

离散小波变换(DWT)域的公有水印技术研究*

Research on the Public Watermarking Technology Based on DWT

李陶深^{1,2},文志强²,兰红星²,陈松乔²

LI Tao-shen^{1,2}, WEN Zhi-qiang², LAN Hong-xing², CHEN Song-qiao²

(1. 广西大学计算机与电子信息学院,广西南宁 530004;2. 中南大学信息科学与工程学院,湖南长沙 410083)

(1. School of Computer, Electronics and Information, Guangxi University, Nanning, Guangxi, 530004, China; 2. School of Information Science and Engineering, Central South University, Changsha, Hunan, 410083, China)

摘要:通过在现有的公有水印模型中引入混沌系统,提出一种新的基于离散小波变换(DWT)域的公有水印技术.该技术在水印嵌入时,由混沌系统生成水印序列,并在离散小波变换的低频子带上嵌入水印,保证了水印的鲁棒性.实验分析不同指数因子嵌入水印的性能,结果表明:当指数因子在0.1~0.2之间时,嵌入水印的鲁棒性能比较好.

关键词:公有水印 鲁棒性 离散小波变换 混沌序列

中图法分类号:TP391 **文献标识码:**A **文章编号:**1005-9164(2006)04-0342-04

Abstract: By introducing chaos system in existing public watermarking model, a new public watermarking technology based on DWT is proposed. While embedding watermarking, the watermarking sequences are produced by the chaos system, and are embedded into the low frequent coefficient of DWT domain to guarantee the robustness of watermarking. In the experiment, the performance of watermark against attacks using the different index factors is analyzed and the experiment results show that the robustness of watermark is better when the value of index factor is between 0.1 and 0.2.

Key words: public watermarking, robustness, DWT, chaos sequence

近年来,数字水印技术逐渐成为国内外多媒体信号处理领域的一个研究热点.不可见性和鲁棒性是数字水印系统的两个最重要的特性.不可见性是指在宿主数字媒体中嵌入一定量的水印信息之后,不会引起原媒体明显的降质现象,隐藏数据不易觉察,即无法人为地看见或听见;鲁棒性是指数字水印必须对施加于宿主媒体的各种变换操作(如有损压缩、滤波等)具有免疫性,即水印信息不能因为施加于宿主媒体的某种变换操作而丢失.

公有水印是一类实际应用较常见而且实现起来

比较难的水印技术,它要求在提取水印时既不需要原始作品,也不需要原始水印,只需要原始密钥,该技术的难点在于水印的鲁棒性差.

人们对公有水印进行了研究,认为图像经离散余弦变换(DCT)或离散小波变换(DWT)后的系数服从高斯分布^[1],从而可实现一种公有水印技术.文献[1]实现的公有水印模型中假设水印序列 $W = \{w_1, w_2, \dots, w_M\}$ 是由一系列伪随机序列组成,每一个 x_i 服从均值为0,方差为1的正态分布.在检测水印时,需要使用嵌入时使用的水印序列.假如把水印序列看成是密钥的话,则该密钥太大,存储起来占用大量的存储空间,而且难于记忆.考虑到混沌系统具有形式简单、对初始条件敏感和具备白噪声的统计特性等,我们在混沌系统中引入公有水印模型,提出一种基于离散小波变换域的改进的公有水印技术,并通过实验对该技术的性能进行分析.

收稿日期:2006-05-16

修回日期:2006-09-19

作者简介:李陶深(1957-),男,教授,博士生,主要从事网络与信息安全、分布式数据库、网络路由算法研究工作.

* 国家自然科学基金项目(90104028)、广西留学回国人员科学基金项目(桂科回0342001)资助.

1 改进的公有水印模型

在改进的公有水印模型(图 1)中,当水印嵌入时,由混沌系统产生水印序列,并生成相应的密钥,在检测水印时只需要使用密钥和混沌系统,生成相应的水印序列就可以进行水印检测. 这样对于用户来说,只需要密钥就可以检测水印的存在,而不需要用大量的存储空间来存储水印序列,这就大大提高了水印技术的实用性. 另外,我们在嵌入水印时引入一个指数因子 r ,使

$$f_i = f_i + \alpha |f_i|^r w_i, \quad (1)$$

当 $r = 0$ 时,(1)式就是文献[2]给出的嵌入方法;当 $r = 1$ 时,(1)式就是文献[1]给出的嵌入方法;当 $r = 2$ 时,(1)式就是文献[3]给出的嵌入方法.

