高技术通讯 2010 年 第 20 卷 第 11 期:1115 ~ 1120

doi:10.3772/j.issn.1002-0470.2010.11.003

基于 BioHashing 和密钥绑定的双重可删除指纹模板方法①

陈开志② 胡爱群③ 宋宇波 刘慧慧 袁红林

(东南大学信息科学与工程学院 南京 210096)

摘 要 针对指纹识别中自身生物特征信息的安全保护问题,提出了一种基于 BioHashing 和密钥绑定的双重可删除指纹模板(DCFT)方法。DCFT 方法首先通过 BioHashing 方法将提取出的原始指纹特征信息不可逆地转化成一串固定长的二进制序列,而后利用 Fuzzy Commitment 绑定密钥,生成一个可删除的指纹模板。验证时利用存储模板和待验证指纹,采用纠错码解码恢复出密钥。采用该方法,即使数据库中存储的模板数据被盗取,甚至密钥被破解,入侵者也不能恢复出原始指纹特征信息;且通过更改 BioHashing 中的随机矩阵或绑定的密钥,就能改变数据库中的模板,使入侵者无法利用先前已泄露的数据通过验证,避免了因为指纹的不可更改性造成永久性安全威胁,从根本上保证了指纹信息的安全。最后,仿真测试说明了 DCFT 方法的有效性。

关键词 指纹识别,生物特征模板保护,密钥绑定,BioHashing,纠错码,fingerCode

0 引 言

生物特征由于具有唯一性、隐私性、不可更改等特性,已越来越广泛地应用于身份鉴别领域。但是传统识别方法所用数据库里存储的匹配模板含有大量生物特征原始信息,甚至有些模板就是本身生物样本,如有些指纹识别系统的模板就是本身指纹图像,一旦模板丢失或被盗取,入侵者可以直接用模板信息通过验证,还可以在不同应用的数据库间进行交叉验证(cross-matching),如可以用指纹门禁系统里盗取的指纹模板信息,入侵其对应的指纹认证的个人银行账户。有的甚至可以从特征模板直接伪造出对应生物特征样本,如可以从指纹细节点模板伪造出对应指纹[1]。同时,由于生物特征具有不可更改性,一旦原始特征信息泄露,造成的危害将会是永久性和广泛性的。因此,生物特征识别系统中,自身特征信息的安全保护处于重要位置。

考虑到生物自身特征信息安全,特别是关于模板的安全,文献[2]提出了一种安全的模板,其所要达到的四个要求是差异性(diversity)、可撤销更新性(revocability)、安全性(security)和高性能(performance),其中可撤销更新性处于核心地位,根据这个目标,近些年开展了很多研究。2001 年,Ratha 等[3]提出了可删除生物特征(cancelable biometrics)模板概念。其基本思想是通过采用不可逆变换,使识别系统模板数据库中保存的不再是原始的生物特征,而是某种变换形式后的模板,并且从变换后的模板不能获取原始生物特征信息。如果特征模板丢失,通过更改不可逆变换的参数就能重新生成新的模板。由于其生物特征匹配是在不可逆变换域中进行的,因此该方法的核心是设计合适的不可逆变换方法,使之对生物特征类内差异不敏感,不降低识别精度。其代表方法有 BioHashing[4,5]和 Ratha 等[6]提出的可删除指纹模板。BioHashing 通过将生物特征序列值映射到一个由正交矩阵决定的空间,而后通过量化来达到不可逆目标。其缺点是要求生物特征必须是一串有序序列值。Ratha 等[6]通过对细节点模板进行不可逆的几何变换来达到安全模板要求。但以上两个方法都是通过变换域变换模板形式,不能产生一串稳定值来充当密钥。

另一种思路是 Uludag 等[7]提出的生物加密系统(biometric cryptosystem),其基本思想是将生物特征和密码无缝绑定起来,生成一些辅助数据充当模板,验证时通过辅助数据和重新输入的生物特征释放出密码。如果没有对应生物特征,入侵者不能从辅助

