

小波域中的鲁棒性盲水印算法

刘宏斌, 王丽君, 王克刚, 陈升

(辽宁科技大学 计算机科学与工程学院, 辽宁 鞍山 114051)

摘要: 提出了自适应的鲁棒性图像水印方案。用密钥选择嵌入的位置, 增加水印的安全性, 并只对有嵌入要求的图像块进行离散小波变换, 这样算法的计算复杂度只与水印容量有关, 与宿主图像无关, 相对减少了计算的复杂度。在水印嵌入过程中, 对相应的有嵌入要求的图像块进行分类来决定不同的嵌入强度, 达到了自适应的嵌入要求。为了更好地增加方案的鲁棒性, 采用基因算法对阈值进行了优化。实验结果表明, 此方案具有很好的透明性, 对通常的图像处理具有很好的鲁棒性。

关键词: 鲁棒性水印; 离散小波变换; 阈值策略; 基因算法

Improved robust blind watermarking algorithm in wavelet domain

LIU Hong Bin, WANG Li Jun, WANG Ke Gang, CHEN Sheng

(School of Computer Science and Engineering, University of Science and Technology, Anshan 114051, China)

Abstract: This paper presented a robust adaptive image watermarking scheme. In order to increase watermark security, key was used for the choice of embedded location, and only a pair of requirements of the embedded image blocks is applied discreted wavelet transform, This algorithm complexity was only determined to the watermark capacity, and had nothing to do with the host image. So the scheme reduced the computational complexity relatively. In embedding process, it classified the requirements of the embedded image block to determine the different embedding strength, so that reached adaptive embedded requirements. In order to further increase the robustness of the program, this paper use genetic algorithm to optimize the threshold. Experimental results showed that this scheme had a good transparency and good robustness to common image processing.

Key words: robust watermark; discrete wavelet transform; threshold strategy; genetic algorithm

数字水印^[1-2](Digital Watermark)技术是将与多媒体内容相关或不相关的一些标示信息直接嵌入多媒体内容当中, 但不影响原内容的使用价值。通过这些隐藏在多媒体内容中的信息, 可以达到确认内容创建者、购买者, 或者确认内容是否真实完整。

变换域算法^[3-8]需要先对源数据进行一个变换, 然后在变换域中完成水印的嵌入和检测, 因而往往会需要较大的运算量。但是, 由于压缩、滤波等图像处理的过程经常也是在变换域完成, 如果处理的过程和水印信号嵌入使用相同的变换域, 则这些处理对数字水印的影响将大大降低。例如, 将图像进行 DWT 变换后再在变换域嵌入水印, 就可以提高水印系统抵抗 JPEG 压缩处理的能力。因此, 选择一个合适的变换操作, 然后在该变换域嵌入水印, 就可以提高水印嵌入系统的鲁棒性。

以前的大部分变换域算法是对图像进行离散小波变换, 对中频子带进行嵌入, 没有对小波系数进行分类及考虑子带之间的关系。本文对需要嵌入水印的图像块进行了离散小波变化, 在分析对应图像块小波系数的特点基础上进行分类, 以自适应调节水印的嵌入强度; 在提取时则采用阈值策略, 不需要原始图像, 真正实现了盲检测; 为了进一步提高水印方案的鲁棒性, 采用基因算法来优化阈值集。

1 算法描述

1.1 图像表示

宿主图像 X 大小为 $M \times N$ 的灰度图像, 可表示为:

$$X = [x(i, j)]_{M \times N} \quad (1)$$

式中, $x(i, j) \in \{0, 1, L, 255\}$, $i \in \{0, 1, L, M-1\}$, $j \in \{0, 1, L, N-1\}$ 。把宿主图像 X 分成 $\lfloor \frac{M}{8} \rfloor \times \lfloor \frac{N}{8} \rfloor$ 个互相不重叠的块, 每

个块的大小为 8×8 , 则 x 的图像块可表示为:

$$K = \{b_{i,j} | i=1, L, \lfloor \frac{M}{8} \rfloor, j=1, L, \lfloor \frac{N}{8} \rfloor, \} \quad (2)$$

