一种基于混沌序列的图象加密技术

张小华 刘 芳 焦李成
(西安电子科技大学雷达信号处理重点实验室, 西安 710071)

摘 要 混沌序列具有易生成性、对初始条件强敏感性、可完全重现性以及整体的伪白噪声统计特性等特点,同时混沌序列的离散映射序列也具有其相似的特性. 基于以上特性,给出了一种基于混沌序列的图象置乱加密算法,其首先,以初始条件为密钥生成混沌序列,并将它映射为 2^K 值混沌序列;然后依据该序列随机地修改图象每个像素点的灰度值. 同时为了度量加密或置乱的程度,还给出了一种基于图象局部方差的图象置乱度的定义. 实验结果证明了该算法实现简单,计算量小,且图象的解密结果对混沌序列的初始值有较强的依赖性,安全性高,同时也证明了给出的图象置乱度能更好反映图象加密前后的视觉差别和加密效果.

关键词 计算机图象处理(520·6040) 图象加密 混沌序列 排列变换 图象置乱度
中图法分类号: TP309.7 TN918.74 **文献标识码**: A **文章编号**: 1006-8961(2003)04-0374-05

An Image Encryption Arithmetic Base on Chaotic Sequences

ZHANG Xiao-hua, LIU Fang, JIAO Li-cheng
(*State Key Laboratory of Rsp, XiDian University, Xi'an* 710071)

Abstract Chaotic sequences have several good properties , such as the ease of their generation, their sensitive dependence on its initial parameters, and specially white noise alike, at the same time it can be reproduced precisely based on the initial condition, and their discrete mapping sequences have a same property. Because of these good properties, chaotic system can be used to image encryption and image preprocessing. In this paper, image encryption arithmetic is proposed based on chaotic system. First, based on the key (initial parameter is the key, here), the chaotic sequences can be generated based on key, then it is mapped to the discrete 2^K value sequences, according to the discrete sequence, gray value of pixel is modified randomly, it is obvious that if attacker dose not know the key, the encrypted image will be looked like white noise and can not be rebuilt. There are many image encryption methods, and different arithmetic gets different results, but up to now there is no suit way to evaluate the result of image encryption. Based on image local variance and human vision system, an efficient definition of encryption degree is proposed. Preliminary results are satisfactory, and security of image completely depend on the key, slight error key results a different result. Hence, it can be used to encrypt image data.

Keywords Computer imgae processing, Image encryption, Chaos sequences, Scrambling transformation, Disorder degree

0 引 言

随着 Internet 技术与多媒体技术的飞速发展,多媒体通信逐渐成为人们进行信息交流的重要手段,如人们可以通过网络交流各种信息,进行网上贸易等. 因此,信息的安全与保密显得越来越重要. 对于多媒体信息,尤其是图象和声音信息,传统的加密技术将其作为普通数据流进行加密,而不考虑多媒体数据的特点,因此有一定的局限性. 图象置乱(排列)变换是一种经典的基于内容的图象加密方法.

对于任一图象 I,设 I 的大小为 $n=M\times N$,且 I 中总共包含 k 种颜色,其中具有颜色 c_i 的像素个数为 n_i,$n_1+n_2+\cdots n_k=n$,则 I 的直方图 H 可以看作是一个具有 k 个元素的多重集 $S=(n_1\cdot c_1, n_2\cdot c_2, \cdots, n_k\cdot c_k)$(其基数为 n). 显然,S 上的任一个全排

基金项目:国家自然科学基金项目(60073053,60133010)
收稿日期:2001-12-29;改回日期:2002-09-17

列 P_i 均对应一幅 $M\times N$ 图象 I_i,即与 I_i 存在一一对应关系.

令集合 $X=\{1,2,\cdots,n\}$,则 X 的一个置换是指 X 到其自身的一个双射 $p:X\to X$. 定义两个置换 p_1 和 p_2 的乘法运算为 $p_1\cdot p_2:X\to X$, $p_1\cdot p_2(x)=p_1(p_2(x))$, $x\in X$,则由 X 的所有置换组成的集合在该乘法运算下构成一个群,称之为 X 上的对称群,记为 S_n.

置换 p 就是将 X 的一个排列变成另一个排列. 由于图象与排列之间有一一对应关系,可将集合 X 的元素看作是图象 I 中各元素顺序排列时的下标,则任何一个置换 p 都可看作是 I 到 $p(I)$ 的一个图象变换. 因此,可利用排列变换对图象进行加密.