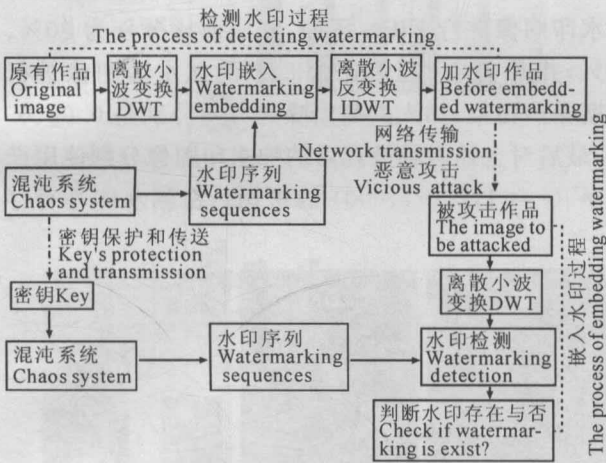


图 1 一种改进的公有水印模型

Fig. 1 A modified public watermarking model

2 公有水印嵌入方案

2.1 混沌序列的生成

混沌现象可以提供数量众多的、非相关的、类随机而又确定可再生的信号. 一类简单且被广泛研究的动力系统是 Logistic 映射:

$$x_{k+1} = 1 - \mu x_k^2, \quad (2)$$

其中, $\mu \in [0, 2]$, $x_i \in [-1, 1]$. 若参数 μ 被限制在 $[0, 2]$ 区间内, 则(2)式是一个从线段 $I = [-1, 1]$ 到它本身的非线性映射, 而且当 μ 逐渐增大时, 迭代出现多次突变. 当 $0 < \mu < 0.75$ 时, 迭代为稳定的 1 点周期; 当 μ 增大到 0.75 时, 迭代出现 2 点周期分岔; 当 μ 增大到 1.25 时, 出现 4 点周期分岔, 这种 2^n 倍周期分岔随 μ 的增大愈来愈快; 当 $\mu \rightarrow \mu_\infty = 1.40115$ 时, 迅速达到周期 $N \rightarrow \infty$, 即进入混沌状态.

根据 Logistic 映射序列的特性, 我们利用(2)式产生一系列 $x_i \in [-1, 1]$ 的混沌实数序列作为水印序列, 将产生这些序列的初始值、选取序列的起始位

置和水印序列的长度作为检测水印时所需要的密钥. 检测水印时, 利用密钥和相应的混沌系统, 就能产生和原始水印相同的水印序列.

2.2 水印嵌入位置的选择

选择离散小波变换系数的方法一般有低频^[4]、中频^[5]和高频^[6]3种. 如果水印嵌入在高频区, 虽然有较好的不可见性, 但是水印图像经过图像处理后很容易被删除, 其鲁棒性比较差; 如果将水印嵌入在低频区, 由于低频区中含有图像重要的信息, 一般的图像处理不会改变这部分数据, 因而嵌入的水印得到很好的保护, 提高了水印的鲁棒性; 在嵌入水印过程中如果要修改低频系数, 那么对图像的重要信息将会造成破坏, 因此, 人们采用折中的办法, 即选择中频系数, 这样可以在不可见性与鲁棒性之间求得平衡. 文献[6]认为, 为了使水印更强壮, 水印必须嵌入在图像信息最重要的地方, 因为如果水印嵌入在不重要的地方, 将容易引起有意识的或无意识的删除, 图像压缩技术会导致水印难于提取出来.

为了保证水印的鲁棒性, 我们采用在离散小波变换的低频域嵌入水印的方法. 为了减少嵌入水印对图像视觉的影响, 我们对图像进行 l 层分解, 则选择在第 $l-1$ 层的 HH_{l-1} 方向上嵌入水印.

2.3 水印的嵌入

水印序列是均值为 0 的伪随机序列, 设 $W = \{w(i, j) \in [0, 1], 0 \leq i < M_1, 0 \leq j < M_2\}$. 对原始图像 I 进行 l 层离散小波变换, 则设变换后子带系数为 $f_{m,k}(i, j)$, m 表示变换的层数 ($m = 0, 1, 2, \dots, l-1$), k 表明 m 层子带的方向 ($k = LH, HL, HH$), 选取低频域 HH 方向的系数即 $F = \{f_{l-1, HH}(i, j)\}$ 作为嵌入水印的系数 (这里系数 F 的个数应与水印序列 W 的个数相等). 由:

$$f'_{M, HH}(i, j) = f_{M, HH}(i, j) + \alpha \times |f_{M, HH}(i, j)|^r \times w(i, j) \quad (3)$$

嵌入水印. (3) 式中, $f'_{M, HH}(i, j)$ 为嵌入水印后的小波系数; α 为嵌入因子, 决定了水印嵌入的深度; r 为引入的指数因子, 当 $0 \leq r \leq 2$ 时, r 值对水印抗攻击鲁棒性的影响.

