

# 基于指纹和数字水印的网络身份认证系统研究

孙印杰<sup>1,2</sup>, 陈智芳<sup>1</sup>, 王敏<sup>1</sup>, 洪力<sup>1</sup>

(1. 河南师范大学 计算机与信息技术学院, 河南 新乡 453007;

2. 阿克苏职业技术学院 计算机系, 新疆 阿克苏 843000)

**摘要:**数字水印作为一种新型的信息隐藏技术而成为目前业界研究的热点。从数字水印和指纹识别技术相结合的角度, 利用数字水印的隐藏性和指纹识别的唯一性, 实现了对用户身份的双重认证, 大大增强了网络身份认证的安全性和可靠性, 是一种强身份认证方案。现提出一种基于离散余弦变换和奇异值分解相结合的数字水印算法。实验结果表明, 该算法具有很好的稳健性, 提高了用户身份验证的效率, 取得了很好的效果。

**关键词:**指纹识别; 数字水印; 身份认证

**中图分类号:** TP393.08

**文献标识码:** A

**文章编号:** 1673-629X(2008)04-0147-04

## Research of Authentication System Based on Fingerprint and Digital Watermarking

SUN Yin-jie<sup>1,2</sup>, CHEN Zhi-fang<sup>1</sup>, WANG Min<sup>1</sup>, HONG Li<sup>1</sup>

(1. College of Computer & Information Technology, Henan Normal University, Xinxiang 453007, China;

2. Department of Computer, Akesu Occupation Technical College, Akesu 843000, China)

**Abstract:** As a new type of information-concealing technology, digital watermarking has become a focus of research in the industry. In light of the combination of the technologies of watermarking and fingerprint recognition, and taking advantage of the invisibility of watermarking and the uniqueness of fingerprint recognition, thus realizing the dual authentication of users' identification. This is a kind of powerful pattern of authentication, and greatly improves the reliability and security of network authentication. It is also proposed a hybrid watermarking algorithm based on DCT and SVD. Experimental results show that the watermarking algorithm performs well in robustness and raises the efficiency of the authentication of users', and has obtained the good effect.

**Key words:** fingerprint recognition; digital watermarking; authentication

## 0 引言

随着计算机网络的不断发展, 全球信息化已成为人类发展的趋势。由于计算机网络具有联结形式的多样性、终端分布的不均匀性及网络的开放性与互联性等特征, 致使网络易受黑客、恶意软件和其他不轨行为的攻击, 所以网上的安全和保密至关重要。随着网络成为信息交流、商务活动的重要手段, 用户身份认证的问题日渐受到人们的重视, 为了保证网络信息的真实性、完整性和不可抵赖性, 需要对用户身份进行认证。身份认证是网络安全的重要机制之一, 它是信息系统对拥有身份的特殊个体提供的, 他/她是谁的证明

进行判断的处理过程, 网络身份认证是依靠用户账号、口令或者生物特征等信息来实现的, 这些认证方法在某种程度上存在着安全隐患, 如账号、口令或指纹特征信息在存储、传输过程中可能被截取、被篡改等。

数字水印作为一种新型的信息隐藏技术, 是将数字、序列号、文字、图像等信息嵌入到数字图像、声音、文档、图书、视频等数字作品中。由于数字水印技术将信息以不可见且不可删除的方式嵌入多媒体作品中, 一旦发生非法侵权等事件时, 通过对数字作品中的水印进行检测和分析, 从而获取嵌入的信息, 并以此作为鉴定、起诉非法侵权的证据, 使数字水印成为知识产权保护与信息安全的有效手段。

## 1 指纹识别技术

### 1.1 指纹识别技术概述

指纹识别技术是世界上最先进的识别技术, 它是

收稿日期: 2007-07-14

基金项目: 河南省自然科学研究计划项目(0624220039); 校科研基金项目(2006ZY-01-03)

作者简介: 孙印杰(1964-), 男, 副教授, 硕士生导师, 研究方向为多媒体技术、网络安全。

利用人体指纹的唯一性和不变性的生理特征,将指纹作为人的一种“活的身分证”,通过取像设备读取指纹图像,然后用计算机识别软件提取指纹的特征数据,最后通过匹配识别算法得到识别结果,以确定指纹所有人身份的生物学特征识别技术。指纹具有唯一性、稳定性、随身性、便于采集等特点,与其他人体生物学特征识别技术相比,指纹各不相同、终生基本不变的特点已经得到公认。指纹识别技术在操作方便、性能稳定、成本低廉、用户易接受等方面具有综合优势。目前,从实用的角度看,指纹识别技术是优于其他生物识别技术的身份鉴别方法。

