

# 基于奇异值分解的双重网络身份认证系统

甘艳芬, 潘保昌, 郑胜林, 周泽华, 黄创辉

(广东工业大学 信息学院, 广东 广州 510090)

摘要: 针对当前网络的发展和面临的安全问题, 提出了一种基于奇异值分解的双重网络身份认证系统. 运用奇异值分解水印技术把 ID 和指纹结合为一体, 实现对指纹特征库 ID 的认证和指纹识别认证的双重认证, 并使 ID 和指纹具有相对独立性, 加强了 ID 的隐藏性和安全性. 实验结果表明本系统有良好的稳定性、安全性、可靠性.

关键词: 数字水印; 身份认证; 奇异值分解

中图分类号: TP391

文献标识码: A

文章编号: 1007-7162(2007) 03-0054-03

随着网络应用逐步拓展到多媒体业务、电子商务等领域, 其安全问题越加受到关注. 身份认证是网络安全体系的基础. 无论是数据加密、访问控制或其它网络安全技术<sup>[1-2]</sup>, 都必须基于有效的身份认证, 否则一旦攻击者伪造或盗用合法身份, 各种安全堡垒都形同虚设. 网络身份认证是对人在网络中身份的确认, 而数字水印技术, 也对数字多媒体等的产权保护有很大的作用. 换句话说, 网络身份认证跟数字水印技术在某个角度上是有交集的. 本文基于此提出一种把数字水印技术运用到网络身份确认中的认证方法. 通过对指纹特征库 ID 的认证和指纹识别认证实现双重认证<sup>[3]</sup>, 并运用奇异值分解水印技术<sup>[4]</sup>把 ID 和指纹结合为一体, 拟提高网络身份认证

体系的稳定性、安全性和可靠性.

## 1 系统的设计实现

### 1.1 基于 SVD 的多重网络身份认证系统的实现

系统可分为加密、嵌入水印部分和解密、提取水印部分. 第一部分作为认证请求过程中所要处理的内容, 实现用户指纹和 ID 的结合, 然后传送到认证端. 第二部分作为认证的验证处理过程. 此过程主要是对水印的提取, 然后根据提取的信息进行认证.

#### 1.1.1 水印嵌入和加密过程

加密部分作为认证请求过程中所要处理的内容, 实现用户指纹和 ID 的结合, 然后传送给认证端. 嵌入和加密过程如图 1 所示.

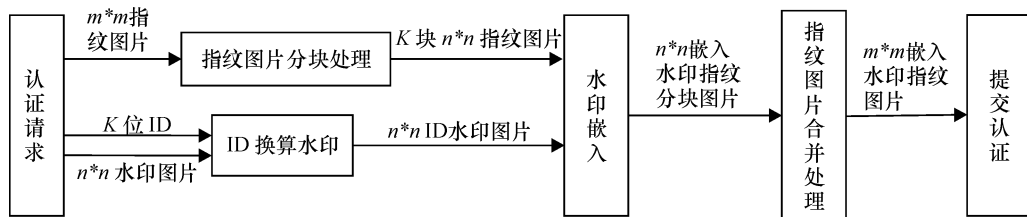


图 1 水印嵌入和加密过程

步骤一: 对指纹图片进行分块处理.

为了增加嵌入信息的量, 本文把原来  $m \times m$  的指纹图片分成  $n \times n$  指纹分块图片, 其中  $m$  等于 256  $n$  等于 32 如图 2 所示.



图 2 原图与分块后图片

步骤二: ID 换算为水印图片.

ID 作为查询指纹特征信息的密码, 是第一重认证的核心所在, 在本文中 ID 采用 6 位十进制数字表示. 但本设计并不在于以数字的形式提交 ID, 而是把它换算为水印图片, 并嵌入到指纹当中的形式提交. 10 个阿拉伯数字用 10 幅相关性小的水印图片表示 (见图 3), 6 位 ID 数字用到了其中的 6 幅.

步骤三: 水印嵌入运算.

