[6],提出基于指纹奇异点的二进制串提取的方法. 实现方案如下.

首先进行指纹奇异点检测,然后以指纹奇异点为基点变换指纹原始细节点,用相对特征向量表示细节点在指纹图像中的相对位置,然后将其投影到预先定义的二维空间矩阵中,并量化标记此矩阵,最后以可变的顺序遍历矩阵元素,提取出指纹二进制串,如图 1 所示.

Bigun 在 1988 年提出了一种对称方向场滤波器来检测指纹奇异点[10],具有很好的效果,在此基础上,给出本文的指纹奇异点的检测方法. 首先,定义一阶复数滤波器模型为 $\exp\{i\varphi\}$. 但是这个模型不能直接用于原始指纹图像,而是用于经过处理的指纹的方向场. 而 $z(x,y)=(f_x+if_y)^2$ 经常用于描述指纹某像素点 (x,y) 的局部方向场,其中 f_x 是指纹原始图片 x 方向上的导数,f_y 是 y 方向上的导数. 可以用一阶复数滤波器模型 $\exp\{i\varphi\}$ 来判断指纹的奇异点,是因为指纹中心点的局部方向场相似于复数一阶滤波器 $z=\exp\{i\varphi\}$,而指纹三角点的局部方向场相似于一阶复数滤波器 $z=\exp\{-i\varphi\}$. 复数滤波器的响应为 $c=\mu\exp\{i\alpha\}$,其中 μ 是某种对称模型,α 是对称模型的几何方向. 通过调整合适的 μ_1 和 μ_2,使得 $|\mu_1|>T_1$,$|\mu_2|>T_2$,T_1 和 T_2 是阈值,则得到的滤波器响应分别近似于中心点和三角点局部方向场,由此便可以检测和提取指纹奇异点.

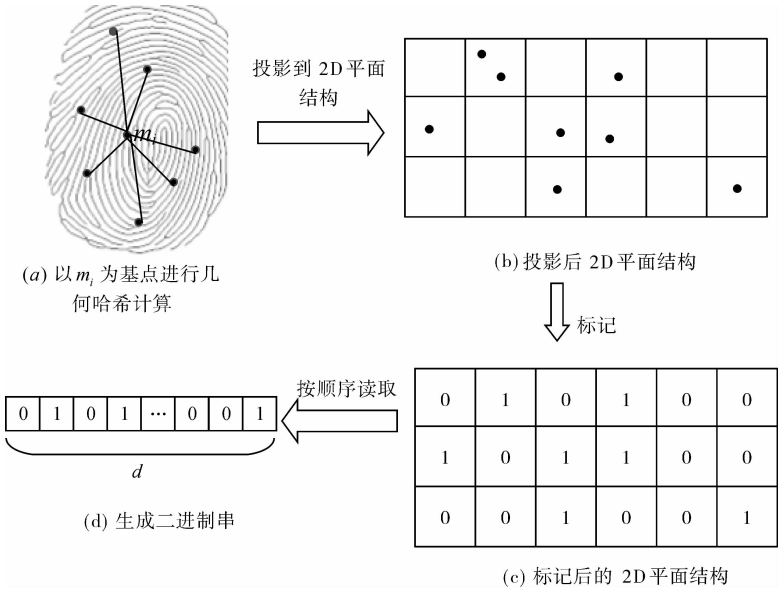

图 1　指纹二进制串提取过程

Fig. 1　Fingerprint binary string extraction process

3.1　基本思想

在生成指纹二进制串之后，Lee 等人分别计算注册和验证指纹特征比特串之间的相似度来判断两个指纹是否匹配[6]. 但这其中存在一个缺陷，即系统必须存储原始注册指纹二进制串信息，而此信息一旦泄露，就会对该方案的安全性造成极大影响.

对于上述缺陷，本文采用模糊提取和纠错码来解决问题. 方案的基本思路是，首先从原始指纹图像中提取出固定的长度为 d 的特征二进制串，然后采用模糊提取算法思想，首先从特征二进制串中提取长度为 l 的指纹密钥 K，将 K 进行纠错编码，并与经过混沌加密后的长度同样为 d 的指纹可撤销模板进行异或操作，所得的结果与 K 的散列值一起存储在数据库中，并抛弃原始的 K. 在解密时如果用于比对的指纹和原始指纹来自同一个人，那么解密成功，恢复出 K.

