

文章编号:1674-2869(2015)06-0067-05

最小二乘支持向量机的自适应数字水印算法

付 港,李 鸣*

南昌大学机电工程学院,江西 南昌 330031

摘 要:为了提高数字水印的安全性,提出了一种新的基于对比度掩蔽特性的数字水印算法. 根据人眼视觉系统(HVS)的视觉特性,人眼对于亮度信号(Y)的改变较色度信号(U、V)的改变更加敏感,在图像学国际标准 CCIR601 当中,图像 YUV 空间中的 Y:U:V 通常会取 4:2:2. 首先引入对比度敏感函数模型,选择一些对比度函数值最大的子块,并升序排列;接着,对于前一半子块,使用最小二乘支持向量机建立图像邻域像素之间的关系模型;最后,通过动态地调整模型的输出值与中心像素值之间的大小关系,在另一半子块中实现水印的嵌入与提取. 同时,还利用粒子群算法优化了最小二乘支持向量机的超参数. 仿真实验表明,该数字水印算法具有着良好的不可感知性与鲁棒性,对一些常规的攻击操作也有着很强的抵抗能力.

关键词:数字水印;最小二乘支持向量机;不可感知性;鲁棒性;粒子群算法

中图分类号:TP309

文献标识码:A

doi: 10. 3969/j. issn. 1674-2869. 2015. 06. 014

0 引 言

数字多媒体的迅猛发展,有关数字作品的版权问题、侵权问题等时有发生,因此研究出一种更加有效的数字水印算法是一个很紧迫的问题. 数字水印算法通常分为空域法和变换域法. 空域法是把水印信息直接地嵌入载体图像当中去,它具有算法比较简单、嵌入速度很快、嵌入的水印容量很大、容易实现等优点,在版权保护等方面都有着相当广泛的应用^[1]. 然而,由于它是直接地在图像的表面修改水印信息,况且水印信息相对原始载体图片来说本身就是一种噪声信号,这些都导致空间域的数字水印算法抵抗一些常规攻击的能力普遍比较弱.

为了获得数字水印系统的不可感知性及稳健性达到最佳平衡,近年来一些学者将统计学习理论及机器学习的思想引入到数字水印中来,像神经网络、遗传算法、模糊聚类等. 黄雄华等^[2]先把载体图像进行小波变换,再使用神经网络自适应地确定水印嵌入的最大强度. 王忠等^[3]利用遗传算法优化不可见性的参数构成的目标函数. 虽然这些方法对数字水印系统的性能有着一定程度的改善,但都还有着一些局限性,像神经网络在确定网络的种类、参数时需要靠经验确定,没有科学的理论指导;遗传算法对于大量的数据集计算量特别地大,且泛化能力不是很好,容易陷入局部最优解.

图像的相关性理论表明:数字图像邻域像素之间存在着一种非线性映射的数学函数关系. Wat-son 提出的人眼视觉模型^[4],在图像水印算法中有着广泛的应用. 根据这个特性,张力等^[5]利用颜色特征模型,进行车辆目标的检测. 生理学家发现,人眼对于色度信号的改变较亮度信号的改变不是很敏感,通过选择对比度函数值较大的图像子小块进行水印信息的嵌入和提取. 最小二乘支持向量机(Least squares support vector machine)(LS-SVM)^[6]基于的是结构风险最小化理论,它有着很强的泛化能力和学习能力,在诸如小样本、非线性、高维数、局部极小值等模式识别问题中有着特有的优势. 此时,将 LS-SVM 理论应用于数字水印系统的嵌入和提取,建立水印嵌入位置的特征和水印信号之间的非线性映射的函数关系,并使用粒子群算法(PSO)优化超参数,这些都将会极大的提高水印嵌入和提取的成功率. 李松等^[7]利用遗传算法优化支持向量机,建立小波系数方向树模型,自适应地确定水印的嵌入位置. 实验结果表明,该算法有着很好的不可感知性及鲁棒性.

1 最小二乘支持向量机

最小二乘支持向量机^[6]是支持向量机(SVM)的一种扩展,它利用误差的 2-范数取代了 SVM 中的松弛变量,将误差的平方和的损失函数当作训练集的损失,这样就将一个二次规划的问题巧妙的转

收稿日期:2015-05-14

作者简介:付 港(1988-),男,湖北汉川人,硕士研究生. 研究方向:精密仪器与机械. * 通信联系人.