① 863 计划(2009AA01Z427)资助项目。
② 男,1983 年生,博士生;研究方向:通信信号处理与生物特征安全;E-mail: chenkaizhi007@gmail.com
③ 通讯作者,E-mail: aqhu@seu.edu.cn
(收稿日期:2009-06-24)

数据中获得原始的生物特征信息或密钥,且通过更改密码就能改变辅助数据(或则称为模板)。可见该方法同样具有可删除更改功能。同时,该方法还有个优点,那就是可以为不同应用绑定不同密钥,让用户不必去记忆各种不同的密码。这是一种基于生物特征的密钥管理系统,具有广泛应用前景。这一类方法主要有 Fuzzy Commitment[8] 和 Fuzzy Vault[9]。Juels 等人提出 Fuzzy Commitment[8]方案,采用纠错码来绑定生物特征信息和密钥,其思想是利用纠错码来消除生物特征中一些不稳定值。Hao[10]等人根据这个思想实现密钥和虹膜特征数据的绑定,取得很好性能。但 Fuzzy Commitment 方法存在局限性,其要求生物特征必须是一串有序值。为了克服这个缺点,Juels 等人又提出了 Fuzzy Vault[9]方案,其适用于点集的情况。其将真实点隐藏在一堆干扰细节点中,验证时通过提取真实点,并利用了 Shamir[11]的多人共享密钥的思想,来恢复密钥。文献[12-16]给出了在指纹条件下的具体实现,并在指纹对齐等方面提出改进方法,并提高了识别性能。Fuzzy Vault 方法也存在不足:对指纹对齐要求严格,抽取指纹细节点、对齐指纹和恢复多项式的计算复杂度高。更严重的是 2007 年 Scheirer[17]等指出的 Fuzzy Vault 的两个安全缺陷:通过交叉比较多个生成的 vault,就能很容易得到原始细节点模板的信息;在密钥被盗取时,由于 vault 中随机添加了很多干扰点对,攻击者可以把其中一部分点对换成自己的点对,可在不影响原合法用户正常使用的情况下,通过系统验证。可见,正是因为模板中含有指纹原始特征信息(虽然是将真实细节点隐藏在一堆干扰细节点中),使之存在安全隐患。一旦被攻破,将造成原始指纹特征信息的泄露,造成永久性威胁。

由以上研究可知,BioHashing 可将特征值不可逆地转化成一串固定长的二进制序列,但该序列值是不稳定的,无法充当密钥使用,而 Fuzzy Commitment 可以将稳定密钥和不稳定特征序列值绑定。为从根本上防止由模板泄露特征信息,本文结合 BioHashing 和 Fuzzy Commitment 各自的优点,提出了应用在指纹领域的特征模板保护方法——双重可删除指纹模板(dual cancellable fingerprint template, DCFT)方法。DCFT 中不含有任何原始特征信息,即使数据库中存储的信息被盗取,甚至密钥被破解,入侵者也不能恢复出原始指纹特征信息。同时,该方法可以为不同应用绑定不同密钥,具有广泛应用前景。

1 相关概念

1.1 Fuzzy Commitment

Fuzzy Commitment 是一种模糊密钥系统,其特点是不要求待验证序列值与注册时完全一致,只要错误小于一定门限,就能恢复密钥。其主要过程如下:

(1)注册:用户选择一个纠错码字 $\boldsymbol{C}$,记 $\boldsymbol{X}$ 为生物特征向量,存储 $\boldsymbol{D}=\boldsymbol{X}-\boldsymbol{C}$ 和 $\boldsymbol{C}$ 的哈希值 hash($\boldsymbol{C}$)。其中 hash()表示哈希函数。

