

联合可逆可见水印与数字指纹的文档图像 版权保护方案*

姜明芳** 张纳新

(湖南第一师范学院图书馆,长沙 410205)

摘要:为有效保护数字文档图像版权,设计了一种新的文档图像版权保护方案,利用可逆可见水印权衡文档共享与版权保护之间的矛盾,依靠用户身份信息的数字指纹追踪认证用户泄密行为。仿真实验表明,该方案具有较高的隐秘图像质量和可见水印清晰度,可应用于数字文档图像版权保护实践之中。

关键词:数字指纹;可逆可见水印;文档图像;版权保护

中图分类号:TP309.2 文献标识码:A doi:10.3969/j.issn.1006-6055.2014.06.007

Documental Image Copyright Protection Scheme Combining Invertible Visible Watermark and Digital Fingerprint*

JIANG Mingfang** ZHANG Naxin

(Library of Hunan First Normal University, Changsha 410205)

Abstract: To protect the copyright of digital documental images, a new documental image copyright protection scheme is proposed. The invertible visible watermark is used to achieve the balance between documental resources share and copyright protection. At the same time, a digital fingerprint sequence dependent of user information is used to trace traitors. Experiment results demonstrate the proposed scheme has high visual quality of watermarked images and good watermark visibility, and it can be applicable to copyright protection of documental images.

Key words: digital fingerprint; invertible visible watermark; documental image; copyright protection

1 引言

随着数字图书的飞速发展与广泛普及,数字图书馆已发展成为知识经济社会中主要的信息资源载体,也必将成为未来社会的公共信息中心和枢纽。它是传统图书馆在信息时代的发展,向社会公众提供综合的公共信息访问服务^[1]。然而,数字图书馆建设的根本点在于信息数字化,各种资源的数字化为信息的整合、处理与利用提供了方便,使得读者可简便有效地进行文献检索与利用。但与此同时,信息处理技术和网络技术的高速发展,使文献资源的格式转换,数字化作品的复制、下载、盗版等变得更加容易,数字化作品的版权保护问题也日渐复杂和突出^[2]。近年来,数字水印技术作为一种数字媒体版权保护的有效手段,得到了较好的发展。其中,可

见水印作为一种特殊的数字水印,以可见方式将水印信号嵌入到原始媒体,半透明浮现于媒体之中,不需要水印检测,就能为数字媒体提供简单而直观的版权告示,由此引起了一些研究人员的关注^[3]。但通常的可见水印图像版权保护方案所嵌入的可见水印不可逆,难以满足特定用户对数字媒体的高质量浏览需求^[4]。而已有的可逆可见水印方案虽然允许合法用户去除可见水印,却不能追踪合法用户对去除水印后的数字图像资源的未认证再次传播^[5,6]。朱从旭等^[7]提出一种多功能图像水印系统模型,利用统一混沌系统和提升小波变换先后在图像空域和小波域嵌入可见水印与不可见水印,从而实现版权告示与非法拷贝追踪,但该方案的可恢复图像质量欠佳。虞晓庆^[8]提出一种基于提升小波的多功能图像双水印算法,在彩色图像蓝色分量 B 的低频系数上嵌入版权水印,由绿色分量 G 生成的认证水印嵌入在量化后的提升小波系数上。该算法可实现版权保护与图像篡改检测和定位,却不能实现违法追踪功能。

为综合权衡数字媒体版权保护与用户高质量浏

2014-05-12 收稿,2014-06-18 接受

* 国家自然科学基金(61073191),教育部人文社会科学研究青年项目(10YJC870014),湖南省哲学社会科学基金(11YBA090),湖南省教育厅科学研究重点项目(12A029)资助

* 通讯作者,E-mail:mingfangjean@gmail.com;Tel:0731-82841021

览需求,并有效追踪合法用户的未认证传播,本文提出一种联合可逆可见水印与数字指纹技术的文档图像资源版权保护方案。

2 文档图像版权保护方案

为确保在保护数字媒体的同时,实现数字媒体视觉质量分级浏览和用户违法行为追踪,本文在有效结合可逆可见水印与数字指纹技术的基础上,设计了一种新的文档图像版权保护方案。其基本思路为:文档图像由服务器端统一加载可见水印;用户欲获取高质量文档图像时,服务器可根据用户请求,在用户密钥控制下去除其中的可见水印,并在嵌入用户数字指纹后再下发给用户。