2.4 水印嵌入算法

步骤 1 对(2)式选取 $\mu = 2$, 循环生成混沌序列 $z(n) (n = 1, 2, \dots, M_n)$, 从 $z(\lambda)$ 开始取 $M_1 \times M_2$ 个元素构成 $M_1 \times M_2$ 的矩阵 $w(i, j)$ (设水印序列的长度为 $M_1 \times M_2$). $z(0)$, λ 和 $M_1 \times M_2$ 就是检测水印时的密钥.

步骤 2 计算 l 的值, 对图像 I 进行 l 层离散小波变换, 然后提取出低频域 HH 方向的系数 (即 $F =$

$\{f_{i-1,HH}(i,j)\}$) 作为待嵌入水印的系数。

步骤 3 根据(3)式嵌入水印。

步骤 4 对图像进行 l 层离散小波反变换 (IDWT), 变换到原来的空间域, 这样就得到加水印图像 I' 。

3 公有水印检测方案

3.1 水印的检测方法

设被检测图像为 I^* , 对 I^* 进行相应的离散小波变换并提取出相应的嵌入了水印的系数 $\{f_{i-1,HH}^*(i,j)\}$, 设 $Y = \{y(i,j)\} (0 \leq i < M_1, 0 \leq j < M_2)$ 为用来检测的伪随机序列, 然后根据

$$Z = \frac{1}{M} \sum_{i=0}^{M_1} \sum_{j=0}^{M_2} |f_{M,HH}^*(i,j) \times y(i,j)| \quad (4)$$

计算 Z 值 (在这里, (4) 式称作线性检测器, 式中, $M = M_1 \times M_2$, 而 Z 值称作线性检测器的输出响应值), 再与阈值 $Thres$ 进行比较. 当 $Z \geq Thres$ 时, 则认为检测到水印, 否则认为没有检测到水印。

3.2 阈值的确定

为了简单起见, 假设图像 I^* 没有受到攻击, 那么在检测的过程中只会有 3 种情况出现: ① 图像 I^* 没有嵌入水印, 即 $W = \Phi$; ② 嵌入了水印序列 Y , 即 $W = Y$; ③ 嵌入了不同于 Y 的水印序列的 W , 即 $W \neq Y$. 这 3 种情况可以用 (5) 式进行分析, 其值可以用来替代 Z . 这里使用 (3) 式嵌入的水印分别为 Φ 、 Y 和 W .

$$\mu_z = \begin{cases} \alpha E(|F|^r) \sigma_w^2, & W = Y; \\ 0, & W \neq Y; \\ 0, & W = \Phi. \end{cases} \quad (5)$$

参考文献 [4] 确定阈值的方法, 阈值

$$Thres = \frac{1}{3M} \alpha \sigma_w^2 \sum_{i=0}^{M_1} \sum_{j=0}^{M_2} |f_{M,HH}^*(i,j)|^r, \quad (6)$$

式中, r 为嵌入时使用的常数, σ_w 表示水印序列的方差。

3.3 水印检测算法

步骤 1 对 (2) 式选取 $\mu = 2$, 根据密钥 $z(0)$ 循环生成混沌序列 $z(n) (n = 1, 2, \dots, M_n)$, 根据密钥 λ 从 $z(\lambda)$ 开始取 $M_1 \times M_2$ 个元素构成 $M_1 \times M_2$ 的矩阵 $w(i,j)$ 。