(2)验证:待识别特征向量 $\boldsymbol{X}'$,计算 $\boldsymbol{C}'=f(\boldsymbol{X}'-\boldsymbol{D})=f(\boldsymbol{X}'-(\boldsymbol{X}-\boldsymbol{C}))=f(\boldsymbol{C}+(\boldsymbol{X}'-\boldsymbol{X}))$,$f$ 为纠错解码,如果 $\boldsymbol{X}'$ 和 $\boldsymbol{X}$ 汉明距离小于 f 的纠错能力,通过纠错码就能恢复出 $\boldsymbol{C}$。通过比较 hash($\boldsymbol{C}$)和 hash($\boldsymbol{C}'$)来获得匹配结果。

其存储的模板 $\boldsymbol{D}$ 相当于是特征信息 $\boldsymbol{X}$ 被 $\boldsymbol{C}$ 加密后的密文,不会泄露生物特征信息,且通过更改 $\boldsymbol{C}$,就能更改模板 $\boldsymbol{D}$。该方法绑定的纠错码(或称密钥)C 是独立于生物特征的,可以为不同应用绑定不同密钥,具有密钥管理功能。该方法存在的不足是要求生物特征必须能编码为一串有序的序列值。

1.2 BCH 纠错码

BCH 码是一种很好的线性循环码。BCH 码可以很容易根据所要求的纠错能力构造出,译码器也容易实现,因而是线性分组码中应用最普遍的一类码。这类码通常用 BCH(n,k,t)表示,其中 n 表示编码后码长,k 是编码前信息长度,t 是纠错能力。本原 BCH 码长 $n=2m-1$,m 为整数,更加详细资料可参考文献[18]。

1.3 BioHashing 方法

BioHashing 方法将生物特征序列值映射到一个正交矩阵产生的空间,而后通过量化转化成一串二进制序列值。其结构图可参考文献[19]中的图 2。

其具体过程如下:

(1)利用保存的种子,产生维数为 $m\times n$ 的随机矩阵,对其进行列单位正交化,获得矩阵 $\boldsymbol{R}$。

(2)对输入生物特征样本进行预处理,抽取维数为 $m\times 1$ 生物特征向量 $\boldsymbol{V}$。

(3)通过计算点积 $<\boldsymbol{V},\boldsymbol{r}_i>$,并量化,获取 BioCode 码 $\boldsymbol{B}$,长度为 n 比特。

$$b_i=\begin{cases}0, & \langle V,r_i\rangle<\tau\\ 1, & \langle V,r_i\rangle>\tau\end{cases}$$

其中 $\boldsymbol{r}_i$ 是 $\boldsymbol{R}$ 的第 i 列向量,τ 是判决门限,可以是固定值,如 0。也可以根据所有的点积 $<\boldsymbol{V},\boldsymbol{r}_i>$ 的统

计结果,选取中间值,使 0 和 1 数量一致。此外,还可以进行多进制量化。

从上面分析可知,其过程是不可逆的,不能从 B 中恢复 V,同时,改变 R 就能得到不同的 B,因此生成的 B 具有可撤销更改性。

1.4 FingerCode 编码

BioHashing 要求输入的特征向量 V 是一串有序序列值,这样才能将其不可逆的转化为二进制序列串。而已有的指纹识别方法中最常用的特征是细节点,主要用指纹的分叉点和终结点来表示,每一个点是一个(坐标,方向,类型)或则更多元的向量。验证时通过比较两个细节点集合的相似点数目,来判断是否是同一个指纹。由于该特征是无序的点向量集合,不适合应用在 BioHashing 中。因此,如何从指纹图像中抽取出可表征其特征的序列值是本文方法的关键。要求抽取出的值既要能区分不同指纹,同时对相同指纹的不同采样又要具有稳定性。

综合已有指纹特征的研究成果,选用 FingerCode[20]。FingerCode 是刻画指纹纹理特征的一串固定长数值,在指纹图像质量较好的情况下,其识别能力接近于最好的基于细节点的指纹识别方法。并且,相对于基于细节点的识别方法,FingerCode 方法计算量低。其对中心点的位置检测误差有一定的容忍力(一般是一个脊线宽度)。由于其有效性依赖于指纹中心点(或索引点)的精确检测,本文采用已有文献中中心点检测精度最高的方法——基于复滤波的方法检测指纹奇异点[21]。但 FingerCode 无法克服指纹旋转问题,验证阶段可采用每次将指纹图像旋转一定角度,再重新尝试验证。

