基于位扩展的灰度图像混沌加密算法

殷肖川， 蒋晓迪， 周翔翔
(空军工程大学 电讯工程学院，陕西 西安 710077)

摘 要:在数字水印的初始化阶段对水印图像进行加密,可以减少原始图像信息的空间相关性,增强秘密信息的随机性和保密性,从而提高算法对各种攻击的鲁棒性。Logistic 混沌序列由于具有对初始条件的敏感性以及类似白噪声的统计特性,已经被广泛应用于二值图像的加密算法。但是传统的基于 Logistic 混沌序列的算法无法加密较为复杂且能够记录更多内容的灰度图像,针对此问题文章提出了一种基于映射序列位扩展的灰度图像混沌加密算法。实验表明,算法在加密灰度图像时效果较好而且同具有类似功能的 Arnold 置乱算法相比,新算法具有更高的安全性和时效性。

关键词:数字水印;图像加密;Logistic 混沌序列;位扩展
中图分类号: TP309 **文献标识码**:A **文章编号**:1009-3516(2008)01-0058-04

伴随着数字技术和互联网的飞速发展,数字产品的安全问题日益突出。数字水印技术能够在开放的网络环境下保护数字产品的版权以及验证其内容的可靠性,水印文件本身的格式通常是记录信息直观明了的数字图像[1]。在数字水印的预处理阶段利用适当的算法对待嵌入的原始水印图像做一定的置乱并加密,不仅可以减少水印信息的空间相关性,增强水印的随机性和保密性,还提高了水印对各种攻击的鲁棒性,加大了非法提取水印的难度。有效地加密待嵌入水印是保证整个水印系统安全性的重要前提[2-3]。目前针对灰度图像的置乱加密算法研究已经取得了较大的进展,实际应用中比较成熟的算法主要有基于 Arnold 变换、幻方、Hilbert 曲线、Conway 游戏、正交拉丁方的数字图像置乱算法。从实际的运行效果来看,基于 Arnold 变换的灰度图像置乱算法由于其简单性和良好的置乱效果,应用较为广泛[4-10]。本文在研究了现有的图像加密算法以及混沌序列的相关知识的基础上,提出了一种针对灰度图像的混沌加密算法。

1 基于位扩展的混沌加密算法

1.1 Logistic 混沌序列及其对二值图像的加密

Logistic 混沌映射是一类非常简单却被广泛研究的动力系统,定义如下:$x_{n+1}=\mu x_n(1-x_n)$,$x_n\in(0,1)$。通过简单的变换,Logistic 映射可以在(-1,1)区间定义:$x_{n+1}=1-\lambda x_n^2$,$\lambda\in(0,2)$。

实验证明,当 $\lambda=1.401\ 15$ 时,动力系统进入混沌状态,在 $\lambda=2$ 的满射条件下由映射所得到的混沌序列可能充满整个定义域(-1,1),此时的迭代公式为:$x_{n+1}=1-2x_n^2$。

通过其密度函数可以得到 Logistic 映射产生的混沌序列的统计特性,结果表明动力系统进入混沌状态以后,产生的混沌序列具有均值为零,δ-like 自相关以及互相关为零的类似白噪声的统计特性[4]。和传统的源于经典加密理论的图像加密方式相比,利用混沌序列加密图像的优势在于:①密钥空间大,混沌系统一般定义在实数空间上,并且产生的序列对初始值十分敏感,因此系统参数或者初始条件的微小差别就会引起混沌序列的巨大变化;②混沌序列的产生比较方便,运算复杂度低、速度快,并且具有自相关强、互相关弱的优

收稿日期:2007-05-28
基金项目:国家自然科学基金资助项目(60672032)
作者简介:殷肖川(1961-),男,陕西西安人,教授,硕士生导师,主要从事计算机应用技术方面的研究.
E-mail:jiangxiaodi1983@hotmail.com

良的随机性,非常适合作为水印嵌入到载体文件中;③实施简单,在空域上替换图像的像素值即可;④鲁棒性好,由于只对像素值进行简单的替换,因而对噪声攻击、锐化处理等具有较好的鲁棒性。

但是,根据 Logistic 序列的特性不难看出,虽然其在加密图像时安全性好、鲁棒性高且易于实现,但是最大的不足在于传统的基于 Logistic 混沌序列的算法只能通过简单的象素替换加密二值图,却无法应用于灰度图像的加密,显然具有 256 级颜色的灰度图像比二值图像利用价值更大。据此,本文提出了一种基于映射序列位扩展的灰度图像混沌加密算法。

