

利用亮度分量的彩色图像信息隐藏算法*

程卫东¹, 刘红梅²

(1. 成都信息工程学院电子系, 四川 成都 610041;

2. 中山大学电子与通信工程系, 广东 广州 510275)

摘 要: 提出了一种利用亮度分量的彩色图像信息隐藏算法. 本算法实现了隐藏信息的盲检测, 并在 512×512 的 RGB 彩色图像中嵌入多达 2048 字节的数据. 算法有效地利用了数字通信理论中的前向纠错编码技术和数据扰乱技术, 使水印抵抗各类攻击的性能得到了有效地提高. 实验证明该算法能较好地平衡隐形水印的不可见性和稳健性之间的矛盾, 所隐藏的数字水印在 StirMark 的攻击下, 具有较好的抵抗能力.

关键词: 盲检测; 彩色图像水印; 稳健性; StirMark

中图分类号: TP391 **文献标识码:** A **文章编号:** 0529-6579 (2001) 05-0047-05

随着互联网及数字媒体信息服务的迅猛发展, 如何防止数字媒体信息的非法复制与非法传播已成为数字媒体产品产权保护亟待解决的问题. 为此, 近几年来人们一直试图利用数字水印技术来为实现数字媒体产品的产权保护提供一个实用而有效的认证工具. 为了实现这一目标, 图像隐形水印的完全盲检测技术研究已成为数字水印研究领域中最为热门的研究课题, 亦是最为困难的研究课题. 其原因有: ①以算法^[1~4]为代表的, 所嵌水印为伪随机序列的水印算法, 其算法尽管具有很好的稳健性, 但由于水印本身所包含的有用信息量仅为 1 bit (1 bit 信息仅能表达有无水印). 因而, 在实际应用时, 具有很大的局限性. ②对于文献 [5~8] 提出的图像隐形水印算法, 虽然这些算法各自都有独到之处, 但是它们都有两个较为明显的缺陷, 一是嵌入的有用信息量太少, 一般为几十个字节的有效数据量级; 二是在水印检测时, 这些算法不是需要借助原始图像, 就是需要借助嵌入水印时所产生的附加控制信息. 从水印检测意义而言, 这些水印算法都不是完全意义上的盲检测. ③现有的彩色图像水印盲检测算法^[9~11]及前面提到的灰度图像水印算法都无法全面地抵抗 StirMark 攻击. 鉴于上述原因, 本文在研究各种水印算法的基础上, 结合数字通信理论中的纠错编码、信号加扰等思想, 提出了一种基于亮度分量的彩色图像信息隐藏算

法.

本文提出的盲检测算法具有如下特点: ①嵌入水印为有意义的文字或图像; ②嵌入水印的数据量大. 如, 在 512×512 的 RGB 彩色图像中, 可嵌入 2048 字节的水印数据; ③实现了完全意义上的盲检测, 即检测时, 完全不依赖于原始图像和其它任何附加信息, 而仅依赖于算法本身; ④采用了前向纠错编码技术和数据加扰技术. 本算法采用了 (61, 8) 的 BCH 编码, 因此, 在嵌入图像中的 2048 字节数据里, 水印有效长度为 268 字节.

1 算法描述

本文算法的水印嵌入原理框图如图 1 所示. 以下 8 个步骤完整地描述了水印嵌入过程.

(1) RGB 到 YUV 变换: 设水印载体 RGB 彩色数字图像表示为 $F = [f_\rho]_{M \times N}$, 其中, $M \times N$ 为图像大小, $f_\rho = [R_\rho, G_\rho, B_\rho]$ 为 R、G、B 彩色分量构成的 3×1 维向量, $R_\rho, G_\rho, B_\rho \in \{0, 1, 2, \dots, 255\}$, $\rho = (x, y)$, $x \in \{1, 2, \dots, M\}$, $y \in \{1, 2, \dots, N\}$. RGB 到 YUV 变换由 (1) 式给出.

$$O = TF \quad (1)$$

在 (1) 式中, $O = [o_\rho]_{M \times N}$ 是以 YUV 表示的彩色数字图像, $o_\rho = [Y_\rho, Cb_\rho, Cr_\rho]$ 为亮度分量 Y 和色度分量 Cb、Cr 构成的 3×1 维向量, $Y_\rho \in \{0, 1, 2, \dots, 255\}$, $Cb_\rho, Cr_\rho \in$

* 基金项目: 国家自然科学基金资助项目 (69975011); 教育部骨干教师资助项目; 广东省自然科学基金资助项目 (980442); 广州市重大科技攻关项目 (2000-z-004-01)

收稿日期: 2001-02-26; 作者简介: 程卫东 (1958-), 男, 副教授.

