一种基于余数判决的数字水印算法

王东建, 蒋铃鸽, 何 晨
(上海交通大学电子工程系, 上海 200030)

摘 要: 本文给出了一种新型的鲁棒水印算法. 首先选择一个混沌映射来置换水印数据和载体图像, 以取得很好的置换效果. 与现有其它空间域算法不同, 本方案不直接修改单个象素的灰度值, 而是根据提出的严格余数条件, 重新设置载体图像象素间的灰度关系以实现水印数据的嵌入. 并根据余数判决准则, 利用基于空间域的纠错技术进行水印提取. 仿真实验表明, 该水印算法在保证载体图像质量的同时, 具有较强的鲁棒性: 在用 JPEG 将载体图像压缩到 27. 4% 时仍能提出可识别的水印信息, 并且能有效地抵抗加性高斯白噪声的干扰, 在同步条件下对剪切、缩放、旋转等几何攻击也具有较好的鲁棒性.

关键词: 余数判决; 水印纠错; 混沌置换; 鲁棒水印
中图分类号: TP309 文献标识码: A 文章编号: 0372-2112 (2004) 07-1099-04

A Watermark Algorithm Based On Remainder Decision

WANG Dong-jian, JIANG Ling-ge, HE Chen
(*Dept. of Electronic Eng., Shanghai Jiaotong Univ., Shanghai 200030, China*)

Abstract: A novel robust watermarking scheme is proposed, in which a permuted watermark is embedded into a permuted image. We use a chaotic map to permute the image and the watermark data. and embed the watermark by resetting the relationship of the pixels instead of changing the pixels individually. A novel idea of remainder decision and a spatial-based error correcting is realized with good performance in the extracted phase. The watermark embedded to the image is imperceptible and the extracted watermarks are still recognizable when JPEG compression ratio reaches 27. 4% or after severe zero-mean AWGN pollution. If well synchronized, this algorithm can also have good robustness to geometrical attacks such as cropping, scaling and rotating.

Key words: remainder decision; error correct; chaotic permuting; robust watermark

1 引言

数字水印作为密码技术的有效补充, 在版权保护、身份认证等方面有着很大的应用潜力, 因而得到广泛的研究. 然而, 一般的算法不能很好的抵抗常见的图像 JPEG 压缩以及加性高斯白噪干扰, 至今还没有一套公认的比较安全实用的水印系统. 按照水印嵌入方法的不同, 可以把水印分为两大类: 基于空间域的数字水印和基于变换域的水印, 本文给出一种基于空间域的鲁棒性较强的水印算法[1]. 根据给出的严格余数条件重新设定载体图像象素之间的灰度值关系以嵌入水印, 而用余数判决准则实现水印数据的提取, 这与以往那些通过直接修改载体图像比特位的方法相比, 既兼顾了水印对图像质量的影响, 又能提高水印的鲁棒性. 文献[2]中提出用加纠错码的方法来提高水印的鲁棒性, 但是增加了水印数据的冗余量, 这样一方面会对图像质量有较大影响, 更重要的是这些纠错比特本身也可能被攻击, 因而对水印鲁棒性提高有一定的限制. 本文提出了一种稳健性较高的基于空域的纠错方法, 并将该方法与余数判决准则相结合, 从而很大程度地提高了系统的鲁棒性. 图 1 中给出了本水印系统的大致流程图.

2 水印算法

载体图像为 $M_1 \times M_2$ 个象素大小, 每个象素为 0~255 灰度等级的灰度图像; 水印为 $N_1 \times N_2$ 象素的黑白图像, 每个象素为 0、1 两种取值. 一般讲, 水印数据要远小于载体图像. 将载体图像分割成 $b \times b$ 大小的小块, 分别进行处理. 用 G 和 $G(i, j)$ 来分别表示载体图像及其在 (i, j) 位置处的灰度值, 用 B 和 $B(m, n)$ 分别表示每个 $b \times b$ 大小的载体图像块和块内 (m, n) 位置的灰度值, 而用 W 来表示水印图像.

