

文章编号:1671-6833(2010)02-0106-03

基于图像子块 DCT 系数对的盲检测数字水印

路 玲, 孙新德

(郑州航空工业管理学院 计算机科学与技术系, 河南 郑州 450015)

摘 要: 提出一种新的基于 Logistic 加密的鲁棒性盲检测数字水印算法. 利用 Logistic 映射特性产生的混沌序列加密生成水印序列; 结合人眼的视觉系统(HVS)对原始图像中的子块进行选择; 在每个被选择的子块上, 根据鲁棒性要求选择 DCT 系数; 通过对相邻系数对的大小进行比较嵌入水印. 实验结果表明, 本算法具有鲁棒性强、安全性高、透明性好、可以盲提取等特点, 可有效用于数字媒体的版权保护.

关键词: Logistic 映射; 数字水印; 鲁棒性; 盲检测

中图分类号: TP181

文献标识码: A

0 引言

数字水印在数字产品版权保护方面的潜在应用越来越受到国内外学者的重视, 并成为近年来多媒体信息安全研究领域的一个热点. 一般来说, 用于数字图像版权保护的数字水印要求具有较高的鲁棒性、安全性和透明性, 而且为了应用方便还应该能够盲检测. 目前, 有关水印的算法比较多, 但是能够同时满足这三种要求的并不多. 陈永强的算法^[1]使用混沌加密提高水印安全性, 结合人类视觉模型把水印自适应地嵌入到小波系数中保证水印的鲁棒性. 其虽然实现了较好的鲁棒性, 但是算法比较复杂, 而且由于对水印只采用了一次加密, 安全性不够强. 余波^[5]提出的基于整数小波变换的盲检测水印算法只适用于脆弱水印. 徐振启^[6]等人的算法使用时空二维混沌序列对水印加密提高了水印安全性, 但是提取水印时需要原始图像, 降低了实用性.

笔者提出的水印方案使用了“三级加密”确保水印安全, 即首先使用 Logistic 映射产生的混沌序列加密水印, 然后在嵌入水印时又引入生成矩阵 A 和 DCT 系数对的行列选择两种加密措施, 形成了对水印的保护体系. 根据人类视觉系统(HVS)的照度掩蔽特性和纹理掩蔽特性选择合适的水印嵌入区域, 再在每一子块 DCT 域合理选择嵌入位置和嵌入水印信息量, 而且使用相邻

DCT 系数对进行 1bit 水印嵌入, 实现了水印鲁棒性和透明性的统一. 由于水印嵌入是基于 DCT 系数关系, 因而提取水印时不需要原始图像, 算法具有较强的实用性.

1 基于 Logistic 映射的混沌加密水印

Logistic 映射可用非线性差分方程描述^[2]:

$$x_{i+1} = \lambda x_i (1 - x_i), \quad i = 0, 1, 2, \dots \quad (1)$$

$\lambda \in [0, 4]$, 初始值 $0 < x_0 < 1$. 这样得到的序列 $X = \{x_i\}$ 是单极性序列, 且 $x_i \in (0, 1)$. 当 $3.569\,945 \leq \lambda \leq 4$ 时, Logistic 映射进入混沌状态, 所产生的序列为混沌序列. Logistic 映射所产生的混沌序列依赖初始条件. 在不同初始条件, 产生的任意两个混沌序列是非周期、不收敛、不相关的, 所以可以把初始条件作为混沌序列的密钥.

混沌序列序列 X 的均值为 $E\{X\} = 0.5$, 因此可以 0.5 为阈值把实值混沌序列 X , 转化为二值序列 S .

水印图像是大小为 $N \times M$ 的二值图像. 对水印图像降维可得到一维的水印序列 $W = \{w(k), k = 1, 2, 3, \dots, N \times M\}$. 把二值混沌序列 S 与二值水印序列 W 进行异或运算, 即 $W_s = W \oplus S$, 即可得到被混沌序列加密的水印 $W' = \{w'(k), k = 1, 2, 3, \dots, N \times M\}$.

利用混沌序列为水印加密简单可行且安全可靠, 是提高鲁棒性优选方案.

