

一种基于 Amold 变换的彩色图像水印算法

李树全, 房冬丽

(电子科技大学 信息与软件工程学院, 四川 成都 610054)

摘 要: 提出了一种基于彩色图像的新型 LSB 半盲数字水印方案, 该方案特点在于通过 Amold 算法置乱水印增强安全性, 将彩色图像作为信息隐藏的载体, 把处理后的水印信息分别隐藏在载体图像的 R、G、B 三个色彩空间. 实验结果表明, 该算法不仅提高了水印的嵌入容量, 而且对图像剪切、滤波和旋转等攻击具有较好的鲁棒性.

关键词: 数字水印; Amold 变换; 彩色图像

中图分类号: TP309

文献标识码: A

文章编号: 1000—7180(2017)01—0053—05

Watermarking in Color Image Based on Amold Transformation

LI Shu-quan, FANG Dong-li

(School of Information and Software Engineering, University of Electronic
Science and Technology of China, Chengdu 610054, China)

Abstract: A new semi-blind color image watermarking algorithm based on Amold transformation was proposed, which featured the following characteristics as scrambling the watermark to enhance the security and embedding watermark information into the R, G, B color space according to the embedding algorithm. The experimental results have shown that the algorithm not only improves embedding capacity of watermark, but also robust against various signal processing attacks such as cropping, filtering and rotation.

Key words: digital watermarking; Amold transformation; color image

1 引言

图像数字水印算法主要包括空间域算法和变换域算法. 变换域算法主要包括 DFT、DCT、DWT 以及多种变换域相结合的算法^[1-3], 空域算法主要包括基于修改像素亮度值的 patchwork 算法^[4]和基于 LSB 的算法^[5-6]. 基于 LSB 的算法即用水印信息代替图像中每个像素点的最低一位或者最低几位, 水印信息嵌入在像素点的最低位, 对图像的视觉效果影响最小, 不会对图像造成严重的失真. 目前, LSB 算法几乎都是基于灰度图像的, 灰度图像可以看成是一个二维矩阵, 利用图像加密技术对水印信息进行预处理, 然后把处理后的水印信息代替矩阵中每个元素(每个像素点 8 位)的最低位, 这样水印的容量就是载体图像的 1/8, 如果代替最低两位, 则容量可

达到载体图像的 1/4. LSB 算法容量大、速度快但安全性和鲁棒性不高, 不能很好应对图像几何攻击、噪声攻击以及滤波攻击等攻击方法.

本文提出了一种基于彩色图像的新型 LSB 半盲数字水印方案, 整个算法简单, 并且具有良好的不可见性和鲁棒性.

2 数字图像

一幅图像是由很多个像素点组成, 像素是构成图像的基本元素. 图像可以分成灰度图像和彩色图像.

灰度图像指每个像素只有一个采样颜色图像, 这类图像常常显示为从最暗黑色到最亮白色的灰度, 从理论上讲这个采样可以是任何颜色的不同深浅, 甚至可以是不同亮度上的不同颜色. 黑白图像只

有黑色与白色两种颜色,但灰度图像在黑色与白色之间还有许多级的颜色深度.灰度图像可以在单个电磁波频谱(如可见光内)测量每个像素的亮度得到的,灰度图像通常用每个采样像素 8 位来保存,这样有 256 级灰度(如果是 16 位,则有 65 536 级).

彩色图像可看作是 3 个类似于灰度图像的矩阵.即指图像中每个像素的值都可以分成 R、G、B 三个基色分量,每个分量直接决定其基色的强度.例如图像深度为 24,用 R:G:B=8:8:8 来表示色彩,R、G、B 分量各占用 8 位来表示各基色分量的强度,每个基色分量的强度等级为 $2^8=256$ 种,可容纳 $2^{24}=16M$ 种色彩.

3 Arnold 变换

图像加密技术主要有两大类型:一是改变像素值,二是改变像素点的位置.典型的改变像素值的有 Logistic 变换,改变像素点位置的是 Arnold.本文采用 Arnold 变换对水印进行加密处理.