图象置乱加密方法已有许多,如经典的 Arnold 变换、Hilbert 曲线变换、E 曲线变换[1]、几何变换[2]、Fibonacci 变换[3]以及骑士巡游置乱变换[4]. 这些方法置乱图象后的直观效果各不相同,但他们都具有一定的确定性,同时在置乱过程中只改变像素点的位置,而不改变其大小,所以置乱后的图象还是具有一定规律性. 一般来说,秘密图象置乱的程度越好,保密性就越高. 但目前的文献中还没有一个合理的图象置乱程度的定义. 为此,利用混沌动力学的特点,提出了一种基于内容混沌序列的图象加密算法,并给出一种有效衡量图象置乱程度的定义.

1　混沌动力系统

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,这种过程既非周期,又不收敛,并且对初始值有极其敏感的依赖性.

一个一维离散时间非线性动力系统定义如下

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

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}. 如果由初始值 x_0,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

$$x_{k+1}=\mu x_k(1-x_k) \tag{2}$$

其中,$0\le\mu\le 4$ 称为分枝参数, $x_k\in(0,1)$. 当 $3.5699456\cdots<\mu\le 4$ 时,Logistic 映射工作于混沌状态. 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,且对初始值非常敏感.

另一类简单的映射是 Chebyshev 映射,以阶数为参数. k 阶 Chebyshev 映射定义如下

$$\tau(x_{k+1})=\cos(n(\cos^{-1}x_k)) \tag{3}$$

其中,x_k 的定义区间是 $(-1,1)$. 事实上是通过简单的变量代换,Logistic 映射同样可以在区间 $(-1,1)$ 上定义. 其形式如下

$$x_{k+1}=1-\lambda x_k^2 \tag{4}$$

其中,$\lambda\in[0,2]$. 在 $\lambda=2$ 的满射条件下,Logistic 映射与 Chebyshev 映射是拓扑共轭的,其所生成序列的概率分布函数 PDF(probability density function)也相同

$$\rho(x)=\begin{cases}\dfrac{1}{\pi\sqrt{1-x^2}} & -1<x<1\\ 0 & \text{else}\end{cases} \tag{5}$$

对于式(2)形式的 Logistic 映射,如果 $\mu=4$, PDF 可改写为

$$\rho(x)=\begin{cases}\dfrac{1}{\pi\sqrt{x(1-x)}} & 0<x<1\\ 0 & \text{else}\end{cases} \tag{6}$$

通过 $\rho(x)$,可以很容易地计算得到 Logistic 映射所产生的混沌序列的一些很有意义的统计特性. 例如,x 的时间平均,即混沌序列轨迹点的均值是

$$\bar{x}=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N-1}x_i=\int_0^1 x\rho(x)\mathrm{d}x=0 \tag{7}$$

关于相关函数,独立选取两个初始值 x_0 和 y_0,则序列的互相关函数为

$$\begin{aligned}c(l)&=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N-1}(x_i-\bar{x})(y_{(i+l)}-\bar{y})\\&=\int_0^1\int_0^1\rho(x,y)(x-\bar{x})(\tau^{(l)}(y)-\bar{y})\mathrm{d}x\mathrm{d}y=0\end{aligned} \tag{8}$$

注意联合 PDF: $\rho(x,y)=\rho(x)\rho(y)$.

而序列的自相关函数 ACF (auto-correlation functions)则等于 delta 函数 $\delta(l)$.

Logistic 序列的以上特性表明,混沌动力系统具有一定的确定性,其遍历统计特性等同于白噪声,具有形式简单,对初始条件敏感等诸多特性.

2　基于混沌序列的图象置乱算法

2.1　算法原理

在传统的迭代乘积密码系统中,排列算子的主

要任务就是对明文数据块中的元素进行置乱(也称为“重排”),使得密文块看起来是随机的.不过,这些排列算子通常是事先确定好的,具有一定的解析表达式,而与密钥无关,这一明显缺陷,使得某些迭代乘积密码系统特别容易受到差分密码分析的攻击.同时在迭代过程中,只改变像素点的位置,而不改变像素点灰度值,使得置乱后的图象依然呈某种规律性,从而很容易引起攻击者的注意,增加受攻击的概率.

基于密钥的排列也可以在频域或空间域进行.排列变换可以是局部的,或是全局的.空间域的排列加密算法实现较为简单,因为不需要使用一般频域算法所必须的空域到频域的变换,计算量相对较少.不过,空间域的局部随机置乱效果不是很好.在频域中每一点的变化对整个数据集合都会产生一定的影响,且一般情况下不能完全恢复原始信息.