2 基于 BioHashing 和密钥绑定的 DCFT 方法

为从根本上防止模板泄露生物原始特征信息,关键是模板不含有原始特征信息,也无法从模板计算出任何物原始特征信息。综合已有研究成果可知,BioHashing 可将一串数值不可逆的转化成一串固定长的二进制序列,但该序列值不是完全稳定的,而 Fuzzy Commitment 可以将稳定密钥和不稳定特征序列值绑定。本文结合 BioHashing 和 Fuzzy Commitment 的各自优点,提出了应用在指纹领域的特征模板保护方法——DCFT 方法。BioHashing 和 Fuzzy Commitment 能为指纹提供双重可删除更改模板的能力,同时 DCFT 方法也是一种指纹密钥绑定方法,可绑定 128 位或更长的密钥,可应用在密钥管理方面。

DCFT 方法的结构如图 1 所示,注册阶段负责生成可撤销的安全模板,执行流程如下:

(1)对要注册的指纹图像进行特征抽取,获取 FingerCode 的特征向量 V。

(2)对 V 采用 BioHashing 方法产生二进制的 BioCode 码 B,其中 BioHashing 中的正交随机矩阵为 R。

(3)选取或随机生成一个长度为 k 的二进制序列值 K 当作密钥,对 K 进行 BCH(n,k,t)编码,编码成 n 位的纠错码 E,其纠错能力为 t。

(4)B 与编码后的纠错码 E 进行异或处理,获得结果 Ks 存储到智能卡或服务器数据库中。同时还存储密钥 K 的哈希值 hash(K)。

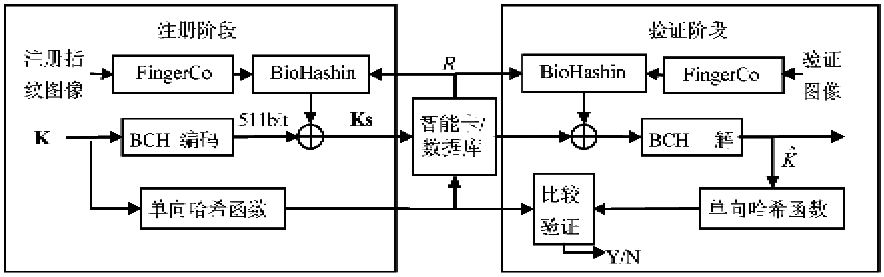

图 1 DCFT 结构

验证阶段负责对待验证指纹进行匹配,恢复绑定的密钥,执行流程如下:

(1)对要注册的指纹图像进行 FingerCode 特征抽取,获取 V'。

(2)对 V' 采用 BioHashing 方法产生 BioCode 码 B'。

(3)B' 与 Ks 进行异或处理,再对所得结果进行相应的 BCH(n,k,t)纠错解码,获得 $\hat{K}$。

(4)通过比较 hash(K)和 hash($\hat{K}$)来验证结果,相同则表明是同一指纹,通过验证。

如果验证阶段提取出的 BioCode 与注册阶段所获得的汉明距离不大于 t，那么纠错码能恢复出 K。DCFT 方法的数据库中存储的是 Ks、R 和 hash(K)。其双重可删除更改能力是：