Arnold 是俄国数学家 Vladimir I. Arnold 提出的,变换原理是改变像素点的位置,将原来点 (x,y) 处的像素移动变换到点 (x',y') 处.一幅 $N \times N$ 的数字图像的 Arnold 变换定义为

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \tag{1}$$

式中, $x,y \in \{0,1,2,3,\cdots,N-1\}$ 表示变换前像素的位置, x',y' 表示变换后的像素位置,mod 是模运算.数字图像可以看成是一个二维矩阵,Arnold 变换之后图像的像素位置会重排,这样图像会显得杂乱无章,从而实现对图像的置乱加密效果. Arnold 置乱具有周期性^[5],并且周期性与图像的大小存在一定的关系,但不是正比例关系,表 1 给出了图像大小和其周期性之间的关系:

表 1 变换周期与图像阶数之间的关系

阶数 N	周期 T	阶数 N	周期 T
4	3	80	60
8	6	110	30
16	12	128	96
32	24	256	62
64	48	512	384

加密算法的步骤如下所示.

- (1)根据水印图像的大小计算 Arnold 变换的周期 T .
- (2)将二值图像的信息存储在一个矩阵中, x,y

代表一个像素点的位置, x',y' 代表变换后像素点的位置.按照 $x' = x + y,y' = x + 2y$,对水印图像进行 n 次变换.

解密算法实际上是对加密后的水印图像进行 $T - n$ 次变换,这样两次变换的次数和是一个周期 T ,从而实现了图像的还原.

一幅 510×510 的图像置乱周期是 384,可以在加密阶段置乱 n 次($n \leq 384$,这样在解密阶段执行 $(384 - n)$ 次即可恢复原图像.图 1 是一幅图像的置乱效果图.

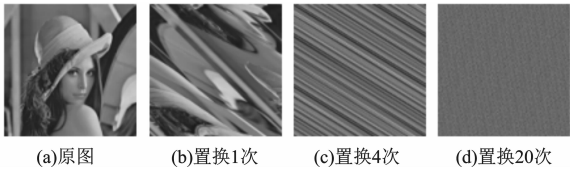


图 1 Arnold 图像加密

由图 1 可以得到,一幅 510×510 的图像,当置乱次数很小时,可以看出图像的信息,当置乱次数为 20 时,已经很难发现原始图像的信息了.可以根据原始图像的变换周期选择合适的变换次数就可以达到很好的置乱效果.

4 LSB 半盲水印嵌入与提取

本算法由水印预处理、水印嵌入、水印提取三部分组成.水印处理利用 Arnold 变换,变换后的水印信息具有更高的安全性;水印嵌入是将加密后的水印信息隐藏到载体图像中;水印提取将加密后的水印信息从载体图像中提取出来并进行解密.

4.1 水印信号生成

为增强水印的保密性,本文采用 Arnold 变换^[7]对水印图像进行加密,其中水印图像是 $N * N$ 的二值图像.根据文献[5],由于 Arnold 变换具有周期性,可计算出 $N * N$ 水印图像的变换周期 T ,对水印图像进行 K 次变换,得到加密后的水印信息,并记录 K 的大小.

4.2 水印嵌入算法

(1)嵌入点的选择.本文提出一种改进的 LSB 算法,它不是在每个像素点的最低位进行替换,而是通过一个 3×3 矩阵来选择嵌入水印信息的像素点.这个 3×3 矩阵在载体图像上移动,判断其 8 邻域和中间像素点的差值,如果差值的绝对值小于等于阈值 t (根据文献[8],每个邻域可能都在一个集合范围内),找出满足邻域在一个集合内的像素点,则说明是可以嵌入水印的像素点,否则继续寻找下一个

合适的像素点. 为了记录嵌入水印的位置,生成一个和载体图像相同大小的零矩阵,如果一个像素点符合预定的嵌入条件,则在对应的位置上置 1,用于在提取阶段确定哪些位置嵌入了水印信息. 像素 $P(i, j)$ 的邻域如表 2 所示.

表 2 $P(i, j)$ 的邻域		
$P(i-1, j-1)$	$P(i-1, j)$	$P(i-1, j+1)$
$P(i, j-1)$	$P(i, j)$	$P(i, j+1)$
$P(i+1, j-1)$	$P(i+1, j)$	$P(i+1, j+1)$

(2)读入载体图像,并进行 R、G、B 三个颜色通道的分离,将分离后的三个通道信息保存在三个矩阵中,用上述步骤在每个通道上进行寻找满足预定条件的像素点,将预处理后的水印序列置换这些像素点的最低位.

