基于指纹特征数字水印算法的身份认证技术研究

张毅刚,焦玉华,牛夏牧,俞龙江
(哈尔滨工业大学信息对抗技术研究所,黑龙江哈尔滨 150001)

摘 要: 本文利用指纹特征信息生成数字水印信号,并隐藏在身份证件之中. 以身份证件作为指纹信息的载体,取代了传统指纹识别系统中的指纹特征参考信息数据库,提高整个自动指纹识别系统(AFIS)的安全性. 同时,嵌入指纹特征信息的身份证件与用户存在本质联系,防止证件被盗用,实现对证件的保护. 实验证明,使用含水印的证件在保证指纹识别系统正常工作的前提下,提高了验证的安全性,并且水印算法具有一定的鲁棒性.

关键词: 数字水印; 指纹识别; 身份认证
中图分类号: TN919 **文献标识码**: A **文章编号**: 0372-2112 (2003) 12A-2131-04

Authentication Based on Fingerprint Feature Watermarking Algorithm

ZHANG Yi-gang, JIAO Yu-hua, NIU Xia-mu, YU Long-jiang
(Dept. of Automatic Test and Control, Harbin Institute of Technology, Harbin, Heilongjiang 150001, China)

Abstract: This paper introduces an application of biometric watermarking algorithm based on the fingerprint minutiae data in Automated Fingerprint Identification system (AFIS). The reference copy of the fingerprint minutiae data is embedded in a host image that is the digital copy of the personal identification paper, such as ID card. The biometric data is hidden in every corresponding personal identification paper, instead of storing in the biometric database, which greatly promotes the security of AFIS. This algorithm is also robust to the JPEG compression and geometric distortion. Furthermore, the fingerprint data provides an additional cue in authenticating the personal identification paper. Experimental results show that authentication with more security is performed provided that the identification system works effectively using the watermarked identification card, and the algorithm is robust to some attacks.

Key words: biometric watermarking; fingerprint identification; authentication

1 引言

近年来,随着多媒体技术和数字网络通讯的飞速发展,信息的发布和传输实现了"数字化"和"网络化". 然而,数字媒体信息极易被仿制、处理、公开和传播. 这样就引发出数字信息传输的安全问题和数字信息的真实性问题. 特别是近年来电子犯罪层出不穷,对国家安全和经济活动造成了很大的威胁和破坏. 因此,对电子用户进行可靠的身份认证,保证电子产品的完整性和可靠性刻不容缓. 目前,信息安全技术领域通常使用密码技术和数字签名技术来保证信息的安全. 利用密钥将明文加密成密文,以保护信息的真实性、完整性,防止伪造、抵赖、冒充和篡改. 但是,由于密钥本身与密钥持有者没有必然的联系,密钥容易被他人窃取或遗忘. 密钥一旦被盗或被遗忘,就会造成严重的后果.

人体生物特征信息包括面孔、指纹、掌纹等,它们具有唯一性、不变性等特性,可以作为身份的唯一标志. 因此利用人体生物特征作为"密钥"的生物识别系统,建立了密钥与密钥持有者的终生不变唯一联系,并且方便易行. 基于指纹特征信息的生物识别技术是发展最早、应用最广泛、技术最成熟的生物识别技术. 但是,生物特征数据的安全是保证指纹识别系统正常有效工作的前提条件. Schneirer[1]指出只有在保证识别系统使用的所有生物特征数据是安全可靠的前提下—即所有的生物特征数据都是在录入时从合法用户那里得到的(而且应当是不能被改变的),识别认证系统才是有效的. 然而,存放生物特征数据的特征数据库本身并不具有安全保密性. 而且,对于需要服务终端的系统来说,也不可能将整个数据库都存放在每个终端当中. 例如银行系统,其用户数据库必然十分庞大,这样庞大的数据库是无法存放在分散各地的 ATM 柜员机中的. 这样做既不现实,又会大大降低整个认证系统的安全性. 指纹特征信息数据库的安全性问题成为了进一步提高系统安全性的瓶颈. 因此,为了实现指纹认证系统的广泛应用,必须引入一种即能完成录入、对比、认证等过程,又能有效保

收稿日期:2003-09-08;修回日期:2003-12-18
基金项目:国家自然科学基金(No. 60372052);全国博士学位论文作者专项资金(No. FANEDD-200238);哈尔滨工业大学跨学科研究基金(No. HIT.MD-2002.11);黑龙江省杰出青年科学基金

护特征参考信息的认证系统.