2.1 置换技术

考虑 Logistic 映射: $x_{n+1} = \mu x_n(1 - x_n)$, $0 < x_n < 1$, 当 $3.6 < \mu < 4$ 时, 迭代产生的序列 x_n 具有混沌特性[3]. 根据如下步骤来完成对 G 的置换: (1) 取 $\mu = 3.93$, $x_0 = 0.711$, 生成一个 $M_1 \times M_2$ 长度的数列; (2) 根据 G 的大小将该数列的每个元素 x_n 从小数点向后展开为一个 $\log_2(M_1 \times M_2)$ 位的二进制序列,

收稿日期: 2002-12-02; 修回日期: 2003-11-14
基金项目: 国家"十五"863 计划(No. 2002AA144110)

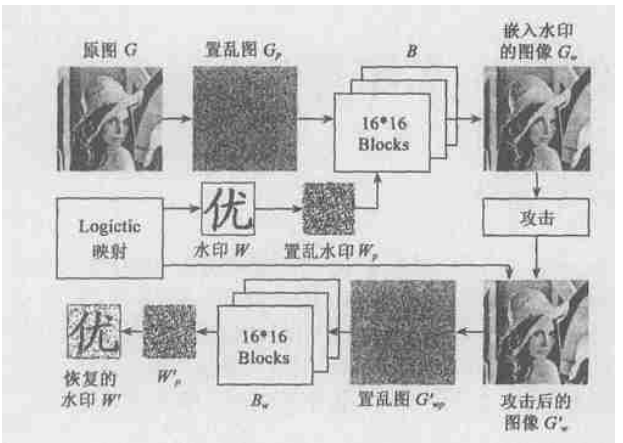

图 1 水印系统流程图

并将前后 $\log_2(M_1)$ 和 $\log_2(M_2)$ 位分别转化为 0~ (M_1-1) 和 0 ~ (M_2-1) 范围的两个随机数; 将该随机数对顺序记录到一个位置数列中, 从而形成一个长度为 $2\times M_1\times M_2$ 的数列 X; (3) 置换过程中, 对 G 的每个象素以及数列 X 进行遍历, 对图像的每个象素从 X 中连续两个元素分别作为该象素目标位置的横纵坐标值, 然后将该象素与新坐标处的象素进行互换, 遍历完成后就可以获得置换过的图像 G_p. 在置换图像 G_p 中嵌入水印后, 采用与步骤(3) 中顺序相反的遍历过程, 利用 X 将置换图像恢复到加过水印的图像 G_w, 称其为逆向置换过程.

参数 μ 和映射初值 x_0 将被作为密钥进行分发, 而没有必要将整个随机序列传送; 同时, 根据混沌系统的初值敏感效应, x_0 的稍微扰动其生成的随机序列差异会很大, 因而是很安全的. 根据人眼的视觉特性, 对载体图像的置换将水印数据的能量分散到载体图像的各个部分, 从而使加过水印的图像主观降质很小(水印能量集中会影响图像的可读性); 同时, 对载体图像和水印的置换过程需要通过密钥来控制, 从而保证水印系统的安全性.

2.2 水印嵌入与提取

文献[3] 等将水印信息嵌入到图像象素的某个中间比特位. 由于没有考虑低位数据对加水印位的影响, 例如: 如水印加在某个象素的第五位, 该象素二进制表示为(01101111), 现在如果对该象素的灰度值加 1 就使灰度值变成(01110000), 加入的水印信息位就由 0 变成为 1, 所以这种算法抗攻击的能力很不稳定. 本文通过重新设定载体图像象素之间的灰度关系来嵌入水印, 从而灵活地解决了这一问题.

为了描述方便, 在附录中给出了几个定义, 由定义 1~ 5, 有:

定理 1 若满足 $[B(m_1,n_1),B(m_0,n_0),B(m_2,n_2)]^M$, 象素 $B(m_1,n_1)$ 和 $B(m_2,n_2)$ 在受到其原始值为中心的轻微扰动, $B'(m_1,n_1)=B(m_1,n_1)+\Delta_1$, $B'(m_2,n_2)=B(m_2,n_2)+\Delta_2$, 如果满足条件: $|\Delta_1|+|\Delta_2|<M/2$, 则 $B'(m_1,n_1)$ 和 $B'(m_2,n_2)$ 相对基准点 $B(m_0,n_0)$ 仍满足准余数条件, 即 $\langle B'(m_1,n_1),B(m_0,n_0),B'(m_2,n_2)\rangle^M$. (证明参见附录)