基于以上讨论,在置乱之前,利用混沌现象的随机性随机扰动像素点的灰度值,然后再置乱扰动后的图象,以此达到加密的目的,具体算法如下:

设图象为 $I(i,j),i=0,1\cdots,M-1,j=0,1,\cdots,N-1$

(1) 根据初始值 x_0(密钥)产生 2^K 值混沌序列 $\{C_i,i=0,1,\cdots,M\times N-1\}$;

(2) 利用 2^K 值混沌序列$\{C_i\}$改变像素点(i,j)的灰度值 $I(i,j)$,得 $I'(i,j)$;

(3) 利用空间域置乱算法置乱图象 $I'(i,j)$,得 $I''(i,j)$;

(4) 图象 $I''(i,j)$即为加密后的图象.

解密算法如下:

设接收方所得到的秘密图象为 $I''_m(i,j),i=0,1\cdots,M-1,j=0,1\cdots,N-1$;

(1) 利用空间域置乱算法重建图象 $I''_m(i,j)$,得图象 $I'_m(i,j)$;

(2) 根据初始值 x_0(密钥)产生 2^K 值混沌序列 $\{C_i,i=0,1\cdots M\times N-1\}$;

(3) 利用 2^K 值混沌序列$\{c_i\}$修改像素点(i,j)的灰度值 $I'_m(i,j)$,得 $I_m(i,j)$;

(4) $I_m(i,j)$即为解密后的图象.

2.2 混沌序列生成

从 Logistic 映射或 Chebyshev 映射生成混沌序列的方法如下:

(1) 实数值序列,即$\{x_l,l=0,1,2,3\cdots\}$,是混沌映射的轨迹点所形成的序列.

(2) 2^K 值序列,可以通过定义一个阈值函数 Γ,由上述的实数值混沌序列得到

$$\Gamma(x)=\begin{cases}00\cdots00 & 0\le x<\dfrac{1}{2^K}\\ 00\cdots01 & \dfrac{1}{2^K}\le x<\dfrac{2}{2^K}\\ \vdots & \vdots\\ 11\cdots10 & \dfrac{2^K-2}{2^K}<x<\dfrac{2^K-1}{2^K}\\ 11\cdots11 & \dfrac{2^K-1}{2^K}<x<1\end{cases}\tag{9}$$

2.3 算法设计

设原始图象为 $I(i,j),i=0,1\cdots M-1,j=0,1,\cdots N-1$.利用密钥值 x_0,采用式(4)生成实数值混沌序列 x_k.取初始值 $x_0=0.123,\mu=4.0$,同时为了增加算法的随机性,不使用该序列的初始段部分.

利用状态信息 x_k 得到混沌 2^K 值序列 $\Gamma(x_k)=C_{K-1}\cdots C_0$ 后,对于某一个像素点(i,j)的灰度值 $I(i,j)$,假设 $0\le I(i,j)\le 255$,将它表示为二进制形式 $I_7I_6\cdots I_0$,然后利用 2^K 值混沌序列 $C_{K-1}\cdots c_0$ 来修改 $I_7I_6\cdots I_0$,一般情况下,假设 $1\le K\le 8$,这里以四值序列为例($K=2$).如果 $C_i=00$,I_6 和 I_7 均不变;如果 $C_i=01$,I_7 不变,I_6 取反,即 0 变为 1,1 变为 0;如果 $C_i=10$,I_7 取反,I_6 不变;如果 $C_i=11$,I_7 取反,I_6 取反,将新的二进制序列 $I'_7I'_6\cdots I'_0$ 变为十进制值,即可得到 $I'(i,j)$.很容易发现对 I_i 取反操作就等价于对 I_i+1 关于 2 取余;不变,就等价于对 I_i+0 关于 2 取余,所以利用 2^K 值序列 $C_{K-1}\cdots C_0$ 来修改 $I(i,j)$就可以写为

$$\begin{cases}I'_i=\mathrm{mod}(I_i+C_{i-K},2) & 8-K\le i\le 7\\ I'_i=I_i & 0\le i<K\end{cases}$$

由于混沌系统的伪噪音特性使得在不同的状态下,相同灰度值加密以后的结果可能不同,而不同灰度值加密后却相同,因此攻击的难度大大增加.

经过上述修改,可将一个随机变量 $x\in[0,2^K]$ 映射到 $x'\in[0,2^K]$,定义 $y=x-x'$,很容易证明:$E(y)=0,E(|y|)=\dfrac{2^K-1}{2}$.

假设随机变量 x 在$[0,2^K]$中服从均匀分布,则 x'在$[0,2^K]$中也服从均匀分布,随机变量 y 在$[-2^K,2^K]$中服从均匀分布,$|y|$在$[0,2^K]$中服从均匀分布,所以 $E(y)=0,E(|y|)=2^{-K}(0+1+\cdots 2^K-1)=\dfrac{2^K-1}{2}$,而 K 越大,加密效果就越好.

