第 38 卷 第 4 期
Vol.38 No.4

计 算 机 工 程
Computer Engineering

2012 年 2 月
February 2012

·开发研究与设计技术· 文章编号：1000—3428(2012)04—0236—03 文献标识码：A 中图分类号：TN918

基于 Chaff Matrix 的可撤销声纹模板设计

徐文华，易法令，熊 伟

(广东药学院医药信息工程学院，广州 510006)

摘 要：基于模糊穹的特征保护方法存在敌手冒充和空间自由度减少的问题。为此，提出一种基于伪矩阵(Chaff Matrix)的可撤销声纹模板设计方法。通过原始特征矢量的构成元素产生伪点，根据定位矩阵将伪点插入原始特征，且在欧氏距离准则下，插入前后特征矢量与模板之间距离的变化量保持一致相同，从而保证系统识别率，实现特征保护。实验结果验证了该方法的正确性。

关键词：声纹认证；可撤销模板；模糊穹 Fuzzy Vault；生物加密；超球体；梅尔倒谱系数

Design of Cancelable Voiceprint Template Based on Chaff Matrix

XU Wen-hua, YI Fa-ling, XIONG Wei

(College of Medical Information Engineering, Guangdong Pharmaceutical University, Guangzhou 510006, China)

【Abstract】 Aiming at the problems of fake and decrease of interspaces in Fuzzy Vault(FV) method, this paper proposes a voiceprint template protection method based on Chaff Matrix(CM). The CM is generated from raw feature and interweaved with raw template according to Orientation Matrix(OM), such that a cancelable template is designed to protect the voiceprint. Problems of fake and decrease of interspaces for Chaff Points(CPs) in Fuzzy Vault(FV) are solved by the mixture on a thinner layer. Mathematical analysis explained the proposal doesn't deteriorate the performance, for the invariability of the distance change between features. Experimental results show the validity of this method.

【Key words】 voiceprint authentication; cancelable template; Fuzzy Vault(FV); biometric encryption; hypersphere; Mel Frequency Cepstral Coefficient(MFCC)

DOI: 10.3969/j.issn.1000-3428.2012.04.077

1 概述

生物特征传输和存储安全问题的解决对生物认证系统的广泛应用具有重要意义[1]。目前的解决方法主要有结合成熟的密码方案[2]、特征转换[3]和生物加密[4-5]3 类。特征转换是指通过类似传统密码学的哈希转换，把原始特征转换到变换域，认证也在变换域进行。特征转换方法主要有 Multispace Random Projection(MRP)[3]方法等。生物加密方法主要有密钥生成[4]和密钥捆绑[5]2 种。密钥捆绑的典型方法是基于模糊穹(Fuzzy Vault, FV)的特征保护。特征转换方法和生物加密方法的一个共性是原始特征泄漏后，可以重新设计新的模板，因此，通过这些模板保护技术设计的模板被称为可撤销模板。目前有不少文献采用 FV 的方法设计可撤销模板[5]，但文献[6-7]分别指出 FV 方法存在冒充和伪点(Chaff Points, CPs)插入过程中空间自由度减少的问题。

本文基于在 FV 中加入 CPs 的思想，提出通过原始特征矢量构成元素产生 CPs，并把 CPs 插入原始特征的方法实现特征保护。该方法在 CPs 的加入方式和认证原理上与 FV 有本质的区别，并且比 FV 具有更强的安全性，因为在 FV 中，CPs 为矢量，而在本文中，CPs 为构成矢量的元素，由这些元素组成伪矩阵(Chaff Matrix, CM)。考虑到声纹认证的独特优势，本文以声纹认证系统为架构，以此类系统中的典型特征梅尔倒谱系数(Mel Frequency Cepstral Coefficient, MFCC)为保护对象阐述所提出的方法。

2 基于 Chaff Matrix 的可撤销模板

设注册过程提取的特征为 X_0，2 个不同的认证特征分别为 $X_I, X_J \in \mathbf{R}^{m\times p}$，其中，$m$ 为特征长度；p 为 MFCC 的阶数；CM 伪矩阵为 $\boldsymbol{C}$，$\boldsymbol{C} \in \mathbf{R}^{m\times r}$；$r$ 为加入 CPs 的数目；定位矩阵(Orientation Matrix, OM)为 $\boldsymbol{O}$，$\boldsymbol{O} \in \mathbf{R}^{m\times r}$。加入 $\boldsymbol{C}$ 后的特征分别为：

$$X_{C0}, X_{CI}, X_{CJ} \in \mathbf{R}^{m\times(p+r)}$$

其中，X_{C0} 即是本文提出的可撤销模板(对于 VQ 算法，X_{C0} 由码本插入 $\boldsymbol{C}$ 矩阵构成)，加入 $\boldsymbol{C}$ 矩阵后的特征统称为 X_C。