步骤 2 对图像进行 l 层离散小波变换, 然后提取出系数 $F = \{f_{i-1,HH}^*(i,j)\}$, 作为待检测水印的系数。

步骤 3 根据 (4) 式计算 Z 值。

步骤 4 根据 (6) 式计算阈值 $Thres$, 当 $Z \geq Thres$ 时, 则认为检测到水印, 否则没有检测到水印。

4 仿真实验

采用 Daubechies 小波基对图像进行小波变换. 原始图像的大小为 256×256 , 水印的大小为 64×64 , 对原始图像进行 2 层分解, 并选择在 HH_1 子带嵌入水印信息. 根据 (2) 式的混沌系统产生 1000 个 64×64 的伪随机序列作为水印序列 (不同水印序列由不同密钥控制产生), 设为: $W_i (i = 1, 2, \dots, 1000)$, 其中 W_{760} 是由嵌入水印时使用密钥产生的水印序列. 根据 2.4 节的水印嵌入算法, 把 W_{760} 嵌入原始图像中。

首先, 分别对著名的 lena 图、man 图、clock 图 (如图 2(a)、(b)、(c) 所示) 嵌入水印, 并对每幅图像分别取 r 为 0.0、0.1、0.2、0.4、0.6、1.0、2.0 嵌入 W_{760} 序列; 其次, 为了检测不同 r 嵌入水印的鲁棒性, 我们对加水印图像进行 JPEG 压缩, 其压缩比分别为 80%、90%, 并对 JPEG 压缩比为 80% 的加水印图像进行高斯噪声污染, 加入的高斯噪声方差分别是 0.02、0.04; 最后对上述各种处理后的加水印图像分别使用产生 $W_i (i = 1, 2, \dots, 1000)$ 的密钥. 检测水印是否存在。

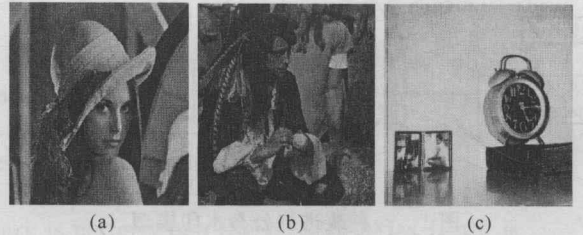


图 2 实验的原图

Fig. 2 The Original Image

(a) lena 图; (b) man 图; (c) clock 图。

(a) lena; (b) man; (c) clock.

图 3 分别给出了上述攻击情况下的实验结果. 从图 3 可以看出, 对于不同 r 取值的水印在无攻击或有攻击的情况下输出的响应值在 W_{760} 的输出位置上都形成了峰值。

从图 3(a) 可以看出, 对所有的 r 取值, $Z - Thres \geq 0$ 成立, 表示能检测到水印的存在, $Z - Thres$ 值越大表明能检测到水印的几率越大, 嵌入的水印鲁棒性越好; 从图 3(b) 可以看出, 当 r 值为 0.0 时, $Z - Thres < 0$, 这时检测不到水印的存在, 而 r 取其他值时 $Z - Thres \geq 0$, 都能检测到水印的存在; 从图 3(c) 和 3(d) 的实验结果来看, 当 r 值为 0.0、0.1、0.2 时 $Z - Thres \geq 0$, 都能检测到水印的存在, 而当 r 值为 0.6、1.0、2.0 时 $Z - Thres < 0$, 不能检测到水印的存在. 综合以上分析可知, 当 r 为 0.1~0.2 时, 嵌入的水印经过 JPEG 压缩和高斯噪声污染后仍然能检测到水印的

存在,所以这种情况下嵌入的水印鲁棒性就比较好.

图 4 给出了被嵌入水印且进行 JPEG 压缩、平滑滤波后恢复的 Lena 图.从图 4 可以看出,图像恢复的效果是比较好的.

