模糊逻辑在人脸特征保护算法中的应用

周玲丽[1] 赖剑煌[2] 吴 娴[3]
(中山大学教学实验中心 广州 510275)[1] (中山大学信息科学与技术学院 广州 510275)[2]
(南方报业传媒集团 广州 510601)[3]

摘 要 随着人脸识别在门禁、视频监控等公共安全领域中的应用日益广泛,人脸特征数据的安全性和隐私性问题成为备受关注的焦点。近年来出现了许多关于生物特征及人脸特征的安全保护算法,这些算法大都是将生物特征数据转变为二值的串,再进行保护。针对已有的保护算法中将实值的人脸特征转换为二值的串,从而导致信息丢失的不足,应用模糊逻辑对人脸模板数据的类内差异进行建模,从而提高人脸识别系统的性能。给出了算法在CMU PIE的光照子集、CMU PIE带光照和姿势的子集和ORL人脸数据库中的实验结果。实验表明,该算法能够进一步提高已有安全保护算法的识别率。

关键词 生物特征,安全性,类内差异,模糊逻辑
中图法分类号 TP309.2 **文献标识码** A

Applications of Fuzzy Logic in the Protection Algorithm of Face Feature

ZHOU Ling-li[1] LAI Jiang-huang[2] WU Xian[3]
(Education & Experiment Center, Sun Yat-Sen University, Guangzhou 510275, China)[1]
(School of Information Science and Technology, Sun Yat-Sen University, Guangzhou 510275, China)[2]
(Nanfang Media Group, Guangzhou 510601, China)[3]

Abstract With the growing use of face recognition in security and video control domain, there is growing concern about the security and privacy of the biometrics data. Recently, technologies for biometric security and privacy have been proposed, which typically transform the biometric data to a binary string. These transformations can lead to some information loss and downgrade the performance of a system. This paper applied fuzzy logic to confirm the reliability of each bit in a binary string and to model the intra-class variations. The experimental results show this method reduces the overlap of imposter distribution and genuine distribution and improves the performance of biometric security technology.

Keywords Biometrics, Safety, Intra-class, Fuzzy logic

1 引言

人脸识别是利用计算机分析人脸图像,进而从中提取有效的识别信息来"辨认"身份的一门技术。与其他生物特征相比,人脸特征具有较好的自然性、不被察觉性、非接触性和唯一性的特点,使得人脸识别技术应用背景广泛,可用于罪犯身份识别、驾驶执照及护照等与实际持证人的核对、银行及海关的监控系统及自动门卫系统等[1-4]。

随着人脸识别等生物特征识别技术的广泛应用,生物特征数据的安全性日益显得重要和紧迫。尽管生物特征识别技术相比传统的身份识别技术具有本质的优势,但确保生物特征数据(包括人脸特征)的安全性和隐私性是一个严峻问题。

由于生物特征(人脸、指纹、虹膜等)的唯一性,导致个人生物特征的丢失就意味着个人身份的丢失。例如,生物特征被破坏或窃取,不能像密码和IC卡那样撤销和重新更新[5]。且每个人的生物特征都是有限的,例如一个人只有一个人脸和10个手指指纹。另外,研究表明运用"Hill Climbing Attacks"[6]技术,能够获得生物特征模板数据库中的特征数据。因此,生物特征数据的安全性尤其重要。

已有的针对人脸特征模板数据的安全保护算法主要有两大类[3,7]:一类是可重建生物特征算法[8,9],这类算法对人脸特征数据进行人为的、不可逆的变换,使得人脸特征模板数据中保存的不再是原始的人脸特征数据,而是人脸特征的变换形式。但是能保持变换前后特征的可辨识性的不可逆函数较难设计,并且不可逆变换对差异特别敏感,人脸特征之间细微的差异会导致变换后的数据有较大的差距。而特征数据受到一些条件的影响,不可避免地具有一定的噪声。另一方面,由于光照、姿势、表情等变化的影响,同一个人的不同时期采集的人脸图像也有一定的差异。这些因素均对特征可辨识性产生很大的影响。

到稿日期:2010-10-12 返修日期:2011-04-13 本文受国家自然科学基金(U0835005,6033030),973项目(2006CB303104),广东省科技计划项目(2010B031000004)资助。