分析特征保护方法是否有效的出发点是认证的判决尺度，如果保护方法不会改变判决尺度或改变具有一致性，则识别结果不会改变和恶化。常用的判决尺度是最小距离和最小量化失真，这 2 个判决尺度都采用欧氏距离准则(欧氏距离的平方)。在此准则下，如果 $\|X_{CJ}-X_{C0}\|^2=\|X_{CI}-X_{C0}\|^2$，即认证特征与模板的距离增量一致，则对于采用欧氏距离准则的认证识别系统，本文方法不会改变系统最终的识别效果，这也是该方法的一个假设(假设实为显然成立，具体分析见实验部分)。下面讨论假设成立的条件，推导如下：

$$\|X_{CI}-X_{C0}\|^2=\sum_{i=1}^{m}\sum_{j=1}^{p}(X_{CI}^{(ij)}-X_{C0}^{(ij)})^2+\sum_{i=1}^{m}\sum_{j=1}^{r}(C_I^{(ij)}-C_0^{(ij)})^2=\sum_{i=1}^{m}\sum_{j=1}^{p}(X_{CI}^{(ij)}-X_{C0}^{(ij)})^2+\delta_I=\|X_I-X_0\|^2+\delta_I \quad (1)$$

$$\|X_{CJ}-X_{C0}\|^2=\sum_{i=1}^{m}\sum_{j=1}^{p}(X_{CJ}^{(ij)}-X_{C0}^{(ij)})^2+\sum_{i=1}^{m}\sum_{j=1}^{r}(C_J^{(ij)}-C_0^{(ij)})^2=\sum_{i=1}^{m}\sum_{j=1}^{p}(X_{CJ}^{(ij)}-X_{C0}^{(ij)})^2+\delta_J=\|X_J-X_0\|^2+\delta_J \quad (2)$$

式(1)和式(2)说明假设成立的条件为 $\delta_I=\delta_J$，即：如果 $\delta_I=\delta_J$，则不同认证特征与模板的距离增量一致，在此假设

基金项目：广东药学院人才引进基金资助项目(2007YGY01)

作者简介：徐文华(1978－)，男，讲师、博士，主研方向：生物认证系统，语音信号处理；易法令，教授、博士；熊 伟，讲师、硕士

收稿日期：2011-09-20 **E-mail：**gzwhxu@163.com

成立的条件下也就不会影响识别率。

对于该方法，存在 3 个问题：(1)如何产生 CPs 及满足 $\delta_I = \delta_J$；(2)如何确定矩阵 $\boldsymbol{O}$ 的元素，即在哪些位置加入 CPs；(3)该方法的安全性分析。

(1)为确定 δ_I 和 δ_J 的值，需要首先产生注册和第一个认证特征的 CPs。对于注册和第一个认证过程中产生的 CPs，如果所有的 CPs 在数值上与原始特征存在明显差异，则敌手可以通过这种差异轻易地获得原始特征。为防止敌手在获得单个特征的情况下轻易找出原始特征，CPs 与原始特征 MFCC 系数之间应尽量具有相似性。在求解过程中，有部分解可能满足不了相似性，并且 MFCC 部分系数自身存在的突变性[8]，这种突变性允许部分解可以不满足相似性要求，这也是“尽量具有相似性”的含义。本文通过原始特征产生注册和第一次认证过程中的矩阵 $\boldsymbol{C}$，具体公式如下：

$$c_{il} = \left[\sum_{j=o_{i,l}}^{o_{i,l+1}} x_{ij} + (-1)^l (o_{i,l+1} - o_{i,l})\varepsilon_l\right] \Big/ o_{i,l+1} - o_{i,l}$$
$$i = 1,2,\cdots,m;\ l = 1,2,\cdots,r \tag{3}$$

式(3)中分子为原始特征中的若干相邻元素累加后再加上一个调整参数 ε，分母为相加元素的个数，这样的目的是保证 CPs 与原始特征元素的相似性。其中，ε 是防止 CPs 与原始特征元素相等。设：

$$\mu_{ij} = \sum_{j=o_{i,l}}^{o_{i,l+1}} x_{ij} \Big/ (o_{i,l+1} - o_{i,l})$$

则 ε 的取值范围为：

$$\varepsilon \in (0, \min(\max(x_{ij}) - \mu_{ij}, \mu_{ij} - \min(x_{ij}))], j = o_{i,l}, o_{i,l}+1, \cdots, o_{i,l+1}$$

