Journal of Computer Applications
计算机应用,2013,33(5):1371 - 1373
ISSN 1001-9081
CODEN JYIIDU
2013-05-01
http://www.joca.cn

文章编号:1001 - 9081(2013)05 - 1371 - 03
doi:10.3724/SP.J.1087.2013.01371

基于混沌和脆弱水印的图像篡改检测算法

刘　敏[1,2],陈志刚[2],邓小鸿[3*]

(1.长沙航空职业技术学院 计算机系,长沙 410024;　2.中南大学 信息科学与工程学院,长沙 410083;
3.江西理工大学 应用科学学院,江西 赣州 341000)

(*通信作者电子邮箱 4011663@qq.com)

摘　要:针对现有基于脆弱水印方法的不足,提出了一种新的结合混沌系统和脆弱水印的图像篡改检测算法。算法首先利用 Arnold cat 映射对原始图像进行 k 次置乱,然后选取置乱图像的最低有效位(LSB)平面作为水印嵌入位置,实际嵌入的水印由 Logistic 混沌映射产生的随机二进制序列与原始水印异或得到,通过 LSB 替换算法嵌入。最后对 LSB 替换后图像进行 $T-k$ 次的 Arnold cat 映射得到水印图像。实验结果表明,混沌系统的引入大大增强了脆弱水印的安全性;另外,针对不同种类的攻击,算法具有良好的篡改检测和定位精确性。

关键词:混沌映射;脆弱水印;篡改检测;定位;安全性

中图分类号:TP391.4　　**文献标志码**:A

Image tamper detection scheme based on chaotic system and fragile watermarking

LIU Min[1,2], CHEN Zhigang[2], DENG Xiaohong[3*]

(1. *Department of Computer, Changsha Aeronautical Vocational and Technical College, Changsha Hunan* 410024, *China*;
2. *School of Information Science and Engineering, Central South University, Changsha Hunan* 410083, *China*;
3. *Collge of Applied Science, Jiangxi University of Science and Technology, Ganzhou Jiangxi* 341000, *China*)

Abstract: In order to solve the shortage of the method based on fragile watermarking, a new chaotic system and fragile watermarking based image tamper detection algorithm was proposed. Firstly, the method used Arnold cat map k times to scramble the original image, and then chose the Least Significant Bit (LSB) plane of the scrambled image as the embedding position. The actual watermark information was formed by using exclusive-or operation between a random binary sequence produced by Logistic map and the original watermark, and the LSB replacement method was utilized to embed watermark. Finally, the watermarked image was obtained by utilizing Arnold cat map $T-k$ times. The experimental results show that, the introduction of chaotic system to a great extend improves the security of the proposed scheme. In addition, the proposed method achieves superior tamper detection and localization accuracy under different common attacks.

Key words: chaotic map; fragile watermarking; tamper detection; localization; security

0　引言

随着网络和移动计算技术的飞速发展,越来越多的数字图像通过公网进行传输,图像的内容安全受到极大挑战。不断发展的数字图像处理技术也使得图像的篡改变得越来越容易,为了保证数字图像本身的使用价值,对网络上发布的数字图像进行篡改检测是十分必要的。图像的篡改检测即对图像的完整性进行认证,一旦证实图像遭到修改能正确定位篡改发生区域[1]。图像篡改检测方法主要有两种。一种是基于数字标识的方法[2],此类方法通过安全 Hash 函数得到整幅图像的认证码,然后将认证码随图像一起发布,接收端收到图像后重新计算认证码来判定图像是否遭到篡改;这类方法虽然简单有效,但不能定位篡改发生区域,而且需要额外的空间来存储图像的原始认证码。另外一种行之有效的方法是基于水印的方法,此类方法很好地解决了前一种方法的不足,通过将图像的认证水印以不可见方式嵌入在图像像素本身,不需额外空间并能实现篡改区域的定位。鉴于脆弱水印对图像像素修改的敏感性,绝大部分基于水印的图像认证方法采用脆弱水印技术[3-7]。