周玲丽(1973-),女,博士,工程师,主要研究方向为图像处理、模式识别等,E-mail:mcszll@mail.sysu.edu.cn;**赖剑煌**(1964-),男,博士,教授,主要研究方向为图像处理、模式识别等;**吴 娴**(1985-),女,博士后,主要研究方向为图像处理、模式识别等。

另一类安全保护算法是生物特征加密系统[10,11]，这类算法从注册的生物特征数据中提取辅助数据，而这些辅助数据不会泄露原始生物特征的相关信息。利用辅助数据和待识别特征提取密钥，通过验证密钥的合法性决定最终的识别结果。此类算法主要运用纠错码来处理类内差异问题。纠错码一般是对二值的串进行纠错编码，而人脸特征数据是实值的，因此需要将实值的特征转化为二值的串。

已有的关于生物特征数据安全性方面的研究大都是关于指纹和虹膜的[12,13]。一方面，人脸特征的维数较大；另一方面，由于人脸特征容易受到光照、表情及姿势变化等外在条件的影响，同一人的图像表现差别很大，人脸特征之间具有较大的类内差异，使得较少涉及人脸特征方面的保护算法。

本文针对已有的人脸特征的保护算法中常常需要将实值的人脸特征转换为二值的串，从而导致信息丢失，应用模糊逻辑对人脸特征数据的类内差异进行建模，从而提高人脸识别系统的性能。给出了改进算法在 CMU PIE 的光照子集、CMU PIE 带光照和姿势的子集和 ORL 人脸数据库中的实验结果。

2 Biohashing 算法

为了解决生物特征识别过程中错误拒绝率(FRR)较高的问题，Goh[14,15] 和 Teoh 等[16,17] 提出了一种基于两因素的生物特征识别算法 Biohashing，使得系统的等错率 EER(Equal Error Rate)能够为零。这种算法是将提取的生物特征向量与 Token(或智能卡)中存储的随机序列进行迭代内积运算，从而得到一些基于用户的编码(BioHashCode)。从某种意义上来说，Biohashing 算法引入了外部因素，近似于不可逆变换和加密算法，从而达到对生物特征进行保护的目的。

Biohashing 算法如图 1 所示，主要过程由两部分组成：

① 随机投影(Random mapping)。将特征向量投影到每个用户各自不同的子空间(子空间是通过用户 Token 中存储的密钥 K 来生成)。

② 阈值化(Thresholding)。通过阈值处理将投影结果二值化，从而将实值的特征向量转化成一个二值的串(BioHashCode)，特征模板数据库中存储的是二值化特征数据，不再是原始的特征数据。BioHashCode 之间的匹配则是通过汉明距离(Hamming distance)来进行，Johnson-Lindenstrauss 引理[18]表明随机投影能保证欧氏距离的不变性，从而满足了可辨识的要求。

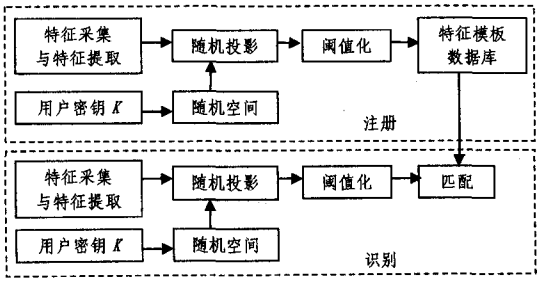

图 1 Biohashing 算法[15]

B. Kong 等[19] 提出的 Biohashing 算法中零等错率的获得是建立在一个不实际的假设之上的，就是假设密钥 K 没有被窃。因此，Alessandra Lumini 等[20] 提出了改进的 Biohashing 算法，通过将特征向量进行循环置换、投影空间增大等方法将 BioHashCode 的长度增加，从而提高算法的性能。

Biohahsing 算法提出的框架引入了外部因素(密钥 K)，因此达到了对生物特征进行保护的目的。目前，越来越多的研究基于这种算法框架展开。

3 模糊 Biohashing 算法

模糊逻辑(Fuzzy Logic)[21] 是 1965 年由加州大学伯克利分校的 Lofty Zadeh 提出的，其根本是在于区别布尔逻辑与清晰逻辑，用来定义那些含混不清、无法量化或精确化的问题。在以模糊逻辑为基础的模糊集合理论中，某特定事物具有特定的隶属度，可以在“是”和“非”之间的范围内取任何值。模糊逻辑是合理的量化数学理论，是以数学基础为根本去处理这些非统计不确定的不精确信息。