由式(3)可以产生 $\boldsymbol{C}_0$ 和 $\boldsymbol{C}_1$，即注册和第一次认证过程产生的 $\boldsymbol{C}$ 矩阵，然后再由 $\sum_{i=1}^{m}\sum_{j=1}^{r}(C_1^{(ij)} - C_0^{(ij)})^2 = \delta_1 = \delta$ 确定 δ。

对于第 2 个及其后认证特征中的 CPs 除了满足相似性要求外，还必须满足 $\delta_1 = \delta_2 = \delta$，如式(1)、式(2)所述，这个约束条件是系统有效性的要求。同时满足对应位置 CPs 不等，这是为了保证敌手在获得多个特征时也不能轻易发现原始特征。以第 I 个特征为例，此问题等价于式(4)。

$$\begin{cases} \sum_{i=1}^{m}\sum_{j=1}^{r}(C_I^{(ij)} - C_0^{(ij)})^2 = \delta & \delta \neq 0 \\ C_I^{il} \in [\min(X_{CI}^{(ij)}), \max(X_{CI}^{(ij)})] & j = o_{i,l}, o_{i,l}+1, \cdots, o_{i,l+1};\ l \neq r \\ C_I^{ij} \neq C_J^{(ij)} \neq C_0^{(ij)} & i = 1,2,\cdots,m;\ j = 1,2,\cdots,r \end{cases} \tag{4}$$

式(4)是带多个约束条件的 $r \times m$ 元二次方程，对于式(4)是否存在数学解析求解方法，目前还未知。本文采用几何方法求解：式(4)从几何角度讲是一个超球面，从球面上任意取一点都满足该方程式，因此，对该式的求解问题归约为在球面上任取一点，并求该点坐标。由于式(4)对解的范围存在约束，因此在求解上等价于在某一特定区域取点再求坐标值，问题的关键也就是如何确定取点区域。从式(4)方程看，未知数个数为 $r \times m$，对应到超空间也就是 $r \times m$ 维，球面上每一维所在区域假设为 $\Omega \in [-\sqrt{\delta}, \sqrt{\delta}]$，每一维解约束空间为：

$$\omega_1^{il} \in [\min(X_{CI}^{(ij)}), \max(X_{CI}^{(ij)})]$$
$$i = 1,2,\cdots m;\ j = o_{i,l}, o_{i,l}+1, \cdots, o_{i,l+1} \tag{5}$$

根据 Ω 与 ω_1^{il} 包含与否的关系可以确定取点的区域，Ω 与 ω_1^{il} 存在 3 种情况，根据这 3 种情况可确定 C_1^{il} 的取值区域：1) $\Omega \cap \omega_I^{il} = \omega_I^{il}$；2) $\Omega \cap \omega_I^{il} = \omega\hat{}_I^{il}, \omega\hat{}_I^{il} \subset \omega_I^{il}$；3) $\Omega \cap \omega_1^{il} = \varnothing$。

在第 1)种情况中，对于 $C_I^{(1,1)} \sim C_I^{(m,r-1)}$，可以在相似性要求下根据式(3)随机选择；对于 $C_I^{(m,r)}$，则在前 $(m \times r) - 1$ 个元素和 δ 确定的条件下计算。这样求出的解也必定在 ω_1^{ir} 的范围内，所有的解都满足相似性要求。

第 2)种情况求解过程与第 1)种情况类似，只是取值区域在 $\omega\hat{}_1^{il}$ 空间。

第 3)种情况的含义是所求解不能同时满足既在球面上，又满足相似性的要求。对于这种情况，本文采用取 Ω 空间一个领域的方法，此处领域定义为 Ω 空间中与 ω_I^{il} 最接近的一段区域，本文中假设这段区域为空间 ξ，根据 MFCC 部分系数自身的突变性，c_{il} 可在 ξ 空间取值。

(2)式(1)和式(2)说明特征与模板的距离只与特征元素和 $\boldsymbol{C}$ 矩阵元素的大小有关，而与插入的位置无关。因此，矩阵 $\boldsymbol{O}$ 可任意给定。必须说明的是方案的有效性与 $\boldsymbol{O}$ 无关，但其安全性却与 $\boldsymbol{O}$ 矩阵的规模大小相关，$\boldsymbol{O}$ 矩阵规模越大，插入的 CPs 则越多，安全性也越高。