(3)将被置换的三个颜色通道合称为含有水印的彩色图像.

LSB 半盲鲨鱼了嵌入模型如图 2 所示.

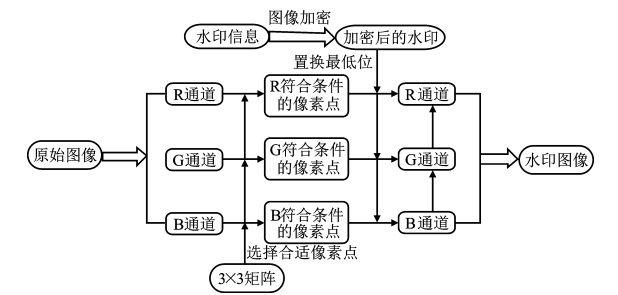


图 2 LSB 半盲水印嵌入模型

4.3 水印提取算法

提取是嵌入的逆过程,并且不需要原始图像,只需要知道原始水印信息的大小.

(1)读取含水印的图像,并对其进行 R、G、B 三个颜色通道分离,存储在三个矩阵中.

(2)利用嵌入过程中生成的零矩阵,寻找其中值为 1 的点,该点对应的水印图像像素点即是嵌入了水印信息的像素点,将其最低位取出放到 sequence 序列中,这个 sequence 序列即保存了水印信息.

(3)将这个提取出的 sequence 序列按照原始水印的大小进行恢复处理,得到提取的水印图像. 并根据水印预处理阶段的 Arnold 变换次数 K 和变换周期 T ,再进行 $(T-K)$ 次变换,即可恢复水印图像.

由于提取的水印与原来的水印可能存在一定的差异,这就需要一个客观的评价标准来衡量提取的水印与原水印之间的相似程度. 除了主观感觉上的判断,还可以通过归一化相似程度计算公式来

评判^[9]:

$$NC = \frac{\sum_{m,n} W_{m,n} W'_{m,n}}{\sum_{m,n} W_{m,n}^2}$$

(2)

式中, $W'_{m,n}$ 表示提取出的水印, $W_{m,n}$ 表示原始载体嵌入的水印.

针对载体图像和含水印图像的相似度衡量可以使用峰值信噪比,表示嵌入水印后的失真程度:

$$PSNR = \frac{M * N * \max_{m,n} I_{m,n}^2}{\sum_{m,n} (I_{m,n} - I'_{m,n})^2}$$

(3)

式中, $I_{m,n}$ 和 $I'_{m,n}$ 分别代表原始图像和嵌有水印图像的相应坐标的像素值.

5 实验结果与分析

本文采用 88×88 的灰度图像为水印图像,载体图像采用 400×300 的彩色图像. 对于 88×88 的水印图像经过计算其置乱周期是 30,这里取置乱次数为 8 进行仿真实验. 嵌入水印的效果图如图 3 所示.

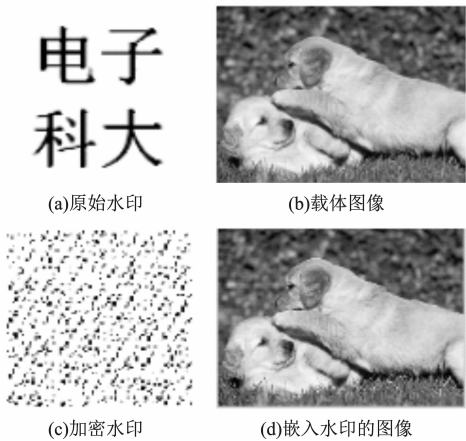


图 3 水印、载体图像、加密水印和嵌入水印图像

在未受到攻击时提取的水印信息和原始水印信息对比如图 4 所示,通过峰值信噪比和归一化相似程度计算公式得出 $PSNR = 31.1943$, $NC = 0.9427$.



图 4 提取水印

5.1 不同攻击条件下算法的鲁棒性

图像在传输或使用过程中可能会受到各种攻

击,本文攻击主要有剪切攻击、旋转攻击、噪声攻击、滤波攻击等.在含有水印信息的彩色图象中加入相应的攻击,然后按照水印提取算法,对经过攻击后的水印进行提取,从而证明该算法具有较好的鲁棒性.

