文章编号:1001 - 9081(2005)08 - 1750 - 03

# 基于 JPEG 2000 实时量化水印和指纹识别的身份认证系统

姜 聃[1],宣国荣[1],杨程云[1],郑伊展[1],刘连生[2],白维朝[2]
(1. 同济大学 计算机系,上海 200092; 2. 深圳宝嘉电子设备有限公司,广东 深圳 518057)
(smartyepp@yahoo.com.cn)

**摘 要**:提出了新的 JPEG 2000 实时量化水印算法,并将其用于改进的基于指纹识别和数字水印的银行养老金发放系统。系统客户端,量化水印在 JPEG 2000 压缩过程中实时嵌入指纹图像,压缩比特流传送到服务端;系统服务端,水印在 JPEG 2000 解压缩过程中实时提取,使用解压缩的指纹图像和水印进行身份认证。实验表明典型指纹图像压缩到 1/4 ~ 1/20 的时候,嵌入的水印能够无损提取,指纹图像虽不能完全恢复但识别率没有明显降低。因而在低网络带宽条件下,新系统有更好的交互性能,在电子商务中有很好的应用前景。

**关键词**:JPEG 2000;实时量化水印;指纹识别;身份认证
**中图分类号**: TP391.41 **文献标识码**:A

# Identity verification system using JPEG 2000 real-time quantization watermarking and fingerprint recognition

JIANG Dan[1], XUAN Guo-rong[1], YANG Cheng-yun[1], ZHENG Yi-zhan[1], LIU Lian-sheng[2], BAI Wei-chao[2]
(1. *Department of Computer Science, Tongji University, Shanghai* 200092, *China*;
2. *Baojia Electronic Equipments, Co. Ltd, Shenzhen Guangdong* 518057, *China*)

**Abstract:** The proposed JPEG 2000 real-time quantization watermarking algorithm was used in an improved online bank pension distribution system. The system was based on fingerprint recognition and digital watermarking technologies. In the client side, real-time quantization watermark was embedded into the sampled fingerprint image in the JPEG 2000 coding pipeline; then the compressed bit-stream was sent to the server side. In the server side, the watermark was extracted from the compressed bit-stream in the JPEG 2000 decoding pipeline; then the decompressed fingerprint image and extracted watermark were used to verify user's identification. Experiments showed when typical fingerprint image was compressed to 1/4 ~ 1/20 of its original size, the embedded watermark could be exactly extracted, and fingerprint recognition rate remained almost the same after lossy compression. The system has a better interaction performance in the band-limited network situation, and is very promising in the E-business applications.

**Key words:** JPEG 2000; real-time quantization watermarking; fingerprint recognition; identity verification

## 0 引言

在文献[1]中,我们提出了基于无损数字水印和指纹识别的网上身份认证系统。在这个系统中,利用了整数小波变换[2]解相关性和小波变换系数的中高位位平面0,1 比特分布具有可压缩性的特点,将用户认证信息作为水印嵌入原始指纹图像一级小波分解的高频子带(即 $HL_1$,$LH_1$,$HH_1$)系数的中高位位平面,同时对这些位平面原来的比特信息使用算术编码进行压缩,并进行了直方图修正以防止反变换后像素值的溢出,从而保证了水印信息和原始指纹图像的无损恢复,因而对后续的指纹识别不产生任何影响。

在实际系统中,我们遇到了一个问题:采集到的指纹为 76K Bytes 的 BMP 图像,在网络带宽很窄的情况下,比如使用 56Kbps 的普通电话线传送这个指纹,如果指纹图像质量不高,系统服务端验证失败,提示用户重新采集指纹。这个过程总共持续 30 多秒,用户需要很长的等待时间,这显然是无法容忍的。因此,在低带宽情况下,如何有效传送嵌入用户认证信息的指纹图像成为我们面临的新的研究课题。