(3)安全性分析。安全性以敌手获得原始特征的概率表示，可由下式表示：

$$P = \left[\frac{C_p^p}{C_{p+r}^p}\right]^m = \left[\frac{1}{C_{p+r}^p}\right]^m,\ r \neq 0 \tag{6}$$

其中，C_{p+r}^p 是在一个加入 CPs 的特征矢量中原始特征的总组合数；C_p^p 是在总组合数中真实点的组合方式，对于本文所提方法，因为采用模板匹配的方式，所以只有一种方式是符合原始特征的组合方式，分子为 1；获得整个特征序列需要获得每一帧真实点的概率相乘，共有 m 帧的特征长度，则最终获得原始特征的概率为获得一帧真实特征向量的 m 次方。

由于该方法与 FV 在特征点层面插入 CPs 的方法不同，CPs 是在特征矢量的构成元素中插入，插入位置与特征点所构成的空间无关，从而避免了点的插入受空间限制的影响。同时，如果要敌手替换真实点，则首先需要找出真实点的位置，式(6)已经说明其概率非常小；如果替换的是 CPs，则其不能满足增量一致的要求，因为式(4)已经说明 $\boldsymbol{C}$ 矩阵是满足增量一致要求的，替换之后必然不满足增量一致要求，所以敌手也无法通过替换的方法达到冒充的目的。从认证原理上分析，本文方法的认证采用的是模式匹配的方法，如果要达到冒充的目的，则需要替换所有的原始点以及 $\boldsymbol{C}$ 矩阵，而不是 FV 的方法只需要替换部分点通过多项式重构就可以达到冒充的目的。所以，该方法的安全性比 FV 的方法更高。

3 实验结果与分析

3.1 识别算法

本文方法适应于采用欧氏距离测度的识别算法，如 DTW 和 VQ 算法。对于统计模型，目前还没有理论分析说明该方法是否有效。本文选用 DTW 和 VQ 算法验证上述方法。

3.2 结果分析

实验 1 语料库为自制的语音库：录音设备为三星 YV-120 录音笔；在安静环境录音；文本格式为“籍贯+姓名”；录制人员共 40 人；年龄为 18 岁~30 岁；文件格式为 16 kHz 采样，16 bit 量化，单声道 wav 格式；样本的最小时长为 3.57 s，最大时长为 7.68 s。特征采用典型 MFCC 语音特征，阶数为 24 阶，每帧 256 点，重叠 156 点，即帧移 100 点。实验中 $\boldsymbol{O}$ 矩阵采用预先给定初始值的方式。实验结果为加入前后的识别率都为 92.5%，与上文分析是一致。

对于式(4)，理论分析 Ω 与 ω_1^{il} 存在如第 2 节所述的 3 种关系，实验结果表明，式(4)中所有解的范围都属于 $\Omega \cap \omega_1^{il} = \omega_1^{il}$，这说明式(4)求解方法的可行性，并且所有解都满足相似性要求。本文用 ω_1 表示第 I 个特征的数值范围，则显然有 $\omega_1 \supset \omega_1^{il}$，所以只需要分析 Ω 与 ω_1 的关系，如果 Ω 与 ω_1 存在包含关系，则 Ω 与 ω_1^{il} 也存在包含关系。在这种包含关系下的解都满足相似性要求。实验结果表明 $dait$=73.42，并且 $Minmfcc<dait<Maxmfcc$，这也就说明 Ω 与 ω_1^{il} 都存在包含关系，同时也说明上述式(4)的求解过程是可行的。

实验 2 实验 2 的实验条件同实验 1。采用 LBG(Linde Buzo Gray)算法训练 VQ 码本，码本大小为 64。实验结果与上文分析一致：加入 CPs 前后的识别率都为 95%。之所以不改变是加入 CPs 前后的码本产生的条件和过程是一样的，而加入 CPs 后认证特征与码本的距离增量又是一致的，这样加入 CPs 前后的最小量化误差也就一样。因此，识别率没有改变，自然没有恶化识别率，符合可撤销模板的要求。而 VQ 算法的识别率高于 DTW 算法的现象，则由算法本身的识别效果决定。

对于 VQ 的识别算法，式(4)的求解过程与实验 1 类似，但需要把 CPs 插入在码本中。实验结果表明 $dait$=82.98，并且 $Minmfcc<dait<Maxmfcc$，Ω 与 ω_1 仍然存在包含关系，这也进一步说明式(4)计算方法的可行性，并且所求解也同样满足相似性要求。

4 结束语

本文提出根据 OM 在原始特征点的元素中加入 CPs，达到了安全传输、存储的目的，满足可撤销模板的安全性要求。实验表明本文设计的可撤销模板是有效的。该方法的安全性随矩阵 $\boldsymbol{O}$ 规模的增大呈阶乘增强。该方法是否适应于统计模型的模板设计有待于进一步研究。

参考文献

[1] Jain A K, Nandakumar K, Nagar A. Biometric Template Security[J]. EURASIP Jounmal on Advances in Signal Processing: Special Issucial on Biometrics, 2008, (1): 1-20.