模糊逻辑提供了一种较为简单的从不精确、带噪声或不完整的数据中得到明确结论的方法。在 Biohashing 算法中，将实值的特征向量转化为二值的串，串中每个 bit 对最终识别结果的影响如何，很难得到一个明确的答案。因此，考虑运用模糊逻辑，得出每个 bit 位的可靠性，从而对类内差异进行建模，最大限度地减少类内差异，进而提高系统的识别性能。

首先，运用 Biohashing 算法或其他相关方法，将特征数据 $x\in R^n$(n 是特征向量的维数)转换为二值的串 $b\in\{0,1\}^m$(m 为串的长度)。在串 b 中，每个 bit 的取值为 0 或 1。二值化处理可能导致信息丢失，进而降低系统最终的识别效果。在二值化的过程中，取值为 0 的 bit 可能错误地取值为 1，而取值为 1 的 bit 可能错误地取值为 0。这些错误对系统最终的识别结果有一定的影响。

同时，二值串中每个 bit 位的重要性是各不相同的，运用模糊逻辑，分析训练样本转换后的二值串，估计每个 bit 位的可靠性，这个可靠性决定每个 bit 位在最终识别中的权重。权重的引入降低了类内差异，进而提高了识别性能。本文算法如图 2 所示，主要过程如下。

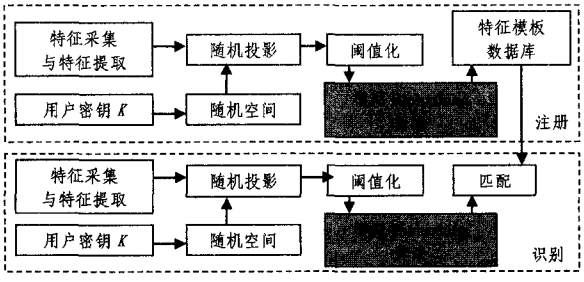

图 2 模糊 Biohashing 算法

(1)$\{x_j^i\in R^n\mid j=1,\cdots,t\}$是第 i 类的 t 个训练特征向量，其中 x_j^i 是实值的特征向量。

(2)将$\{x_j^i\in R^n\mid j=1,\cdots,t\}$转换为二值的串$\{b_j^i\in\{0,1\}^m\mid j=1,\cdots,t\}$，$b_{jk}^i$ 为向量 b_j^i 的第 k 个 bit，取值 0 或 1，则 $b_j^i=\{b_{j1}^i,\cdots,b_{jk}^i,\cdots,b_{jm}^i\}$。这种转换可以通过 Biohashing 算法或其他方法得到。本文应用 Biohashing 算法，将实值的特征向量转换为二值的串。

(3)对$\{b_j^i\in\{0,1\}^m\mid j=1,\cdots,t\}$取平均：

$$\{\overline{b_k^i}=\frac{1}{t}\sum_{j=1}^{t}b_{jk}^i\mid k=1,\cdots m\} \tag{1}$$

(4)计算第 i 类每个 bit 位的权重：

$$w_k=f(\overline{b_k^i}) \tag{2}$$

式中，w_k 为相应 bit 位的可靠性，f 是隶属函数。权重系数 w_k 的取值由隶属函数 f 决定。隶属函数 f 将每个 bit 位的可靠性投影到 0 到 1 之间。本文中隶属函数具有对称性，隶属函数必须满足以下两个条件：

（Ⅰ）如果一个 bit 位上取值为 0 和 1 的百分比相同，则无法判别这个 bit 位的取值是否正确。因此，这个 bit 位的可靠性是最低的，隶属函数取值应该为 0。

（Ⅱ）如果一个 bit 位取值为 0 的百分比是 100%，取值为 1 的百分比是 0，则这个 bit 位的取值是正确的，反之亦然。此时，可靠性是最高的，相应的隶属函数取值为 1。