准则 受到扰动后的 $B'(m_1,n_1)$ 和 $B'(m_2,n_2)$ 满足 $\langle B'(m_1,n_1),B(m_0,n_0),B'(m_2,n_2)\rangle^M$, 根据似然准则, 判定扰动前满足 $[B(m_1,n_1),B(m_0,n_0),B(m_2,n_2)]^M$, 称该准则为余数判决准则.

在本水印方案中, 根据要嵌入的水印数据来选取不同相对位置的点作为 $B(m_1,n_1)$ 和 $B(m_2,n_2)$, 并采用定义 5 的余数设定操作实现水印数据嵌入; 在水印提取时, 根据余数判决准则来预测水印嵌入阶段的设定, 从而提取出水印数据.

2.2.1 水印嵌入

第一步 对载体图像和水印分别进行混沌置换, 生成了置换后的图像 G_p 和 W_p; G_p 被分成 $b\times b$ 的块, W_p 则展开成一行.

第二步 从上向下依次选取每个 $b\times b$ 的块进行水印嵌入, 每块中最多嵌入 $2\times(b-1)$ 个比特的水印, 直到嵌完为止(根据水印数据的不同, 有可能最后一个块中加的水印比特数小于 $2\times(b-1)$ 比特). 对每个 B, 取 $B_p=B(u,u)$, $u=b/2$ 作为基准点, 用余数设定操作来嵌入水印数据. 为了使基准点在受到攻击时对检测不产生影响, 我们将其后 5 位的数据透明化, 即用 $B_p=B(u,u)-B(u,u)_{(mod\ 32)}$ 作为参考值, 从而保证了基准值的可靠性. 当 $b=16$ 时, 即载体图像被分割成 16×16 的小块, 具体的处理过程如下(k 的初值取 1, 用来遍历水印信息 W_p):

For $j=1$ to 7

If $W_p(k)=1$ Then set $[B(u,u-j),B_p,B(u,u+j)]^M$

Else set $[B(u,u+j),B_p,B(u,u-j)]^M$ end; $k=k+1$;

If $W_p(k)=1$ Then set $[B(u-j,u),B_p,B(u+j,u)]^M$

Else set $[B(u+j,u),B_p,B(u-j,u)]^M$ end; $k=k+1$; End.

可见, 若水印数据为 1, 则设定左(上) 方的象素为 $B(m_1,n_1)$, 右(下) 方的象素为 $B(m_2,n_2)$; 反之右(下) 方的象素为 $B(m_1,n_1)$, 左(上) 方的象素为 $B(m_2,n_2)$. 对其它块也进行类似处理直到水印数据全部嵌入完毕, 因此获得了含水印数据的小块 B_w.

第三步 将各 B_w 块组合起来, 并使用逆向置换方法生成加过水印的载体图像 G_w.

2.2.2 水印提取 G_w 在发行过程中可能受到一些攻击(包括无意的和恶意的), 接收到的图像记为 G'_w. 为了在水印受到有限攻击时仍然要能提出可识别的水印信息, 水印提取算法如下:

第一步 与水印嵌入过程第一步类似, 先将 G'_w 转换得到 G'_{wp}. 然后同样将其分割成 $b\times b$ 象素的块 B_w. 每块按照水印嵌入时的处理顺序, 根据余数设定操作和余数判决准则(准则 1) 来判定对应位置对称点相对基准点的关系, 从而判定所嵌入的水印比特, 提取水印数据 W'_p.

第二步 将 W'_p 变为原来的 $N_1\times N_2$ 形状, 并且使用逆向置换方法, 得到可视域的水印图像 W'.

由于载体图像可能受到干扰, W' 相对原来的水印图像 W 可能有些错误, 但只要错误少于一定的比例, 得到的 W' 还是可识别的, 就认为是有效的.

3 仿真实验及结果分析

采用 512× 512 象素的 Lena 图作为载体图像, 水印是 64×

64 的二值图像. 载体图像被分割成 16× 16 大小的块, 每个小块中最多嵌入 14 个比特的水印信息, 模 M 取 32.