(1)更改 R 就能改变 B，进而改变最终存储的 Ks。

(2)更改 K 就能改变纠错码，进而改变最终存储的 Ks。

3 仿真实验结果

为评价 DCFT 方法的性能，对其进行了仿真。测试的指纹数据选用 FVC2004 DB2 _ A[22]，并从中删除掉图像质量较差(如索引点在图像边缘，无法获取 FingerCode 完整的 512 个值)，最后选用其中的 54 个指纹，每个指纹 7 幅图像，共 378 幅图像。其中抽取的特征向量 FingerCode，其参数是同心圆数为 4，半径间隔 20 像素，分成 16 个扇区，对每个扇区进行 8 个方向的 Gabor 滤波，最后统计每个扇区里滤波后的灰度方差，共 512 个值。这里不采用旋转图片，多次尝试验证的方法。BioHashing 里随机矩阵 R 维度是 512 × 511，与 V 内积并量化后生成的 BioCode 为 511 比特。

其中 BioHashing 产生的 BioCode 码的稳定性是整个方法识别性能的关键，其目标是同一指纹产生的 BioCode 码汉明距离很小，而不同指纹的汉明距离很大。为此，仿真了产生的 BioCode 的类内距离(同一指纹生成的 BioCode 的汉明距离)和类间距离(不同指纹生成的 BioCode 的汉明距离)，其结果如图 2 所示。当存储的 R 不被泄露时，指纹类间距离(未知参数 R)分布在 256 比特附近，几乎都大于 230 比特。而指纹类内距离分布在 50 比特附近，都不大于 100 比特。可知 R 不泄露时，很容易根据汉明距离识别指纹。同时，仿真了存储的 R 已泄露的情况。从图中可知，指纹类间距离(已知参数 R)大为减小，大多分布在 50 到 125 这个区间，和类内距离有一部分重合。在这种情况下，根据汉明距离识别指纹，将造成一定的识别错误率。

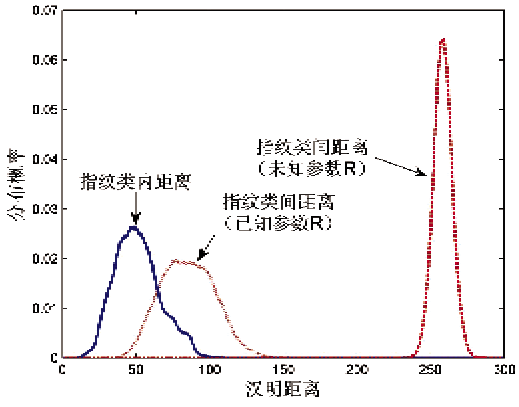

图 2 BioHashing 输出类内和类间距离分布

图 3 仿真了根据 BioCode 码的汉明距离识别指纹的性能，主要性能参数是错误拒绝率(false reject rate，FRR)和错误接受率(false accept rate，FAR)。从图可知，随着汉明距离门限的增大，FRR 减小，而 FAR 增大。如果门限设在 100 到 230 比特之间，一次验证时的 FRR 和未知 R 时的 FAR 都接近 0，此时既不会误判，也不会漏判，是理想状态；当 R 泄露时，其 FAR 性能将下降，对应的是已知 R 时 FAR 曲线。由图可知，此时 FAR = 0，对应的一次验证时 FRR 高达 60%以上。在实际应用中，验证失败后重新刷指纹是合理的。因此为提高 FRR 性能，可采用多次刷指纹验证，只要有一次通过，即认为验证成功，这里尝试验证三次时的性能。从仿真结果可以看出，三次验证后 FRR 性能大大改善。如在汉明距离门限设为 50 比特时，其 FAR 约为 3.5%，一次验证时 FRR 大于 40%，而三次验证后 FRR 小于 10%。