目前提出的基于脆弱水印的图像认证方法大致可分为两大类。第一类是基于像素的图像认证方法,这类方法为了实现对每个像素点的精确认证,需要将图像全部像素值嵌入在图像本身,水印嵌入容量的瓶颈问题制约了该方法的广泛使用。第二类是基于图像块的认证方法,是当前主流的图像认证技术,方法将图像进行分块,抽取每块的特征值作为水印嵌入在图像中,通过重新计算块的特征值和提出的值进行比较实现图像的篡改检测和定位。典型的方法如 Guo 等[4]提出的基于区域的图像认证方法中,将图像每块区域的 Hash 值作为水印嵌入,虽然 Guo 的方法能够对区域进行矩形和多边形的划分,但是不能对任意区域的篡改进行认证,另外水印的嵌入时间花费较大。为了提高算法效率,Phadikar 等[5]提出将图像块的均值作为水印,并利用修改的量化索引调制方法实现嵌入,该方法最大的缺点就是算法安全性不高,利用均值作为特征值进行篡改检测精确度不高。

为了解决当前图像认证方法中存在的水印算法安全性不高和篡改区域固定的缺点,本文提出了一种结合混沌系统和脆弱水印的图像认证新方法,该方法采用 cat 映射获取水印嵌入位置,然后采用 Logistic 映射生成混沌水印。混沌系统的

收稿日期:2012-12-04;**修回日期**:2012-12-31。

基金项目:国家自然科学基金资助项目(61103202, 61272494);江西理工大学校级科研项目(jxxj12149)。

作者简介:刘敏(1972 -),男,湖北新洲人,副教授,硕士,主要研究方向:网络与信息安全;　陈志刚(1964 -),男,湖南益阳人,教授,博士,CCF 会员,主要研究方向:信息安全;　邓小鸿(1982 -),男,湖北天门人,讲师,博士研究生,CCF 会员,主要研究方向:数字水印。

引入大大增强了算法的安全性，另外由于混沌系统的初始敏感性，混沌水印能精确定位图像任一像素和区域的篡改。

1 混沌系统

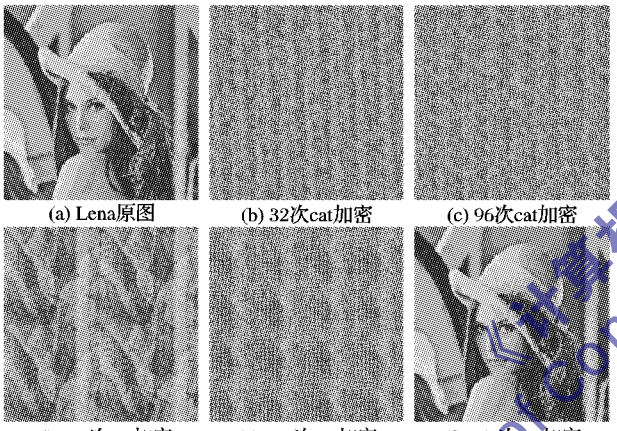
混沌系统具有随机性、确定性、初值敏感性和遍历性等良好特性，广泛应用于图像加密中[8-11]。近来，混沌系统逐步被引入到水印算法中增强其安全性，如采用混沌序列选择水印嵌入位置[7]。

1.1 Arnold cat 映射

Arnold cat 映射[12]是一个二维可逆的非线性系统，可由式(1)表示。

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \tag{1}$$

其中：a 和 b 为正整数，N 为原始图像的尺寸(以 512×512 图像为例，$N=512$)。Arnold cat 映射具有良好的周期性，也就是说一个坐标为 (x,y) 的像素点在经过 T 次迭代后会回到它原始的位置。T 的值由 a，b 和 N 的值决定，如当 $a=2$，$b=1$ 时，一幅 512×512 的 Lena 图像的周期 $T=256$。图 1 给出了 Lena 图像在经过指定次数 cat 映射后的图像。



