第16卷 第2期
2006年2月

计算机技术与发展
COMPUTER TECHNOLOGY AND DEVELOPMENT

Vol.16 No.2
Feb. 2006

基于混沌序列的二值图像加密算法

杨格兰[1,2],张建明[2,3],向德生[1]

(1.国防科技大学 计算机学院,湖南 长沙 410073;
2.湖南城市学院 计算机科学系,湖南 益阳 413049;
3.湖南大学 计算机与通信学院,湖南 长沙 410082)

摘 要:随着Internet和多媒体技术的飞速发展,多媒体通信成为人们进行信息交流的重要手段,信息的安全和保密显得越来越重要,促进了多媒体信息、图像信息和声音信息的加密研究。信息隐藏和信息安全技术越来越重要,成为大家研究的一个重要课题。这里提出了一种以混沌二值序列为基础的图像加密算法,改进了灰度差置乱度算法来评价二值图像加密效果,最后对混沌序列对初始条件的敏感性、相邻像素差置乱度、图像加密/解密速度进行了大量测试。实验表明本算法具有加密速度快、加密效果好、安全性高等特点。

关键词:二值图像;混沌序列;置乱变换;加密

中图分类号:TP301.6 **文献标识码**:A **文章编号**:1005-3751(2006)02-0148-03

Binary Image Encryption Algorithm Based on Chaotic Sequences

YANG Ge-lan[1,2], ZHANG Jian-ming[2,3], XIANG De-sheng[1]

(1. Sch. of Computer, National University of Defense Technology, Changsha 410073, China;
2. Dept. of Computer, Hunan City University, Yiyang 413049, China;
3. Sch. of Computer and Communication, Hunan University, Changsha 410082, China)

Abstract: With the advent of the Internet and multimedia technology, the multimedia communication has become more and more important, which makes research multimedia information and picture information and sound information. This paper discusses an image encryption algorithm based on chaotic binary sequences and improves algorithm of gray distance to evaluate the effect of binary image encryption. Experiment on chaotic sequence sensitivity on their initial condition, the scrambling of distance pixels, and the encrypting and de encrypting speed of images. The result shows that the encryption algorithm effect is good and has low computational complexity and high security.

Key words: binary image; chaos sequences; scrambling transformation; encryption

0 引 言

数字图像信息安全是伴随着计算机网络和多媒体技术的迅速发展而产生的新问题。数字图像加密方法是近几年探讨和研究的热点。目前,图像加密的方案主要有如下几个方面:

(1)基于矩阵变换/像素置换的加密技术;

(2)基于秘密分割和秘密共享的图像加密技术;

(3)基于现代密码体系的图像加密技术;

(4)基于混沌的图像加密技术。

这些方案中,基本上都采用了图像置乱技术,只是不同加密方案的安全性、复杂性和加密/解密速度不同,没有考虑到多媒体数据的特点,因而存在一定的局限性。因此,在设计图像信息安全加密全算法时,必须考虑其特殊性,数据冗余性,对大数据加密可实现性,能否经受常见数据有损压缩、格式变换等操作。

混沌系统具有良好的伪随机特性、轨道的不可预测性、对初始状态及控制参数的敏感性等一系列特性,这些特性与密码学的很多要求是吻合的。混沌密码学在1990年前后开始兴起,大致可以分为两个大的研究方向:

a.以混沌同步技术为核心的混沌保密通信系统,主要基于模拟混沌电路系统;

b.利用混沌系统构造新的流密码和分组密码,主要基于计算机有限精度下实现的数字化混沌系统。

实际上,其他很多领域也开展了利用混沌系统应用的研究工作,不少研究结果可资混沌密码学借鉴。比较重要的研究包括:混沌通信(混沌调制、混沌键控、混沌扩频、混沌掩盖等);混沌伪随机序列(与混沌扩频有密切关系);混沌信号检测(与混沌密码分析相关);混沌数字水印(大部分思路与数字混沌密码类似)。