采用了奇异值分解的水印技术, 先对选取的指纹分块图片  $A_i$  进行奇异值分解, 根据奇异值分解定

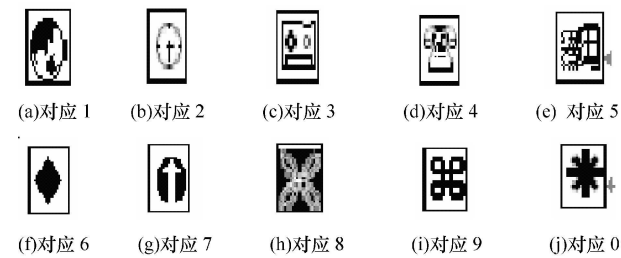


图 3 水印图片与数字对应图

理,可以分解为正交矩阵  $U_i$ 、 $V_i$  和奇异值矩阵  $S_i$  (见式 (1)),

$$A_i = U_i S_i V_i^T, \tag{1}$$

$S_i$  为奇异值矩阵, 矩阵  $A_i$  的奇异值为它的特征值的开平方.  $S_i$  矩阵可表示为式 (2),

$$S_i = \begin{bmatrix} \sigma_1 & & 0 \\ & \ddots & \\ 0 & & \sigma_n \end{bmatrix}. \tag{2}$$

$U_i$  为  $A_i^T A_i$  的正交特征向量矩阵, 见式 (3), 而  $V_i$  为  $A_i A_i^T$  的正交特征向量矩阵. 见式 (4),

$$U_i = \begin{bmatrix} X_{B11} & \cdots & X_{B1n} \\ M & O & M \\ X_{Bn1} & \cdots & X_{Bnn} \end{bmatrix}; \tag{3}$$

$$V_i = \begin{bmatrix} X_{C11} & \cdots & X_{C1n} \\ M & O & M \\ X_{Cn1} & \cdots & X_{Cnn} \end{bmatrix}. \tag{4}$$

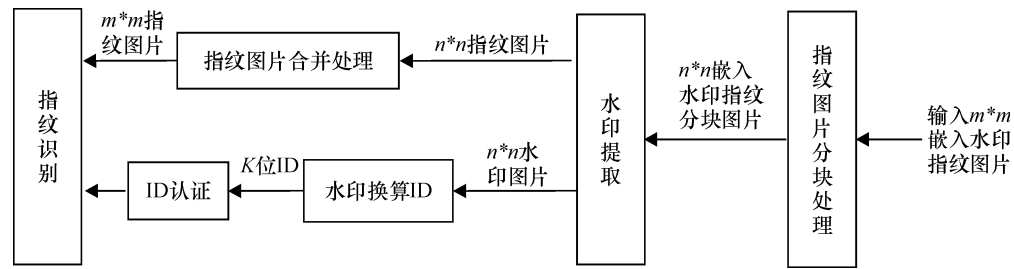


图 4 水印提取和认证过程

$X_B$ 、 $X_C$  分别为  $A_i^T A_i$ 、 $A_i A_i^T$  的特征向量.

然后把水印图片水印强度系数  $a$  相乘后叠加到  $S_i$  中生成新矩阵  $R_i$  (见式 5), 对新矩阵  $R_i$  再进行奇异值分解, 同样可以得到  $U_{ri}$ 、 $V_{ri}$ 、 $S_{ri}$  3 个矩阵 (见式 6), 最后把  $S_{ri}$  代替式 (1) 中的  $S_i$ , 再与  $U_i$ 、 $V_i$  组合成新的图片矩阵  $A'$  (见式 7),  $A'$  即为嵌入了水印信息的指纹图片.

$$R_i = S_i + aW_i, \tag{5}$$

$$R_i = U_{ri} S_{ri} V_{ri}^T, \tag{6}$$

$$A_i' = U_i S_{ri} V_i^T, \tag{7}$$

其中  $i = 1, 2, \dots, 6$  并保存  $U_{ri}$ 、 $V_{ri}$ 、 $S_{ri}$ .

步骤四: 把  $A'$  代替原指纹图中的  $A$ .

由于是分块进行水印的嵌入, 把步骤三重复 6 次, 就可以得到 6 幅嵌入水印的分块指纹图片  $A' = \{A_i' | i = 1, 2, \dots, 6\}$ , 最后组成嵌入水印的完整指纹图片.

1.1.2 水印提取和认证过程

水印的提取和认证过程是水印的嵌入和加密的反过程, 这一过程的框图如图 4 所示.

步骤一: 对获取的嵌有水印信息的指纹图片进行分块处理.

因为本设计的过程是以分块图片为单位进行处理的, 所以要进行水印的提取也必须要进行分块处理. 方法和嵌入水印过程的步骤一一样.

片合并成完整指纹图片用于指纹识别.

步骤四: 认证.

通过对 ID 的认证, 获取相关信息进行指纹识别认证.

2 实验分析

实验中输入一组  $D$  (为 123456), 对不同情况进行测试. 图 5 是在正常情况下的实验结果. 图 6 显示出了在嵌入了水印指纹图片受损情况下的一组实验结果. 图 6 中嵌入指纹的水印图片有轻微损坏. 这两种情况都能提取正确的  $D$  号.