化成一个线性方程组的求解,这在一定程度上提高了求解速度和收敛的精度.

(1) 设样本集是一个 n 维向量,给定 l 个样本的数据集, x_i, y_i 分别表示样本的输入、输出向量,数据集可以表示为

$$(x_i, y_i), \dots, (x_n, y_n) \in (R_n \times R) \quad (1)$$

(2) 对于最小二乘支持向量机,优化问题为

$$\min J(w, \varepsilon) = \frac{1}{2} w^2 + c \sum_{i=1}^l \varepsilon_i^2 \quad (2)$$

$$s.t. y_i [\phi(x_i) \cdot w + b] = 1 - \varepsilon_i$$

式(2)中: $i=1, 2, \dots, l$

(3) 使用拉格朗日算子求解公式(2)得

$$\begin{bmatrix} 0 & y_1 & \dots & y_l \\ y_1 & y_1 y_1 K(x_1, x_1) + \frac{1}{c} & \dots & y_1 y_l K(x_1, x_l) \\ & & \ddots & \\ y_l & y_l y_1 K(x_l, x_1) & \dots & y_l y_l K(x_l, x_l) + \frac{1}{c} \end{bmatrix} \times \begin{bmatrix} b \\ a_1 \\ \vdots \\ a_l \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} \quad (3)$$

(4) 超参数的优化: 选择最常见的 RBF 核函数, 其中正则化参数 c 和宽度参数 σ^2 的选择, 对于 LS-SVM 的性能发挥有着极其重要的影响, 利用粒子群算法对其进行优化处理, 各个粒子的适应度函数值取预测值与真值的均方误差为

$$MSE = \frac{1}{n} \sum_{i=1}^n (p_i - p_i')^2 \quad (4)$$

式(4)中: p_i, p_i' 分别是测试集的实际值与预测值, n 表示测试样本的个数.

(5) 粒子群初始参数的设定: 进化次数 200 次, 粒子数 20, 局部搜索能力与全局搜索能力均为 2, 设定超参数范围 $c=[0.01 \ 1000]$, $g=[0.01 \ 100]$ 精度 $eps=1.0e-06$; 惯性权重 $w_{\max}=0.9, w_{\min}=0.4$, 且采用线性递减方式为

$$w = w_{\max} - (w_{\max} - w_{\min}) \times \frac{k}{\max \text{ gen}} \quad (5)$$

2 水印信息的嵌入与提取

数字图像空间域邻域像素之间具有很强的相关性, 利用 LS-SVM 强大的学习与泛化能力, 建立中心像素与邻域像素之间的关系模型. 通过一些实验的综合比较, 选取比较常见的图像 3×3 邻域.

设载体图像 I 是 512×512 的灰度图像, 水印图像 W 是 word 上制作的含“南昌大学”字样的二值图像, 其大小是 32×32 , $I = \{I_{i,j} | 1 \leq i \leq M, 1 \leq j \leq N\}$, 其中 $I_{i,j}$ 代表 (i, j) 位置的像素点的灰度值大小, $W =$

$\{W_{i,j} | 1 \leq i \leq P, 1 \leq j \leq Q\}, W_{i,j} = \{0, 1\}$, 水印的嵌入与提取步骤如下:

步骤 1: 用于 LS-SVM 操作子小块的选取, 在空间域的 YUV 空间当中^[8-9], 首先引入对比度敏感函数模型^[10]:

若背景亮度值 $\beta \geq 128$ 时,

$$H(g) = \begin{cases} \ln \left| \frac{c_l(c_l - g)}{c_l(127.5 - (g - c_l))} \right| & 0 \leq g < 128 \\ \ln \left| \frac{(g - c_l)(g - c_H)}{c_l(255 - c_H)} \right| & 128 \leq g < 255 \end{cases} \quad (6)$$

$$\text{式(6)中: } c_l = \frac{127.5}{2}, c_L = \frac{128}{1 - e^{-k}}, c_H = \frac{128 - 255e^k}{1 - e^{-k}}, k = \frac{2.5}{1 + e^{(255 - \beta/55)}}.$$