结合上述思想,笔者利用混沌二值序列的特性结合二值图像的特点,提出了一种基于混沌序列的二值图像加密算法。该混沌加密算法充分结合图像的特征,使得到的加

收稿日期:2005-05-06

作者简介:杨格兰(1975—),男,湖南益阳人,讲师,硕士研究生,研究方向为图像处理、信息隐藏、数字水印。

密图像对密钥非常敏感,并可以实现"一次一密"的加密目标,具有较高的安全性能,同时解密算法简单、速度快,解密后的图像和原图像的位(bit)没有任何变化。

1　混沌系统模型

一维离散时间非线性动力系统定义如下[1]:

$$x_{k+1}=\tau(x_k)$$

其中,$x_k\in V$,$k=0,1,2,\cdots$称之为状态。而 $\tau:V\to V$ 是一个映射,将当前状态 x_k 映射到下一个状态 x_{k+1}。如果从一个初始值 x_0开始,反复应用 τ,就得到一个序列$\{x_k;k=0,1,2,\cdots\}$。这一序列称为该离散时间动力系统的一条轨迹。

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,$0\leqslant\mu\leqslant4$ 称为分枝参数,$x_k\in(0,1)$定义同上。混沌动力系统的研究工作指出,当 $3.5699456\cdots<\mu\leqslant4$ 时,logistic 映射工作于混沌态。也就是说,由初始条件 x_0 在 logistic 映射的作用下所产生的序列$\{x_k;k=0,1,2,\cdots\}$是非周期的、不收敛的并对初始值非常敏感的。logistic 映射可以在区间 $(-1,1)$上定义。其形式如下:

$$x_{k+1}=1-\lambda x_k^2 \tag{1}$$

其中 $\lambda\in[0,2]$。

2　基于混沌序列的二值图像置乱算法

2.1　二值图像的特点

二值图像即黑白图像,其每个像素点只用一位表示,"0"代表黑,"1"代表白。其存储简单、结构紧凑的独特优势使得在数据传真、文字识别、条码和数字签名、自动控制技术、图像分析、模式识别理论中得到了广泛应用。基于二值图像处理的算法简单、易于理解和实现、计算速度快等特点,很多数字水印系统是用二值图像作为水印信息,使水印更加直观,提取的水印容易,另外,二值图所具有的数据量最低的特点有利于简化后续处理算法及二值图的硬件实现的复杂度,因此成为信号处理工作中一个令人关注的焦点[2],故二值图像的安全保护有极其重要的意义。基于二值图像信息隐藏的研究[3]也有其独特的应用价值。

2.2　混沌二值序列产生及性质

定义:对于一个由式(1)给定的 Logistic 混沌映射初始值 x_0,令

$$a_n=\mathrm{sgn}(x_n)\quad n=0,1,\cdots,N-1 \tag{2}$$

称序列$\{a_n\}\in\{-1,1\}$为长度为 N 的 Logistic 混沌二值序列。这里 $\mathrm{sgn}(x)$为符号函数。混沌二值序列具有 3 个重要性质:部分自相关特性;部分互相关特性;平衡特性。

2.3　算法原理

为了描述算法的需要,定义映射 f 为:$f(0)=1$,$f(1)=-1$。

定义乘积运算符"$\otimes$",设矢量 $\boldsymbol{a}=\{a_1,a_1,\cdots,a_n\}$和 $\boldsymbol{b}=\{b_1,b_2,\cdots,b_n\}$,则:$\boldsymbol{a}\otimes\boldsymbol{b}=\{a_1b_1,a_2b_2,\cdots,a_nb_n\}$

其中 a_ib_i 表示它们在实数域中 a_i 与 b_i 的乘积。

当 a_i 和 $b_i\in\{-1,1\}$时,容易证明:$\boldsymbol{a}\otimes\boldsymbol{b}\otimes\boldsymbol{b}=\boldsymbol{a}$,如果取 $\boldsymbol{a}$ 为明文序列,$\boldsymbol{b}$ 为加密序列,$\otimes$为加密操作,则上式表明只要将密文再经过同样一次加密操作后可获得明文。

2.4　算法设计

加密算法如下:

(1)先将待加密的二值图像 I 拉直成一个向量 $\boldsymbol{V}$,并利用映射 f 作用于该向量得到 $\widetilde{\boldsymbol{V}}$。

(2)选取初始值(密钥)x_0,u 和序列长度利用式(1)的 Logistic 映射计算出混沌序列并按序排列成矢量 $\boldsymbol{P}'$,利用式(2)把 $\boldsymbol{P}'$映射计算出 $\boldsymbol{P}$。

(3)$\widetilde{\boldsymbol{D}}=\boldsymbol{P}\otimes\widetilde{\boldsymbol{V}}$ 并将向量 $\widetilde{\boldsymbol{D}}$ 在 f^{-1}的作用下得到 $\boldsymbol{D}$,然后根据原始二值图像的行列关系排列成新的二值图像 $\widetilde{I}$ 即加密后的二值图像。