(1)高斯滤波攻击

对嵌入水印的图像进行高斯滤波攻击,滤波参数分别为 0.1,0.2,0.3,0.4,从受到高斯滤波攻击后的图像中提取水印信息,得到的水印信息与原始水印信息的相似度分别为 0.930 9,0.913 9,0.907 3,0.858 8.由图 5 可以看出在参数为 0.4 时,仍可以正确的提取水印信息.

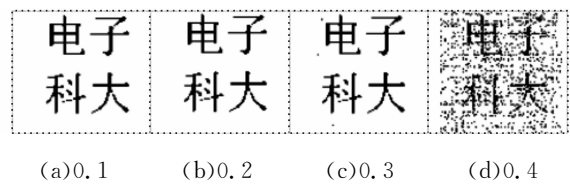


图 5 高斯滤波攻击

(2)旋转攻击

对嵌入水印的图像进行旋转攻击,分别旋转的度数为 1°,2°,4°,8°,从受到旋转攻击的图像中提取水印信息,得到的水印信息与原始水印的相似度分别为 0.909 9,0.906 6,0.897 4,0.821 8.由图 6 可知该算法对旋转攻击具有一定的抵抗能力,旋转 8°时还可以看出提取的水印.

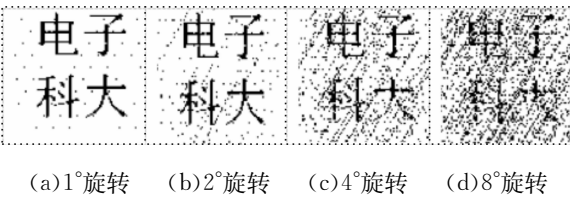


图 6 旋转攻击

(3)剪切攻击

对嵌入水印的图像进行剪切攻击(见图 7),分别剪切掉 10%,25%,50%,75%,从受到剪切攻击的图像中提取水印信息,得到的水印信息与原始水印的相似度分别为 0.962 1,0.920 3,0.912 3,0.893 7.



图 7 剪切攻击

各种攻击情况下提取出的水印和原水印的相似度对比如表 3 所示.

表 3 原水印和提取出的水印相似度对比

攻击方法	NC	攻击方法	NC
0.1 高斯滤波	0.930 9	4°旋转攻击	0.897 4
0.2 高斯滤波	0.913 9	8°旋转攻击	0.821 8
0.3 高斯滤波	0.907 3	10%剪切攻击	0.962 1
0.4 高斯滤波	0.858 8	25%剪切攻击	0.920 3
1°旋转攻击	0.909 9	50%剪切攻击	0.912 3
2°旋转攻击	0.906 6	75%剪切攻击	0.893 7

5.2 同类算法实验结果对比

本文采用的算法与大部分 LSB 算法的不同之处在于采用彩色图像作为载体图像,对于彩色图像的处理要比灰度图像复杂,但其优点在于彩色图像可分离为 RGB 三个颜色空间,在三个颜色空间嵌入相同的水印信息可提高算法的安全性同时嵌入水印信息其容量可以达到灰度图像的三倍.本文和文献[10]都是基于 LSB 算法的水印算法,我们在相同的攻击条件下对实验结果进行了对比,一是对图像进行 50%的剪切攻击,二是进行 0.01 的高斯噪声攻击,可以看出本文算法具有较好更好的鲁棒性,参见图 8.



(a)文献[10]中的效果 (b)本文效果

图 8 方案攻击效果对比
算法参数对比如表 4 所示.