隶属函数的值即为上述(3)中的权重系数 w_k。根据隶属函数必须满足的条件，本文选择抛物线型的隶属函数，其定义如下：

$$f(x)=\begin{cases}-4x^2+1\\-4(x-1)^2+1\end{cases} \tag{3}$$

图 3 为隶属函数的图形。

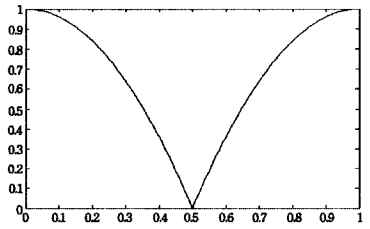

图 3　隶属函数

(5)在匹配阶段，采用汉明距离进行匹配的度量。距离越小，表明匹配对象的相似度越高。其中，汉明距离依下式计算：

$$H\_w(Q,R)=\sum_{k=1}^{m}w_k(Q_k\oplus R_k) \tag{4}$$

式中，⊕是异或运算，Q 是测试样本的二值特征向量，R 是训练样本的二值特征向量。$Q_k\oplus R_k$ 表示 Q_k 与 R_k 之间不同 bit 位的个数。由于每个 bit 位的可靠性不同，因此加入了权重系数 w_k。

4　实验结果与分析

4.1　人脸数据库

本文的实验中，使用的人脸库有 CMU PIE 光照子集、CMU PIE 姿势和光照子集以及 ORL 库。CMU PIE 人脸库的光照子集有 68 人，每个人有 21 幅人脸图像。人脸图像的光照变化较大，其中 10 幅用来训练。CMU PIE 光照和姿势的子集由 68 人、每人 105 幅人脸图像组成，同一人的人脸图像之间同时具有光照和姿势的变化，其中 40 幅用于训练；ORL 人脸库有 40 个人，每个人有 10 幅人脸图像，其中 5 幅用来训练，5 幅用来测试。

我们通过同一个人的训练样本计算类内的汉明距离，不同人的训练样本计算出类间的汉明距离。训练样本之间的类内汉明距离形成 genuine 分布，类间的汉明距离形成 imposter 分布[22]。

4.2　实验分析

本文采用错误接受率(FAR，False Acceptance Rate)、错误拒绝率(FRR，False Rejection Rate)和 ROC(Receiver Operating Characteristic curve)曲线来衡量算法的性能。

图 4 和图 6 分别是 CMU PIE 姿势和光照子集与 ORL 人脸库采用汉明距离得到的误差分布，图 5 和图 7 分别是运用本文算法后得到的加权 genuine-imposter 分布。

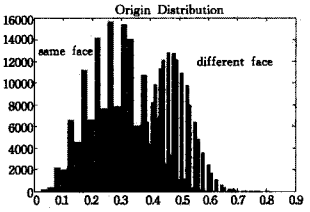

图 4　CMU PIE 姿势和光照子集的 Genuine-imposter 分布

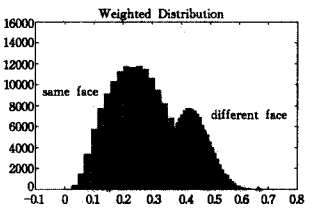

图 5　CMU PIE 姿势和光照子集的加权 Genuine-imposter 分布

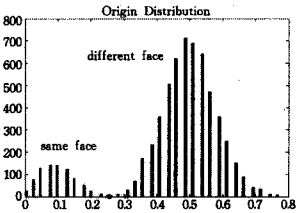

图 6　ORL 人脸库的 Genuine-imposter 分布

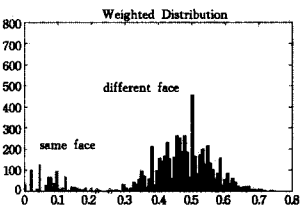

图 7　ORL 人脸库的加权 Genuine-imposter 分布

genuine 分布由训练样本的类内汉明距离形成，imposter 分布由训练样本的类间汉明距离形成。genuine 分布与 imposter 分布如果完全分离，则可以正确地匹配；如果 genuine 分布与 imposter 分布有重叠，则会导致错误的匹配，进而降低系识别性能。