若背景亮度值 $\beta < 128$ 时, 则有

$$H(g) = \begin{cases} \ln \left| \frac{c_l \times c_L}{(127.5 - (g - c_l)(c_l - g))} \right| & 0 \leq g < 128 \\ \ln \left| \frac{(g - c_l)(255 - c_H)}{c_l(g - c_H)} \right| & 128 \leq g < 255 \end{cases} \quad (7)$$

$$\text{式(7)中: } c_l = \frac{127.5}{2}, c_L = -\frac{28e^k}{1 - e^{-k}}, c_H = \frac{255 - 128e^k}{1 - e^{-k}}, k = \frac{2.5}{1 + e^{\beta/55}}.$$

计算每一个 3×3 小块的对比度函数 $H(g)$ 值, 并且升序排列, 选取其中最大的 $2 \times P \times Q$ 个子块当作 LS-SVM 的数据集^[11].

步骤 2: 选取 LS-SVM 训练样本. 选取步骤 1 中前面一半子块的中心像素 $P(i, j)$ 及其 3×3 邻域分别作为输出输入向量, 建立 LS-SVM 的训练模型.

步骤 3: 修改回归样本值. 选取步骤 1 中后面一半子块, 记作密钥 III, 修改中心像素 $Q(i, j)$ 的值, 采用自适应加性嵌入法则:

$$I'_i = I_i + \alpha \times w(k) \times |H(B_k)| \quad (8)$$

式(8)中: α 是自适应强度因子.

步骤 4: 嵌入水印. 根据中心像素 $Q(i, j)$ 的邻域作为测试数据, 修改中心像素 I'_i 的值, 并与式(8)中 I'_i 作比较, 这样就嵌入了水印信息:

$$I'_i = \begin{cases} \max(I'_i, I_i^p + \lambda), (w_i = 1) \\ \min(I'_i, I_i^p - \lambda), (w_i = 0) \end{cases} \quad (9)$$

步骤 5: 提取水印. 水印提取与嵌入是一个逆过程, 前面的步骤基本一样. 根据密钥 III 定位到相关子块, 根据中心像素 $Q(i, j)$ 的 3×3 邻域预测其中心像素值 I_i^p , 与实际值 I'_i 作比较, 这样就提取了水印信息:

$$w'_i = \begin{cases} w_i = 1, (I'_i > I_i^p) \\ w_i = 0, (I'_i \leq I_i^p) \end{cases} \quad (10)$$

下面将采用 $PSNR$ 、 SNR 、 NC 、 BER 作为水印系统性能评价指标。

3 实验结果及分析

3.1 粒子群优化超参数部分

实验结果:均方根误差 $RMSE=40.664$ 1,平方相关系数 $r=0.819$ 03,训练时间 $t=1.683$ 5 s;参照文献[11]中的算法,对于同样的数据集,若采用BP神经网络, $RMSE=48.454$ 8,平方相关系数 $r=0.739$ 03,训练时间 $t=90.982$ 0 s.可见LS-SVM在提高数据集的预测精度及训练时间等方面,优势比较明显.如果数据集的噪点进行有效处理,特定载体图像的特征提取更加完美,并且设定的PSO相关初始化参数非常恰当,其优势将会更加突出。

PSO优化超参数的过程当中,适应度曲线刚开始下降得很明显,最终稳定在迭代40代左右,适应度值在2.348左右.多次实验过程中,随着迭代次数增加,适应度值得到了一定程度的改善,但时间成本及计算机内存损耗都非常大,优化过程也容易陷入局部最优解.参数的初始化设置也是PSO优化过程中的难点所在.即便如此,由以下的图、表及相关数据可知,本套数字水印算法的主客观性能指标也是相当不错的。