解密算法:输入相同的密钥再做一遍加密算法。

3　加密算法的分析

加密算法的安全性主要依赖于密钥的安全性,而密钥的安全性则与密钥空间的大小、密文对密钥的敏感性、算法的复杂性都有很大关系。文中首先分析上述算法的安全性,尤其是对密钥选择的敏感性。传统图像加密方法一是位置置乱,二是灰度置乱。无论何种置乱方法,其目的都是通过改变图像中各像素的位置或灰度值,使图像内容从视觉上不可见,达到隐藏图像信息的目的。文中是利用混沌二值序列的特性来对二值图像加密,加密算法没有改变图像像素的位置,属于灰度置乱的加密算法。由于二值图像的像素点是{0,1}构成,不存在各种灰度值{0,1,…,255},用一般的改变二值图像像素的算法很难取得满意的效果,如 Fibonacci－Q 变换,是灰度置乱的加密方法,对二值图像加密几乎没有作用;还有骑士游加密算法,通过变局部像素点位置交换,也不能对二值图有很好的加密效果。加密的效果可以由人类视觉主观进行判断,但由于这种方法往往受观察者经验和环境条件等因素的影响,因此,有必要采取定量的方法来描述。文中在灰度图像平均灰度差、相邻灰度置乱程度的思想下,提出平均像素差、相邻像素置乱程度指标来评价二值图像的置乱度。最后对各种不同的二值图片,进行加密/解密平均用时测试。

3.1　测试混沌序列对初始条件的敏感性

为了验证该加密算法的有效性,取二种 64×64 大小的二值图像,即 64×64 的纹理较为简单的文本图像(见图 1(a))和 lena 图(见图 1(d)),密钥选择为 $x_0=0.1415926$,$\mu=2$。图 1 显示了加密结果,很显然加密后的二值图像已经不可辨认。图 1(c)表明了密钥的敏感性,当 x_0 密钥相差 10^{-7} 时,图像都无法辨认。只有在相同的密钥下解码才能恢复到原始图像,否则无法恢复。实验表明密钥

x_0 可精确到 10^{-15}。

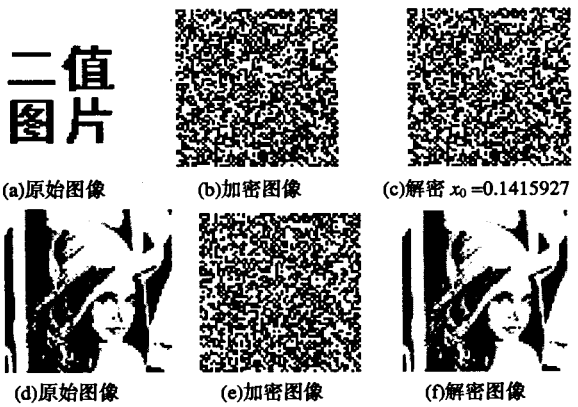

图 1 二值图加密

3.2 相邻像素差置乱度

文献[4]中提出图像中某像素与其相邻像素的灰度差的公式，式 $G(x,y)$ 表示坐标(x,y)处的灰度值，GD 表示灰度差或灰度距离(Gray Distance)，即图像中某像素的灰度值与周围上下左右相邻 4 个像素的平均灰度差。由于文中是对二值图像的加密，二值图像只有{0,1}二种像素，文献[3]中用到平方来突出较大的"灰度差"值对置乱度结果的影响在本算法中没有作用。故改为：

$$GD(x,y)=\frac{\sum_{i,j}|G(x,y)-G(x'_i,y'_j)|}{4}$$

除去图像边缘上的像素外，计算图像中其余各个像素与其相邻像素差，然后相加平均即得到整个图像的平均相邻像素差为：

$$E(GD(x,y))=\frac{\sum_{x=2}^{M-1}\sum_{y=2}^{N-1}GD(x,y)}{(M-2)\times(N-2)}$$

置乱对像素值的随机分布具有很大的影响。因此，定义像素置乱度为：

$$GDD(I,I')=\frac{E'(GD(x,y))-E(GD(x,y))}{E'(GD(x,y))+E(GD(x,y))}$$

上式中，GDD 表示相邻像素差置乱度(Gray Disorder Degree)。E 和 E' 分别表示置乱前、后的平均相邻像素差。这样定义的 GDD 的取值范围为$(-1,1)$，若置乱度小于 0，则表示置乱效果比原图还差，当然这种情况较少出现；若置乱度大于 0，则表示像素置乱效果比原图要好，而且越趋近于 1 越好。