如图 2 所示，基于模糊提取的可撤销指纹模板保护方案分为注册阶段和鉴别阶段两个阶段. 注册阶段，即输入注册指纹信息，并提取指纹密钥 K，将 K 纠错编码后的结果和指纹二进制串结合生成辅助可公开的数据 P. 鉴别阶段，输入同源查询指纹，利用模糊提取算法和可公开的数据 P 恢复出密钥 K，即可完成身份鉴别. 此方法不再需要存储原始指纹比特串信息，解决了上述安全隐患，此外还提出了一种密钥生成方法，将基于指纹二进制串的模板保护方案拓展到生物加密技术领域.

3.2　方案实现过程

（1）注册阶段

Step 1　采用指纹二进制串提取方法，从指纹图像中生成指纹二进制串 $B^T=(101\cdots10)$，且指纹二进制串的长度为 d. 再结合模糊提取技术提取出均匀分布的指纹密钥 K，且密钥 K 的长度为 l.

Step 2　利用 BCH(m,l,t)纠错编码对指纹密钥 K 进行编码得到 BCH$_k$[11]，并存储指纹密钥的哈希值 $H(K)$在数据库中. BCH(n,k,t)算法中 n 为编码后的码元长度；k 为密钥 K 的长度；t 为纠错的位数.

Step 3　以用户口令为初值构造基于分段 Logistic 混沌映射的混沌序列 C，对指纹二进制串进行扰乱加密得到可撤销指纹模板 $B_C^T=(101\cdots10)$.

Step 4　将指纹密钥 K 经过 BCH 编码后的结果 BCH$_k$ 与置换加密后的指纹模板 B_C^T 进行二进制按位异或运算，生成公开信息 P 存储在数据库中，即 $P=(B_C^T\oplus\text{BCH}_k)$.

（2）鉴别阶段

Step 1　从查询指纹图像中提取指纹二进制串 $B^Q=(101\cdots10)$.

Step 2　若是合法用户，则会提供相同的用户口令用来生成相同的基于分段 Logistic 混沌映射的混沌序列 C，用此混沌序列对 B^Q 进行扰乱加密，生成可撤销的查询指纹二进制串 $B_C^Q=(101\cdots10)$.

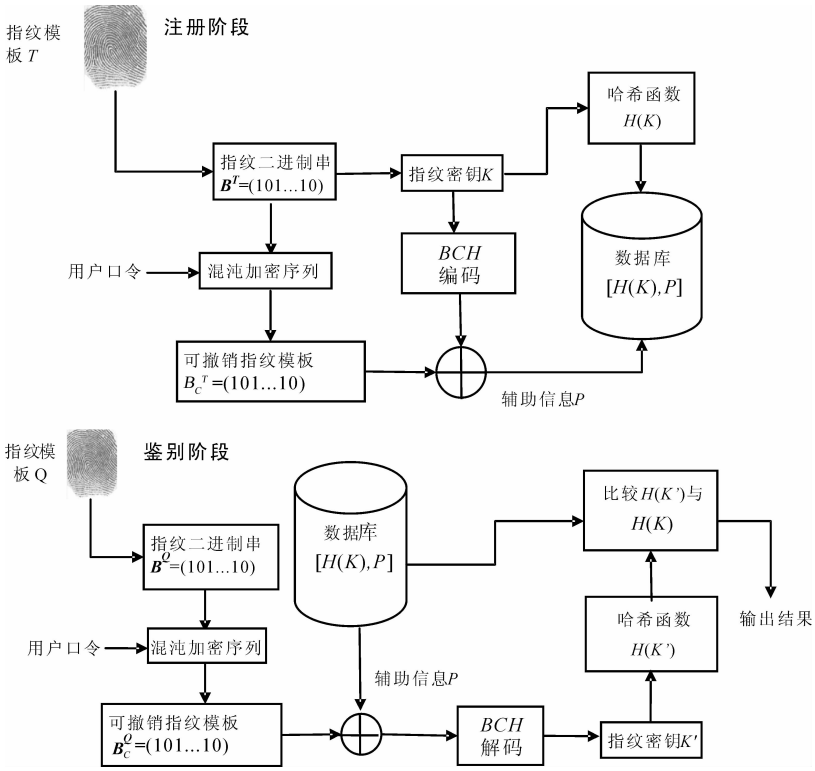

图 2 方案的注册鉴别阶段

Fig. 2 Registration and authentication phase

Step 3 将指纹二进制串 B_C^Q 与数据库中的公开信息 P 进行二进制按位异或运算,生成 $\mathrm{BCH}_{K'}$,即 $\mathrm{BCH}_{K'}=(B_C^Q \oplus P)$.