(a) Lena原图 (b) 32次cat加密 (c) 96次cat加密

(d) 128次cat加密 (e) 192次cat加密 (f) 256次cat加密

图 1 Lena 图像的 cat 映射加密结果

1.2 Logistic 映射

Logistic 映射[12]是最简单的一种混沌映射系统，可由式(2)表示。

$$x_{n+1} = \mu x_n (1 - x_n) \tag{2}$$

其中 $\mu \in (0,4]$，当 $\mu \in (3.5699456,4]$ 时，x 的值呈现混沌状态。Logistic 映射产生的序列对初值具有高敏感性，即 $x(0)$ 取不同值时，获得 x 的值序列呈现截然不同的状态。另外，Logistic 映射产生的序列其值域为[0,1]。

2 本文算法

2.1 算法总体模型

本文算法的总体模型如图 2 和图 3 所示，图 2 给出了水印的嵌入过程，图 3 给出了水印的提取和篡改检测过程。算法具体执行过程将在 2.2 和 2.3 节中详细给出。

2.2 水印嵌入

水印嵌入步骤如下：

1) 将原始图像 I(尺寸 $m \times n$) 使用 cat 映射方法迭代 k 次进行置乱，得到置乱后的图像 I_{ck}；

2) 获取 I_{ck} 的最低有效位平面作为嵌入水印位置；

3) 将原始水印图像 W 转换为二进制序列 SW；

4) 使用 Logistic 映射方法得到 $m \times n$ 长度的混沌序列，然后四舍五入得到二进制序列 LS；

5) 将 SW 和 LS 异或得到混沌水印，即 $CW = SW$ XOR LS；

6) 采用 LSB 替换算法将用 CW 替换掉 I_{ck} 的最低有效位平面，得到修改后的加密图像 MI_{ck}；

7) 将 MI_{ck} 用 cat 映射迭代 $T-k$ 次得到水印图像 I_w。

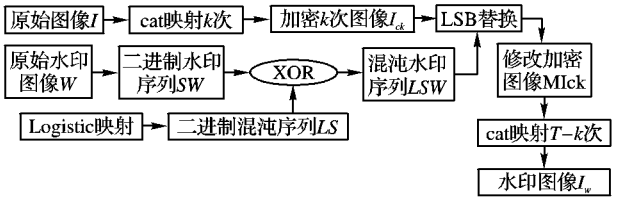


图 2 水印嵌入过程

2.3 水印提取与篡改检测

水印提取和篡改检测步骤如下：

1) 将水印图像 I_w 用 cat 映射迭代 k 次，得到 I_{wck}；

2) 提取 I_{wck} 的最低有效位平面 LSB_I_{wc}；

3) 使用与嵌入过程中相同的 Logistic 映射方法得到 $m \times n$ 个长度的二进制序列 LS；

4) 将用 LSB_I_{wc} 与 LS 异或得到提取出水印序列，即 $EWS = LSB\_I_{wc}$ XOR LS，将 EWS 转换成图像模式可得提取出水印图像 EW；