无损图像压缩技术虽然具有数据无损压缩和恢复的优点,但是其压缩率不高,例如使用流行的无损文本压缩软件 WinRAR 3.20 版对采集的指纹图像进行压缩,只能由 76K Bytes 压缩到 60K Bytes 左右,能否进一步压缩指纹图像减少传送时间以提供更好的用户交互性能成为我们关心的问题。很自然的,我们想到了使用有损图像压缩技术,有损图像压缩如 JPEG 2000 具有很好的压缩效果,同时如果压缩后的指纹图像识别性能没有很大下降,那么系统在低带宽情况下将获得更好的性能。

本文中,提出基于 JPEG 2000 的实时量化水印算法,改进了文献[1]中提出的系统。在客户端,采集用户指纹图像并用 JPEG 2000 压缩,压缩过程中用户认证信息作为水印以量

收稿日期:2005 - 01 - 27;修订日期:2005 - 04 - 18 基金项目:国家自然科学基金资助项目(90304017)
作者简介:姜聃(1981 - ),男,江苏武进人,硕士研究生,主要研究方向:图像处理、模式识别; 宣国荣(1935 - ),男,上海人,教授,博士生导师,主要研究方向:图像处理、模式识别; 杨程云(1978 - ),男,江西瑞金人,博士,主要研究方向:图像处理、模式识别; 郑伊展(1981 - ),男,广东人,硕士,主要研究方向:图像处理、模式识别; 刘连生(1945 - ),男,陕西人,工程师,主要研究方向:银行安全支付; 白维朝(1955 - ),男,陕西人,工程师,主要研究方向:信息处理.

化的方式实时嵌入压缩码流;在服务器端,用 JPEG 2000 解码器解码压缩码流,并从中实时提取水印信息,然后将解压缩的指纹图像与中央数据库中存放的用户指纹信息匹配认证用户身份。

新系统保持了原系统的优点:1)利用生物特征识别提高了认证系统的可靠性; 2)将水印信息嵌入指纹图像一起传送不易被人察觉,增加了系统的隐蔽性; 3)由于采用了 JPEG 2000 压缩,传送的图像数据量比在文献[1]中提出的系统更小,有利于在低带宽情况下的传输; 4)水印嵌入/提取分别在 JPEG 2000 压缩/解压缩过程实时进行,只需进行一次小波变换,与 JPEG 2000 压缩的开销基本相同。实验表明水印信息能够无损提取,并且虽然指纹图像不能无损恢复但对于典型指纹库的测试,识别性能并没有明显的降低。

## 1　JPEG 2000 压缩过程中嵌入水印的算法

JPEG 2000 是新一代的静止图像压缩标准[3,4],与 JPEG 相比低码率下的压缩性能得到了很大的提升。

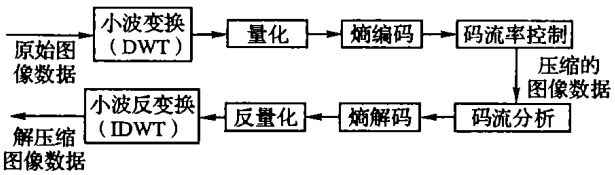



图 1　JPEG 2000 编码器/解码器结构

文献[5]中提出了 JPEG 2000 小波变换后嵌入 QIM (Quantization Index Modulation) 水印的方法,该算法具有一定的鲁棒性和抗攻击性。我们的系统主要利用了水印的隐蔽性,所以对抗攻击性要求不高,因此设计了一个新的、更加简单的、基于 JPEG 2000 的实时量化水印算法。

*水印嵌入算法*　水印在 JPEG 2000 压缩过程的量化之后和熵编码之前嵌入。设采用 $R$ 级小波分解,为了提高水印在低码率下的可靠性,水印嵌入在最后一级小波分解的低频子带 $LL_R$ 中,如图 2 所示。设嵌入的二进制水印数据为 $w = w_1, \cdots, w_m$,$m$ 为水印长度,$\Delta$ 为量化步长。