Step 4 对 $\mathrm{BCH}_{K'}$ 中的指纹二进制串再进行 BCH 解码.若解码成功,则恢复出指纹密钥 K',否则恢复失败.

Step 5 计算 K'的哈希值 $H(K')$,并与数据库中 $H(K)$进行比较,如果相同则认定为合法用户,通过验证;否则,鉴别失败,拒绝该非法用户.

4 实验测试与安全性分析

4.1 实验参数选取

本文采用的 BCH(n, k, t)编码算法存在三个参数,即编码后的码元长度 n,密钥 K 的长度 k,以及容错位数 t.

4.1.1 参数 n 的选取 选取编码后的码元长度 n 等于指纹二进制串的长度 d,而指纹二进制串的长度等于 2D 平面结构中的单元格的个数 d,当 2D 平面结构的大小确定时,单元格的长宽决定了单元格的总个数 d.实验中发现,不同的单元格参数,对应的指纹二进制串长度不同,并且相对应的真匹配与假匹配的汉明距离均值不同.表 1 给出了在选取最优单元格参数下所对应的码元长度和汉明距离均值.根据表 1 实验数据,在指纹库 FVC2000-DB2 实验中,矩阵单元格参数为长度 $C_x=15$,宽度 $C_y=\frac{\pi}{4}$,而在指纹库 FVC2002-DB2 和实际采集指纹库实验中,矩阵单元格参数均为 $C_x=10$,$C_y=\frac{\pi}{3}$,指纹特征串的识别性能最佳,长度分别为 512 bit,588 bit,588 bit.

表 1 最优参数下的汉明距离均值

Tab. 1 The optimal parameters of the average Hamming distance

指纹库	单元格长度 Cx	单元格宽度 Cy	码元长度(bit)	汉明距离均值(bit)	
				真匹配	假匹配
FVC2000-DB2	15	π/4	512	18.19	32.54
FVC2002-DB2	10	π/3	588	18.53	32.27
实际采集指纹	10	π/3	588	16.28	35.12

4.1.2　参数 t 的选取　BCH 编码的容错位数 t 能够纠正随机错误的个数. 由于指纹具有类内模糊性，同源指纹每次的采集结果都不完全一样. 参数 t 的选择方法是使同源指纹间类内差异的纠错概率很大，同时对非同源指纹的纠错概率极小. 图 3 给出了指纹库 FVC2002-DB2 和实际采集指纹库在最优参数下，同源指纹与非同源指纹的汉明距离分布密度函数.

从图 3 可以看出，同源指纹二进制串与非同源指纹二进制串的汉明距离分布具有较为明显的区分. 因为同源指纹二进制串间的汉明距离较小，集中分布在[15～25]的区间内，而非同源指纹二进制串的汉明距离较大，集中分布在[25～40]的区域内，所以可以据此来设定纠错位数 t 的取值在同源指纹集中分布的区域内.

4.1.3　指纹密钥的长度 k　当通过实验选择出指纹特征串长度 n，并根据同源指纹与非同源指纹的汉明距离区分度来确定参数 t 的选择范围后，则可根据 BCH 编码算法原理计算出指纹密钥长度 k. 如首先根据码长关系式 $n=2^m-1$ 计算 m，并确定 m 阶本原多项式 $p(x)$，计算 GF(2)上的最小多项式，找出次数为 s 生成多项式 $g(x)$，则信息码长度 $k=n-s$. 具体步骤可参阅文献[11]，本文不必赘述.