## 1.2 指纹识别技术原理

指纹识别主要涉及指纹图像采集、指纹图像处理、特征提取、保存数据、特征值的比对与匹配等。首先,通过指纹采集仪采集到人体指纹的图像,并对原始图像进行初步的处理,使指纹图像中蕴涵的特征信息更明显。然后,运用指纹特征提取算法建立指纹的数字表示——特征数据。这是一种单方向的转换:可以从指纹转换成特征数据,但不能从特征数据转换成为指纹,而且两枚不同的指纹不会产生相同的特征数据。从指纹上找到被称为“细节点”(minutiae)的数据点存储到指纹特征文件中,这些细节点也就是那些指纹纹路的分支点或末梢点。最后,通过计算机模糊比较的方法,把两个指纹的模板进行比较,计算出它们的相似程度,最终得到两个指纹的匹配结果。指纹识别原理框图如图 1 所示。

手指 → 指纹采集仪 → 图像预处理 → 指纹特征提取 → 指纹匹配

图 1 指纹识别原理框图

## 1.3 只采用指纹识别进行身份认证的缺点

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 指出<sup>[1]</sup>,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(且应是不能被改变的),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。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,为实现指纹认证系统的广泛应用,必须引入一种既能完成录入、对比、认证等过程,又能有效保护特征参考信息的认证系统。

## 2 数字水印技术

### 2.1 数字水印技术概述

所谓数字水印是指用信号处理方法在数字多媒体

数据中嵌入隐蔽的标记,这种标记通常是不可见的,只能通过专用的检测器或阅读器提取。数字水印的基本思想是利用人类感觉器官的不敏感及数字信号本身存在的冗余,在图像、音频和视频等数字产品中嵌入秘密信息以便记录其版权,同时嵌入的信息能够抵抗一些攻击而生存下来,以达到版权认证和保护的功能。数字水印并不改变数字产品的基本特性和使用价值。

一个完整的数字水印系统应包含三个基本部分:水印的生成、嵌入和水印的提取或检测。水印嵌入算法利用对称密钥或公开密钥实现把水印嵌入到原始载体信息中,得到隐秘载体。水印检测/提取算法利用相应的密钥从隐秘载体中检测或恢复出水印,没有解密密钥,攻击者很难从隐秘载体中发现和修改水印。

### 2.2 DCT 和 SVD 结合的数字水印算法

文中提出了一种将 DCT(离散余弦变换)和 SVD(奇异值分解)结合的水印方法<sup>[2,3]</sup>,假定水印的长度是  $n \times n$ ,整个图像的长度是  $2n \times 2n$ ,进行以下操作。

#### 2.2.1 水印的嵌入方法

(1) 对整个图像应用 DCT,按照“之”字型的顺序,绘制 DCT 系数到 4 个象限:  $B_1, B_2, B_3, B_4$ ;

(2) 在每个象限,运用 SVD:  $A^K = U_A^K \sum_A^K V_A^{KT}, K = 1, 2, 3, 4$ ,这里  $K$  代表这 4 个象限;

(3) 对整个水印  $W$  运用 DCT,然后对已经运用 DCT 转换的水印  $W$  运用 SVD:

$$W = U_W \sum_W V_W^T$$

(4) 利用已经运用 DCT 转换的水印  $W$  的奇异值,来修改每个象限  $B_K (K = 1, 2, 3, 4)$  的奇异值:  $\lambda_i^{*K} = \lambda_i^K + a_k \lambda_{wi}, i = 1, \dots, n, \lambda_i^K (i = 1, \dots, n)$  是  $\sum_A^K$  奇异值,  $\lambda_{wi} (i = 1, \dots, n)$  是  $\sum_W$  的奇异值;

(5) 得到 4 组已经修改了的 DCT 系数:

$$A^{*K} = U_A^K \sum_A^{*K} V_A^{KT}, K = 1, 2, 3, 4;$$

(6) 利用修改的 DCT 来嵌入水印。

#### 2.2.2 水印的提取方法

(1) 对已嵌入了水印的整个图像运用 DCT,按照“之”字型的顺序,绘制 DCT 系数到 4 个象限:  $B_1, B_2, B_3, B_4$ ;

(2) 在每个象限,运用 SVD,  $A^{*K} = U_A^K \sum_A^{*K} V_A^{KT}, K = 1, 2, 3, 4$ ,这里  $K$  代表 4 个象限;

(3) 提取每个象限  $B_K (K = 1, 2, 3, 4)$  的奇异值:

$$\lambda_{wi}^K = (\lambda_i^{*K} - \lambda_i^K) / a_k, i = 1, \dots, n;$$

(4) 使用奇异向量构造 4 个水印的 DCT 系数:  $W^K = U_W^K \sum_W^K V_W^{KT}, K = 1, 2, 3, 4;$

(5) 利用 DCT 来提取 4 个水印。

### 2.3 只采用数字水印进行身份认证的缺点

自1994年V. Schyndel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提出了在指纹图像模板中嵌入水印<sup>[4]</sup>,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。