$E(GD(x,y))$ 是加密前图像 I 的平均相邻像素差，表 1 表明该值在 0.1 左右，说明原始图像存在大面积像素值相近的平滑区域(全是 1 或全是 0)，平均相邻像素灰度差变化小。$E'(GD(x,y))$ 是加密后图像 I' 的平均相邻像素灰度差，从表中可看到，图像加密后 $E'(GD(x,y))$ 比 $E(GD(x,y))$ 有很大变化，说明图像各个像素倾向随机分布，不同像素值的像素交错分布，加密后平均相邻像素差变化较大。$GDD(I,I')$ 值都大于 0.5，表明相邻差置乱度大，加密起到很好的作用，$GDD(I,I')$ 算法能够很好体现二值图像的加密效果，而且对不同的图像，其值变化比较大。

表 1 各种置乱度评价表

	图像(a) 64×64	图像(d) 64×64	图像(a) 128×128	图像(a) 256×256	图像(d) 512×512
$E(GD(x,y))$	0.11941	0.11713	0.052091	0.02573	0.030619
$E'(GD(x,y))$	0.49371	0.49831	0.49778	0.49963	0.5
$GDD(I,I')$	0.61015	0.61936	0.81053	0.90205	0.88459

3.3 测试图像加密、解密速度

为了验证该加密、解密算法的高效性，取 4 种如图 1(a)原始图像的二值图像，图像的宽度和高度分别为 64×64，128×128，256×256，512×512。分别对各种图像做 20 次测试，速度取 20 次/秒测出时间的平均值(见表 2)。

表 2 测试加密/解密速度表

	图像(a) 64×64	图像(a) 128×128	图像(a) 256×256	图像(a) 512×512
加密平均时间	0.7972	0.80682	0.84799	1.3603
解密平均时间	0.3393	0.35581	0.38153	0.4412

上表表明，混沌加密/解密效率高，运算量不大。混沌解密耗时几乎是加密的一半，说明解密效率更高，图像加密耗时随着图像的增大而增大，而解密变化不是很大。加密/解密时间复杂度为 $O(m\times n)$(m,n 分别表示图像的宽度和高度(像素数))。

4 结 论

大量的实验表明本算法的最大优点是：

(1)容易实现，密钥量大，安全性好，置乱图像将很难被破解；

(2)仅一次置乱就有很好的置乱效果，而其它的算法(如 Arnold 置乱)需多次置乱才有较好的置乱效果；

(3)置乱速度快；

(4)对图像的宽度和高度值没有限制，而其它很多算法对图像的宽度或高度都有不同程度的限制，如基于幻方变换、正交拉丁方[5]、广义 Gray 码变换、Hilbert 曲线等的置乱方法都是针对方形图像的。基于面包师变换的数字图像置乱要求图像的高为偶数[6]。

正由于这些优点，该置乱算法可以安全地隐藏图像信息，因此笔者将其用于数字图像的预处理和后处理。对于生成的混沌序列，最好不选用初始段部分序列，这样更能加强加密效果。

参考文献：

[1] Xiang Hui. Digital Watermarking Systems with Chaotic Sequences[A]. Electronic Imaging'99, Security and Watermarking of Multimedia Contents[C]. [s. l.]:[s. n.],1999. 449-457.

[2] 乔长阁.一种用于图像二值化的细胞神经网络模型[J].通信学报,1995,16(2):7-9.

[3] 周琳娜.基于二值图像的信息隐藏研究综述[J].中山大学学报(自然科学版),2004(11):12-15.

(下转第 153 页)

平分裂算法虽仍无法克服类似图 2 中存在的奇点环问题,但对于偶点环上的无穷计算问题则可完全解决。如图 3 所示,假设线路 AB 突然断开(相当于结点 A 下线)。根据水平分裂算法,B 在第一次交换后将自己标为到 A 不可达,并告诉 C 和 D。同样,第二次交换后 C 和 D 也知道了 A 不可达。第三次交换后,所有结点都将 A 标为不可达。这样,A 断网的消息以每次一个树深的速度向下传递到所有的叶结点,避免了偶点环 BCED 上的无穷计算问题[4]。