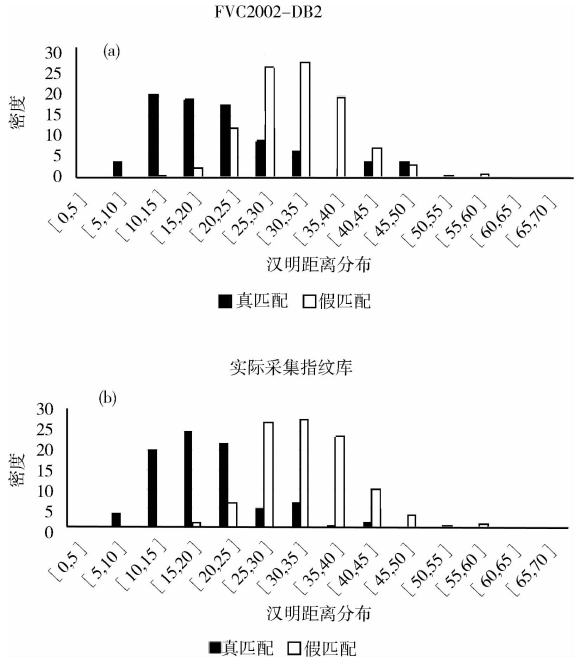

图 3　汉明距离密度分布图

Fig. 3　The Hamming distance density distribution map

4.2　实验结果分析

在实验测试中本文采用公开指纹库 FVC2002-DB2 和实际采集指纹库中的各 80 幅指纹图像进行测试，每幅指纹图像的大小均为 256 * 360 像素，这 80 幅指纹图像采集于 10 个不同的手指，每个手指采集 8 次. 真匹配实验是将每个手指其中任意一幅图片为模板，其余 7 幅为样本进行比较，所以一共进行了 $10\times(8\times7)/2=280$ 次真匹配实验计算拒识率 FRR；假匹配实验是选取任意手指的一幅图片为模板，与其余不同手指的所有图片进行比较，所以一共进行了 $10\times(8\times9)/2=360$ 次假匹配实验计算误识率 FAR. 计算在不同允许容错的位数 t 下的 FRR 和 FAR，结果如表 2 所示.

表 2　不同 BCH 编码参数下的拒识率和误识率

Tab. 2　FRR and FAR under different BCH coding parameters

指纹库	$BCH(n,k,t)$	$FRR(\%)$	$FAR(\%)$
FVC 2002-DB2	$BCH(588,528,11)$	13.288	0.106
	$BCH(588,516,13)$	12.596	0.415
	$BCH(588,504,15)$	10.315	0.588
	$BCH(588,492,17)$	10.005	0.917
	$BCH(588,480,19)$	9.196	1.236
	$BCH(588,468,21)$	8.347	1.851
	$BCH(588,456,23)$	6.275	2.399
	$BCH(588,444,25)$	4.685	2.821
	$BCH(588,432,27)$	1.448	3.352
实际采集指纹库	$BCH(588,528,11)$	9.523	0.024
	$BCH(588,516,13)$	7.531	0.088
	$BCH(588,504,15)$	6.253	0.135
	$BCH(588,492,17)$	3.782	0.189
	$BCH(588,480,19)$	2.276	0.232
	$BCH(588,468,21)$	1.366	0.456
	$BCH(588,456,23)$	1.254	0.597
	$BCH(588,444,25)$	0.987	0.769
	$BCH(588,432,27)$	0.501	0.882

针对指纹模板保护方面的研究工作，文献[12]也是采用模糊提取算法的生物加密方案，该在 FVC2002-DB2 上的鉴别性能为 FRR= 26.48%，FAR= 0.23%. 文献[13]也是研究利用 BCH 纠错编码实现指纹特征的加密方案，该方案同样在 FVC2002-DB2 公开指纹库上的鉴别性能为 FRR =8.03%，FAR=0. 本文提出方案与上述方案相比，除了鉴别性能有所提高，且在保护指纹隐私不被泄露方面的安全性更高.

与文献[14]基于几何哈希的指纹加密方案相比，两个方案在鉴别性能上实验结果相近，但本文方案的计算复杂度和空间复杂度由文献[14]的 $O(n^2)$ 减少为 $O(n)$，在计算和存储代价方面优势明显，更有利于实际应用.

4.3　安全性分析

(1) 抵抗多模板交叉匹配攻击与模板可撤销性.