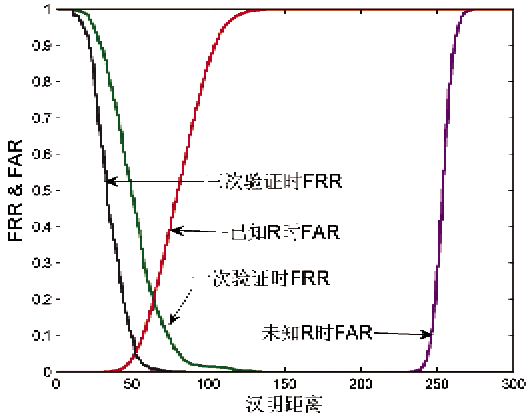

图 3 根据 BioCode 码的汉明距离识别指纹的性能

最后结合 BCH 纠错码仿真整个 DCFT 方法的性能，选取 $m = 9$，$n = 511$，其性能曲线和图 3 是一样的。表 1 列出了几组纠错码组合，如采用 BCH(511，157，53)时，三次验证后 FRR = 4.81%，未知 R 时 FAR = 0，即使 R 被泄露，FAR 仍可达到 5.33%。同时，从图 3 可知，若将纠错码纠错能力提高到 100 比特以上，将达到一次验证 FRR 和未知 R 时 FAR 都趋向 0，达到识别理想状态。此时主要不足是密钥长度只有 40 比特，当然，可以采用文献[23]中的方法，通过增长 FingerCode 里值的长度，以及扩大矩阵

$\boldsymbol{R}$,多级量化等方法来增长 BioCode 码,进而来提高密钥长度,这里不做具体仿真。

表 1 DCFT 方法性能

BCH(n,k,t)	一次验证 FRR(%)	三次验证 FRR(%)	未知 R 时 FAR(%)	已知 R 时 FAR(%)
(511,184,45)	60.68	19.07	0	1.12
(511,157,51)	48.25	9.44	0	3.79
(511,148,53)	43.91	4.81	0	5.35
(511,130,55)	39.78	3.70	0	7.09
(511,121,58)	28.52	1.75	0	11.33
(511,40,95)	1.74	0	0	76.3

将本方法分别与已有的指纹识别方法[4,20]比较。文献[20]中的 Table 1 给出了单独采用 FingerCode 的指纹识别性能,如表 2。和图 3 比较知,在 $125 < t < 230$ 时,DCFT 方法的 FAR(未知 R 时)和 FRR(一次验证)都达到 0,其识别性能要远优于 FingerCode 方法。且 FingerCode 方法里直接采用 FingerCode 作为模板,容易被盗取、替换,且无法撤销更新,安全性无法保证。文献[4]中的 Table 1 给出了单独采用 BioHashing 时的指纹识别性能,其 FAR 和 FRR 和本文 DCFT 方法相近,都能同时达到 0。但 BioHashing 是直接存储 BioCode 码当模板,通过比对汉明距离来验证,其虽然可以通过更改 R 更新 BioCode 码,但无法抵挡盗取、替换模板(BioCode 码)的攻击。而 DCFT 方法不是采用比对汉明距离,而是采用纠错解码的方法,不可能通过盗取、替换模板 $\boldsymbol{Ks}$ 来非法通过验证。同时 BioCode 码是不稳定的序列值,无法充当密钥使用。

表 2 基于 FingerCode 的指纹性能

欧式距离阈值	FAR(%)	FRR(%)
30	0.10	19.32
35	1.07	7.87
40	4.59	2.83

4 安全性简要分析

分析数据库里存储的相关信息(包括 $\boldsymbol{Ks}$、随机矩阵 $\boldsymbol{R}$ 和 Hash($\boldsymbol{K}$))泄露后,是否可造成指纹原始特征信息和其它保密参数的泄露。从结构图中可知,需要保密的数据(包括最原始的指纹信息)是指纹图像,还有从指纹图像抽取出的 FingerCode 特征向量 $\boldsymbol{V}$,最后是存储的密钥 $\boldsymbol{K}$。目前还没有方法能从 FingerCode 恢复出指纹图像,因此指纹图像可以认为是完全安全的。而对于 $\boldsymbol{V}$,由于采用了 BioHashing 技术,如果入侵者不知道 $\boldsymbol{R}$ 和 BioCode 码 $\boldsymbol{B}$ 中的任何一个,则无法获取任何 $\boldsymbol{V}$ 的信息,即使 $\boldsymbol{R}$ 泄露,但由于量化步骤造成部分信息丢失,是不可逆的。因此,$\boldsymbol{V}$ 也可以认为是安全的。