本次PSO优化结果,取 $sig2=16980$ 8, $gam=0.01$,然后将此值初始化LS-SVM的超参数,应用于相关的数字水印算法当中去。

图1是适应度曲线,图2为LS-SVM的训练模型。

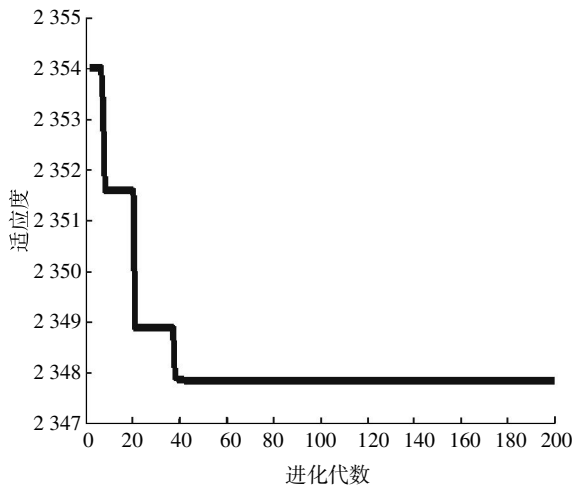


图1 适应度曲线图

Fig.1 Fitness graph

注:适应度曲线(参数 $c1=2, c2=2$, 终止代数=200)

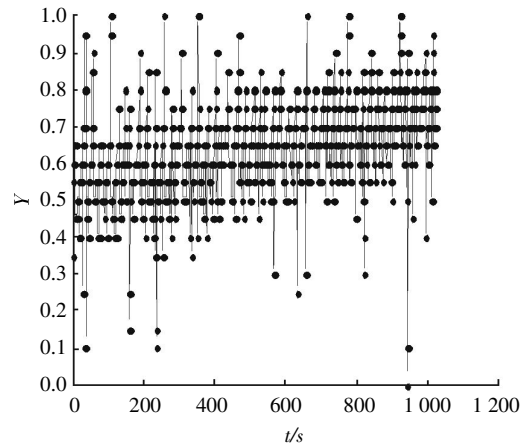


图2 LS-SVM的回归模型图

Fig.2 Regression model figure of the LS-SVM

3.2 数字水印仿真实验结果

仿真实验使用的是MATLAB2013b版本,分别选取图像数据库中大小为 512×512 的灰度图像lena.bmp、brain.bmp、rice.bmp 3组图片作为原始载体图像;水印图像是含“南昌大学”字样的二值图像,大小 32×32 ,经过多次实验,最终确定水印信息的嵌进强度 $\alpha=3.5$.图3~5是几组图片的测试效果。



图3 测试图片 lena.bmp

Fig.3 The test image of lena.bmp

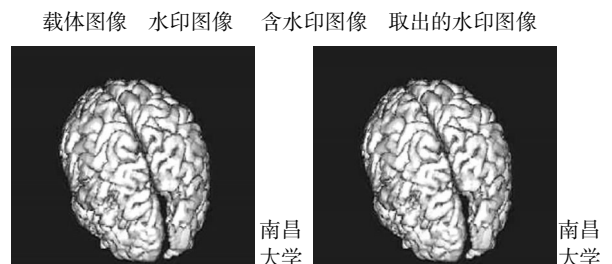


图4 测试图片 brain.bmp

Fig.4 The test image of brain.bmp

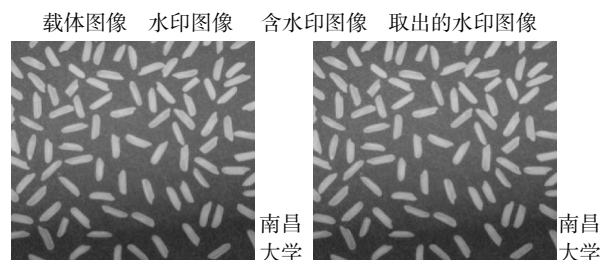


图5 测试图片 rice.bmp

Fig.5 The test images of rice.bmp

通过观察以上三组测试图片的仿真结果,肉眼几乎观察不出原始载体图像与嵌入水印信息之后图像之间的区别所在,这说明水印信息的不可见性很强,提取出来的水印图像与原始水印图像也极为相似. 它们的主客观评价参数均为:峰值信噪比 $PSNR=Inf$ 、信噪比 $SNR=Inf$ 、 $NC=1$ 、错位率 $BER=0$,这些都表明本套数字水印算法的主客观质量都比

较优良. 相比文献 [11] 中算法的结果: $PSNR=55.37$ 、 $NC=0.994$,本算法在没有受到攻击时其性能要比文献[11]相关部分的效果好一些.

为测试本套数字水印算法的鲁棒性能,下面还将对上述三组含有水印信息的图像作一些常规性的攻击操作. 其中 rice.bmp 图片攻击测试实验结果与文献[11]对比如下表 1 所示.