数字水印技术是一种新兴的信息隐藏技术.它的基本思想是在数字图像、音频和视频等媒体中嵌入秘密的信息以保护数字作品的版权.自 1994 年 V Schyndel[2]等人发表了第一篇有关数字水印的文章至今,随着媒体技术和数字网络的快速发展,数字水印技术的应用从版权保护发展到数据鉴别、数据监测、用户跟踪以及保密通信等领域,并收到了良好的效果.但是,水印信号的唯一性问题一直没有得到很好地解决.

Yeung 和 Pankanti[3]提出了在指纹图像模板中嵌入水印,以防止指纹模板被恶意篡改.但是,水印以噪声的形式嵌入指纹模板,必然影响特征提取,从而可能提高系统误判率,降低整个系统的可靠性.而 Jain 和 Uludag[4]提出直接将特征数据嵌入到媒体图像或其他载体中,实现对传输中的指纹特征数据的保护.但是,该算法没有提供样本数据库的安全保密措施.一旦数据库发生非法改动(无论是故意的还是无意的),整个识别系统的可靠性仍会大大降低.

本文提出利用每个合法用户的指纹特征信息参考样本生成水印信号,并将其嵌入该用户的证件之中.在进行识别或验证时,首先对用户证件图像进行水印的提取.识别系统根据提取出的水印信息,重建特征信息参考样本,并与当时采集的指纹信息进行比对,完成识别过程.这样,指纹特征信息参考样本不是直接来自于数据库,其安全保密性得到了很大提高.同时,嵌入指纹特征信息后的证件也与其持有者建立了本质联系,可有效防止证件被盗用的现象.其基本思想如图 1.

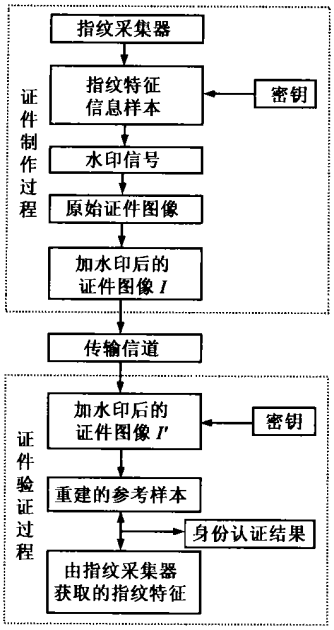

图 1 身份验证流程图

2 算法研究

2.1 水印生成算法

目前,指纹识别系统通常采用特征点表示法来描述指纹图像.以指纹纹路中终点、分叉点的位置与方向信息,通常被称之为细节数据(minutiae),作为指纹的特征数据[5].如果直接将指纹样本作为水印信息,嵌入数字图像中,样本数据的安全无法保证.因此,本文将指纹特征数据加密成密文,作为水印信号嵌入载体图像中.

本文采用 RSA 算法[6]对指纹信息进行加解密.RSA 算法是第一个能同时用于加密和数字签名的算法,易于理解和操作.它是研究得最为广泛的公钥算法,从提出到现在已近二十年,经历了各种攻击的考验,逐渐为人们接受,普遍认为是目前最优秀的公钥方案之一.RSA 算法的缺点在于它的速度较慢,但是对于指纹信息这一类较小的数据来说,还是可以接受的.

RSA 使用一对密钥:公钥和私钥.公钥由 n 和 e 组成,其中 n 是两个大素数 p 和 q 的乘积(p 和 q 必须保密),e 与 $(p-1)\times(q-1)$ 互素.私钥 $d = e^{-1}((\mathrm{mod}\ (p-1)(q-1)))$.在证件的制作过程中,利用私钥对指纹信息进行加密,加密后的指纹信息作为水印信息.在证件的验证过程中,利用公钥将提取的水印信息进行解密得到原始的指纹信息.表 1 给出了 RSA 软件速度的实例.

表 1 有 8-位公开密钥的 RSA 对于不同长度模数的加密速度.(在 SPARC Ⅱ中)

模数长度(bit)	512	768	1024
加密时间(s)	0.03	0.05	0.08
解密时间(s)	0.16	0.48	0.93

如果选择一个合适的 e 值,RSA 加密速度将快的多.最常用的三个 e 值是 3,17 和 65537.本文中选择 $e = 17$.考虑到算法的安全性,本文选择的模数长度为 1024bit.