## 3 采用指纹识别和数字水印的网络双重身份认证系统

文中利用了数字水印技术可以在图像中嵌入信息并且隐藏嵌入的信息,将数字水印与指纹认证相结合,提出了一种网络双重身份认证的模型(见图2),从而实现了用户合法身份的双重认证,保障了网络信息的安全。网络双重身份认证的过程如下<sup>[5]</sup>:

(1)生成数字水印。访问时,首先采集用户指纹图像,并从该指纹图像中提取指纹特征信息A;同时,要求用户录入ID、口令以及编号(该用户的原始指纹特征信息B在指纹特征库中的编号)等信息;最后将两种信息进行组合,构成数字水印。水印是将ID、口令、编号以及指纹特征信息A以ASCII码形式连续排列,构成二进制位0、1的序列,为了提高水印的安全性,在水印嵌入载体图像前,对水印还需进行置乱处理。

(2)从用户端发送已嵌入水印的载体图像到服务器端,将经过置乱处理的水印嵌入到某一指定的载体图像中,然后将已嵌入水印的载体图像发送到用户将要访问的服务器端。

(3)服务器端提取水印并取得两个指纹特征信息A和B。服务器端接收从用户端发来的载体图像,从该载体图像中提取水印,并对其进行置乱恢复,接着从恢复后的水印中提取该用户的指纹特征信息A;与此同时,通过从水印中得到的编号提取存储在指纹特征库中该用户的原始指纹特征信息B。

(4)匹配比较两个指纹特征信息A和B。将来自两个处理过程的指纹特征信息A和B进行比较,若两者匹配,则证明该用户为合法用户。

作为身份认证的前提条件,用户的原始指纹特征信息必须首先在指纹特征库中注册,并与其姓名或其标识(ID, PIN)等信息联系起来,以一定的存储格式存入数据库中。在匹配比较时,先验证用户个人标识,例如ID和口令,然后通过系统数据库中存储的指纹特征信息B与水印中得到的指纹特征信息A的比较来再次证明用户的合法身份。由此可见,所有的信息资源访问权限都在身份认证系统(服务器端)的管理之下,经过两个物理认证因素的验证,确保了信息资源访问的合法性。这样,将数字水印与指纹识别技术相结合,实现了用户合法身份的双重认证:

1)水印信息中的ID、口令——第一重认证。服务器端从用户端发送来的载体图像中提取水印信息,该水印信息中包含用户的ID、口令,若ID和口令不正确,则可判断为非法用户。

2)指纹特征信息——第二重认证。服务器端将从用户端发送来的载体图像中所提取的指纹特征信息A与存储在指纹特征库中的该用户的原始指纹特征信息B进行比较,再次验证用户的合法性。