表 1 rice.bmp 攻击测试实验结果
Table1 Attack test results of rice.bmp

攻击方法	本文算法		文献[11]算法	
	$PSNR/db$	NC	$PSNR/db$	NC
JPEG(90)	Inf	1	65.446 3	0.956 9
JPEG(70)	73.462 6	0.997 1	56.995 3	0.895 9
高斯噪声(0.01)	62.551 8	0.963 9	55.245 3	0.791 9
椒盐噪声(0.05)	64.809 6	0.978 5	55.980 7	0.831 3
乘性噪声(0.04)	60.751 9	0.945 3	54.970 4	0.773 9
剪切右下角 1/9	59.600 6	0.928 7	55.633 1	0.806 2
剪切中间 1/4	55.053 2	0.796 9	53.609 8	0.674 6
亮度增强(50%)	55.492 2	0.816 4	57.442 0	0.872 0
对比度增强(50%)	67.819 9	0.989 3	54.889 3	0.751 2
高斯低通滤波(3×3)	69.202 9	0.992 2	56.772 5	0.864 8
中值滤波(3×3)	55.492 2	0.816 4	51.183 7	0.496 4
平均值滤波(3×3)	58.021 9	0.897 5	53.904 1	0.739 2
旋转 30°	55.053 2	0.796 9	53.985 0	0.706 9
旋转 60°	55.223 5	0.804 7	54.001 3	0.708 1
高斯模糊	69.202 9	0.992 2	56.772 5	0.864 8
运动模糊	55.032 3	0.795 9	54.654 5	0.779 9
Sobel 梯度锐化	50.893 8	0.470 7	50.991 0	0.477 3
Prewitt 梯度锐化	50.861 9	0.466 8	50.982 9	0.476 1
Log 梯度锐化	48.130 8	0	48.308 3	0.039 5
尺寸扩大 2 倍	Inf	1	63.609 8	0.970 1
尺寸缩小 2 倍	56.835 0	0.865 2	52.245 9	0.602 9
JPEG(80)+尺寸扩大 2 倍	78.233 8	0.999 0	58.939 6	0.918 7
JPEG(80)+尺寸缩小 2 倍	56.930 5	0.868 2	52.224 1	0.605 3
JPEG(80)+剪切中心 1/9	59.782 8	0.931 6	56.165 5	0.826 6
JPEG(80)+旋转 90°	75.223 5	0.998 0	57.703 0	0.892 3
JPEG(80)+中值滤波	58.838 6	0.915 0	53.376 6	0.697 4
直方图均衡化	61.244 1	0.951 2	59.973 1	0.962 9
直方图匹配	55.585 6	0.820 3	59.043 0	0.958 1

从表 1 看出,本套数字水印算法除了对亮度增强、中值滤波、平均值滤波、旋转、模糊、锐化及缩小等操作,其抵抗能力稍弱一点,对于其它常规攻击与联合攻击操作,其鲁棒性相当地不错. 参照文献[11]相关部分的算法,本套数字水印算法对于绝大多数常规攻击的抵抗能力明显优于文献[11].

4 结 语

本套数字水印系统充分利用人眼 HVS 及 LS-SVM 很强的学习能力和泛化能力,体现出如下优点: (1)水印系统的不可感知性及稳健性非常优良,肉眼几乎观察不出载体图像与含水印图像的细微区别,提取的水印图像与原水印图像也是极为相似,水

印系统的主客观评价参数非常好,有着一定的实用价值;(2)对于一些常规性攻击操作,水印系统表现得也很不错,可为空间域水印算法的继续深入研究提供一种新的思路;(3)更加充分合理的利用HVS特性,结合性能优良的机器学习算法,这些都有利于水印系统的不可感知性与稳健性达到最佳的平衡。

致 谢

本研究是在南昌大学机电学院微流控实验室完成的,向给予帮助和支持的同仁表示衷心的感谢!