具体过程如下:

(1)由指纹采集器获得指纹特征数据,指纹信息长度在 1400bit～1600bit 之间;

(2)将信息进行分组,分组的长度应小于模数的长度.由于本文采取的模数长度为 1024bit,因此将指纹信息分成两组分别进行加密;

(3)将指纹特征数据加密成密文,并对密文进行适当的扩充,以满足嵌入算法的要求.

2.2 水印嵌入算法

本文采用基于分块 DCT 变换的水印嵌入算法.具体算法如下:

对原始图像进行 8×8 分块 DCT 变换.为提高水印的鲁棒性,又不过多地影响图像质量,选择位于中低频位置的 N 个系数 $C[1], C[2], \cdots\cdots, C[N]$.为提高水印算法的鲁棒性,尤其是针对 JPEG 压缩.本文根据 Lin 和 Chang[7]提出的算法思想,对 DCT 系数进行量化调制,得到调制后 DCT 系数的水印形式:$C_w[1], C_w[2], \cdots, C_w[N]$.即:

$$C_w[I] = \alpha q[i]\, C_{wI}[i] \tag{2}$$

2.3 水印提取算法

进行水印提取时,对含水印图像进行分块 DCT 变换后,得到系数 $C'_w[i]$.根据式(3),计算出量化结果

$$C'_{wI}[i] = \frac{C'_w[i]}{\alpha q[i]} \tag{4}$$

对 $C'_{wI}[1], C'_{wI}[2], \cdots, C'_{wI}[N]$ 作异或运算,则得到嵌入的水印信息 b'_e.

2.4 抗几何攻击对策

在证件验证过程中,识别系统通过扫描仪获得含水印数字图像.但是,由于证件摆放不正以及扫描仪本身的误差,通常会引入几何失真.目前各种证件如身份证等,都存在一个黑色的矩形框作为贴照片处,如图 2 所示.因此,利用图像已有

的这种矩形框,作为几何失真的检测标志. 通过测得的检测失真数据,对图像进行恢复,形成有效的抗几何失真对策. 详细算法见[8].

图 2　图像中几何失真检测标志的添加

3　密钥的管理

为了防止非法用户使用自己的指纹特征信息参考样本,伪造证件. 在水印的嵌入和提取过程中,本文采用公钥密码学中数字证书方式解决证件本身的信任问题. 具体思想如图 3 示:

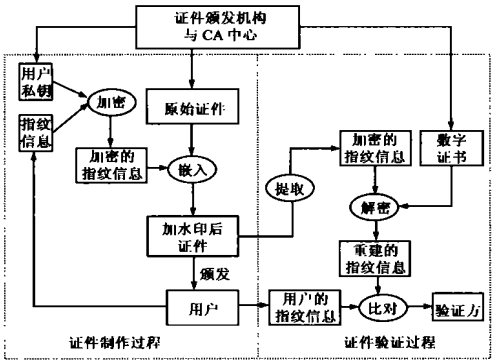

图 3　数字证书方式实现证件的制作和验证

公开密码学方式下证件的制作与验证步骤如下:

(1) 证件颁发机构(同时作为数字证书机构中心 CA) 为每一个合法用户设立一个数字证书.

(2) 将用户的私钥作为密钥对用户的指纹信息进行加密,加密的指纹信息作为水印嵌入到该用户的证件中.

(3) 当需要对用户的证件进行验证时,验证方先将证件中的水印信息提取,然后使用证件颁发机构发布的该用户的数字证书对水印信息进行解密得出用户的指纹信息,最后将证件中的指纹信息与用户的指纹信息进行比对完成校验过程.

4　实验结果

实验中使用的原始图像为大小为 512 ×512 的 256 级灰度的证件图像. 指纹特征数据通常在 180 字节到 200 字节之间,随手指纹路的不同而不同. 图 4(*a*) 是原始图像,图 4(*b*) 是已嵌水印后的数字图像. 图 5(*a*) 和(*b*) 是由指纹采集器获取的指纹特征值与从数字图像中提取出的特征值进行比对的结果. 其中(*a*) 表示的是两次都采集同一手指的特征后的比对结果,而(*b*) 表示的是两次采集不同的手指特征值后的比对结果. 实验结果表明,水印嵌入后,PSNR 值为 24. 4dB,不影响证件的一般使用.