为了客观地衡量图像降质和水印质量, 参考文献[3] 定义两个评价图像的客观指标, 峰值信噪比和数据失真率. 图像 G_w 相对图像 G 的峰值信噪比(Peak signal-to-noise ratio, PSNR):

$$\mathrm{PSNR}=-10\lg\left(\frac{1}{255^2\times M_1\times M_2}\left(\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}(G_w(i,j)-G(i,j))^2\right)\right)$$

提取的水印数据 W' 相对原始水印数据 W 的失真率 DR(Distortion Ratio):

$$DR\equiv\frac{1}{N_1\times N_2}\sum_{i=1}^{N_1}\sum_{j=1}^{N_2}|W'(i,j)-W(i,j)|\times 100\%$$

以上只是两个客观指标, 可以用来作为参考, 实际应用中还要结合主观指标.

图 2　(a) 原图像, (b) 水印, (c) 水印嵌入后的图像, (d) 图像未受攻击时提取的水印

图 2 中分别给出了载体图像、水印图像、嵌入水印后的图像以及没有受攻击时从中提出的水印图像. 嵌入水印后的图像降质人眼无法察觉, 其峰值信噪比(PSNR) 保持在 42 左右; 水印算法完全可逆, 在没有受到攻击时是能够完全无误地提出水印信息.

表 **1**　水印在 JPEG 压缩和 AWGN 攻击下的失真率

File size(KB)	169	98.3	64.0	46.3	42.6
Ratio(%)	100	58.17	37.87	27.4	25.2
DR(%)	0	0	5.371	24.14	28.101
AGWN δ^2	6.5	13.0	26.0	52.0	65.0
DR(%)	0.00	0.391	5.542	19.873	28.027

根据文献[5] 中列出的常见水印攻击方法, 表 1 中给出了加过水印后的图像在经过不同程度的 JPEG 压缩和零均值加性高斯白噪声(AWGN) 污染后提出的水印失真率. 载体图像被压缩到原来 JPEG 文件大小的 27.4%(文献[3] 中能抵抗 39%JPEG 压缩) 以及当加性高斯白噪声(AWGN) 的方差达到 52 时仍然能奶有效地提取出可以识别的水印, 而此时污染过的图像已经不再适于观看. 图 3 给出了在同步条件下, 经过剪切、缩放以及旋转等几何攻击后的载体图像及从中提取的水印. 本水印算法在水印同步条件下能够对一般几何攻击具有鲁棒性, 由于对载体图像和水印数据进行了置换, 剪切后图像中提取的水印仍然相对完整(否则, 水印数据会成块丢失).

总结该算法: (1) 使用混沌序列来构造的置换算法具有很好的置换效果, 利用人眼主观视觉特性使嵌过水印的图像看不出降质, 而且保证系统安全性及水印数据的完整性. (2) 水印信息的嵌入不再是直接嵌入到载体图像的单个象素的灰度值, 而是使象素间的灰度差值满足预先设定的严格余数条件, 从而设定一个确定的相对距离(克服了直接改比特位方法容错能力不确定的缺陷) 来容纳一定的污染, 这对使算法对噪声干扰具有较好鲁棒性[4]. (3) 利用空间纠错的思想加入数据冗余, 一个水印比特同时改动了两个象素的灰度; 提取时, 只要这两个象素灰度值扰动绝对值得和小于 $M/2$, 就能使之相对基准点仍满足准余数条件, 从而根据余数判决准则对该比特水印做出正确的判决. 当然, 它也是以一定的数据冗余为代价的, 但与直接加纠错码相比具有更好的稳健性能[2]; 而且这种纠错技术与上面的余数判决准则紧密结合在一起加以实现, 并且充分考虑了载体图像资源, 因而不同于通信中的纠错码(ECC). (4) 在水印同步条件下, 算法在对几何攻击具有一定的鲁棒性.