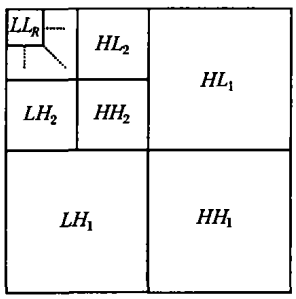



图 2　小波分解子带结构

根据水印的长度,选择一定数量的码块,码块中的每个系数 $c$ 用奇偶标量量化的方法嵌入 1 bit 水印数据,嵌入公式为(1)。如果嵌入的水印数据 $w_i = 0$,则将该系数量化为与它最接近的 $\Delta$ 的偶数倍;如果嵌入的水印数据 $w_i = 1$,则将该系数量化为与它最接近的 $\Delta$ 的奇数倍。为了增加系统的安全性,我们使用置乱的方法打乱嵌入的系数的顺序,$y = (k_0 + k_1 \times x) \bmod s$,其中 $x$ 和 $y$ 分别是置乱前后系数的位置。对于 $M \times N$ 的图像可以计算出水印的容量为 $\frac{M \times N}{2^{2R}}$。

$$c = \begin{cases} \text{与 } c \text{ 最接近的 } \Delta \text{ 的偶数倍} & \text{if } w_i = 0 \\ \text{与 } c \text{ 最接近的 } \Delta \text{ 的奇数倍} & \text{if } w_i = 1 \end{cases} \quad (1)$$

*水印提取算法*　水印在 JPEG 2000 解压缩过程的熵解码之后和反量化之前提取,提取公式如下:

$r = round(c/\Delta)$　其中 $round$ 取整数运算

$$watermark\_bit = \begin{cases} 0 & \text{if } r \text{ 为偶数} \\ 1 & \text{if } r \text{ 为奇数} \end{cases} \quad (2)$$

整个算法的流程如图 3。该算法压缩前原始指纹图像和解压缩后指纹图像如图 4。

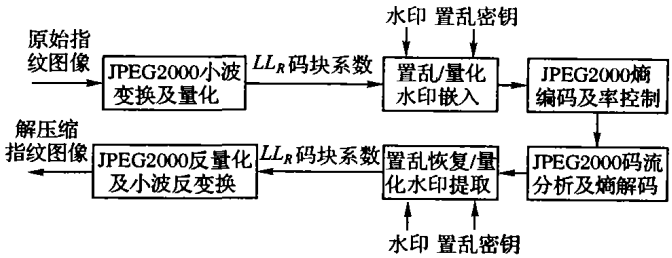



图 3　基于 JPEG 2000 实时量化水印算法的嵌入/提取流程图

(a) 原始图像　(b) 0.4bpp(PSNR=33.84)　(c) 4bpp(PSNR=38.57)

图 4　原始图像和解压缩图像

## 2　实验

由于采用的是有损图像压缩算法,在压缩过程中,原始指纹图像中的特征信息必然有所损失,那么由于压缩带来的指纹图像的失真对指纹识别性能的影响成为我们关心的问题。

在典型指纹库上测试我们的水印算法。实验指纹库有两个,分别用 db1 和 db2 表示。每个指纹库有 10 个类别,每个类别有 8 个指纹。db1 为 FVC2000[6] 的指纹库 1,图像大小为 300 × 300,256 级灰度图;db2 用 Veridicom 指纹鼠标[7] 采集,图像大小为 256 × 300,256 级灰度图。

表 1　db1 实验结果

| 压缩率/bpp | 平均识别率(%) | 平均拒识率(%) | 平均误识率(%) |
|---|---|---|---|
| 0 | 96.75 | 3.25 | 0 |
| 0.4 | 95.98 | 4.02 | 0 |
| 0.8 | 96.39 | 3.60 | 0.004 688 |
| 1.2 | 96.38 | 3.61 | 0.003 125 |
| 4 | 96.49 | 3.53 | 0.006 250 |