对于密钥 $\boldsymbol{K}$ 的安全,采用比较 $\boldsymbol{K}$ 和 $\hat{\boldsymbol{K}}$ 二者哈希值的方法来验证,而不是直接比较二者,其目的是可以不存储 $\boldsymbol{K}$,杜绝密钥 $\boldsymbol{K}$ 泄露的可能;此外没有 $\boldsymbol{B}$,无法由 $\boldsymbol{Ks}$ 纠错解码恢复出 $\boldsymbol{K}$。唯一可非法获得 $\boldsymbol{K}$ 的方法,是在 $\boldsymbol{R}$ 已泄露的情况下,利用较高的错误接收率 FAR,采用暴力破解的方法,如采用 BCH(511,157,51)时,其 FAR = 3.79%,相当于平均尝试约 26 次,就能破解 $\boldsymbol{K}$。在这种情况下,会额外造成信息 $\boldsymbol{K}$ 和 $\boldsymbol{B}$ 的泄露。但由上面分析,入侵者还是无法获得信息 $\boldsymbol{V}$,更不可能获得指纹图像信息,不会造成指纹原始信息的泄露。并且通过更改 $\boldsymbol{R}$ 和 $\boldsymbol{K}$,就能重新更新模板,使入侵先前获得的信息失效。

5 结 论

为保证指纹原始特征信息的安全,本文结合 BioHashing 和 Fuzzy Commitment 各自的优点,设计了一种双重可删除指纹模板方法——DCFT 方法。同时 DCFT 方法能为不同应用绑定不同密钥,可应用在密钥管理方面。用一个指纹就能管理多个密码,避免记忆多个密码引起遗忘、混淆或盗取等安全威胁。对 DCFT 方法的仿真结果和安全性的简要分析表明,该方法能在有效释放密钥、识别指纹的同时,保证模板不泄露原始特征信息。即使数据库信息被盗取,也不会泄露原始特征信息,并通过更改参数重新生成新的模板,使原来泄露数据失效。本方法仍存在改进地方,由于 FingerCode 无法克服旋转、形变等问题,同时索引点检测存在误差,这些都会引起 FingerCode 的偏差。FingerCode 的偏差又导致转化成 BioCode 后,在 R 泄露情况下,类内距离和类间距离分离度不够,造成此时存在较高的 FRR 和 FAR。因此,研究在不泄露或泄漏很少指纹原始特征信息的条件下,如何精确对齐指纹图像,对提高识别性能具有重要意义。这也是后续研究工作的重点。

参考文献

[1] Ross A, Shah J. Jain A K. From template to image: reconstructing fingerprints from minutiae points, *IEEE Transactions on PAMI*, 2007, 29(4):544-560