每一个 $b_{i,j}$ 的大小为 8×8 。

1.2 水印的表示

在本文实验中, 水印采用有意义的二维二进制位图, 把二维图像通过行优先扫描转化为一维的二进制序列。水印 W 表示为:

$$W = \{w_i | i=1, L, L\} \quad (3)$$

式中, L 表示水印的长度, $w_i \in \{-1, 1\}$ 。

1.3 水印嵌入

首先设定两个密钥 k_1 和 k_2 作为伪随机数产生器的种子, 产生两个长度与水印长度 L 等长的伪随机数序列。 k_1 产生对应图像块行的序列 R , k_2 产生对应图像块的序列 C , 产生如下对应嵌入位置的图像块集合:

$$\Phi = \{b_{k=(i,j)} | i \in R, j \in C\} \quad (4)$$

1.3.1 分类算法

自适应嵌入算法: 对图像块进行分类来决定每一块的嵌入强度, 计算得到每一图像块的 2-级离散小波系数计算 2 级小波子带 HL 、 LH 、 HH 的中值 $Med_k^{HL_2}$ 、 $Med_k^{LH_2}$ 、 $Med_k^{HH_2}$ 。

对图像块进行分类:

类 1: 满足 $Med_k^{HH_2} > \text{Max}\{Med_k^{HL_2}, Med_k^{LH_2}\}$ 。

类 2: 满足 $Med_k^{HH_2} < \text{Min}\{Med_k^{HL_2}, Med_k^{LH_2}\}$ 。

类 3: 满足 $\text{Max}\{Med_k^{HL_2}, Med_k^{LH_2}\} > Med_k^{HH_2} > \text{Min}\{Med_k^{HL_2}, Med_k^{LH_2}\}$ 。

$Med_k^{LH_2}$ 。

具体算法描述如下:

第一步: 输入图像 X 。

第二步: 初始化三个类, 使其为空, 即 $Class_c = \phi, c=1, 2, 3$ 。

第三步: 根据密钥 k_1 和 k_2 得到预嵌入水印的块 b_k 。

第四步: 对水印的块 b_k 进行离散小波变换, 得到对应小波系数块:

$$B_k^\theta = DWT(b_k), \theta = \{LL_2, HL_2, LH_2, HH_2\}$$

第五步: 计算 HL_2 、 LH_2 、 HH_2 的中值:

$$Med_k^\theta = \text{median}\{B_k^\theta(i, j), 1 \leq i, j \leq 2\}, \theta = \{LL_2, HL_2, LH_2, HH_2\}$$

第六步: case1: 当 $Med_k^{HH_2} > \text{Max}\{Med_k^{HL_2}, Med_k^{LH_2}\}$

$$Class_1 = Class_1 \cup \{B_k^{2,\theta}\}$$

case2: 当 $Med_k^{HH_2} < \text{Min}\{Med_k^{HL_2}, Med_k^{LH_2}\}$

$$Class_2 = Class_2 \cup \{B_k^{2,\theta}\}$$

case3: $Class_3 = Class_3 \cup \{B_k^{2,\theta}\}$

第七步: 输出三个类, 即 $Class_c, c=1, 2, 3$ 。

1.3.2 计算阈值

在水印的嵌入和提取中使用阈值。首先计算 HL 、 LH

的中值 $Med_k^{HL_2}$ 、 $Med_k^{LH_2}$ 以及与 HH 的中值 $Med_k^{HH_2}$ 的距离。

具体算法描述如下:

第一步: 输入三个类, 即 $Class_c, c=1, 2, 3$ 。

第二步: 循环 $c=1, 2, 3$ 。

第三步: 循环 $B_k^\theta \in Class_c$ 。

(1) 计算 HL 、 LH 的中值 $Med_k^{HL_2}$ 、 $Med_k^{LH_2}$ 与 HH 的中值

$Med_k^{HH_2}$ 的距离:

$$d_{k'}^i = \text{abs}(Med_{k'}^i - Med_k^{HH_2}), i = LH_2, HL_2$$

(2) 计算 HL 、 LH 距离的最大值 $dl_{k'}$ 和最小值 $ds_{k'}$:

$$dl_{k'} = \text{max}\{d_{k'}^{HL_2}, d_{k'}^{LH_2}\}, ds_{k'} = \text{min}\{d_{k'}^{HL_2}, d_{k'}^{LH_2}\}$$

(3) 结束循环。

第四步: 结束循环。

第五步: 计算对应类中的最大和最小距离:

$$ds_{\text{min}}^c = \min_{\forall B_k^\theta \in Class_c} \{ds_{k'}\}, ds_{\text{max}}^c = \max_{\forall B_k^\theta \in Class_c} \{ds_{k'}\}$$

$$dl_{\text{min}}^c = \min_{\forall B_k^\theta \in Class_c} \{dl_{k'}\}, dl_{\text{max}}^c = \max_{\forall B_k^\theta \in Class_c} \{dl_{k'}\}$$

