文章编号: 1671-8860(2006)09-0832-03 文献标志码: A

基于随机分块的脆弱性水印算法设计

李 睿[1] 李 明[1] 张贵仓[2]

(1 兰州理工大学计算机与通信学院, 兰州市兰工坪路287号, 730050)
(2 西北师范大学数学与信息科学学院, 兰州市安宁东路967号, 730070)

摘 要: 提出了一种基于混沌系统的图像脆弱性水印(易损水印)算法。经过验证, 此算法设计较为合理, 具有良好的性能, 能达到满意的效果。

关键词: 数字水印; 脆弱; 混沌映射
中图法分类号: P237.3

在信息化社会, 数字化信息与网络给人们带来方便的同时也带来了隐患, 敏感信息可能轻易地被窃取、篡改、非法复制和传播等。因此, 信息的安全与保护显得越来越重要, 已成为人们关心的焦点, 也是当今信息领域研究的热点之一[1-2]。目前公认的解决该问题的比较有效的技术是数字水印技术。

数字水印技术属于信息隐藏的范畴[3-4], 数字水印主要有鲁棒水印与脆弱水印两种[5-6]。鲁棒水印主要用于版权保护, 具有很强的鲁棒性, 不容易被破坏; 脆弱水印主要用于数字信息的完整性保护, 随着数字作品的破坏而被破坏。它能够根据其受破坏的情况进行动态跟踪, 从而实现对数字信息被篡改区域的定位, 是当前数字水印技术研究的一个重点内容。

1 混沌系统

混沌现象是在非线性动力系统中出现的确定性的、类似随机的过程, 这种过程既非随机又非收敛, 并且对初始值具有极其敏感的依赖性。通过混沌系统对初始值的敏感依赖性, 可以提供数量众多、非相关、类随机而又确定可再生的信号。

一类非常简单却被广泛研究的动力系统是Logistic映射, 其定义如下:

$$X_{k+1} = \mu X_k(1 - X_k)$$

其中, $0 \leqslant \mu \leqslant 4$ 称为分支参数, $X_k \in (0, 1)$, $k = 0, 1, 2, \cdots$, 称之为状态。如果从一个初始状态 X_0 开始, 反复应用上述映射, 就得到一个混沌序列 $\{X_k \mid k = 0, 1, 2, \cdots\}$, 那么, 这一序列就称为该离散时间动力系统的一条轨迹。

混沌动力系统的研究工作者指出[7], 当 $3.569\,945\,6 < \mu \leqslant 4$ 时, Logistic映射工作于混沌状态。也就是说, 有初始条件 X_0 在Logistic映射的作用下所产生的序列 $\{X_k \mid k = 0, 1, 2, \cdots\}$ 是非周期的、不收敛的并对初始值非常敏感的。利用这一特性来控制水印序列的生成, 使得不知道初值(即密钥)的人无法破坏、复制水印信息, 这对系统的安全性是非常重要的。

2 脆弱水印算法设计

2.1 水印的生成

原始图像为 $I_{M \times N}$, M 和 N 分别是图像的宽度和高度。

水印是基于图像内容生成的。在文献[5]中采用了对图像任一元素进行混沌映射的方法, 虽然定位效果不错, 但实现时的时间性能较差。为了改进这个缺陷, 本算法首先将图像的LSB位平面置零后不重叠分块, 求出各块灰度平均值, 利用混沌系统将其映射为二值序列, 嵌入到图像的LSB平面上。

密钥的产生方法如下: 利用Logistic混沌系统产生混沌序列——图像拥有者首先生成自己的

收稿日期: 2006-06-28。
项目来源: 甘肃省自然科学基金资助项目(3ZS042-B25-007); 甘肃省科技攻关计划资助项目(IGS035-A052-011)。

关键密钥 key,以 key 作为混沌映射初值,产生一个混沌序列{$X_k \mid k=0,1,2,\cdots,s$}($s$ 的个数由图像的分块数决定),再以离散化的 x_k 序列作为混沌映射的次数(此为系统的第二级密钥)对灰度平均值进行映射,最后通过二值映射函数 Q 将结果映射为 0、1 序列作为水印信息。