[2] Xu Wenhua, He Qianhua, Li Yanxiong, et al. Cancelable Voiceprint Templates Based on Knowledge Signatures[C]//Proc. of ISECS'08. Washington D. C., USA: IEEE Press, 2008: 412-415.

[3] 徐文华, 贺前华, 李 韬. 一种基于 MRP 的可撤销模板设计及其分析[J]. 电子学报, 2009, 37(12): 2792-2795.

[4] 冯 全, 苏 菲, 蔡安妮. 生物加密综述[J]. 计算机工程, 2008, 34(10): 141-143.

[5] Uludag U, Pankanti S, Jain A K. Fingerprint Template Protection Using Fuzzy Vault[C]//Proc. of ICCAS'07. Portsmouth, UK: Springer, 2007: 1141-1151.

[6] Nandakumar K, Nagar A, Jain A. Hardening Fingerprint Fuzzy Vault Using Password[C]//Proc. of ICB'07. Seoul, Korea: Springer, 2007: 927-937.

[7] Chang E C, Shen R, Teo F W. Finding the Original Points Set Hidden Among Chaff[C]//Proc. of ASIACCS'06. Taipei, China: [s. n.], 2006: 182-188.

[8] Shaughnessy D O. Invited Paper: Automatic Speech Recognition: History, Methods and Challenges[J]. Pattern Recognition, 2008, 41(10): 2965-2979.

编辑 金胡考

(上接第 235 页)

基于云服务的会议服务平台，技术上通过虚拟化技术，实现对计算、存储、网络、设备等资源的管理和调度，为客户降低成本，节约资源。功能上以简洁的方式快速创建功能全面的会议管理网站，提供一键建站，灵活定制，全方位的服务。

6 结束语

目前，云计算及云服务的发展尚未成熟，相关工具和技术还在不断完善中。云服务只能应用于某些任务而不是全部的业务环节。对于 e-science 而言，需要重点关注的是，清晰了解、充分掌握各种云服务的技术实质与应用价值并将之有所选择地引入，进一步提升技术对科研的服务能力。基于云服务的会议服务平台是云计算在 e-science 的创新应用，解决了传统软件资源利用率低、安装维护成本高的弊端，实现了按需服务，是面向科研的协同工作平台中不可缺少的组成部分，该平台将对中科院国际学术会议的组织管理产生积极深远的影响。

参考文献

[1] Jankowski N W. Exploring E-science: An Introduction[J]. Journal of Computer-mediated Communication, 2007, 12(2): 549-562.

[2] Hey T. E-science and Cyber Infrastructure: A Middleware Perspective[C]//Proceedings of the 15th International Conference on World Wide Web. New York, USA: ACM Press, 2006.

[3] Gurav U, Shaikh R. Virtualization——A Key Feature of Cloud Computing[C]//Proceedings of International Conference and Workshop on Emerging Trends in Technology. Mumbai, India: [s. n.], 2010.

[4] Torbacki W. SaaS——Direction of Technology Development in ERP/MRP Systems[J]. Archives of Materials Science and Engineering, 2008, 32(1): 57-60.

[5] Hayes B. Cloud Computing[J]. Communications of the ACM, 2008, 51(7): 9-11.

[6] Watson P, Lord P, Gibson F, et al. Cloud Computing for E-science with CARMEN[C]//Proceedings of the 2nd Iberian Grid Infrastructure Conference. [S. l.]: IEEE Press, 2008.

[7] 南 凯, 董科军, 谢建军, 等. 面向云服务的科研协同平台研究[J]. 华中科技大学学报: 自然科学版, 2010, 38(增刊 1): 14-19.

[8] 南 凯, 李华飚, 董科军, 等. 支持 E-science 的协同工作环境[J]. 科研信息化技术与应用, 2008, 1(1): 35-40.

[9] Duckling[EB/OL]. [2011-02-15]. http://duckling.escience.cn.

[10] Spring[EB/OL]. [2011-02-15]. http://www.springsource.org.

[11] 中科院国际会议服务平台[EB/OL]. [2011-02-15]. http://csp.escience.cn.

编辑 陆燕菲