第六步: 计算 T_1 、 T_2 、 T_3 和 T_4 :

$$T_i = \text{median}\{\{ds_{k'} | \forall B_k^\theta \in Class_1\} \cup \{dl_{k'} | \forall B_k^\theta \in Class_1\}\}, i=1, 2$$

$$T_3 = \text{median}\{\{ds_{k'} | \forall B_k^\theta \in Class_3\}\}$$

$$T_4 = \text{median}\{\{ds_{k'} | \forall B_k^\theta \in Class_4\}\}$$

第七步: 输出 T_1 、 T_2 、 T_3 和 T_4 。

1.3.3 具体的嵌入水印算法

第一步: 输入原始图像 X 和水印 W 。

第二步: 根据密钥 k_1 和 k_2 产生伪随机序列。

第三步: 根据伪随机序列选择要嵌入的目标图像块 Φ 。

第四步: 对水印元素个数进行循环, $i=1 \sim L$ 。

(1) 对目标图像块进行离散小波变换 $DWT(b_k)$ 。

(2) 计算目标图像块 2 级离散小波系数对应的 $B_k^\theta, \theta = \{HL_2, LH_2, HH_2\}$ 。

(3) case 1: 该块属于 1 类, 即 $B_k \in Class_1$ 。如果 $w_i=1$ 及 $(ds_k < T_1$ 或 $dl_k < T_1)$, 则修改 $B_k^{HH_2}$ 使其满足 $ds_k, dl_k > T_1$; 如果 $w_i=-1$ 及 $(ds_k > T_1$ 或 $dl_k > T_1)$, 则修改 $B_k^{HH_2}$ 使其满足 $ds_k, dl_k < T_1$ 转到 (6)。

(4) case 2: 该块属于 2 类, 即 $B_k \in Class_2$ 。如果 $w_i=1$ 及 $(ds_k < T_2$ 或 $dl_k < T_2)$, 则修改 $B_k^{HH_2}$ 使其满足 $ds_k, dl_k > T_2$; 否则, 如果 $w_i=-1$ 以及 $(ds_k > T_2$ 或 $dl_k > T_2)$, 则修改 $B_k^{HH_2}$ 使其满足 $ds_k, dl_k < T_2$ 转到 (6)。

(5) case 3: 该块属于 3 类, 即 $B_k \in Class_3$ 。如果 $w_i=1$ 及 $(Med_k^{01_2} < Med_k^{HH_2} < Med_k^{02_2}), \theta_1, \theta_2 \in \{HL_2, LH_2\}$, 则: 如果 $ds_k < T_3$, 修改 $B_k^{01_2}$ 使其满足 $ds_k < T_3$; 如果 $dl_k < T_4$, 则修改 $B_k^{02_2}$

使其满足 $dl_k < T_4$; 如果 $w_i = -1$ 及 $(Med_k^{\theta_1} < Med_k^{HH_2} < Med_k^{\theta_2})$, $\theta_1, \theta_2 \in \{HL_2, LH_2\}$, 则: 如果 $ds_k > T_3$, 修改 $B_k^{\theta_1}$ 使其满足 $ds_k > T_3$; 如果 $dl_k > T_4$, 则修改 $B_k^{\theta_2}$ 使其满足 $dl_k > T_4$ 。

(6) 对该小波块进行逆离散小波变换 $b_k' = IDWT(B_k')$ 。

第五步: 结束循环。

第六步: 输出加水印图像 X' 。

1.4 提取水印

第一步: 输入加水印图像和伪随机序列密钥种子和四个阈值 T_1, T_2, T_3, T_4 。

第二步: 根据密钥 k_1, k_2 产生伪随机序列。

第三步: 根据伪随机序列选择嵌入的目标图像块 Φ 。

第四步: 对水印元素个数进行循环 $i=1 \sim L$ 。

(1) 对目标图像块进行离散小波变换 $DWT(b_k')$ 。

(2) 计算目标图像块 2 级离散小波系数对应的

$B_k^{\theta}, \theta = \{HL_2, LH_2, HH_2\}$ 。

(3) case 1: 该块属于 1 类, 即 $B_k' \in Class_1$ 。如果 $ds_k < T_1, dl_k < T_1, w_i' = 1$; 否则, $w_i' = -1$ 。

(4) case 2: 该块属于 2 类, 即 $B_k' \in Class_2$ 。如果 $ds_k < T_2, dl_k < T_2, w_i' = 1$; 否则, $w_i' = -1$ 。