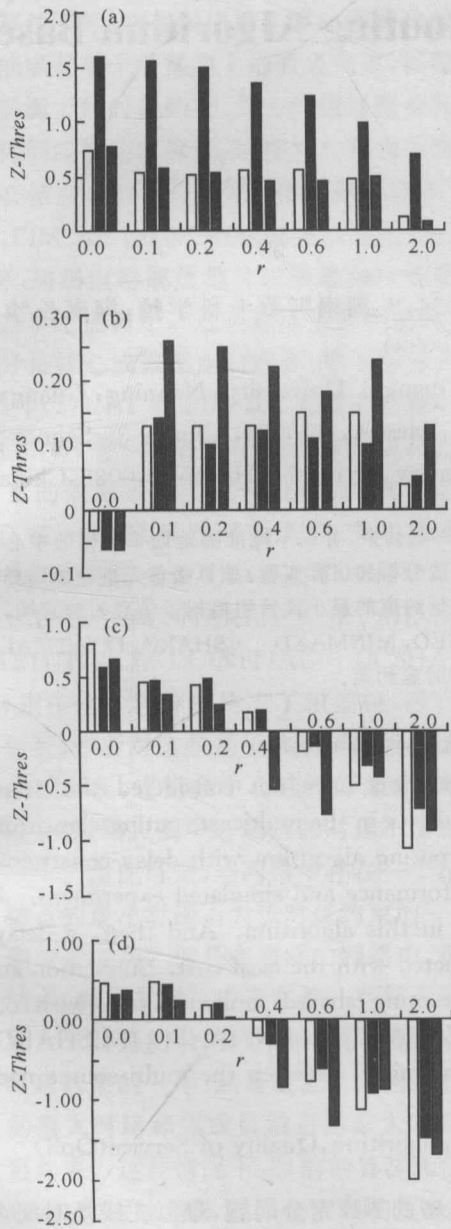


图 3 抗攻击实验结果

Fig. 3 The result of experiment against attack

(a) JPEG 压缩,压缩率 80%;(b) JPEG 压缩,压缩率 90%;(c)高斯噪声污染,均值为 0.02;(d)高斯噪声污染,均值为 0.04.

(a) JPEG compression,compression ratio is 80%;(b) JPEG compression,compression ratio is 90%;(c) adding Gaussian noises and its variation is 0.02;(d)adding Gaussian noises and its variation is 0.04.

5 结束语

本文着重研究了基于离散小波变换的公有水印技术,通过改进现有的公有水印模型,使模型更加实用;通过引入混沌理论,使水印序列的生成更加简单、

实用、安全;通过选择在离散小波变换低频子带上嵌

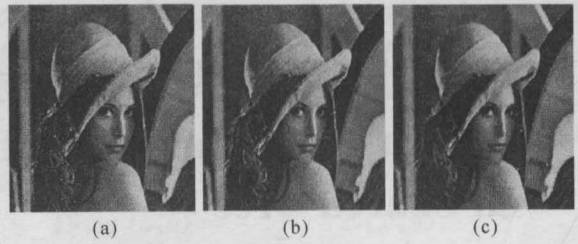


图 4 被嵌入水印后恢复的 Lena 图

Fig. 4 The recovered lena image before embedded watermarking

(a)加水印后的图像;(b)JPEG 压缩后的图像;(c)平滑滤波后的图像.

(a) The image before embedded watermarking;(b) The image before JPEG compression;(c) The image before smooth filtering.

入水印,保证了水印的鲁棒性;通过引入一个指数因子,研究指数因子对水印性能的影响的实验表明,当指数因子为 0.1~0.2 时,嵌入的水印效果比较好.

我们在实验中发现,对于其他的一些图像处理,如平滑滤波、模糊化等,线性检测器虽然也能形成峰值,但要小于阈值,难以检测到水印的存在.阈值的选择还有待进一步研究.

另外,如果压缩比例比较大,或者噪声污染比较严重时,水印检测的效果并不十分明显.今后还有必要对该水印算法做进一步研究,以提高水印的鲁棒性.

参考文献:

- [1] BARNI M, BARTOLINI F, CAPPELLINI V, et al. A DCT-domain system for robust image watermarking[J]. Signal Processing, 1998, 66: 357-372.
- [2] COX I J, KILIAN J, LEIGHTON T et al. Secure spread spectrum watermarking for multimedia[J]. IEEE Trans on Image Processing, 1997, 12(6): 1673-1678.
- [3] XIA X G, BONCELET C G, ARCE G R. A multiresolution watermark for digital images: processing of the IEEE Int Conf on Image Processing[C]. Santa Barbara, CA, Oct, 1997, 3: 584-591.
- [4] INOUEA H, MIYAZAKIB A, KATSURAA T. A digital watermark for images using the wavelet transform[J]. Integrated Computer-Aided Engineering, 2000, (7): 105-115.
- [5] BARNI M, BARTOLINI F, CAPPELLINI V, et al. A DWT-based technique for Spatio-Frequency masking of digital signatures: proceedings of the SPIE/IS&T Int Conf on Security and Watermarking of Multimedia Contents, San Jose, CA, January 25-27, 1999, vol, 3657, pp. 31-39[C]. [s. l.]; SPIE, 1999.
- [6] KUNDUR D, HATZINAKOS D. Digital watermarking using multiresolution wavelet decomposition: proceedings of the IEEE Int Conf on Acounitics [C]. Speech and Signal Processing, 1998: 2969-2972.

(责任编辑:凌汉恩 邓大玉)