水印生成的具体过程如图 1 所示。

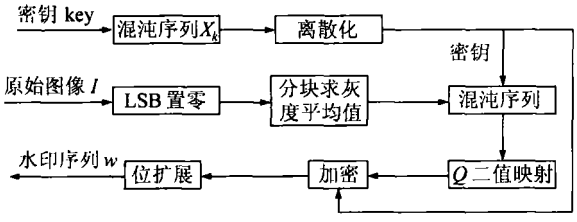

图 1　水印的流程

Fig. 1　Framework of Watermarking

1) 原始图像 $I_{M\times N}$ 可以分成 $c_1 \times c_2$ 任意大小的块(c_1、c_2的大小任意可以保证水印的安全性,c_1 可以为 1~ M 之间的任一值,c_2 可以为 1~ N 之间的任一值,一般取 M/c_1 和 M/c_2 为整数,以保证能完整地分割原始图像),那么总的块数是 $M/c_1 \times N/c_2$;

2) 对分块灰度平均值利用离散序列进行混沌映射得到的新序列,再利用 Q 二值映射函数映射并加密后得到二值序列 W'_s(s: 1~ $M/c_1 \times N/c_2$)。假设嵌入时将原始图像同样分为 $c_1 \times c_2$ 大小的块,则扩张因子为 $l=c_1 \times c_2$。那么嵌入原图像第 j 块水印序列 $W[j]$的扩展规则如下:

$$W[j]=\begin{cases}1 & W'_s=1\\ 0 & W'_s=0\end{cases} \quad ls \leqslant j \leqslant l(s+1)$$

即一个比特的水印信息由 l 个比特的序列携带,冗余度越大,水印的抗攻击能力越强。

2.2　水印的嵌入

水印在嵌入时为了增加系统的安全性,我们首先对分块之后的原始图像用约瑟夫环序列进行置乱,其中置乱时所选择的起始位置 start 和步长 skip 是从混沌序列 X_k 中随机选取的两个值 key_1、key_2,使 start= key_1, skip= key_2(这两个值可以作为整个算法的二级密钥,在下面的仿真实验中,选择 skip 和 step 均为 10)。

嵌入效果如图 2 所示,从视觉上看不出嵌入水印后有什么变化。从所对应的峰值信噪比 PSNR 和均方误差 MSE 得知,其嵌入效果是非常好的,PSNR= 51.121, MSE= 0.502 323。

2.3　水印的提取及完整性验证

对于脆弱性水印系统而言,水印的提取一般

图 2　水印嵌入后图像

Fig. 2　Image with Embedded Watermarking

应实现盲检测。本算法在检测时既不需要原始图像,也不需要知道原始水印,惟一需要的是在嵌入时所使用的用户关键密钥 key。检测和完整性验证过程如图 3 所示。

检测矩阵 Test= $\mid W-W' \mid$,其中 Test 中等于 1 的点即为被篡改的像素点。

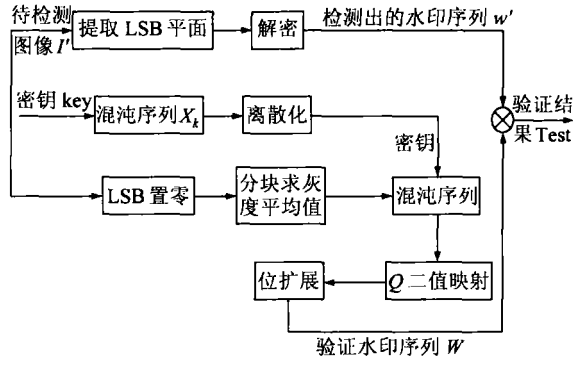

图 3　实验流程

Fig. 3　Framework of Experiment

3　实验结果与性能分析

3.1　实验结果

为了测试算法的性能,笔者用一组实验来验证算法的定位能力,结果如图 4~ 图 6 所示。

对于图 4~ 6 所示实验结果,笔者所计算出的被篡改图像与原图像相比较的 PSNR 和 MSE 如表 1 所示。

3.2　性能分析

1) 敏感性。一般通过 PSNR 来衡量嵌入水印图像和原始图像之间的差别。本文提出的算法

表 1　被篡改图像 PSNR、MSE

Tab. 1　PSNR and MSE of Attacked Image

攻击类型	值	
	PSN	RMSE
椒盐噪声(0.5%)	32.115	39.958
剪切(32× 32)	33.856 6	26.759 9
替换(32× 32)	36.679 7	13.967 3