收稿日期: 2009-09-27; 修订日期: 2009-12-28

基金项目: 河南省科技厅国际科技合作项目(094300510077)

作者简介: 路玲(1964-), 女, 河南洛阳人, 郑州航空工业管理学院副教授, 硕士, 研究方向为图像处理和信息安全,

E-mail: luling@zzia.edu.cn

2 数字水印算法

2.1 嵌入水印

(1)嵌入区域选择. 把原始图像分割为互不覆盖的 8×8 子块,然后根据人类视觉系统(HVS)选择嵌入水印的子块,以便提高水印的鲁棒性.

由人类视觉系统(HVS)的照度掩蔽特性和纹理掩蔽特性可知^[6],背景的亮度越高,纹理越复杂,人类视觉对其修改就越不敏感. 为了保证原始图像和嵌入水印后图像之间的感知相似性,将水印信号尽可能地嵌入到纹理较复杂的子块. 这里用子块的方差值 σ^2 衡量子块纹理的复杂度(m 为子块的平均灰度)^[3].

$$m = \frac{1}{n^2} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} x(i, j) \quad (2)$$

$$\sigma^2 = \frac{1}{n^2} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} [x(i, j) - m]^2 \quad (3)$$

当 σ^2 较小时,可认为该块比较均匀,反之,则认为该块包含着较为复杂的纹理或边缘. 本算法选取 σ^2 较大的 $t = (N \times M)/2$ 个 8×8 子块作为水印嵌入区域.

(2)DCT 系数对的选择. 对选择的每一个子块进行 DCT 变换,每一子块的 DCT 系数表示为:

$$V = \begin{bmatrix} V_{LL} & V_{LH} \\ V_{HL} & V_{HH} \end{bmatrix}$$

式中: V_{LL} 、 V_{LH} 、 V_{HL} 、 V_{HH} 均为 4×4 的矩阵,分别对应低频、中频、次高频和高频系数. 通过对人类视觉系统(HVS)的研究,发现人眼对低频部分的噪声相对敏感,为了使水印不易被察觉,应将水印嵌入到较高频部分;但很容易因量化、低通滤波等处理而丢失信息. 为了解决低频和高频的矛盾,本算法根据密钥 key1(矩阵 A) 把加密后的水印序列嵌入到宿主图像的次高频 V_{HL} 中.

在一个子块中嵌入水印位数不能太多,否则会降低水印的透明性和载体图像质量. 本算法在每一个 8×8 的子块中选取 4 个 DCT 系数嵌入 2bit 水印.

$$A = \begin{bmatrix} 0, 0, 0, 0, 0, 0, 0, 0 \\ 0, 0, 0, 0, 0, 0, 0, 0 \\ 0, 0, 0, 0, 0, 0, 0, 0 \\ 0, 0, 0, 0, 0, 0, 0, 0 \\ 1, 1, 0, 0, 0, 0, 0, 0 \\ 1, 1, 0, 0, 0, 0, 0, 0 \\ 0, 0, 0, 0, 0, 0, 0, 0 \\ 0, 0, 0, 0, 0, 0, 0, 0 \end{bmatrix}$$

矩阵 A 中的“1”表示该位置系数被选中,“0”表示不选.

(3)1bit 水印嵌入规则. 在每一子块中被选中的系数对上嵌入 1bit 水印.

嵌入规则:对两个相邻系数 i 和 j ,如果 $i < j$ 且水印 $W'(k)$ 为 1 则把 i 和 j 交换位置;如果 $i > j$ 且水印 $W'(k)$ 为 0 则交换 i 和 j 位置;其他情况则保持 i 和 j 位置不变.

经过 $2t$ 次就把数字水印序列所包含的 $N \times M$ 位信息全部嵌入到已选择的子块中. 选择系数对时是基于行相邻还是基于列相邻由另一个密钥 key2 决定.

(4)图像重构. 对所有嵌入水印信息的子块进行 IDCT 变换,再对所有子块重构得到含水印的载体图像.

2.2 提取水印

提取水印时不需要原始宿主图像,本算法为水印盲检测算法. 提取水印的过程与嵌入水印过程相反.

(1)把嵌入水印的图像分成互不覆盖的 8×8 子块,根据每个子块的方差大小选出纹理较大的 t 个子块.

(2)根据矩阵 A 和 key2 依此对 t 个子块中相邻元素值进行比较提取水印 W' . 经过 $2t$ 次比较可将混沌加密的水印序列提取出来.