1.2　基于位扩展的混沌加密算法基本思想

灰度图像的每个像素可由 8 位二进制表示,其包含的信息量比相同分辨率的二值图像丰富,利用灰度图像有利于我们构建数字水印系统时嵌入更多的版权保护信息。进而从理论上分析如果能够利用性能优良的混沌序列去加密灰度图像,应该能够在取得良好的置乱效果和一定加密效率的前提下保证算法的安全性。本文在充分研究了原有的二值图像加密算法的基础上,结合混沌序列的特性提出了一种基于位扩展的灰度图像加密算法,算法基本思想是通过混沌迭代公式生成一组实数,由规则转化成二进制数组,这个数组的个数为灰度图像大小的 8 倍,即让每个像素点值对应 8 个二进制数。依次将 8 个二进制数与灰度图像每个像素点值的二进制形式逐位比较运算,得到一组新的二进制数,将产生结果 8 个一组形成十进制数据,即为置乱后的图像灰度值。

1.3　算法描述

设灰度水印图像为 W,大小为 $M\times N\times 256$,则位扩展灰度图像加密算法的步骤描述如下:

1)设定参数 λ 和 x_0,由迭代公式 $x_{n+1}=1-\lambda x_n^2(n\geqslant 0)$ 生成序列 $\{x_1,x_2,\cdots,x_l\}$,其中 $l>M\times N\times 8$。将前面的若干位舍去,从中间某一位开始选定长度为 $M\times N\times 8$ 的实数序列记为 S,则序列中每个元素为 s_i;

2)将 S 二值化,得到一个 $M\times N\times 8$ 位二值序列 $P=\{p_0,p_1,\cdots,p_{M\times N\times 8-1}\}$,二值化规则为

$$p_i=\begin{cases}0 & 0\leqslant|s_i|<T_r\\ 1 & T_r\leqslant|s_i|\leqslant 1\end{cases}\quad(i=0,1,2,\cdots,M\times N\times 8-1)(T_r\text{ 为设定阈值});$$

3)由于灰度图像的每个象素值的范围在 0 到 255 之间,可表示为 8 位二进制数。将灰度水印图像 W 表示成二进制数组 Q,每个元素 $q_j(j=\{0,1,\cdots,M\times N-1\}$)是 8 位二进制数;

4)将二值序列 P 中的第 $8\times j$ 位到第 $8\times j+7$ 位的 8 个二进制位组成数据 t_j,将 t_j 与灰度图像二进制表示的元素 q_j 中的每一位按公式 $q'_{ji}=\begin{cases}1 & t_i=q_{ji}\\ 0 & t_i\neq q_{ji}\end{cases}$ 生成加密后的二进制元素,并将之转换成一个十进制数 W'_j,以上 $j\in\{0,1,\cdots,M\times N-1\}$;

5)从而得到一个十进制序列,最后将新的十进制序列按行展开成一个大小为 $M\times N$ 的二维矩阵即可得到置乱后的灰度图像,步骤 1 中的 λ、x_0作为加密密钥 key1、key2。

1.4　算法实现

采用 VC + +6.0 编写算法实现的代码,具体流程如图 1 所示。通过实验,发现一次混沌置乱在原始图像较复杂的情况下仍会留下图像的细微轮廓,可用不同的两组密钥将上述算法执行两次,以达到更好的效果。在实际算法中,第 2 组密钥由第 1 组密钥 key1 和 key2 自动形成:key1 = key1 +0.01,key2 = key2 +0.001。解密的过程同加密时进行的操作基本相同,解密时只需首先由正确的密钥生成第 2 组密钥,用第 2 组密钥先解密 1 次,再用原密钥解密 1 次,即可恢复出水印图像。