图 4　原始数字图像和嵌水印后的数字图像

图 5　指纹采集与比对结果

本水印算法使用标准水印测试平台 Stirmark 进行 JPEG 攻击,表 2 列出经攻击后水印的提取结果.

表 2　水印经 JPEG 攻击后的提取结果

JPEG 压缩品质因数(%)	汉明距(%)
60	0. 05
50	0. 06
40	0. 08
35	0. 08
25	0. 10

表 3 列出含水印图像发生旋转并利用文献[8]中算法恢复后水印的提取结果.

表 3　旋转失真的含水印图像恢复后水印的提取结果

旋转角度(°)	汉明距(%)
10	0. 04
5	0. 04
1	0. 06

在生物识别系统中,通常当汉明距为 0. 26 时,系统的误判率为 1. 5 ×10^{-10}. 从实验结果中可见,随 JPEG 压缩程度的增加,汉明距随之增大,但仍小于 0. 26,不影响系统的正确识别,并由此可见,本水印算法具有一定的鲁棒性. 使用文献[8]中算法对发生旋转失真的含水印图像进行恢复,可获得较好的水印提取结果,满足识别系统的要求.

5　结论

基于人体生物特征的数字水印技术,利用生物特征的不变性和非易失性生成数字水印信号,从而综合了数字水印和生物识别二者的优势,有着广阔的发展前景. 基于生物特征的数字水印技术已申请专利. 本文利用指纹特征信息生成数字

水印信号,并隐藏在身份证件之中,取代传统的特征数据库,提高指纹识别系统的安全性,并实现对证件的保护.实验证明,基于指纹特征的数字水印可以成功地完成身份认证,并具有一定的鲁棒性.

本文还将在以下几方面进行深入研究:

(1)根据指纹识别系统的原理及特征提取、匹配算法,改进水印嵌入方案,使其对指纹识别系统的影响降至最小;

(2)对密钥进行更加安全有效的管理.

参考文献:

[1] B Schneier. The uses and abuses of biometrics[J]. Comm ACM. 1999, 42(8):136.

[2] R G van Schyndel, A Z Tirkel, C F Osborne. A digital watermark [A]. Proc of IEEE Int Conf Image Processing [C]. USA: IEEE, 1994, Ⅱ:86 - 90.

[3] M Yeung, S Pankanti. Verification watermarks on fingerprint recognition and retrieval [A]. Proc. of SPIE Conference on Security and Watermarking of Multimedia Contents [C]. San Jose: SPIE, 1999.

[4] K Jain, U Uludag. Hiding fingerprint minutiae in images [A]. Proc. Automatic Identification Advanced Technologies [C]. New York: AutoID, 2002.

[5] A K Jain, L Hong, S Pankanti, R Bolle. An identity-authentication system using fingerprints [A]. Proc. IEEE [C]. USA: IEEE, 1997.

[6] B Schneier. Applied Crytography: Protocols, Algorithms, and Source Code in C [M]. USA: John Wiley & Sons, Inc. 1996.

[7] C-Y Lin, S-F Chang. A robust image authentication algorithm surviving JPEG lossy compression, storage and retrieval of image/video databases [A]. SPIE [C]. USA: SPIE, 1998, 3312: 296 - 307.

[8] 俞龙江,牛复牧,孙圣和. 一种旋转、尺度变换和平移鲁棒水印算法[J]. 电子学报, 2003, 31(12A): 2071 - 2073.

作者简介:

张毅刚 男,1953 年生于黑龙江省鸡西市,1982 年获哈尔滨工业大学无线电技术专业学士学位;1996 年获哈尔滨工业大学测试计量技术学科硕士学位;2003 年至今攻读哈尔滨工业大学仪器科学与技术学科博士学位,他是哈尔滨工业大学自动化测试与控制系教授,主任,中国电子学会高级会员,主要研究方向为数字信号处理、人体生物特征识别、自动化测试与控制,发表论文 20 余篇,其中 EI 检索 6 篇,出版译著、教材共 10 本,获国家科技进步二等奖一项,省部级科技进步一等奖 1 项;省部级科技进步二等奖 2 项.