5) 将原始水印图像 W 转换为二进制序列 SW；

6) 将 EWS 与 SW 求绝对值差并转换成图像得到差值水印图像 DWI；

7) 将 DWI 利用 cat 映射迭代 $T-k$ 次定位水印图像的篡改区域。

算法实施过程中，将 cat 映射和 Logistic 映射的初始参数 a，b，k，μ 和 $x(0)$ 作为密钥，以安全渠道进行分发，用于水印的嵌入和提取。

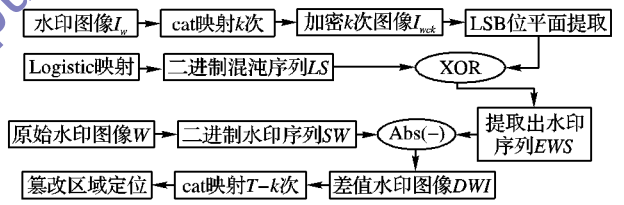


图 3 水印提取和篡改检测过程

3 实验结果与讨论

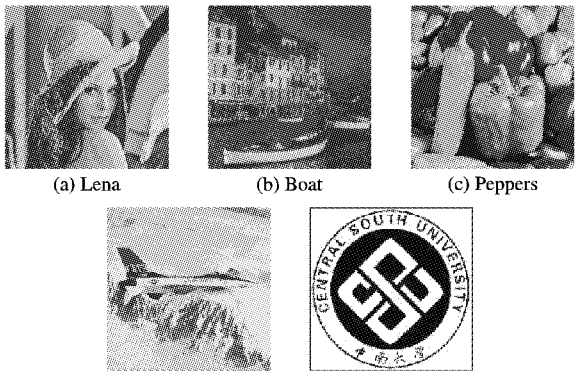
为了证明算法的可行性，实验中选取了大量的不同类型的图像作为测试对象，均得到了较好的实验结果。限于篇幅，选取常见的四幅自然图像作为载体(均为 512×512×8 bit，BMP 格式)说明，如图 4 所示。算法所采用的两个混沌映射的初始参数值为 $a=2$，$b=1$(cat 映射)，$\mu=3.854$，$x(0)=0.654$(Logistic 映射)，所有实验数据均来自于 Matlab7.0 仿真结果。图像认证水印的主要四个性能指标为嵌入容量、水印图像质量(用峰值信噪比(Peak Signal-to-Noise Ratio，PSNR)衡量)、算法安全性和篡改检测精确度。混沌系统的特性很好地保证了算法的安全性，如在 cat 映射初始参数未知情况下，推导出 cat 映射的周期 T 是不可能的。虽然水印嵌入算法采用最简单的 LSB 替换算法，但在 k 值不确定的情况下正确定位水印嵌入位置也是十分困难的。本文实验重点对其他三个性能指标进行分析。表 1 给出了四幅图像在给定 k 值情况下的嵌入容量和水印图像质量。从表 1 中可以看出，不同载体图像的 cat 映射周期一样，容量均可达到 262 144 bit，嵌入率为 1 bit/pixel，水印图像的质量在51.14 dB 左右，具有很高的视觉质量。

图 5 给出了 Lena 图像在嵌入水印后无篡改情况下的水印提取图以及检测篡改区域图。值得注意的是根据本文检测篡

改方式,当图像未受到篡改时,检测篡改区域图像的所有像素值为0,即对应黑色区域,否则发生篡改区域为白色区域。图5(d)为全黑区域,证明了图5(b)的水印图像未受到任何修改。

表1　不同载体图像的嵌入容量和水印图像质量

载体图像	k	T	容量/bit	PSNR/dB
Lena	30	256	262 144	51.140
Boat	60	256	262 144	51.149
Airplane	90	256	262 144	51.141
Peppers	120	256	262 144	51.146