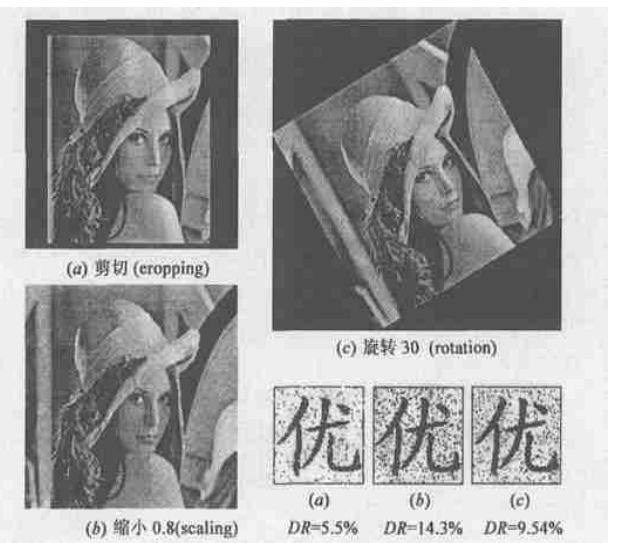

图 3　几何攻击后图像及提取的水印

4　结论

本文给出一个鲁棒性强的空间域水印算法. 给出一种基于混沌映射的置换方法, 并引入余数判决准则和空间域纠错的思想, 从而有效地提高水印系统的安全性和鲁棒性. 仿真实验表明, 本算法能够有效抵抗 27.4% 的 *JPEG* 压缩和较强高斯白噪声的干扰, 在同步条件下对剪切、缩放以及旋转等几何攻击具有一定的鲁棒性; 另外, 水印检测不需要原始图像信息, 这十分适用于网络环境的应用. 进一步的工作将把该算法扩展到变换域和视频图像中, 以期更好的综合效果.

附录:

定义 **1**　两个象素灰度值差值的绝对值称为两个象素之间的距离 d.

定义 **2**　若对两个非负整数 n_1, n_2 除以 M 所得余数分别为 r_1 和 r_2, 则称:

$$d^M(n_1,n_2)=\begin{cases}|r_1-r_2|, & |r_1-r_2|<M/2\\ M-|r_1-r_2|, & |r_1-r_2|\geq M/2\end{cases},$$

$$d^M\in\{0,M/2-1\},$$

$d^M(n_1,n_2)$ 为 n_1, n_2 在模 M 内的距离.

定义 **3** 如果象素 $B(m_1, n_1)$ 和 $B(m_2, n_2)$ 相对于基准点 $B(m_0, n_0)$ 的距离 d_1 和 d_2 分别满足 $d_1 \pmod M = 1$, $d_2 \pmod M = 1 + M/2$, M 为偶数, 则称象素 $B(m_1, n_1)$ 和 $B(m_2, n_2)$ 相对于点 $B(m_0, n_0)$ 满足模为 M 的严格余数条件, 记做 $[B(m_1, n_1), B(m_0, n_0), B(m_2, n_2)]^M$.

定义 **4** 象素 $B(m_1, n_1)$ 和 $B(m_2, n_2)$ 相对于点 $B(m_0, n_0)$ 的距离为 d_1 和 d_2, d_1、d_2 在模 M 内相对于 1 和 $(1 + M/2)$ 距离最小值 $d_{\min}$ 为 $\min(d^M(d_1, 1), d^M(d_1, 1 + M/2), d^M(d_2, 1), d^M(d_2, 1 + M/2))$. 若有 $d_{\min} = d^M(d_1, 1)$, 或 $d_{\min} = d^M(d_2, 1 + M/2)$, 则称 $B(m_1, n_1)$ 和 $B(m_2, n_2)$ 相对于基准点 $B(m_0, n_0)$ 满足准余数条件, 记作 $\langle B(m_1, n_1), B(m_0, n_0), B(m_2, n_2)\rangle^M$.

定义 **5** 操作 $\mathrm{set}[B(m_1, n_1), B(m_0, n_0), B(m_2, n_2)]^M$ 用于重新设定 $B(m_1, n_1)$ 和 $B(m_2, n_2)$ 的灰度值, 使相对基准点 $B(m_0, n_0)$ 满足模为 M 的严格余数条件, 并且, $B(m_1, n_1)$ 和 $B(m_2, n_2)$ 的修改尽量接近其原始值, 则称该操作为余数设定.