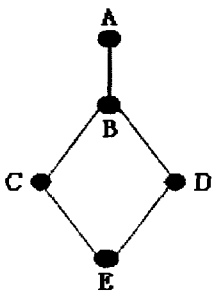

图 3　偶点环的水平分裂算法分析

3　一种改进的水平分裂算法——下一跳算法

3.1　基本思想

为了解决上述奇点环上的无穷计算问题,在水平分裂算法的基础上,提出了一种新的改进算法——"下一跳"算法。

下一跳算法思想很简单:每个路由器在原有的两列路由交换信息上增加一列"下一跳"信息(Next hop),即通往目的地的下一个结点,并在返回自己从邻结点获得的路由信息时将距离设为无穷大。例如,假定路由器 A 到路由器 R 的距离为 X,下一跳为结点 B,则 A 中相应的路由交换信息格式如表 1 所示。

表 1　下一跳算法路由交换信息格式

目的地	距离	下一跳
R	X	B

路由广播表增加下一跳信息后,路由器便可根据这列信息做出相应的决策。如上所述,路由器 B 收到结点 A 广播的信息,发现 A 到路由器 R 有一条距离为 X 的路径,但下一跳为自己,于是它将 A,R 的距离视为无穷大,这就避免了 A,B 两结点间路由环的产生。

3.2　实例分析

对于图 2 中的奇点环问题,采用上述改进算法可作如下分析:当线路 CD 突然断开时,C 从 D 得不到任何消息。根据下一跳算法蕴含的水平分裂思想,C 知道自己到 D 不可达,并告知 A 和 B。与 C 交换信息后,A 发现 B 有一条经 C 到 D 距离为 2 的路,B 也一样,于是都认为经对方有一条到 D 距离为 3 的路径。下次交换时,A 发现 B 的路由交换信息中下一跳是自己,于是它将 B 到 D 的距离视为无穷大,现在从 B 和 C 都无法到达 D,于是 A 将自己标为到 D 不可达。同理 B 也将自己标为到 D 不可达,这样便克服了水平分裂算法无法解决的奇点环上的无穷计算问题。

3.3　存在的问题

下一跳算法通过在传统水平分裂算法的基础上增加一列信息,较好地避免了奇点环和偶点环上的无穷计算问题,但对于两者的混合乃至更复杂的拓扑结构还不能加以有效地解决。由于到目标结点路径上的各结点获得的路由交换信息受到了邻接结点个数的限制,该算法仍无法完全摆脱无穷计算问题的困扰[5]。另外,该算法要求向所有的邻接结点多广播一列路由交换信息,因而路由器的计算复杂程度也相应增加。与 DVR 算法和传统水平分裂算法相比,下一跳算法需要消耗更多的网络和路由器资源。

4　结束语

综上所述,无穷计算问题的核心是如何发现并避免路由环。加快收敛速度的水平分裂算法虽不能完全避免路由环,但在实际应用中 RIP 的"无穷大"通常设为 16,因而即使出现了无穷计算问题,收敛速度还是可以接受的。文中在对原有的水平分裂算法进行 MST 分析的基础上,提出了改进后的下一跳算法,它的思想和实现简单,能较好地解决奇点环和偶点环上的无穷计算问题,但对于更复杂的网络拓扑结构效果仍不够理想。当然,改进算法本身也存在一些问题:如因增加了一列信息而带来新的网络流量,以及因检查下一跳信息而增加路由器的计算开销等。这些都需要在进一步的研究中提出更好的路由选择算法来解决。

参考文献:

[1] Tanenbaum A S. 计算机网络(第 3 版)[M]. 熊桂喜,王小虎等译. 北京:清华大学出版社,1998.

[2] Schmid A, Steigner C. Avoiding counting to infinity in distance vector routing[J]. Telecommunication Systems - Modeling, Analysis, Design and Management, 2002, 19(3): 497 - 514.

[3] Hendrick C. Routing Information Protocol[R][s. l.]: IETF Network Working Group, 1988.

[4] Bellman R. On a Routing Problem[M]. Virginia: William Byrd Press, 1958.

[5] 苏传蓉. 几种常见路由协议的应用[J]. 湖北邮电技术, 2002, 9(3): 48 - 50.

(上接第 150 页)

[4] 向德生,熊岳山. 基于约瑟夫遍历的图像置乱算法[J]. 计算机工程与应用, 2005, 41(10): 44 - 46.

[5] 李国富. 基于正交拉丁方的数字图像置乱方法[J]. 北方工业大学学报, 2001, 13(11): 123 - 125.

[6] 赵学峰. 基于面包师变换的数字图像置乱[J]. 西北师范大学学报, 2003, 39(2): 26 - 29.