提取规则:对于两个相邻系数 i 和 j ,如果 $i > j$,则 $W'(k) = 1$;如果 $i \leq j$,则 $W'(k) = 0$.

(3)利用混沌序列的密钥(产生混沌序列的初始条件)生成混沌序列,把生成的混沌序列与 W' 异或进行解密得到水印序列 W ,最后对水印序列 W 进行升维操作还原出二值水印图像.

3 仿真实验结果

实验用的水印图像为 56×56 的二值图像,载体图像为 536×536 的灰度图像. Logistic 映射的初始条件为 $x_0 = 0.4123$,控制参数 $\lambda = 4$. 根据矩阵 A 对子块的 DCT 系数进行选择,以两个行相邻系数作为 DCT 系数对. 实验平台为 MATLAB 6.5.

水印嵌入和提取的结果如图 1 所示,说明本算法的水印加密、隐藏以及提取效果都是非常好的.

为定量说明水印算法的隐蔽性和鲁棒性,在此用客观评价标准峰值信噪比(PSNR)和相关系数(NC)来度量. 峰值信噪比的定义为^[5]:

$$PSNR = 10 \log \frac{225^2}{MSE} \quad (4)$$

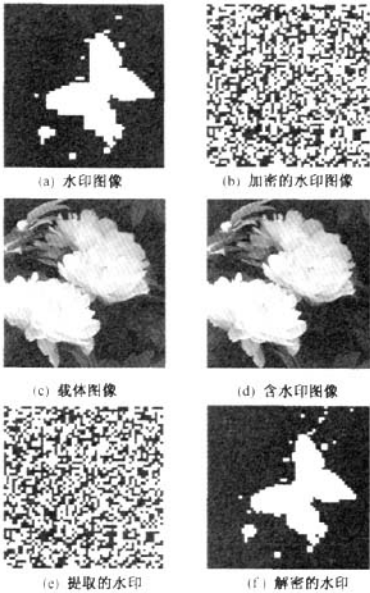


图1 水印的嵌入与提取结果

Fig.1 Watermark embedding and extraction

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (S'(i,j) - S(i,j))^2 \quad (5)$$

式中: S' 和 S 分别表示嵌入水印的载体图像和原始载体图像; $M \times N$ 表示图像大小.

相关系数 NC 用来衡量原始水印和提取水印的相似性.其定义为^[5]:

$$NC = \frac{\sum_{x=1}^M \sum_{y=1}^N w(x,y)w'(x,y)}{\sum_{x=1}^M \sum_{y=1}^N w(x,y)w(x,y)} \quad (6)$$

式中: $w(x,y)$ 和 $w'(x,y)$ 分别表示原始水印和提取水印.

实验测得峰值信噪比 $PSNR = 72.660\ 2\ \text{dB}$,说明载体图像受损极小,同时也证明水印的隐蔽性很强.

为了验证本水印算法的鲁棒性,对图像进行了剪切、抽取、椒盐噪声、滤波等多种处理和攻击.实验结果如图2所示,相关系数(NC)测试结果如表1所示.从实验结果来看,本算法可以经受剪切、抽取、椒盐噪声、滤波等处理和攻击,具有较强的鲁棒性.

与已有算法^[6]相比,本算法的贡献在于水印透明性好且可以盲提取,实用性更强.

表1 相关系数 NC 测试结果

Tab.1 The results of the NC test

条件	未受攻击	椒盐噪声	剪切	抽取破坏	滤波
NC	1	0.965 5	0.924 5	0.887 9	0.902 1

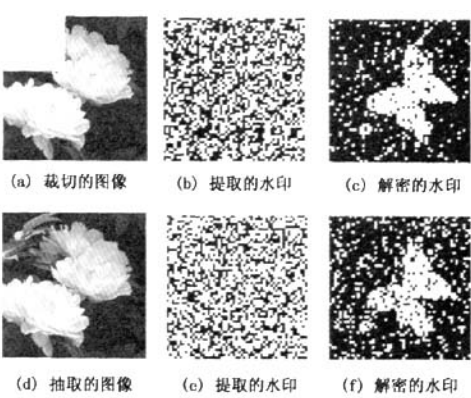


图2 算法鲁棒性测试结果

Fig.2 Results of the robustness test

4 结束语

笔者基于Logistic映射的数字水印技术,采用混沌序列对水印加密,同时又引入生成矩阵 A 和随机选择矩阵行列构成系数对等措施,形成了对水印的三级加密保护体系.根据人类视觉系统(HVS)的照度掩蔽特性和纹理掩蔽特性选择合适的水印嵌入区域,在每一块上合理选择嵌入位置和嵌入数量,而且使用相邻DCT系数对进行1bit水印嵌入,达到了鲁棒性和透视性的统一,此外水印还实现了盲检测.本算法具有加密简单、速度快、稳健性强等优点,具有较强的实际应用价值.