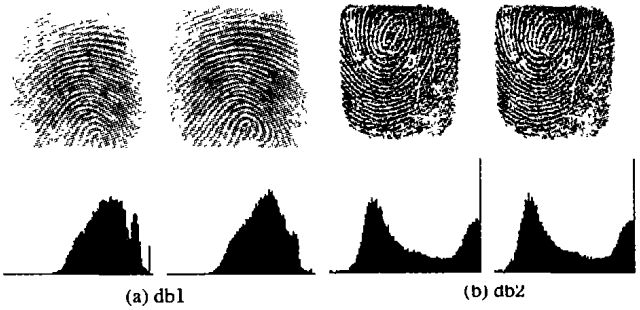
表 2　db2 实验结果

| 压缩率/bpp | 平均识别率(%) | 平均拒识率(%) | 平均误识率(%) |
|---|---|---|---|
| 0 | 98.86 | 1.14 | 0 |
| 2 | 98.86 | 1.13 | 0.001 563 |
| 2.4 | 98.85 | 1.15 | 0 |
| 2.8 | 98.85 | 1.15 | 0 |
| 4 | 98.89 | 1.11 | 0 |

对原始指纹图像采用三级小波分解,根据上面的水印容量计算公式,在 db1 和 db2 图像中嵌入最大量的水印数据(db1 嵌入 160 字节随机数据,db2 嵌入 130 字节随机数据),重复 10 次,分别得到 10 个压缩后的指纹库。

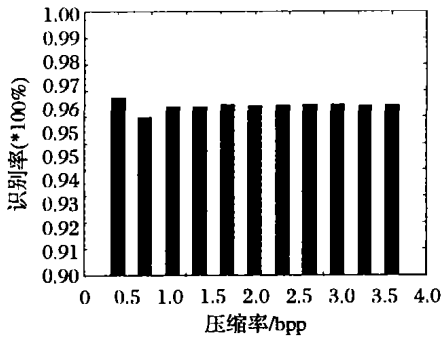
对每一个压缩后的指纹库,从中提取水印数据,并与嵌入的水印数据进行比较,验证算法能否无损提取水印信息。采用 Veridicom 的指纹识别软件,用原始指纹库中的每一个指纹作训练,用解压缩后的 80 个指纹作匹配,对 10 次结果统计识

别率、拒识率和误识率。

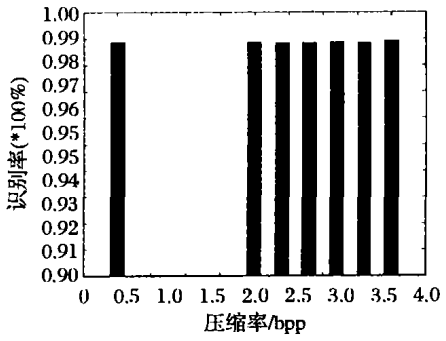


(a) db1 (b) db2

图5 db1 和 db2 类别一中两个指纹及直方图




(a) db1




(b) db2

图6 db1 和 db2 在不同压缩率下的平均识别率曲线
(0 bpp 表示原始指纹库下的识别率)

实验中发现,db1 和 db2 这两个指纹库具有很不同的性质。图5显示了它们类别一中两个指纹的直方图。db1 指纹库中指纹直方图很密集,而 db2 指纹库中指纹直方图很稀疏,因而影响了水印的嵌入能力。实验表明,我们的算法在 db1 上能获得比 db2 高很多的压缩率,db1 的指纹能压缩到原来的 1/20,而 db2 指纹只能压缩到原来的 1/4。

典型指纹库的实验数据表明,本文提出的基于 JPEG 2000 的实时量化水印算法能无损提取水印信息,同时对指纹识别没有产生太大的影响,即使有很小的误识率(6400 次识别中一次误识),也可以采取提高匹配阈值或三次验证的方法来提高系统性能。