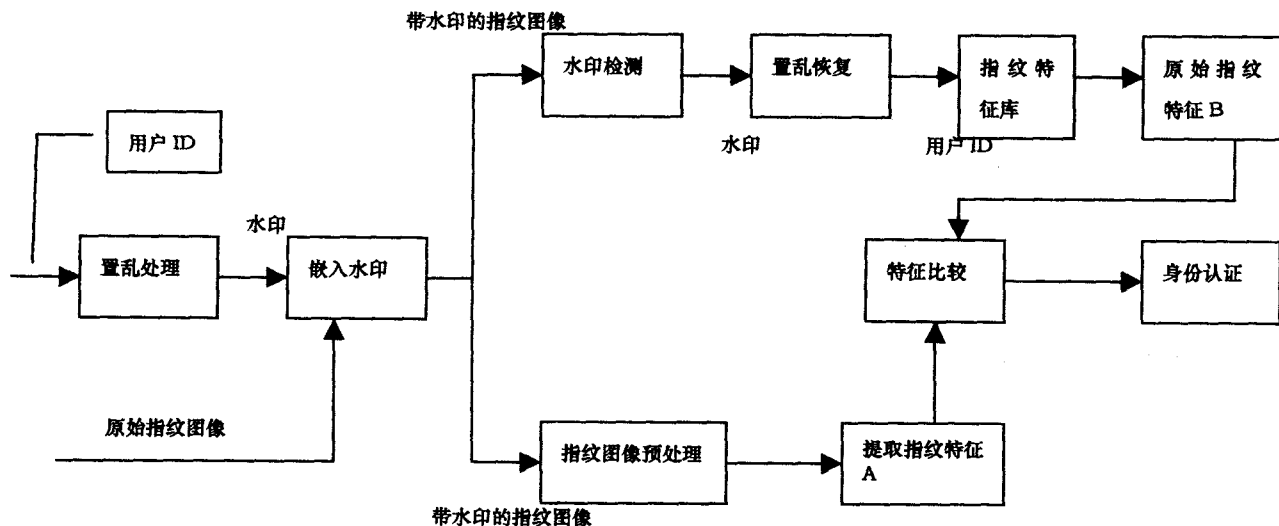


图2 网络双重身份认证系统

为了提高水印的安全性,在水印嵌入前,先对水印进行置乱处理,扰乱水印信息之间的相关性,即使攻击者提取了水印,也会因为其难以辨别而无法判断是否正确地提取了水印。

#### 4 仿真实验

采用  $384 \times 384$  的 lena 灰度图像,水印是  $32 \times 32$  的二值图像,仿真软件为 matlab7.0,采用频域水印嵌入法将重要信息嵌入指纹图像中,为衡量算法的质量,引入两个评价指标:PSNR(峰值信噪比)和 NC(水印相似度),定义如下:

$$PSNR = 10 * \log \left\{ \frac{M * N * \max[C_0(i, j)]^2}{\sum_{i=1}^M \sum_{j=1}^N [C_w(i, j) - C_0(i, j)]^2} \right\}$$

其中,  $M$ 、 $N$  代表图像的宽度和高度,  $C_0(i, j)$ 、 $C_w(i, j)$  代表原始图像和嵌入水印图像的像素值。

$$NC = \frac{M * N - \sum W(i, j) \otimes W'(i, j)}{M * N}$$

其中,  $M$ 、 $N$  代表图像的宽度和高度,  $W(i, j)$ 、 $W'(i, j)$  表示原始水印和提取出来的水印的像素值。

本算法取嵌入强度  $\alpha$  值为 0.08, 阈值  $T$  为 0.3, 得到嵌入水印图像 PSNR = 46.02。在视觉上与原图没有什么区别, 水印相似度 NC = 0.9941。实验结果表明, 利用指纹识别和数字水印进行身份认证, 取得了很好的效果。仿真结果如图 3~6 所示。

#### 5 结论

基于人体生物特征和数字水印技术的网络双重身份认证, 是利用生物特征的不变性和数字水印信号的非易失性, 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。仿真实验表明, 指纹特征和数字水印可以成功地完成身份认证, 提高了用户身份验证的效率, 具有一定的鲁棒性。



图 3 原始图像

图 4 加入水印后的图像



图 5 原始水印

图 6 提取水印

#### 参考文献:

- [1] Schneier B. The uses and abuses of biometrics[J]. Comm A CM, 1999, 42(8): 136 - 139.
- [2] 张毅刚, 焦玉华, 牛夏牧, 等. 基于指纹特征数字水印算法的身份认证技术研究[J]. 电子学报, 2003, 31(12A): 2131 - 2134.
- [3] 邵利平, 覃征, 衡星辰. 一种基于图像置乱变换的空域图像水印算法[J]. 计算机工程, 2007, 33(2): 122 - 124.
- [4] Yeung M, Pankanti S. Verification watermarks on fingerprint recognition and retrieval[C] // Proc. of SPIE Conference on Security and Watermarking of Multimedia Contents. San Jose: SPIE, 1999.
- [5] 谢 勋. 基于数字水印与指纹识别的网络双重身份认证[J]. 计算机工程与科学, 2006, 28(6): 27 - 29.

(上接第 146 页)

越复杂、应用系统的数量越来越多的时候, 解决应用系统、操作系统、数据库系统等资源的统一用户管理问题就显得特别重要, 有效的用户管理不但能够降低诸如密码保密性能不足之类的安全风险, 并且最大程度地消除可能影响用户生产力的障碍。

#### 参考文献:

- [1] Altmann J, Sampath R. A User - Centric Framework for Network Identity Management[C] // Presented at Network Operations and Management Symposium. Vancouver, BC: [s. n.], 2006: 495 - 506.
- [2] Gaedke M, Meinecks J, Nussbaumer M. A Modeling Approach to Federated Identity and Access Management[C] // Presented at Poster Proceedings of the 14th International

World Wide Web Conference. Japan: [s. n.], 2005: 1156 - 1157.

- [3] 孙丽萍, 王 新, 刘志俊, 等. 异构环境中统一用户管理的研究与规划[J]. 计算机工程与应用, 2005, 41(32): 225 - 228.
- [4] Microsoft TechNet. 针对 UNIX 的 Microsoft Windows 安全和目录服务解决方案指南[EB/OL]. 2005. <http://technet.microsoft.com>.
- [5] 赵保翠, 刘 岗. 基于 LDAP 的统一用户管理系统的设计和实现[J]. 微电子学与计算机, 2005, 22(11): 59 - 62.
- [6] Samur W. Unified Login with Pluggable Authentication Modules(PAM)[C] // Presented at the 3rd ACM Conference on Computer and Communication Security. India: [s. n.], 1996: 1 - 10.