参考文献:

[1] 陈永强.一种基于混沌加密的自适应图像水印方法[J].计算机应用,2007(10):2453-2455.
[2] 胡梅,高万林.基于Logistic映射的小波域图像加密技术[J].中国农业大学学报,2006,11(3):98-100.
[3] PLANITZ B M, MAEDER A J. A Study of Block-based medical image watermarking using a perceptual Similarity Metric[A]. In Proc of the DICTA 2005[C]. 2005:856-859.
[4] 张登银,孙俊彩.空间域信息隐藏算法性能分析[J].微机发展,2005(12):53-55.
[5] 余波,陈建勋等.基于整数小波变换和混沌映射的盲数字水印算法[J].计算机与自动化,2008(3):54-55.
[6] 徐振启,卢洵,罗少鹏.基于时空二维混沌的自适应彩色图像水印算法[J].郑州大学学报:工学版,2007,28(2):84-87.

(下转第112页)

上的信息提供更为可靠的保护。

参考文献:

- [1] BERROU C, GLAVIEUX A, THITIMAJSHIMA P. Near shannon limit error - correcting and decoding: Turbo - codes [A]. 1993 IEEE Int Conf on Communication [C]. 1993:1064 - 1070.
- [2] BENEDETTO S, MONTORSI G. Design of parallel concatenated convolutional codes [J]. IEEE Trans On Communications, 1996, 44(5):591 - 600.
- [3] TAKESHITA O Y, COSTELLO D J. New deterministic interleaver designs for turbo codes [J]. IEEE Trans On Information Theory, 2000, 46(6):1988 - 2006.
- [4] FENG W, YUAN Y, VUCETIC B S. A code - matched interleaver design for turbo codes [J]. IEEE Trans On Commu, 2002, 50(2):926 - 937.
- [5] 张卫党, 袁聪, 王新梅. 分解法求 Turbo 码的低码重分布 [J]. 系统工程与电子技术, 2005, 27(7): 1207 - 1210.
- [6] 王新梅, 肖国镇. 纠错码—原理与方法 [M]. 西安: 西安电子科技大学出版社, 2001.

Analysis of the Ber Distributions of Interleavers

SHAO Xia¹, ZHANG De - hui², ZHANG Wei - dang²

(1. Department of Information Engineering, North China University of Water Conservancy and Electric Power, Zhengzhou 450011, China; 2. School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China)

Abstract: The ber distributions, which can give a detailed description about the error correcting ability of error control codes, are introduced in this paper to analyze the interleavers of 3GPP interleaver, block interleaver and random interleaver. The ber distributions are given under different puncturing patterns. The results show that the ber distribution of block interleaver is periodic apparently and that of the random interleaver is spread more randomly. As for the 3GPP interleaver, because of its combination construction, its ber distribution has the advantages of both block and random interleavers, i. e. it has more flat distribution and lower averaged ber.

Key words: error - control code; Turbo code, interleaver; biterror; 3gpp

(上接第 108 页)

A Blind Detection Digital Watermarking Algorithm Based on Pairs of Blocks DCT Coefficients

LU Ling, SUN Xin - de

(Department of Computer Science and Application, Zhengzhou Institute of Aeronautical Industry Management, Zhengzhou 450015, China)

Abstract: A new blind detection digital watermarking algorithm based on Logistic mapping is proposed in this paper, which can be more effective for digital media copyright protection. At first watermarking image is encrypted by the chaotic sequence generated by Logistic mapping. According to the human visual system (HVS) some small blocks with size 8×8 that have more texture complexity will be chosen. In each chosen sub-block some DCT coefficients are selected effectively in accordance with the property of common digital signal processing. Each pair of adjacent DCT coefficients can carry one bit watermarking information. Simulation experiments show that the algorithm improves effectively the robustness and the systems security.

Key words: logistic mapping; digital watermark; robustness; blind detection