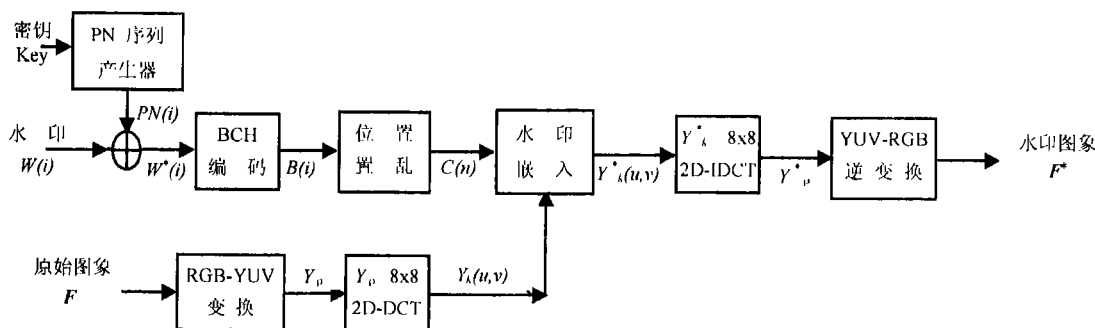


图1 水印嵌入算法

Fig.1 Watermark hiding algorithm

$\{-128, -127, \dots, 126, 127\}$, $\rho = (x, y)$, $x \in \{1, 2, \dots, M\}$, $y \in \{1, 2, \dots, N\}$, T 为 RGB 到 YUV 的变换矩阵.

(2) 2D-DCT (two dimensional - discrete cosine transform) 变换: 对亮度分量 Y_p 进行 8×8 的分块 2D-DCT 变换, 得到亮度分量的 DCT 域系数 $Y_k(u, v)$ ($u, v = 1, 2, 3, \dots, 8$; $k = 1, 2, 3, \dots, K$; 这里设 M 和 N 能被 8 整除).

(3) 加扰: 对水印 $W(i)$ 进行加扰. $W^*(i) = W(i) \oplus PN(i)$ ($i = 1, 2, 3, \dots, I$). $PN(i)$ 为初始状态 Key 产生的伪随机“0”、“1”序列. 加扰在这里具有两个作用. 一是使有意义的水印数据通过加扰后“0”、“1”数据分布更具随机性; 二是对水印数据进行加密.

(4) 前向纠错编码: 对加扰后的水印 $W^*(i)$ 进行 $B(i) = GW^*(i)$ ($i = 1, 2, 3, \dots, I$) 的 (61, 8) BCH 纠错编码, 其中 G 是 (61, 8) BCH 纠错编码的生成矩阵.

(5) 数据位置置乱: 先对字节顺序 i ($i = 1, 2, 3, \dots, I$) 置乱, 当 i 为偶数时, $B'(i) = B(k)$ ($k = 1, 2, 3, \dots, I/2$); 当 i 为奇数时, $B'(i) = B(k + I/2)$ ($k = 1, 2, 3, \dots, I/2$). 然后对比特位置 j ($j = 1, 2, 3, \dots, 8$) 置乱, 当 j 为偶数时, $C_j^*(i) = B_l'(i)$ ($l = 1, 2, 3, 4$); 当 j 为奇数时, $C_j^*(i) = B_{l+4}'(i)$ ($l = 1, 2, 3, 4$). 最后, 按先 i 后 j 的顺序, 对 $C_j^*(i)$ 进行比特抽取, 构成长度为 $8 \times I$ 比特的比特流 ($i = 1, 2, 3, \dots, I$; $j = 1, 2, 3, \dots, 8$).

(6) 数据嵌入: 依据文献 [12] 的水印嵌入策略, 算法在每个 8×8 的 2D-DCT 亮度系数 $Y_k(u, v)$ ($u, v = 1, 2, 3, \dots, 8$; $k = 1, 2, 3, \dots, K$) 中, 选用了 4 个分量 $Y_k(u, v)$ ($u, v = 1, 2$; $k = 1, 2, 3, \dots, K$), 即 DC、AC1、AC2、AC3 来嵌入数据.

当比特流 $S(i, j) = "1"$ 时, 用序号为 2^{P-1} 的 P 位的格雷码置换所选系数 $Y_k(u, v)$ 的整数最低 P 个比特位; 当比特流 $S(i, j) = "0"$ 时, 用序号为 $2^{P-1} - 1$ 的 P 位的格雷码置换所选系数 $Y_k(u, v)$ 的整数最低 P 个比特位; 其中, $k = 1, 2, 3, \dots, K$; $i = 1, 2, 3, \dots, I$; $j = 1, 2, \dots, 8$; $u, v = 1, 2$. 从而构成水印图像的亮度分量的 2D-DCT 系数 $Y_k^*(u, v)$.