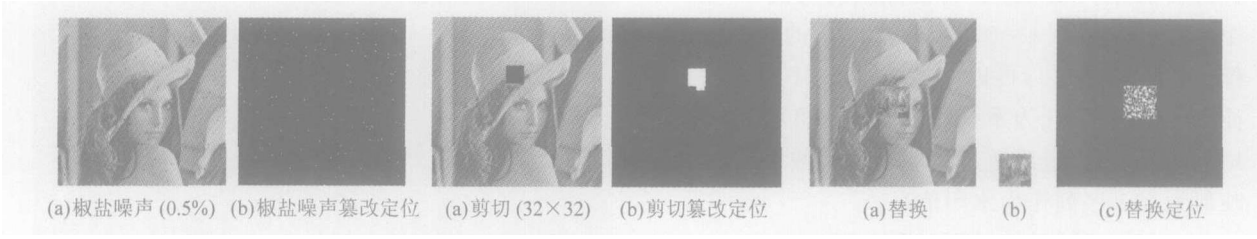

图 4 椒盐噪声检测
Fig. 4 Testing of Adding Salt and Pepper Noise

图 5 剪切检测
Fig. 5 Testing of Cropping

图 6 替换检测
Fig. 6 Testing of Replacing

PSNR= 51. 121; 而文献[8] 的 PSNR= 51. 18, 低于本文算法。

2) 篡改定位能力。本文中通过理论上的篡改像素数和实际检测到的篡改像素数的比较来进行篡改定位能力的分析。文献[8] 中相应像素被篡改而检测到的概率为 50%; 本文中从理论上分析仍为 50% (由混沌的伪随机性得出), 但通过对上面的实验结果分析, 就 0. 5% 椒盐噪声而言, 理论上的篡改像素数为 1 310, 而实际检测到的篡改像素数为 1 244, 即被篡改而检测到的概率为 95% , 远远高于 50%。

3) 安全性。由于算法利用了混沌映射的非周期、不收敛并对初始值非常敏感的特性, 所以整个系统的安全性仅仅依赖于用户的关键密钥 key, 算法完全可以公开; 同时算法利用了混沌系统的特性, 所以要想通过蛮力获得系统的各级密钥从而重构混沌序列几乎是不可能的, 这对于算法的安全性是非常重要的。

参 考 文 献

[1] Bender W, Gruhl D, Morimoto N, et al. Techniques for Data Hiding[J]. IBM System Journal, 1996, 35 (3/4): 313-335

[2] Petitcolas F A P, Anderson R J, Kuhn M G. Information Diding: a Survey[J]. IEEE, 1999, 87(7): 1 062-1 078

[3] 吴秋新, 钮心析, 杨义先, 等. 信息隐藏技术——隐写术与数字水印[M]. 北京: 人民邮电出版社, 2001

[4] 张贵仓, 章毓晋, 李睿. 图像混合信息隐藏技术的研究[J]. 西北师范大学学报. 2003, 39(4): 35-38

[5] 王宏霞, 何晨, 丁科. 基于混沌映射的鲁棒性公开水印[J]. 软件学报, 2004, 15(8): 101-105

[6] Cox I J, Kilian J, Leighton F T, et al. Secure Spreadspectrum Watermarking for Muitimedia[J]. IEEE Trans. on Image Processing, 1997, 6 (12): 1 673-1 687

[7] Cox I J, Miller M L, Bloom J A. 数字水印[M]. 王颖, 黄志蓓译. 北京: 电子工业出版社, 2003

[8] 丁科. 一种定位精确的脆弱数字水印技术[J]. 电子学报, 2004, 32(6): 1 009-1 012

第一作者简介: 李睿, 讲师, 硕士, 研究方向为图形图像处理、数字水印。
E-mail: lirui@ nwnu. edu. cn

Design of Fragile Watermarking Algorithm Based on Random Blocks

LI Rui[1] *LI Ming*[1] *ZHANG Guicang*[2]
(1 College of Computer and Communication, Lanzhou University of Technology, 287 Langongping Road, Lanzhou 730050, China)
(2 College of Mathematics and Information Science, Northwest Normal University, 967 East Anning Road, Lanzhou 730070, China)

Abstract: The fragile digital watermarking scheme is presented. The results of experiments reveal that the scheme presented here is greatly practical, with an excellent ability to locate juggling actions and of high security, as the same time, because of non-overlapping, time complexity is good than others algorithm.

Key words: digital watermarking; fragile; chaotic mappin

About the first author: LI Rui, lecturer, master, majors in image processing, digital watermarking.
E-mail: lirui@ nwnu. edu. cn