定理 **1** 证明 已知 $B'(m_1, n_1) = B(m_1, n_1) + \Delta_1$, $B'(m_2, n_2) = B(m_2, n_2) + \Delta_2$, $|\Delta_1| + |\Delta_2| < M/2$, 且有 $[B(m_1, n_1), B(m_0, n_0), B(m_2, n_2)]^M$, 则 $B(m_1, n_1)$ 和 $B'(m_1, n_1)$ 到 $B(m_0, n_0)$ 的距离分别为 $d_1 = k_1 M + 1$ 和 $d'_1 = k_1 M + 1 + \Delta_1$, 其中 $k_1 \in N$.

由定义 2, 得

$d^M(d'_1, 1) = |\Delta_1|$, $d^M(d'_1, 1 + M/2) = M/2 - |\Delta_1|$;

以及 $d^M(d'_2, 1) = M/2 - |\Delta_2|$, $d^M(d'_2, 1 + M/2) = |\Delta_2|$.

又因为 $|\Delta_1| + |\Delta_2| < M/2$, 则有 $d^M(d'_1, 1 + M/2) = M/2 - |\Delta_1| > |\Delta_2|$ 及 $d^M(d'_2, 1) > |\Delta_1|$.

若 $|\Delta_1| \le |\Delta_2|$, 则 $d_{\min} = |\Delta_1| = d^M(d'_1, 1)$; (a)

否则, $|\Delta_1| > |\Delta_2|$, 则 $d_{\min} = |\Delta_2| = d^M(d'_2, 1 + M/2)$; (b)

根据定义 4, 不管是 (a) 还是 (b), 都满足 $\langle B'(m_1, n_1), B(m_0, n_0), B'(m_2, n_2)\rangle^M$, 证毕.

参考文献:

[1] Yong Liang Guan, Jing Jin. An objective comparison between spatial and DCT watermarking schemes for MPEG video[A]. Proc Info Tech: Coding and Computing[C]. Las Vegas, NV, USA: 2001. 207- 211.

[2] Ching-Tang Hsieh, Yur-Lung Lu and etc. A study of enhancing the robustness of watermark[A]. Proc Multimedia Software Engineering[C], Taipei, Taiwan: MSE, 2000. 325- 327.

[3] Jui-Cheng Yen. Watermark embedded in permuted domain[J]. Electronics Letters, 2001, 37(2): 80- 81.

[4] Cohen A S, Lapidoth A. The Gaussian watermarking game[J]. IEEE Trans. on Information Theory. 2002, 48(6): 1639- 1667.

[5] 吴崇明, 王晓丹. 数字水印系统的鲁棒性和常见的攻击[J]. 空军工程大学学报(自然科学版), 2002, 3(1): 90- 94.

作者简介:

王东建 男, 1979 年 1 月生于江苏南通, 2002 年毕业于南京邮电学院, 获学士学位, 现为上海交通大学电子工程系硕士研究生, 主要从事数字水印以及无线通信信号处理方面的研究.

蒋铃鸽 女, 1959 年 9 月生于江苏省南京市, 1982 年 1 月毕业于东南大学无线电工程系无线电技术专业, 1993 年 9 月和 1996 年 9 月分别获得日本国立德岛大学电子系统工学硕士和工学博士学位; 现为上海交通大学电子工程系教授, 博士生导师, 主要研究领域为无线通信系统中的智能信息处理, 移动 IP 技术、数字水印及混沌理论在现代通信中的应用等, 已在国内外学术期刊和会议上发表论文 40 余篇.

何 晨 男, 1952 年 5 月生于江苏省苏州市. 上海交通大学教授, 博士生导师, 上海交通大学现代通信研究所副所长. 1982 年毕业于南京工学院无线电系, 获工学学士, 1985 年毕业于南京工学院通信与电子系统专业, 获工学硕士. 1994 年毕业于日本国立德岛大学研究生院通信与电子系统专业, 获工学博士. 目前的主要研究方向为新一代无线通信系统理论, 智能信息处理以及自适应信号处理在通信中的应用, 信息论与编码理论等.