参考文献:

- [1] 邢丹,王雷,乔玉.一种基于图像统计特性的空域水印算法[J].电子技术与软件工程,2015(8):102.
XING Dan, WANG Lei, QIAO yu. A airspace watermarking algorithm based on the statistical properties of the image [J]. Electronic Technology & Software Engineering, 2015(8):102.
- [2] 黄雄华,王宏霞,蒋伟贞,等.基于BP神经网络和SNR的自适应音频水印算法[J].光电子.激光,2012(12):2391-2397.
HUANG Xiong-hua, WANG Hong-xia, et al. The adaptive audio watermarking algorithm based on the BP neural networks and SNR[J]. Journal of Optoelectronics. Laser, 2012(12):2391-2397.
- [3] 王忠,叶雄飞.遗传算法在数字水印技术中的应用[J].武汉工程大学学报,2008,30(1):95-97.
WANG Zong, YE Xiong-fei. The application of genetic algorithm in the digital watermarking technology [J]. Journal of Wuhan Institute of Technology, 2008,30(1):95-97.
- [4] HU R, CHEN F, YU H M. Incorporating Watson's perceptual model into patchwork watermarking for digital images [C]//17th IEEE International Conference on Image Processing, 2010:3705-3708.
- [5] 张力,邓亚航,饶小李.颜色特征模型在静态车辆检测中的应用[J].武汉工程大学学报,2015(1):73-78.
ZHANG Li, DENG Ya-hang, RAO Xiao-li. Color feature model in application of static vehicle detection [J]. Journal of Wuhan Institute of Technology, 2015(1):73-78.
- [6] STEVE R G. Support vector machines for classification and regression [R]. Technical report, Southampton University of Southamp-ton, Faculty of Engineering, Science and Mathematics Scod of Electronics and Computer Science, 2003:1-28.
- [7] 李松,顾巧论,高铁杠.信息嵌入位置自适应选择的鲁棒水印算法 [J]. 计算机应用,2013 (2):438-440,446.
LI Song, GU Qiao-lun, GAO Tie-gang. Robust watermark algorithm for adaptive choice of information embedding position.[J] Journal of Computer Applications, 2013(2):438-440,446.
- [8] 何娟芝.基于YUV颜色空间的边缘检测算法研究[D].杭州:杭州电子科技大学,2013.
HE Juan-zhi. A study of the edge detection algorithm based on the YUV color space[D]. Hangzhou: hangzhou dianzi university, 2013.
- [9] 陈军,胡福乔.YUV空间的彩色图像HDR合成算法[J].计算机工程,2012(9):214-216,233.
CHEN Jun, HU Fu-qiao. A HDR synthesis algorithm of the color image in the YUV space[J]. Computer Engineering, 2012(9):214-216,233.
- [10] 吴明巧.数字图像信息隐写与隐写分析技术研究[D].长沙:国防科学技术大学,2007.
WU Ming-qiao. The research on steganography and steganalysis of digital image[D]. Changsha: National university of defense technology, 2007.
- [11] 倪顾伟.基于神经网络的数字水印算法的研究与实现[D].南京:南京理工大学,2012.
NI Gu-wei, The study and implementation of the digital watermarking algorithm based on the neural network[D]. Nanjing: Nanjing university of science and technology, 2012.

Adaptive digital watermarking algorithm based on least squares support vector machine

FU Gang, LI Ming

Nanchang University College of Mechanical and Electrical Engineering, Nanchang 330031, China

Abstract: To improve the security of digital watermark, a novel digital watermarking algorithm based on the contrast masking properties was proposed. The human eye to the change of luminance signal (Y) is more sensitive compared with that of the chrominance signals (U, V), according to the visual characteristics of human eye vision system (HVS). In the YUV image space, the values of Y:U:V are 4:2:2 by the international image standard CCIR601. First, we introduced the contrast sensitivity functions, and chose some sub-images of the maximum contrast sensitivity functions, then ascended them. Second, for the front half of sub-images, the relational model of image neighborhoods pixels was established by the least squares support vector machine (LS-SVM); Finally, the magnitude relation between the output and the central pixel of the model was dynamically adjusted, meanwhile, the watermark was embedded and extracted in the other half of sub-images. The hyperparameters of LS-SVM were also optimized by the particle swarm algorithm. The digital watermarking algorithm has good robustness and imperceptibility, and has a strong resistance to aggressive operation.

Keywords: digital watermarking; LS-SVM; imperceptibility; robustness; particle swarm algorithm

本文编辑:陈小平