通过图 4 与图 5，图 6 与图 7 的对比，可以看到加权后的 CMU PIE 姿势和光照子集与 ORL 人脸库的 genuine-imposter 分布的重叠比加权前减少了，分布的峰值更是大幅度降低，表明应用模糊逻辑来估计每个 bit 位的可靠性，能够纠正二值特征中由于光照和姿势变化所导致的某些误差，从而提高匹配的正确率，使得系统的识别性能得到提高。

图 8 和图 9 分别是 CMU PIE 姿势和光照子集和 ORL 人脸库的 ROC 曲线。从图中可以看到，我们提出的算法与原始的保护算法相比，识别性能得到了提升。而在这两个人脸库中，人脸图像均有姿势变化，二值串中每个 bit 的权重都能够估计出每个 bit 的可靠性，因而能够降低由于姿势变化所带来的误差。

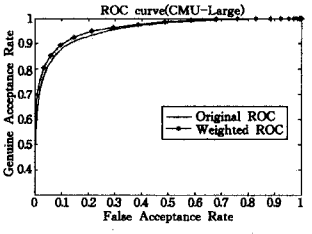

图 8　CMU PIE 姿势和光照子集的 ROC 曲线

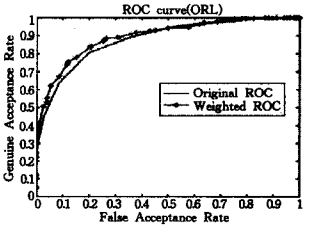

图 9　ORL 人脸库的 ROC 曲线

本文提出的算法能够提高安全保护算法的识别性能。如果原有安全保护算法的性能已经很好，则采用本文的算法并不会降低系统的识别性能。图 10 为 CMU PIE 光照子集的 ROC 曲线，可以看出，保护算法的识别能力已经很好，继续采用我们的改进算法后，识别性能与之前相比没有多大差异。因此，表明在保护算法识别性能已经很高的情况下，本文提出的改进算法不会降低系统的识别性能。

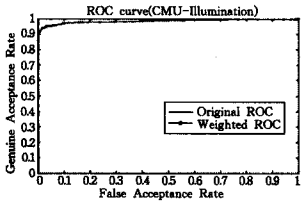

图 10 CMU PIE 光照子集的 ROC 曲线

结束语 随着人脸识别等生物特征识别技术的广泛应用，关于生物特征尤其是人脸特征的安全性和隐私性问题越来越受到关注。已有的关于人脸特征的保护算法大都是将实值的人脸特征数据转换为二值的串，再进行保护。为了弥补这种二值转换带来的信息丢失所导致的识别性能的下降，本文应用模糊逻辑分析了二值串中各个 bit 位的可靠性，从而提高了安全保护算法的识别率。

参 考 文 献

[1] Jain A K, Ross A, Pankanti S. Biometric: A Tool for Information Security [J]. IEEE Transactions on Information Forensics and Security, 2006, 1(2): 125-143

[2] Uludag U, Pankanti S, Prabhakar S, et al. Biometric Cryptosystems: Issues and Challenges [J]. Proceedings of the IEEE, 2004, 92(6): 948-960

[3] Jain A K, Nandakumar K, Nagar A. Biometric Template Security [C]// EURASIP. 2008

[4] Nagar A, Nandakumar K, Jain A K. Biometric Template Transformation: A Security Analysis [C]// Proc. of SPIE, Electronic Imaging, Media Forensics and Security XII. 2010

[5] Schneier B. Inside Risks: the Used and Abuses of Biometrics [J]. Communications of the ACM, 1999, 42(8): 136

[6] Adler A. Images Can Be Regenerated from Quantized Biometric Match Score Data [C]// Proceedings of Canadian conference of Electrical and Computer Engineering. 2004, 1: 469-472

[7] 周玲丽，赖剑煌. 生物特征数据安全保护技术的发展[J]. 计算机科学，2008，35(10)：33-38

[8] Ratha N K, Connell J H, Bolle R M. Enhancing Security and Privacy in Biometrics-based Authentication System [J]. IBM Systems Journal, 2001, 40(3): 614-634

[9] Feng Y C, Yuen P C, Jain A K. A Hybrid Approach for Generating Secure and Discriminating Face Template [J]. IEEE Transactions on Information Forensics and Security, 2010, 5(1): 103-117

[10] Uludag U, Pankanti S, Prabhakar S, et al. Biometric Cryptosystems: Issues and Challenges [J]. Proceedings of the IEEE, 2004, 92(6): 948-960