2.1 可见水印嵌入

任何版权所有者上传文档图像资源至数据库,都将由服务器在文档图像中嵌入可见水印,以宣示所有者版权。

步骤 1:由用户指定文档图像 I 中可见水印嵌入区域,并将可见水印 W 缩放为指定嵌入区大小,生成待嵌入可见水印 W' 。

步骤 2:考虑到文档图像中存在大面积的高亮度和低灰度平滑区,可见水印嵌入时应使低灰度区有亮水印,高亮度区有暗的可见水印。若已知灰度 t ,灰度变换双射函数 f 可定义为

$$f(t) = \begin{cases} t + 128 & \text{if } t < 128 \\ 255 - t & \text{if } t \geq 128 \end{cases} \tag{1}$$

步骤 3:对二值水印图像进行 JBIG 无损压缩和公钥加密处理,获得加密水印信号。

步骤 4:将水印嵌入区坐标与加密水印信号一起无损隐藏^[9]在文档图像中,获得含可见水印的隐秘图像 I_1 。

2.2 可见水印去除

对于拥有正确密钥的认证用户,应允许其删除隐秘文档图像中的可见水印,以浏览高质量文档图像资源。其实施过程如下:

步骤 1:首先从隐秘文档图像中无损恢复出水印嵌入区坐标与加密水印信号。

步骤 2:认证用户利用私钥对加密水印信号进行解密与解压缩,从而获得可见水印信号 W 。

步骤 3:根据恢复出的坐标信息得出水印嵌入区大小,将可见水印 W 缩放至水印嵌入区大小,得水印信号 W' 。

步骤 4:对水印信号‘0’对应的隐秘文档图像灰度值 t 做如下的逆映射,即可去除隐秘图像中的可见水印从而恢复原始文档图像。

$$f^{-1}(t) = \begin{cases} 255 - t & \text{if } t < 128 \\ t - 128 & \text{if } t \geq 128 \end{cases} \tag{2}$$

2.3 数字指纹嵌入

为防止认证用户在去除可见水印后,未经许可非法传播给其他未认证用户,服务器端在给认证用户下发高清文档图像时,应事先嵌入数字指纹以追踪用户的违法行为。

步骤 1:利用混沌映射将用户身份信息调制成二值数字指纹序列 H 。

步骤 2:鉴于人眼对高亮度和低亮度区域灰度变化不敏感,仅对中等亮度改变较为敏感,图像亮度敏感性可由式(3)近似计算。

$$\alpha(i) = \frac{|I(i) - 127.5|}{127.5} \tag{3}$$

进一步将 α 归一化到区间 $[a,b]$ (实验中取区间 $[5,45]$),得到自适应量化步长 $\Delta(i)$ 。

步骤 3:通过量化索引调制^[10],将数字指纹 $h(i)$ 嵌入到恢复图像中,得到隐秘文档图像 I_2 。

$$I_2(i) = \begin{cases} \left[\frac{I(i)}{\Delta(i)} \right] \times \Delta(i) + \frac{\Delta(i)}{3} & \text{if } h(i) = 0 \\ \left[\frac{I(i)}{\Delta(i)} \right] \times \Delta(i) + \frac{2}{3}\Delta(i) & \text{if } h(i) = 1 \end{cases} \tag{4}$$

其中,方括号 $[\]$ 表示四舍五入运算,以下同。

2.4 指纹判决与违法追踪

对于任何待检文档图像资源,可提取数字指纹,以判决用户行为是否违法。

步骤 1:使用与数字指纹嵌入过程相同的方法构造指纹序列 H 和计算自适应量化步长 $\Delta(i)$ 。

步骤 2:根据待检文档图像灰度值所属区间来提取指纹信息,如式(5)所示,

$$h'(i) = \begin{cases} 0 & \text{if } I_2(i) < \left[\frac{I'_2(i)}{\Delta(i)} \right] \times \Delta(i) + \frac{\Delta(i)}{2} \\ 1 & \text{if } I_2(i) \geq \left[\frac{I'_2(i)}{\Delta(i)} \right] \times \Delta(i) + \frac{\Delta(i)}{2} \end{cases} \tag{5}$$