(5) case 3: 该块属于 3 类, 即 $B_k' \in Class_3$ 。如果 $ds_k < T_3, dl_k < T_3, w_i' = 1$; 否则, $w_i' = -1$ 。

第五步: 结束循环。

第六步: 输出估计的水印 W 。

2 基因算法(GA)

为了增加图像对各种信号处理的鲁棒性, 本文引入基因算法对阈值集进行优化训练。基因算法 GA^[9-12] 是一种启发式的优化法 (heuristic optimization method), 它是通过既定的随机搜索进行操作, 优化问题可能的解的集合被认为是个体 (individuals) 组成的人群 (population)。一个个体对它的环境的适应程度由它的健康度 (fitness) 表示。

一个个体在搜索空间里的参照物用染色体 (chromosomes) 表示, 实际上那是一套字符串。一个基因 (gene) 是染色体的一个片段, 基因对被优化的单个参数进行编码, 对一个基因的典型的编码可以是二进制或整数。

通过仿真进化过程的重组、突变和选择找到新一代的搜索点, 它们的平均健康度要比它们的祖先好。

基因算法结构化框图如图 1 所示。图中, $S(t)$ 为原始的阈值集合 (祖先), $S''(t)$ 为优化后的阈值集合 (后代)。表 1 给出了针对本实验的基因算法对应的参数。

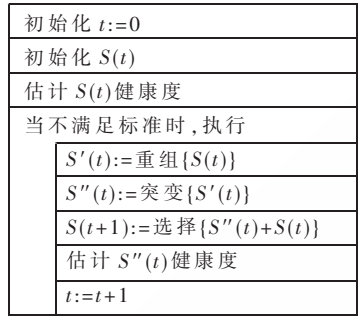


图 1 基因算法结构化框图

表 1 基因算法对应的参数

染色体长度 l / 位	192
人群数量	100
次数 l	50
遗传的概率	0.8
突变的概率	0.05

3 实验结果

在实验中, 采用一个印章图像, 对其进行二进制图像处理作为所有者的版权信息, 对 Lena、Man、Couple 和 Baboon 四副图像进行了水印嵌入, 左侧是原始图像, 右侧为加入水印图像, 如图 2 所示。表 2 为鲁棒性水印对应阈值和进行基因算法优化阈值。

用峰值信噪比 (PSNR) 来衡量图像的质量。定义为:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}, MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (x_{ij} - x'_{ij})^2$$

通过公式计算水印 w 与提取水印 w' 的相似度:

$$s(w, w') = \frac{\sum_{i=1}^L w_i w_i'}{\sqrt{\sum_{i=1}^L w_i^2} \sqrt{\sum_{i=1}^L w_i'^2}}$$



图 2 水印图像、原始图像及对应嵌入水印图像

表 2 水印算法对应阈值

提出鲁棒性水印对应阈值					基因算法优化阈值				
S	Lena	Man	Baboon	Couple	S''	Lena	Man	Baboon	Couple
T_1	2.132 0	3.687 5	1.187 5	1	T_1	2.105 74	1.969 0	2.201 0	2.147 2
T_2	3.250 0	4.250 0	1.750 0	1.500 0	T_2	3.198 8	3.462 7	4.069 1	2.064 6
T_3	1.325 0	1.687 5	0.562 5	0.500 0	T_3	3.572 6	3.723 8	3.319 6	3.674 3
T_4	3.332 5	5.500 0	2.312 5	2.312 5	T_4	4.016 2	3.396 1	3.708 4	4.944 2

表 3 为鲁棒性水印的相似度(Sim),图 3 为鲁棒性水印(Sim 的折线图),表 4 为基因算法优化水印的相似度(Sim),图 4 为基因算法优化水印(Sim 的折线图)。通过分析图表可以看出,基因算法优化水印在噪声处理方面具有很好的鲁棒性,可补偿所提出水印方案在躁声处理方面的不足。从实验结果分析表明,此方案具有很好的视觉效果和抵抗图像处理的鲁棒性。

表 3 鲁棒性水印(Sim)

提出鲁棒性水印(Sim)	Lena	Man	Baboon	Couple	均值
无攻击	1.0000	1.0000	1.0000	1.0000	1.0000
亮化	0.9817	0.9034	0.9582	0.9483	0.9479
剪切 25%	0.8486	0.8486	0.8486	0.8486	0.8486
滤波	0.9409	0.9355	0.9402	0.9385	0.9387
躁声 5%	0.7349	0.8103	0.7446	0.7637	0.7634
直方图均衡	0.8254	0.9553	0.7795	0.8538	0.8535
JPEG2000(5)	0.9750	0.9914	0.9795	0.9824	0.9821