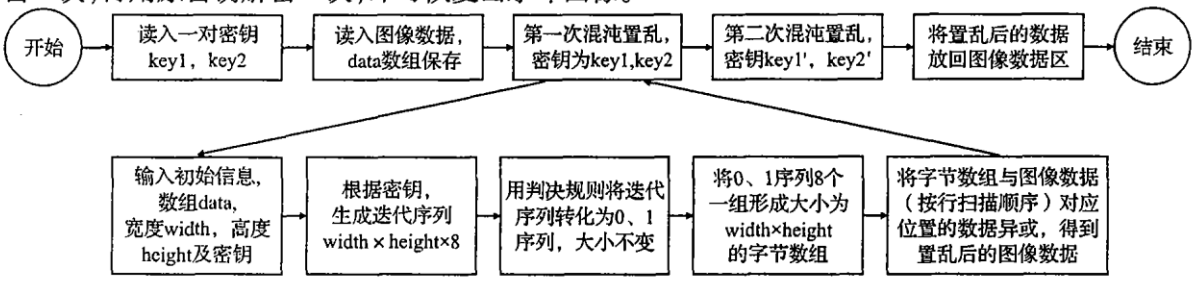


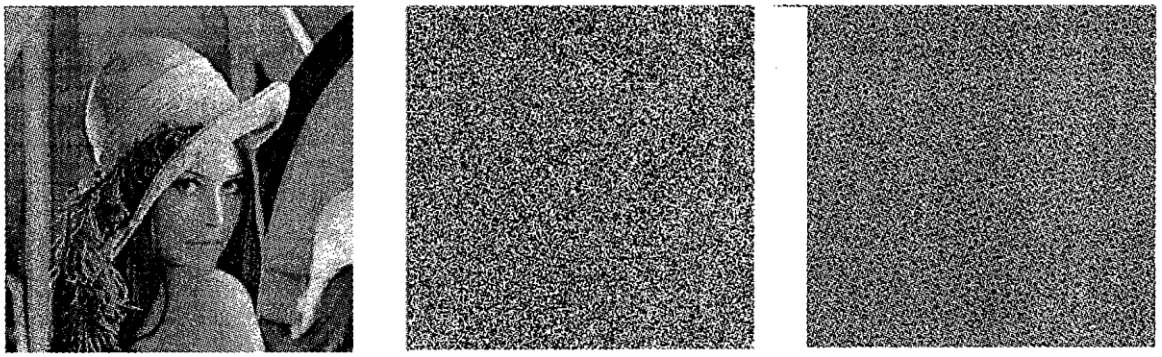
图 1　加密算法流程

Fig. 1　Encrypt algorithm flow

2 实验结果分析

2.1 置乱效果

本文实验所用计算机处理器主频为 1.8 GHz,内存为 512 MB。使用尺寸为 256 × 256 的灰度图像进行置乱,基于位扩展的混沌置乱算法的密钥设定为 $\lambda = 1.952, x_0 = 0.143$;Arnold 置乱算法的密钥设定为 14。原图和置乱后的结果如图 2 所示,可以看出,文中提出的置乱算法具有较好的置乱效果。



(a) 灰度水印 (b) 位扩展混沌置乱图 (c) Arnold 置乱图

图 2 图像置乱效果

Fig. 2 Image chaos effect

2.2 耗时测试

实验的目的是验证位扩展混沌算法的实效性。Arnold 算法在图像尺寸为 128 × 128、256 × 256、512 × 512 的周期依次为 96、192、384,分别设定置乱密钥为 50、100、200;位扩展混沌算法的密钥统一设定为 $\lambda = 1.952, x_0 = 0.143$,则结果如表 1、表 2 所示,精确到毫秒级。

表 1 Arnold 算法耗时

Tab. 1 Arnold algorithm time - consume s

	128 × 128	256 × 256	512 × 512
Arnold 置乱	0.050	0.240	1.583
Arnold 逆置乱	0.050	0.232	1.472
Arnold 算法总耗时	0.100	0.472	3.055

表 2 位扩展算法耗时

Tab. 2 Bits expanding algorithm time - consume s

	128 × 128	256 × 256	512 × 512
位扩展混沌置乱	0.041	0.149	0.425
位扩展混沌逆置乱	0.040	0.162	0.417
位扩展算法总耗时	0.081	0.311	0.842

实验表明:基于位扩展的混沌算法在实效性上优于 Arnold 算法,图像越大优势越明显。

3 结论

本文提出的基于映射序列位扩展的混沌加密算法在加密灰度图像时取得了较好的置乱效果,并且能够保证较高的时效性。对于颜色信息更多的彩色图像来说,应用位扩展算法进行加密从理论上分析同样是可行的,只需将扩展的位数由 8 位增加到 24 位。新的算法能够广泛应用于信息安全领域,特别是数字水印系统中对水印图像的预处理阶段,亦可用于其他领域的图像加密,且加密算法具有较高的安全性和鲁棒性。

参考文献:

[1] Ingemar J, Matthew L, Jerry A. 数字水印[M]. 北京:电子工业出版社,2003.