## 3 结语

本文提出了一个新的在 JPEG 2000 压缩过程中嵌入量化水印的算法,并利用这个算法对我们原来的基于无损数字水印和指纹识别的网上身份认证系统进行了改进。

新系统水印信息在压缩过程中实时嵌入,能将 FVC2000 测试指纹图像压缩到 1/20,将采集的指纹图像压缩到1/4,缩短了用户交互的时间,提高了系统的交互性能,同时嵌入的水印信息能够无损提取,算法对指纹识别没有很大影响,系统的安全性得到了很好的保持。

实验中,发现两个不同的测试指纹库指纹图像具有不同的直方图特征,对水印嵌入能力和压缩率产生很大的影响,研究原始指纹图像不同的统计特性对于水印嵌入能力的影响将是下一步的工作。

**参考文献:**

[1] XUAN GR, ZHENG JX, YANG CY, *et al*. A Secure Internet-Based Personal Identity Verification System Using Loseless Watermarking and Fingerprint Recognition[A]. The 3rd International Workshop on Digital Watermarking (IWDW'04)[C]. Korea Seoul, 2004.

[2] XUAN GR, CHEN JD, ZHU J, *et al*. Distortionless data hiding based on integer wavelet transform[A]. Proceedings of IEEE Workshop on Multimedia Signal Processing (MMSP'02)[C]. IEE Electronics Letters, 2002, 38(25): 1646 - 1648.

[3] ISO/IEC 15444-1: Information Technology, JPEG 2000 image coding system, Part 1[S]. Core coding system, 2000.

[4] ADAMS MD. The JPEG-2000 Still Image Compression Standard[S]. ISO/IEC JTC 1/SC 29/WG 1 N 2412, 2002.

[5] MEERWALD P. Quantization Watermarking in the JPEG2000 Coding Pipeline[A]. Communications and Multimedia Security Issues of The New Century, IFIP TC6/TC11 Fifth Joint Working Conference on Communications and Multimedia Security[C], 2001.

[6] http://bias.csr.unibo.it/fvc2000/[EB/OL], 2005 - 01.

[7] http://www.veridicom.com[EB/OL], 2005 - 01.

(上接第 1749 页)

$B$ 发送消息 $B\{N_b\ A\ N_a\ X_b\{Y_b\}_{pk(A)}\}_{sk(B)}$, $sk(A) \notin k_\beta = k_\beta$,根据定理1,$Y_b$ 是机密的。

$A$ 发送消息 $A\{B\ N_b\}sk(A)$ 不涉及 $Y_b$,$Y_b$ 仍然是机密的。协议完成时 $Y_b$ 是机密的。

由上述机密性、认证性分析可知 BAN 修改后的 CCITTX.509(3)协议能提供保密性、认证性安全服务。

## 5 结语

串空间模型中的推理方法简洁直观,但串空间的理论框架不统一,而且有些协议特性仍不能以串的形式表达,有待进一步研究。

**参考文献:**

[1] THAYER FJ, HERZOG JC, GUTTMAN JD. Strand spaces: Proving security protocols correct[J]. Journal of Computer Security, 1999, 7(2,3): 191 ~ 230.

[2] THAYER FJ, HERZOG JC, GUTTMAN JD. Strand spaces: Why is a security protocol correct[A]. Proceedings of the 1998 IEEE Symposium on Security and Privacy[C]. Los Alamitos: IEEE Computer Society Press, 1998. 160 - 171.

[3] THAYER FJ, HERZOG JC, GUTTMAN JD. Strand spaces: Honest ideals on strand spaces[A]. Proceedings of the 1998 IEEE Computer Security Foundations Workshop[C]. Los Alamitos: IEEE Computer Society Press, 1998. 66 - 77.

[4] HOARE CAR. Communicating Sequential Processes[M]. Prentice Hall, 1985.

[5] SYVERSON PF, VAN OORSCHOT PC. A Unified Cryptographic Protocol Logic[R]. NRL CHACS Report 5540 - 227, 1996.