步骤 3:将构造指纹 H 与提取数字指纹 H' 进行相似性比较^[10],若相似性值大于阈值 T ,即可认定该用户为共谋者。

3 性能测试

实验中用 256 × 256 的文档图像为测试图像,可见水印为 128 × 128 大小的二值图像(如图 1 所示)。仿真实验针对不同类型文档图像进行测试。图 2 给出了两幅不同类型测试文档图像。图 3 是嵌入可见水印的隐秘图像效果,从中可以清晰地辨别出可见水印的存在,同时又不影响对文档图像的初步浏览使用。这说明该方案生成的隐秘文档图像具有较好的视觉质量和较高的水印可见性。在无需可见水印的条件下,认证用户使用正确密钥即可擦除可见水印,擦除水印后效果如图 4 所示,其峰值信噪比(PSNR)达 63.0 dB 以上(由于灰度双射函数的可逆性,可见水印是可完全去除的,即可无损恢复原始图像,PSNR 值应为无穷大。但由于服务器下发文档图像资源时嵌入了用户数字指纹,所以恢复文档



图 1 可见水印图像
Figure 1 Visible watermark image

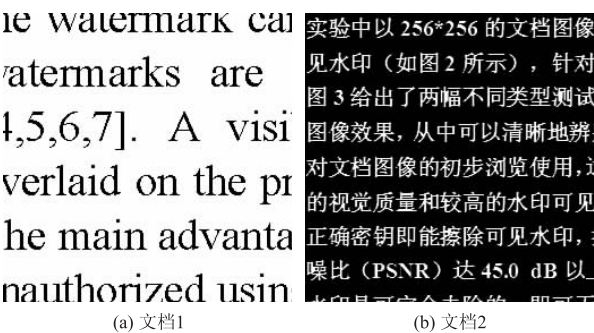


图 2 测试文档
Figure 2 Test documents

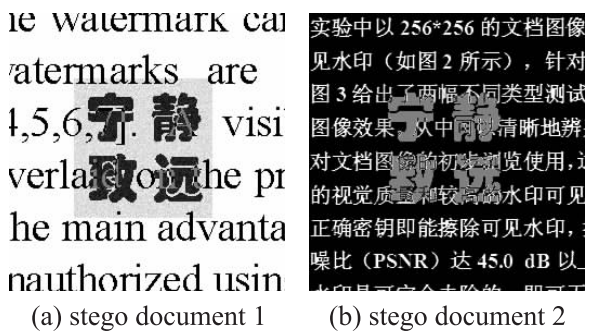


图 3 隐秘文档图像
Figure 3 Stego documental images

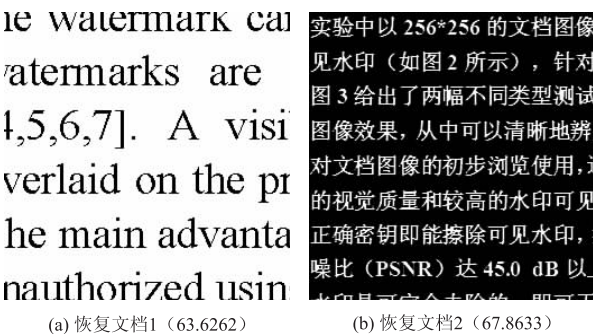


图 4 可见水印去除(正确密钥)
Figure 4 Visible watermark removal with correct key

表 1 不同方案恢复图像质量比较(dB)
Table 1 Visual quality comparison of restored image under different schemes(dB)

	文献[7]	本文方案
Lena	39.78	61.28
Baboon	39.12	61.03
F-16	39.24	58.52
Barbara	39.70	59.81
文档 1	39.15	63.63
文档 2	38.67	67.86
平均	39.28	62.02

图像 PSNR 值不为无穷大)。针对一些典型的文档测试图像,表 1 列出了不同方案的恢复图像质量比较。从中可以发现,相对于朱从旭等方案^[7],本文方案恢复图像 PSNR 值平均高出约 22.70 dB。

为验证方案安全性,图 5 给出了试图使用错误密钥去除可见水印后的文档图像,此时 PSNR 值在 15.0 dB 以下,可见未认证用户无法有效去除隐秘文档图像中的可见水印。与已有可擦除可见水印算法^[6]的安全性能比较如表 2 所示。表 2 中的测试结果表明,在未获得正确密钥的情况下,本文方案去除水印后的图像 PSNR 值平均仅为 14.46 dB,远低于文献^[6]方案的 32.55 dB。这说明无正确密钥的用户更难以去除其中的可见水印。