[11] Nandakumar K, Jain A K. Multibiometric Template Security Using Fuzzy Vault [C]// Biometrics: Theory, Applications and Systems(BTAS08). 2008

[12] Nagar A, Nandakumar K, Jain A K. A Hybrid Biometric Cryptosystem for Securing Fingerprint Minutiae Templates [J]. Pattern Recognition Letters, 2010, 31(8): 733-741

[13] Nagar A, Jain A K. On the Security of Non-invertible Fingerprint Template Transforms [C]// IEEE Workshop on Information Forensics and Security(WIFS). 2009

[14] Goh A, Ngo D L. Computation of Cryptographic Keys from Face Biometrics[M]. Communications and Multimedia Security, 2003: 1-13

[15] Jin A T B, Ling D N C, Goh A. Biohashing: Two Factor Authentication Featuring Fingerprint Data and Tokenized Random Number [J]. Pattern Recognition, 2004, 37(11): 2245-2255

[16] Teoh B J A, Ngo C L D. Cancellable Biometrics Featuring with Tokenised Random Number [J]. Pattern Recognition Letters, 2005, 26(10): 1454-1460

[17] Teoh B J A, Ngo C L D, Goh A. Personalised Cryptographic Key Generation Based on FaceHashing [J]. Computers and Security, 2004, 23(7): 606-614

[18] Johnson W B, Lindenstrauss J. Extensions of Lipschitz Mappings into a Hilbert Space [J]. Contemporary Mathematics, 1984, 26: 189-206

[19] Kong B, Cheung K, Zhang D, et al. An Analysis of Biohashing and Its Variants [J]. Pattern Recognition, 2006, 39: 1359-1368

[20] Lumini A, Nanni L. An Improved BioHashing for Human Authentication [J]. Pattern Recognition, 2007, 40(3): 1057-1065

[21] Hajek P. Fuzzy Logic as Logic, Mathematical Model for Handling Partial Knowledge in Artificial Intelligence [M]. New York: Plenum Press, 1995: 2130-2130

[22] Teoh B A J, Kar-Ann T, Jaihie K. Hashing Solution for the Biometric Template Protection Problem [J]. Journal of Biomedicine and Biotechnology, 2007

(上接第 259 页)

手指静脉图像的预处理工作要求很高，其准确程度直接影响手指特征提取和匹配的结果。所以，今后的研究中我们也将着重深化图像预处理的效果，提高细化图像质量和特征点提取的精度，进而进一步提高手指静脉识别的鲁棒性和可靠性。

参 考 文 献

[1] Shimizu K. Optical trans-body imaging: feasibility of non-invasion CT and functional imaging of living body [J]. Jpn. J. of Medicine Philosophica, 1992, 11: 620-629

[2] Miura N, Nagasaka A, Miyatake T. Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification[J]. Machine Vision and Applications, 2004, 15(4): 194 -203

[3] 王科俊，袁智. 基于小波矩融合 PCA 变换的手指静脉识别[J]. 模式识别与人工智能，2007(10)：692-697

[4] 李雪妍. 融合指纹和指静脉的多模态生物识别技术的研究[D]. 长春：吉林大学，2008

[5] 钱晓华. 手指静脉识别算法[D]. 长春：吉林大学，2009

[6] 刘加伶，余成波. 基于人体手指静脉特征提取算法的研究[J]. 计算机科学，2008，35(8)：218-230

[7] O'Gorman L, Lindeberg, Nickerson J V. An approach to fingerprint filter design[J]. PR, 1989, 22(1): 29-38

[8] Ain A K, Ross A, Prabhakar S. An introduction to biometric recognition[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2004, 14(1): 4-20

[9] Roberts C. Biometric technologies-palm and hand [EB/OL]. http://www. ccip. govt. nz/newsroom/information-notes/2006/biometrics-technologies-palmhand. pdf, March 22, 2008

[10] 苑玮琦，柯丽，白云. 生物特征识别技术[M]. 北京：科学出版社，2009：164-165

[11] 张玲，张钹，吴福朝. 对图形识别具有平移、旋转、伸缩不变性的神经网络[J]. 计算机学报，1998，2(21)：127-136