Ingemar J, Matthew L, Jerry A. Digital Watermarking[M]. Beijing: Publishing House of Electronics Industry, 2003. (in Chi-

nese)

[2] Voyatzis G, Pitas I. Chaotic Mixing of Digital Images and Applications to Watermarking[J]. Proceeding of ECMAST96, 1996, 2:687 - 694.

[3] 吴崇明,王晓丹. 数字水印系统的鲁棒性和常见的攻击[J]. 空军工程大学学报:自然科学版,2002,3(1):90 - 93.
WU Chongming, WANG Xiaodan. Robusticity of Digital Watermarking System and Familiar Attacking[J]. Journal of Air Force Engineering University: Natural Science Edition, 2002, 3(1): 90 - 93. (in Chinese)

[4] 田云凯,贾传荧,王庆武. 基于 Arnold 变换的图像置乱及其恢复[J]. 大连海事大学学报,2006, 32(4): 107 - 109.
TIAN Yunkai, JIA Chuanying, WANG Qingwu. Image Scrambling and Restoring Algorithm Based on Arnold Transform [J]. Journal of Dalian Maritime University, 2006, 32(4): 107 - 109. (in Chinese)

[5] 刘德鹏,蔡翔云. 水印图像的混沌置乱算法[J]. 云南大学学报:自然科学版,2006, 28(SI): 145 - 148.
LIU Depeng, CAI Xiangyun. Watermarking Image Scrambling Algorithm Based on Chaotic Sequence[J]. Journal of Yunnan University: Natural Science Edition, 2006, 28(SI): 145 - 148. (in Chinese)

[6] 韩毅娜,尹忠海,简剑锋. 基于数字指纹的叛逆者追踪技术[J]. 空军工程大学学报:自然科学版,2006,7(1),60 - 63.
HAN Yina, YIN Zhonghai, JIAN Jianfeng. Traitor Tracing Techniques Based on Digital Fingerprinting[J]. Journal of Air Force Engineering University: Natural Science Edition, 2006, 7(1): 60 - 63. (in Chinese)

[7] 郑成勇. 基于混沌的数字信息置乱方法及应用[J]. 佛山科学技术学院学报:自然科学版,2006,24(1): 21 - 24.
ZHENG Chengyong. Chaotic - based Digital Information Disorder and Its Application[J]. Journal of Foshan Engineering University: Natural Science Edition, 2006, 24(1): 21 - 24. (in Chinese)

[8] Boneh D, Shaw J. Collusion - Secure Fingerprinting for Digital Data[C]. //In Advances in Cryptology - CRTPTO95, New York: Lecture Notes in Computer Science, 1995: 453 - 465.

[9] Kennedy M P, Ogorxalek. Special Issue on Chaos Synchronization and Control: Theory and Application [J]. IEEE transactions on Circuits and Systems, 1997, 44(10): 853 - 1039.

[10] Fabien A, Petitcolas P, Anderson R J, et al. Information Hiding A Survey[J]. IEEE Special Issue on Protection of Multimedia Content, 1999, 87(7): 1062 - 1078.

(编辑:田新华,徐楠楠)

An Gray Image Encryption Algorithm Based on Bits Expanding Chaotic Transform

YIN Xiao - chuan, JIANG Xiao - di, ZHOU Xiang - xiang
(The Telecommunication Engineering Institute, Air Force Engineering University, Xi'an 710077, China)

Abstract: It will reduce the space relativity of original image information and strengthen the randomicity of encrypted information and largely improve the safety of watermarking system if the image had been encrypted during the phase of initializing digital watermarking. Logistic chaotic sequence has been used in shuffling and encrypting the binary image widely, because it sensitively depends upon its initial value and it has the statistical characteristic like which the white noise has. But the original Logistic arithmetic can't encrypt the gray image that can record more information. The paper has designed a new encrypting arithmetic which is based on expanding the bits of mapped sequence and Logistic chaotic sequence. The experiment shows that the new arithmetic is excellent and effective in encrypting the gray image, and also is safer and faster than Arnold arithmetic in encryping the gray image.

Key words: Digital Watermarking; Image Encryption; Logistic Chaotic Sequence; Bits Expanding