[2] Maltoni D, Maio D, Jain A K, et al. Handbook of Fingerprint Recognition. New York: Springer-Verlag, 2003. 398-401
[3] Ratha N K, Chikkerur S, Connell J H, et al. Generating cancelable fingerprint templates. *IEEE Transactions on PAMI*, 2007, 29 (4): 561-572
[4] Teoh A B J, Ngo D C L, Goh A. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*, 2004, 37(11): 2245-2255
[5] Teoh A B J, Goh A, Ngo D C L. Random multispace quantization as an analytic mechanism for Biohashing of biometric and random identity inputs. *IEEE Transactions on PAMI*, 2006, 28(12):1892-1901
[6] Ratha N, Connell J, Bolle R. Enhancing security and privacy in biometrics-based authentication system. *IBM Systems Journal*, 2001,40 (3):614-634
[7] Uludag U, Pankanti S, Prabhakar S, et al. Biometric cryptosystems: issues and challenges. *Proceedings of IEEE*, 2004, 92(6):948-960
[8] Juels A, Wattenberg M. A fuzzy commitment scheme. In: Proceedings of the 6th ACM Conference on Computer and Communications Security, Singapore, 1999. 28-36
[9] Juels A, Sudan M. A fuzzy vault scheme. In: Proceedings of IEEE International Symposium on Information Theory, Switzerland, 2002. 408
[10] Feng Hao, Anderson R, Daugman J. Combining crypto with biometrics effectively. *IEEE Transactions on Computers*, 2006, 55(9): 1081-1088
[11] Shamir A. How to share a secret. *Communications of the ACM*, 1979, 22(11): 612-613
[12] Clancy T C, Kiyavash N, Lin D J. Secure smartcard-based fingerprint authentication, In: Proceedings of ACM SIGMM Workshop on Biometrics Methods and Applications, Berkley, USA, 2003. 45-52
[13] Yang S, Verbauwhede I. Automatic secure fingerprint verification system based on fuzzy vault scheme. In: Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, Philadelphia, USA, 2005. 5:609-612
[14] Chung Y, Moon D, Lee S, et al. Automatic alignment of fingerprint features for fuzzy fingerprint vault. In: Proceedings of the Conference on Information Security and Cryptology, Beijing, China, 2005.358-369
[15] Uludag U, Pankanti S, Jain A. Fuzzy Vault for Fingerprints. In: Proceedings of Audio and Video based Biometric Person Authentication, Rye Town, USA, 2005. 310-319
[16] Uludag U, Jain A K. Securing fingerprint template: fuzzy vault with helper data. In: Proceedings of the Conference on Computer Vision and Pattern Recognition Workshops (CVPRW '06), New Jersey, 2006.163
[17] Scheirer W J, Boult T E. Cracking fuzzy vaults and biometric encryption. In: Proceedings of the Biometrics Symposium, Baltimore, USA, 2007.1-6
[18] 王新梅,肖国镇. 纠错码——原理与方法(修订版). 西安:西安电子科技大学出版社, 2001,242-295
[19] Kong B, Cheung K, Zhang D, et al. An analysis of BioHashing and its variants. *Pattern Recognition*, 2006,39 (7): 1359-1368
[20] Hong L, Prabhakar S, Jain A K, et al. Filterbank-based fingerprint matching. *IEEE Transactions on Image Processing*, 2000,9(5):846-859
[21] Nilsson K, Bigun J. Localization of corresponding points in fingerprints by complex filtering. *Pattern Recognition Letters*, 2003, 24(13):2135-2144
[22] Maio D, Maltoni D, Cappelli R, et al. FVC2004: Third Fingerprint Verification Competition. In: Proceedings of International Conference on Biometric Authentication, Hong Kong, China, 2004.1-7
[23] Lumini A, Nanni L. An improved BioHashing for human authentication. *Pattern Recognition*, 2007, 40 (3):1057-1065

A dual cancellable fingerprint template method for securing the original fingerprint biometric information based on BioHashing and key bindings

Chen Kaizhi, Hu Aiqun, Song Yubo, Liu Huihui, Yuan Honglin
(College of Information Science and Engineering, Southeast University, Nanjing 210096)

Abstract

For the original biometric information security in a fingerprint recognition system, this paper proposes a dual cancellable fingerprint template (DCFT) method based on BioHashing and key bindings. In the phase of enrollment, it firstly irreversibly converts the feature value extracted from the original fingerprint image into a string of binary sequence with a fixed length by BioHashing, and then binds the key to the binary sequence by the Fuzzy Commitment scheme to generate a cancellable fingerprint template which can be stored in the database or a smartcard. In the phase of identification, the error correcting code is employed to regain the binding key from the cancellable template with the help of query fingerprint images. If using the DCFT method, even if all the data in the database is stolen, none of the original fingerprint biometric information will be leaked. Moreover, the stored template can be regenerated by changing the random matrix in BioHashing or the bingding key, so that the leakage of information is not available in verification. It avoids the permanent security threat caused by non-changeability of fingerprint. In the end, the simulation result is showed to illuminate the validity of the DCFT method.

Key words: fingerprint recognition, biometric template protection, key binding, BioHashing, error correcting code, fingerCode