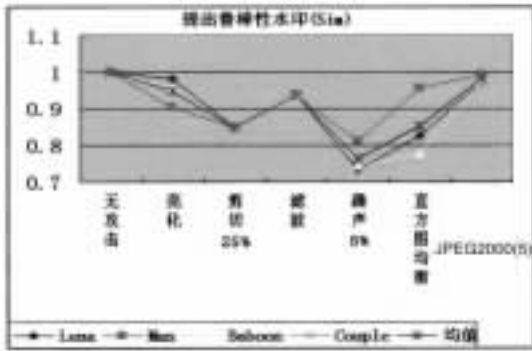


图 3 鲁棒性水印(Sim 的折线图)

表 4 基因算法优化水印(Sim)

基因算法优化水印(Sim)	Lena	Man	Baboon	Couple	均值
无攻击	1.0000	1.0000	1.0000	1.0000	1.0000
亮化 0.9882	0.9763	0.9848	0.9836	0.9832	
剪切 25%	0.8587	0.836	0.858	0.8513	0.851
滤波	0.9235	0.8996	0.9169	0.9138	0.9135
躁声 5%	0.8825	0.8619	0.8896	0.8779	0.878
直方图均衡	0.8437	0.8331	0.854	0.8438	0.8437
JPEG2000(5)	0.9154	0.9966	0.9283	0.9135	0.9385

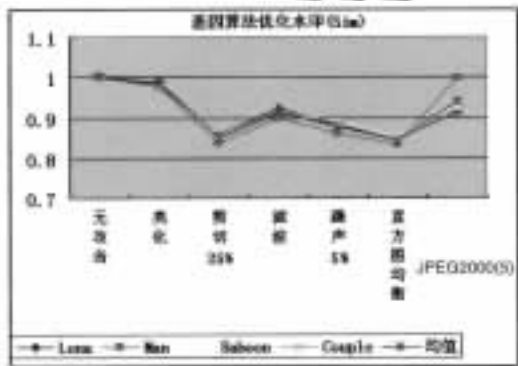


图 4 基因算法优化水印(Sim 的折线图)

本文提出了改进的数字水印算法,在算法中采用了小波技术、分类策略和阈值策略,而且在提取中不需要原始图像,实现了盲检测。文中引用了基因算法对阈值集进行优化,增强了算法的鲁棒性。实验结果表明,方案具有不可感知性和抵抗各种图像处理的鲁棒性。因此,该方案可用于数字版权管理(DRM)、知识产权管理和系统中版权的保护。

参考文献

- [1] 赵翔,郝林.数字水印综述[J].计算机工程与设计,2006,27(6):1946-1950.
- [2] HARTUNG F,KUTTER M. Multimedia watermarking techniques[C]. Proceedings of the IEEE, 1999:1079-1094.
- [3] 牛夏牧,陆哲明,孙圣和.彩色数字水印嵌入技术[J].电子学报,2000,28(9):10-12.
- [4] 刘九芬,黄达人,胡军全.数字水印中的正交小波基[J].电子与信息学报,2003,25(4):453-459.
- [5] 王慧琴,李人厚.一种基于DWT的彩色图像数字水印算法[J].小型微型计算机系统,2003,24(2):299-302.
- [6] 刘挺,尤韦彦.一种基于离散小波变换和HVS的彩色图像数字水印技术[J].计算机工程,2003,19(4):115-117.
- [7] 周翔,段晓辉,王道宪.利用DCT与小波变换的一种数字水印算法[C].全国第三届信息隐藏学术研讨会论文集,西安电子科技大学出版社,2001.
- [8] 强英,王颖.基于小波域的数字图像水印算法综述[J].计算机工程与应用,2004,40(11):46-49.
- [9] 祁建清.基因算法在密码学中的应用分析[J].信息工程大学学报,2003,4(1):93-95.
- [10] 张利萍.一种基于基因算法的函数优化问题求解方法研究[C].中国控制与决策学术年会论文集,2006:457-459.
- [11] 阎春宁,王晶晶,陈志宏,等.利用遗传算法选择最优管理决策[J].上海大学学报(自然科学版),2000,6(1):67-70.
- [12] 林顺刚.遗传算法概述[J].科技信息(学术研究),2007,5(22):90-91.

(收稿日期:2007-08-13)