步骤二: 水印提取过程.

首先对获取的可能受损嵌有水印信息指纹分块图片  $A_i^*$  进行奇异值分解 (见式 8), 然后把获得的  $S_{ri}^*$  与  $U_{ri}$ 、 $V_{ri}$  相乘得矩阵  $R_i^*$  (见式 9), 然后去除指纹奇异值矩阵信息, 可获得水印矩阵 (式 10).

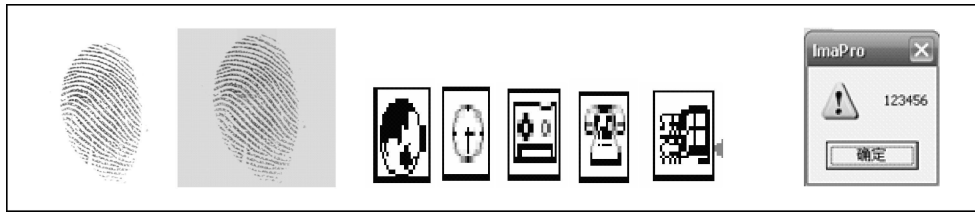
$$A_i^* = U_i^* S_{ri}^* V_i^{*T}, \tag{8}$$

$$R_i^* = U_{ri} S_{ri}^* V_{ri}^T, \tag{9}$$

$$W_i^* = \frac{1}{a} (R_i^* - S_i). \tag{10}$$

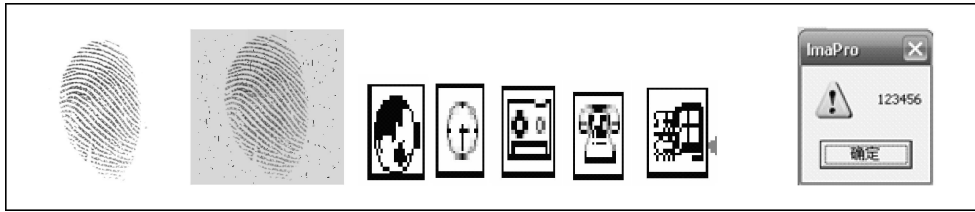
步骤三: 水印换算  $D$ .

由步骤二获得水印图片后, 要换算成数字的  $D$ . 用来做第一重的 ID 认证. 同时把分块的指纹图



(a)原图 (b)嵌入水印受损图 (c)输出水印结果图 (d)输出 ID图

图 5 正常情况的测试结果



(a)原图 (b)嵌入水印受损图 (c)输出水印结果图 (d)输出 ID图

图 6 水印指纹图片受损的测试结果

结果表明,当图片受到中小程度损坏时,系统仍然能够正确验证结果,可见系统具有较好的可靠性.

3 设计总结

本设计运用奇异值分解 (SVD)水印技术的稳定性、非视觉性等特点,把 ID 和指纹结合为一体,完整保留了指纹信息用来做指纹识别认证.把用于指纹特征库的 ID 换算为水印图片,加强 ID 的隐藏性、安全性及 ID 和指纹的独立性.实验结果表明基于奇异值分解的双重身份认证系统有高度的可靠性、稳定性和安全性,能够实现安全、准确的认证.

参考文献:

[ 1 ] 刘瑞祯,谭铁牛. 基于奇异值分解的数字图像水印方法 [ J]. 电子学报, 2001, 29( 2): 168-171.  
[ 2 ] 王飞,汤光明,孙怡峰,等. 基于易损水印和数字签名的电子印章系统 [ J]. 计算机应用研究, 2004, 21( 4): 118-121  
[ 3 ] 李丽娟. 双重身份认证方法的设计与实现 [ J]. 计算机仿真, 2005, 22( 6): 102-104, 167.  
[ 4 ] 姚鹏,杨珍. 动态口令认证技术 [ J]. 电子商务, 2006( 1): 54-57.

Authentication System Based on Singular Value Decomposition Dual Network

GAN Yan-fen, PAN Bao-chang, ZHENG Sheng-li, ZHOU Ze-hua, HUANG Chuang-hui  
(Faculty of Information Engineering, Guangdong University of Technology, Guangzhou 510006, China)

**Abstract** In order to resolve the problem on current network development and security, the dual network authentication system was proposed, based on singular value decomposition. ID and fingerprints were authenticated via the singular value decomposition watermark technology which combined ID with fingerprints, making ID and fingerprints relatively independent, thus strengthening the concealment and security of ID. Experimental results indicate that the system is stable, safe and reliable.

**Key words** digital watermarking; authentication; singular value decomposition