在指纹安全域转换过程中,生成的指纹比特串除了与指纹特征点相关,还与矩阵单元的参数取值、二维空间矩阵元素的遍历方式相关,若比特串长度为 d,理论上有 $d!$ 个遍历方式.因此,在不同的应用系统中可通过设置不同参数和遍历方式,使得从同源指纹中提取的比特串完全不同,无法进行匹配,从而有效抵抗针对同源指纹的多模板交叉匹配攻击[14].

由于生物特征具有恒定不变的特性,注册生物特征模板的可撤销性对于模板保护具有重要意义.当注册模板丢失或泄露后,可以生成新的模板,并使同源指纹的新模板和原始模板完全不相匹配.本方案通过口令来改变混沌系统的初值,生成不同的混沌序列对指纹特征串进行加密保护.当注册模板受到攻击或泄漏时,只需修改用户口令就可以生成新的注册模板,且这两个模板完全不相匹配,从而实现生物特征模板的可撤销性.

(2) 抵抗暴力破解攻击.

对于本方案来说,可以进行暴力破解攻击的地方有以下三个.

(a) 如果攻击者想通过暴力破解的方式直接获得 $BCH(n, k, t)$编码过后的指纹密钥,则需要尝试次数 N 为

$$N=\frac{C_n^t+C_n^{t-1}+C_n^{t-2}+\cdots+C_n^1+C_n^0}{2}$$

(b) 攻击者要想直接暴力破解指纹密钥,则攻击成功的概率为 2^{-k}.

(c) 如果攻击者想直接得到通过哈希函数加密的指纹密钥,则安全性取决于哈希函数的安全性.通常得到的散列值长度为 128 位、160 位、256 位,则成功的概率分别为 2^{-64}、2^{-80}、2^{-128}.

(3) 抵抗中间人攻击.

在网络应用环境中,用户需要提供自己的指纹模板通过不安全的传输信道传递给远程鉴别服务器,如果攻击者通过中间人攻击的方式截获到用户指纹模板,便可以进行重放攻击,向鉴别服务器再一次提交指纹模板,从而攻击成功.而在本方案中,用户不需将自己的指纹模板在不安全的网络信道中进行传输即可完成鉴别过程.

5 结 论

本文研究了对指纹信息进行特征比特串提取,并结合模糊提取与纠错编码技术提取出生物密钥的实现方法,该方法具有指纹特征比特串自动配准、不需保存指纹原始特征信息、能有效抵抗交叉匹配攻击的优势,在生成密钥的同时保证了指纹模板的安全性.

参考文献:

[1] 游林.生物特征密码技术综述[J].杭州电子科技大学学报:自然科学版,2015,35:1.

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

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

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

[5] Moujahdi Cb, Bebis G, Ghouzali S, *et al*. Fingerprint shell: Secure representation of fingerprint template [J]. Pattern Recognition Letters, 2014, 45: 1242.

[6] Lee C, Kim J. Cancelable fingerprint templates using minutiae-based bit-strings [J]. Journal of Network & Computer Applications, 2010, 33: 236.

[7] 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,2014,51:1205.

[8] 唐宇.基于指纹比特串的生物特征加密技术研究与应用[D].成都:四川大学,2015.

[9] 李林.基于掌纹和双层编码的生物特征机密算法研究[D].北京:北京交通大学,2011.

[10] Nilsson K, Bigun J. Localization of corresponding points in fingerprints by complex filtering [J]. Pattern Recognition Letters, 2003, 24: 2135.

[11] 王新梅,肖国镇.纠错码——原理与方法[M].西安:西安电子科技大学出版社,2003.

[12] Hartloff J, Dobler J, Tulyakov S, *et al*. Towards fingerprints as strings: Secure indexing for fingerprint matching[C]// International Conference on Biometrics. [s. l.]: [s. n], 2013.

[13] Li P, Yang X, Qiao H, *et al*. An effective biometric cryptosystem combining fingerprints with error correction codes [J]. Expert Systems with Applications, 2012, 39: 6562.

[14] Xie C Y, Liu J Y, Yao X, *et al*. Research of biometric key generation based on fingerprint bit-strings [J]. Journal of Fiber Bioengineering & Informatics, 2015, 8: 713.