(a) Lena　(b) Boat　(c) Peppers

(d) Airplane　(e) 原始水印图像

图4　原始测试图像和二值水印图像

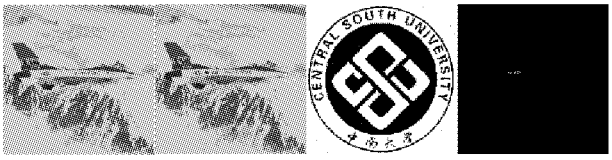
(a) 原图　(b) 水印图像　(c) 提取水印　(d) 篡改检测结果

图5　Lena 测试结果

为了测试算法的篡改检测精确度,实验中针对常见的几种图像攻击,如复制(拼贴)攻击、添加文本攻击和剪切攻击进行了测试,测试结果如图6、7、8所示。

(a) 水印图像　(b) 篡改图像　(c) 提取水印　(d) 篡改检测结果

图6　Boat 复制(拼接)攻击测试结果



(a) 水印图像　(b) 篡改图像　(c) 提取水印　(d) 篡改检测结果

图7　Airplane 添加文本攻击测试结果

(a) 水印图像　(b) 篡改图像　(c) 提取水印　(d) 篡改检测结果

图8　Peppers 剪切攻击测试结果

在图6中,在 Boat 图像的左下角区域复制粘贴了两只小船,篡改图像如图6(b)所示,提取出的水印图像如图6(c)所示,可以看出提取出的水印图像和原始水印图像具有明显区别。另外算法成功对篡改区域进行了定位,如图6(d)所示的两个白色区域。在图7中,在飞机尾部添加"NO.001"字样的文本,由于篡改幅度较小,提取出的水印图接近于原始水印图,但算法仍能精确检测出发生篡改区域,并显示"NO.001"字样。在图8中,对 Peppers 水印图像的左上角区域进行了不规则剪切,提取出的水印图像和原图像相比具有明显的高斯噪声现象。图8(d)表明算法对不规则区域的篡改实现了精确认证。

4　结语

图像篡改检测技术在数字图像数据安全中发挥着越来越重要的作用,本文提出了一种融合混沌系统和脆弱水印技术的图像篡改检测算法,将水印信息嵌入在置乱后的图像的最低有效位平面中。由于水印的嵌入限制在最低有效位平面,隐秘图像具有较好的视觉质量;另外混沌系统极大增强了水印算法的安全性,攻击者在不知道混沌算法相关初值的情况下很难破坏水印。算法利用原始水印和提取出水印的差异实现图像的精确认证。本文算法最大的优点就是将混沌系统的特性和脆弱水印结合在一起,混沌系统的高随机性确保了算法的安全性;而遍历性使得生成高质量的水印图像成为可能;初值敏感性确保了篡改检测精度和检测区域的多样性。实验结果验证了本方法的优越性,但方法仍有不完善的地方,算法对图像篡改区域缺乏恢复能力,这将是下一步的工作重点。

参考文献:

[1] MARTINO F D, SESSA S. Fragile watermarking tamper detection with images compressed by fuzzy transform[J]. Information Sciences, 2012, 195(1): 62-90.

[2] DENG X H, CHEN Z G, DENG X H, *et al*. A novel dual-layer reversible watermarking for medical image authentication and EPR hiding[J]. Advanced Science Letters, 2011, 4(11): 3678-3684.

[3] CHIANG K H, CHIEN K C C, CHANG R F, *et al*. Tamper detection and restoring system for medical images using wavelet-based reversible data embedding[J]. Journal of Digital Imaging, 2008, 21(1): 77-90.

[4] GUO X T, ZHUANG T G. Lossless watermarking for verifying the integrity of medical images with tamper localization[J]. Journal of Digital Imaging, 2009, 22(6): 620-628.

[5] PHADIKAR A, MAITY S P, MANDAL M. Novel wavelet - based QIM data hiding technique for tamper detection and correction of digital images[J]. Journal of Visual Communication and Image Representation, 2012, 23(3): 454-466.

[6] LI C L, WANG Y H, MA B, *et al*. Tamper detection and self-recovery of biometric images using salient region-based authentication watermarking scheme[J]. Computer Standards and Interfaces, 2012, 34(4): 367-379.

[7] 黄斌, 史亮, 邓小鸿, 等. 自适应高容量医学图像可逆数据隐藏算法[J]. 计算机应用, 2012, 32(10): 2779-2782.

[8] ZHU Z L, ZHANG W, WONG K W, *et al*. A chaos-based symmetric image encryption scheme using a bit-level permutation[J]. Information Sciences, 2011, 181(6): 1171-1186.

[9] WANG Y, WONG K W, LIAO X F, *et al*. A new chaos-based fast image encryption algorithm[J]. Applied Soft Computing, 2011, 11(1): 514-522.

[10] 朱从旭, 黄大足, 郭迎. 结合多混沌映射和输出反馈的图像加密算法[J]. 武汉大学学报: 信息科学版, 2010, 35(5): 528-531.

[11] 任丽梅, 刘建民, 贾双盈. 一个新混沌系统的自适应模糊同步[J]. 计算机工程与科学, 2012, 34(7): 146-149.

[12] RAWAT S, RAMAN B. A chaotic system based fragile watermarking scheme for image tamper detection[J]. International Journal of Electronics and Communications, 2011, 65(10): 840-847.