(7) 2D-IDCT (two dimensional - inverse discrete cosine transform) 逆变换: 对带有水印信息的亮度分量的 2D-DCT 系数 $Y_k^*(u, v)$ 进行 2D-IDCT 变换, 得到带有水印信息的亮度分量的空域系数 Y_p^* .

(8) YUV 到 RGB 逆变换: 最后, 对带有水印信息的 YUV 信号 $O^* = [o_p^*]_{M \times N}$, $o_p^* = [Y_p^*, Cb_p, Cr_p]$, 按 (2) 式进行 YUV 到 RGB 的逆变换, 获得 RGB 水印图像 F_p^* .

$$F^* = T^{-1} O^* \quad (2)$$

2 水印检测

水印检测是上述嵌入过程的逆过程. 需要注意的是, 有的攻击将改变水印图像的几何尺寸. 因此, 在进行水印检测时, 对于几何尺寸发生变化的 (非 $M \times N$ 的) 待检图像, 需要对待检图像进行几何尺寸变换预处理, 将非 $M \times N$ 的待检图像变为 $M \times N$ 的待检图像.

3 实验结果

实验中, 本算法使用纹理复杂度完全不同的 RGB 彩色图像 “Lena” 和 “Baboon” 作为水印载体, 在 $M = N = 512$ 的彩色图像中, 按本文算法嵌入了如图 2 (a) 所示的 48×48 的二值图像水印. 本节给出了 “Lena” 的实验结果.

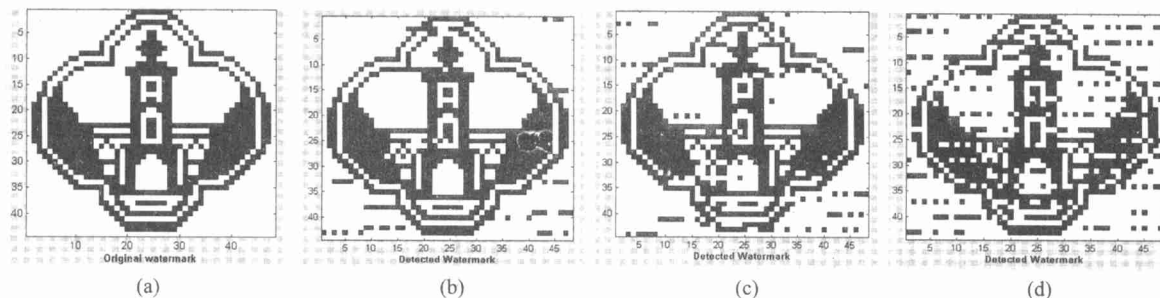


图 2 原始水印和受到攻击后检测得到的水印

Fig.2 The original watermark and the recovered watermarks survived the attacks

图 3 显示了水印的不可见性. 图 3 (a) 是“Lena”的原图像. 图 3 (b) 是嵌入水印后的“Lena”图像. 由图可知, 水印算法很好地满足了不可见性的要求.

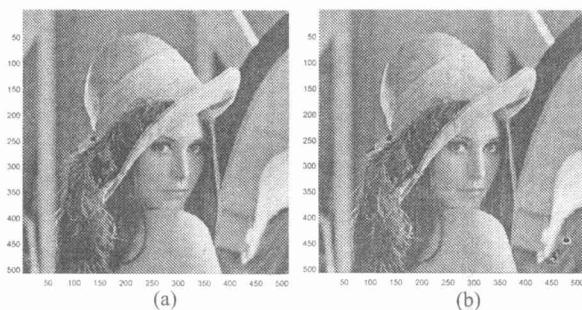


图 3 不可见性演示

Fig.3 Demonstration of invisibility

(a) Lena 原始图像;

(b) Lena 水印图像, PSNR = 41.78 dB

本算法采用了 StirMark3.1 水印攻击系统对算法性能进行攻击测试. StirMark3.1 水印攻击系统产生的攻击可分为 14 大类共 88 种攻击. StirMark3.1 的 14 大类攻击中, 有的将会改变水印图像的几何尺寸, 如裁剪、移去 n 行 m 列、 x 、 y 拉伸或压缩、比例放大或缩小、旋转攻击等.