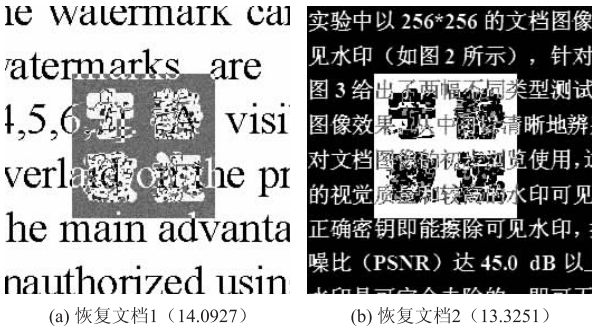


图 5 可见水印去除(错误密钥)
Figure 5 Visible watermark removal with wrong key

表 2 未认证用户原始图像恢复效果比较(dB)

Table 2 Visual quality comparison of restored image under different schemes for unauthorized users(dB)

	文献[6]	本文方案
Lena	33.21	14.56
Baboon	32.85	15.20
F-16	32.37	14.33
Barbara	32.49	15.25
文档 1	32.42	14.09
文档 2	31.96	13.35
平均	32.55	14.46

指纹判别有效性实验从 20 个认证用户中随机选取两个用户为合谋者,两名合谋者拟采用平均攻击方式生成合谋的文档图像内容。依据伪造文档图像构造指纹 H 提取数字指纹 H' ,并计算相似性,该方案成功检测到合谋者的概率如图 6 所示。在水印信噪比(Watermark to Noise Ratio)高于 -10dB 时,合谋用户正确检测率高达 99% 以上。这说明本文方案能跟踪到认证用户的合谋行为,对平均攻击具有一定的鲁棒性。

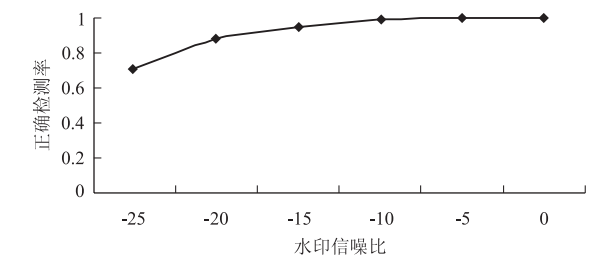


图 6 抗合谋攻击性能

Figure 6 Performance against collusion attack

4 结论

本文结合可逆可见水印与数字指纹技术,设计

了一种新的文档图像版权保护方案。通过嵌入可见水印来宣示文档图像版权,仅允许拥有正确密钥的认证用户有效去除隐秘文档图像中半透明呈现的可见水印,以阻止非认证用户获得无水印文档图像版本。同时,通过嵌入其中的数字指纹可追踪合法用户的泄密行为。实验结果表明,该方案生成的隐秘文档图像视觉效果好、可见水印清晰度高,可较好地应用于数字图书馆中的数字资源安全通信。

参考文献

[1]黄立冬. 国家数字图书馆建设模式新探[J]. 情报资料工作, 2013,(2):109-112.

[2]张立彬,贾鑫,董亚男. 数字图书馆版权保护的技术措施及其发展趋势[J]. 情报科学,2012,30(10):1 471-1 477.

[3]赵星阳,孙继银. 一种可抗二值化攻击的文本图像可见水印算法[J]. 计算机应用,2009,29(1):165-167.

[4]计云倩. 基于可见水印的古籍图像版权保护技术研究[D]. 苏州:苏州大学,2010.

[5]姜明芳. 基于自适应可见水印的文档资源版权保护机制[J]. 情报杂志,2011,30(12):165-170.

[6]YANG Y,SUN X M,YANG H F,et al. Removable visible image watermarking algorithm in the discrete cosine transform domain [J] Journal of Electronic Imaging,2008,17(3):033008.

[7]朱从旭,陈志刚. 一种安全多功能图像水印系统模型与算法[J]. 中国图象图形学报,2008,13(5):894-899.

[8]虞晓庆,李宏昌,张茂. 基于提升小波的多功能彩色数字图像双水印算法[J]. 计算机应用与软件,2013,30(2):50-53.

[9]张晓杰,童学锋,宣国荣,等. 基于预测误差和直方图对的无损数据隐藏方法[J]. 计算机应用,2012,32(11):3 125-3 128.

[10]郑旭平. 抗合谋攻击的量化数字指纹技术研究[D]. 上海:上海交通大学,2012.

作者简介

姜明芳(1979-),女,硕士,馆员,主要研究方向:信息安全、多媒体技术、数字图书馆技术;

张纳新(1969-),女,本科,馆员,主要研究方向:信息管理、图书馆学理论。