表 4 算法对比

NC	50%剪切攻击	0.01 高斯噪声攻击
本文算法	0.912 3	0.911 0
文献[10]算法	0.881 6	0.871 3

6 结束语

数字水印一般需要具有安全性、鲁棒性、隐蔽性等特点.本文用 Amold 变换对有意义的灰度水印图像实现置乱加密,近似满足“一次一密”要求,具有良好的安全性,将彩色图像作为信息隐藏的载体,对

LSB 水印算法进行了改进,提出一种基于模板矩阵来选择符合一定条件的像素点,把处理后的水印信息分别隐藏到载体图像的 R、G、B 三个色彩空间,从而提高了水印容量。实验结果表明,本文算法对各种常见的攻击均具有一定的抵抗能力,能够满足实际应用中的需求,有效地解决数字作品的版权保护问题和为信息完整性提供保证。

参考文献:

- [1] Huang Zhanping, Liu Jinxing, Lv Qing, et al. Digital watermarking algorithm based on spread spectrum and fourier transform[C]//3rd International conference on Management, Education, Information and Control. Shenyang, 2015.
- [2] Cedillo-Hernandez, Garcia-Ugalde, Nakano-Miyatake, Perez-Meane. Robust hybrid color image watermarking method based on DFT domain and 2D histogram modification[J]. Signal image and video Processing, 2014, 8 (1):49-63.
- [3] Deepti Shukla, Nirupama Tiwari, Deepika Dubey. Survey on digital watermarking technologies[J]. International Journal of Signal Processing, Image Process-
- ing and Pattern Recognition, 2016, 9(1):239-244.
- [4] Ingemar J Cox, Linnartz J P. Some general methods for tampering with watermarks[J]. IEEE Journal on Selected Area in Communication, 1998, 16 (4): 587-593.
- [5] 李刚. 一种改进的 LSB 数字水印技术研究[J]. 现代计算机, 2015, 32(2):69-73.
- [6] 马刚,蒋志新,卫红春. 一种基于 LSB 的易碎性数字盲水印算法[J]. 微电子学与计算机, 2008, 25(8):49-50.
- [7] 和煦,常淑娟. Arnold 变换在 LSB 算法中的应用研究[J]. 通信与信息技术, 2008, 31(19):77-79.
- [8] 章毓晋. 图像处理和分析技术[M]. 北京:高等教育出版社, 2008.
- [9] 于万波. 基于 matlab 的图像处理[M]. 北京:清华大学出版社, 2008:1-201.
- [10] 江营,周萍. 基于混沌和 LSB 的盲水印算法研究[J]. 仪器仪表与分析监测, 2009, 26(4):16-18.

作者简介:

李树全 男, (1971-), 硕士, 高级工程师. 研究方向为信息安全、数字水印等. E-mail: shuquanli@uestc.edu.cn.

(上接第 52 页)

- [5] Sen S, Xiong J, Ghosh R, et al. Link layer multicast with smart antennas: No client left behind [C] // IEEE International Conference on Network Protocols. Orlando: IEEE, 2008:53-62.
- [6] Donghoon Lee, Sung-Il Kim, Jaeyoung Lee, et al. Performance of multihop decode-and-forward relaying assisted Device-to-Device communication underlaying cellular networks [C] // Information Theory and its Applications. Hawaii: IEEE, 2012: 455-459.
- [7] Zhou B, Hu H, Huang S, et al. Intra-cluster device-to-device relay algorithm with optimal resource utilization [J]. IEEE Transactions on Vehicular Technology, 2013, 62(5): 2315-2326.
- [8] 王俊义, 巩志帅, 符杰林, 等. 基于多跳 D2D 转发的簇内数据共享方案[J]. 计算机科学, 2015, 42(8): 124-127.
- [9] Kaufman Brett, Azhang Behnaam. Cellular networks with an overlaid device to device network[C]//Asilomar Conference on Signals, Systems and Computers. Pacific Grove: IEEE, 2008: 1537-1541.
- [10] 文凯, 卢彦博, 刘敏, 等. D2D 通信系统中一种资源分配算法的研究[J]. 南京邮电大学学报, 2015, 35(6): 31-38.
- [11] 李方健. D2D 通信系统中的最优中继选择及功率分配策略研究[J]. 重庆邮电大学学报, 2015, 26(5): 605-610.
- [12] Li Zhou, Feng Yan. The complexity of routing algorithm in small world networks [C] // International Conference on Computer Science and Electronics Engineering. Hangzhou: IEEE, 2012:423-427.

作者简介:

马 克 男, (1964-), 硕士, 教授. 研究方向为网络通信技术. E-mail: makelucky@tom.com.

吴 洋 男, (1988-), 博士, 讲师. 研究方向为无线通信技术、无线网络安全防护.