算法测试结果由表 1 给出. 从表 1 结果可知, 该算法对移去 n 行 m 列、裁剪、JPEG 压缩、 X 或 Y 方向压扩具有很好的稳健性. 而对中值滤波、旋转并裁剪、旋转并拉伸、修剪、线性几何变换等攻击稳健性较差.

图 2 (b) 是图 3 (b) 所示的水印图像经过 StirMark3.1 水印攻击系统移去 17 行 5 列的攻击后, 盲检测出来的图像水印. 被检水印图像的峰值信噪比 PSNR = 29.89 dB, 检测误比特率为 3.22%. 图 2 (c) 是图 3 (b) 所示的水印图像经过 StirMark3.1 水印攻击系统的 JPEG 压缩攻击 (质量因子为 40) 后, 盲检测出来的图像水印. 被检水印图像的峰值信噪比 PSNR = 31.18 dB, 检测误比特率为 5.60%. 图 2 (d) 是图 3 (b) 所示的水印图像经过 StirMark3.1 水印攻击系统的四周裁剪去 25% 攻击后, 盲检测出来的图像水印. 被检水印图像的峰值信噪比 PSNR = 35.55 dB, 检测误比特率为 11.43%. (注: BER 为 bits error rate)

4 结 论

本文探讨并实现了在彩色图像中嵌入有意义隐形水印的完全盲检测算法. 本算法可以在 512×512 的 RGB 彩色图像中嵌入多达 2048 字节的数据, 而且该算法在检测水印时, 不需要原始图像和任何附加信息, 而仅仅依赖算法本身. 同时, 算法还有机地利用了数据通信理论的前向纠错编码技术和数据扰乱技术, 有效地提高了算法抵抗各类攻击的性能. 因此, 本算法从完全盲检测意义上优于需要大量的附加信息的算法^[1,7]; 在隐藏数据量方面优于文献 [6] 的算法.

表 1 对抗 Stirmark3.1 的稳健性

Tab.1 The robustness to Stirmark 3.1

攻击描述		PSNR dB	BER %	攻击描述		PSNR dB	BER %
移去	移去 1 行 1 列	33.22	0.09	压扩	X 方向压缩 20%, Y 方向不变	31.38	3.78
	移去 1 行 5 列	31.88	0.28		X 方向不变, Y 方向压缩 20%	30.55	8.26
	移去 5 行 1 列	30.66	4.90		X 方向不变, Y 方向拉伸 10%	29.16	13.25
	移去 5 行 17 列	29.85	7.60		X 方向拉伸 10%, Y 方向不变	30.02	6.58
	移去 17 行 5 列	29.89	3.22		X 方向不变, Y 方向拉伸 20%	30.58	5.69
	中值滤波 (2×2)	27.95	34.70	旋转并 裁剪	X 方向拉伸 20%, Y 方向不变	31.30	2.75
	中值滤波 (3×3)	29.81	19.50		正旋 0.25 度并裁剪为 510×510	27.34	50.23
	中值滤波 (4×4)	23.89	47.29		反旋 0.25 度并裁剪为 510×510	29.56	49.39
裁剪	剪去原图 1%	33.88	0	旋转并 比例 拉伸	正旋 0.50 度并裁剪为 508×508	30.91	49.63
	剪去原图 2%	33.88	0		反旋 0.50 度并裁剪为 508×508	31.18	5.60
	剪去原图 5%	34.00	1.82		正旋 0.25 度并拉伸为 512×512	26.95	40.49
	剪去原图 10%	34.26	4.10		反旋 0.25 度并拉伸为 512×512	28.28	39.13
	剪去原图 25%	35.02	11.43		正旋 0.50 度并拉伸为 512×512	23.31	47.48
	剪去原图 50%	36.79	26.59		反旋 0.50 度并拉伸为 512×512	24.66	47.90
JPEG	Qut = 40	31.18	5.60	修剪	X 方向修剪为 506 点, Y 不变	25.09	39.37
质量	Qut = 50	31.55	11.05		X 方向不变, Y 修剪为 506 点	23.10	41.70
因子	Qut = 60	31.98	0		X、Y 方向都修剪为 506 点	22.92	48.09
按比例 压扩	X、Y 方向尺度都压缩 50%	29.09	4.80		X 方向修剪为 486 点, Y 不变	19.72	48.18
	X、Y 方向尺度都压缩 25%	30.66	1.82	线性 变换	$(u, v) = [1.007, 0.010; 0.010, 1.012](x, y)$	20.41	45.80
	X、Y 方向尺度都压缩 10%	31.00	12.36		$(u, v) = [1.010, 0.013; 0.009, 1.011](x, y)$	19.98	48.51
	X、Y 方向尺度都扩张 10%	27.52	25.14		$(u, v) = [1.013, 0.008; 0.011, 1.008](x, y)$	21.10	45.66
	X、Y 方向尺度都压缩 50%	33.76	0.09	高斯滤波 (3×3) [1 2 1; 2 4 2; 1 2 1]		31.39	2.94
	X、Y 方向尺度都压缩 100%	33.33	5.64	锐化 (3×3) [0 -1 0; -1 5 -1; 0 -1 0]		21.16	50.79
				Stirmark 随机弯曲		18.96	49.21
				Frequency mode Laplacian removal attack		30.79	47.99

参考文献:

- [1] WOLFGANG R B, PODILCHUK C I, DEPL E J. Perceptual watermarks for digital images and video[J]. Proceedings of the IEEE, 1999, 87(7): 1108 - 1126.
- [2] COX I J, KILIAN J, LEIGTON F T, et al. Secure spread spectrum watermarking for multimedia[J]. IEEE Trans On Image Processing Dec, 1997, 6(12): 1673 - 1687.
- [3] PODILCHUK C I, ZENG W J. Image-adaptive watermarking using visual models[J]. IEEE J Selected Areas in Comm, 1998, 16(4): 525 - 539.
- [4] HUANG J W, SHI Y Q. An adaptive image watermarking scheme based on visual masking[J]. IEE Electronics Letters, 1998, 34(8): 748 - 750.
- [5] INOUE H, MIYAZAKI A, YAMAMOTO A, et al. A digital watermark based on the wavelet transform and its robustness on image compression[J]. IEEE Int Conf On Image Processing, 1998, II.
- [6] SHAPIRO M. Embedded image coding using zerotrees of wavelet coefficients[J]. IEEE Trans Image Processing, 1993, 41(12): 3445 - 3462.
- [7] TSAI M J, YU K Y, CHEN Y Z. Joint wavelet and spatial transformation for digital watermarking[J]. IEEE Trans On Consumer Electronics, 2000, 46(1): 241 - 245.
- [8] DELAIGLE J F, VLEESCHOUWER C De, MACQ B. Watermarking algorithm based on a human visual model[J]. Signal Processing, 1998, 66(3): 319 - 335.
- [9] CHO J S, SHIN S W, LEE W H, et al. Enhancement of robustness of image watermarks embedding into colored image, based on WT and DCT[A]. In: Coding and Computing, Proceedings International Conference on Information Technology. 2000. 483 - 488.
- [10] PIVA A, BARTOLININ F, CAPPELLINI V, et al. Exploiting the cross-correlation of RGB-channels for robust watermarking of color images[A]. In: ICIP 99 Image Processing Proceedings of IEEE 1999 International Conference on Image Processing, 1999. 306 - 310.
- [11] WU C F, HSIEH W S. Digital watermarking using zerotree

of DCT[J]. IEEE Transaction on Consumer Electronics, 2000, 46(1):87–93.

marks in DC components[J]. IEEE Trans on Circuits and Systems for Video Technology, 2000, 10(6):974–979.

[12] HUANG J W, SHI Y Q, SHI Y. Embedding image water-

An Information Hiding Algorithm for Color Images Using the Luminance Component

CHENG Wei-dong¹, LIU Hong-mei²

(1. Department of Electronics, Chengdu University of Information Technology, Chengdu 610041, China;

2. Department of Electronics, Zhongshan University, Guangzhou 510275, China)

Abstract: An information hiding algorithm for color images using the luminance component is proposed. This algorithm not only can hide data as many as 2048 bytes, but also can implement blind extraction of the hidden information without resorting to the original image and any side information. The proposed algorithm adopts error-correcting coding and data interleaving techniques to improve the performance of resisting diverse attacks. The algorithm trades off the conflict of invisibility and robustness of the invisible watermark well. The experimental results show that the hidden watermark is robust to most attacks in StirMark.

Keywords: blind extraction; color image watermarking; robustness; StirMark

(上接第 46 页)

A Niche – based Genetic Algorithm for the Optimization of Multimodal functions

PAN Zhong-liang¹, XIONG Yin-gen²

(1. Department of Physics, South China Normal University, Guangzhou 510631, China;

2. Department of Electronics, Zhongshan University, Guangzhou 510275, China)

Abstract: A genetic algorithm based on niche is proposed, it can efficiently exploit the historical information to speculate on new search points. The new operators of selection and mutation are designed in the algorithm under the principles of niche. The implement approaches with the genetic algorithm for multimodal function which have several local optimal solutions are introduced. The simulation results demonstrate that the niche-based algorithm is effective.

Keywords: genetic algorithm; niche; multimodal function; optimization