至于空间域置乱算法,可以取 Arnold 算法或其他算法,为了简单,这里取序列 $P_0,P_1,\cdots,P_{255}$(满足

$P_i=i$)的一个置换 $P'_0,P'_1,\cdots,P'_{255}$，然后将像素点 (i,j)的灰度值 $I'(i,j)=g$ 变为 P'_g，即可得加密后的图象 $I''(i,j)$.

解密算法和加密算法较为近似，差别在于，在加密算法中，空间域置乱算法为最后一步，而在解密算法中，其为第 1 步，其他各步完全相同.

3　图象置乱程度的度量

图象置乱变换既是一种简单而有效的图象加密方法，又是一种常用的图象预处理和后处理方法，近年来得到人们的广泛关注，并出现了许多有效的算法. 但却很难找到一种关于置乱效果的有效度量方法[5]. 置乱的目的在于打乱图象，使得攻击者不能识别图象的内容，一般来说，置乱后图象相对于原始图象越“乱”，表明该算法就越有效，“乱”是视觉效果，带有一定主观性，不同的观察者的评价结果可能不同. 本文认为“乱”和“整齐”的区别在于，一幅较“乱”图象应满足每一个像素点的灰度值和周围像素点灰度值的差别较大，而“整齐”的图象正好相反，同时置乱效果与像素点的位置没有关系，位置不同灰度值相同的两个像素点在观察者的眼中是没有区别的. 所以图象置乱度应是一个只与图象内容(即灰度值)有关，而与像素点的位置没有关系的量值. 基于以上讨论提出如下图象置乱度的定义.

设子图象为：$I_{loc}(i,j),i=0,1,\cdots,k-1,j=0,1,\cdots,k-1$，灰度均值 E_{loc}定义为

$$E_{loc}=\frac{1}{k\times k}\sum_{i=0}^{k-1}\sum_{j=0}^{k-1}I_{loc}(i,j) \tag{10}$$

子图象 I_{loc}的方差 σ^2_{loc}定义为

$$\sigma^2_{loc}=\frac{1}{k\times k}\sum_{i=0}^{k-1}\sum_{j=0}^{k-1}(I_{loc}(i,j)-E_{loc})^2 \tag{11}$$

σ^2_{loc}描述了子图象块的变化程度，其值越大，说明各点的灰度值与均值的差别就越大，图象变化越剧烈，图象就越“乱”. 对于图象 $I(i,j),i=0,1,\cdots,M-1,j=0,1,\cdots,N-1$，将它分割成 L 个互不相交的子图象：$I^{(n)}_{loc}(i,j),n=1,\cdots,L$，图象 $I(i,j)$的方差 σ^2 定义为

$$\sigma^2=\frac{1}{L}\sum_{n=1}^{L}\sigma^{(n)2}_{loc} \tag{12}$$

设置乱前图象的方差为 σ^2_{org}，置乱后的方差为 σ^2_{new}，则图象的置乱度 η 定义为

$$\eta=\frac{\sigma^2_{new}}{\sigma^2_{org}} \tag{13}$$

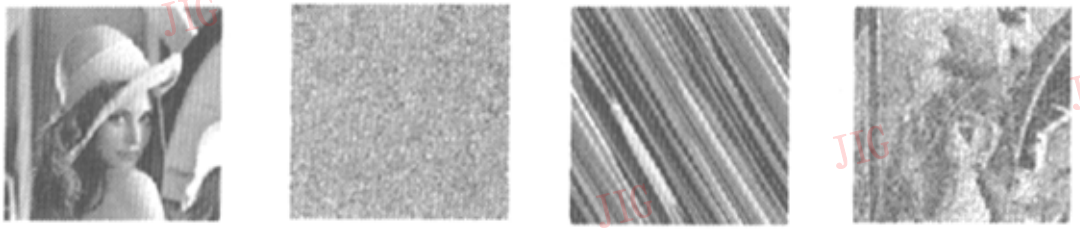
由此可见，η 越大，置乱效果越好，增益就越大，相对于原始图象越“乱”，受攻击的可能性就越小，加密的程度就越高. 一般来说，图象子块不能取得太小，也不能太大，本文取 5×5.

4　实验结果与结论

采用本文算法针对 Lena 图象进行加密，取初始值(密钥)$x_0=0.123$，分枝参数 $\mu=4.0$，为了证明该算法的有效性，将该算法和著名的 Arnold 算法进行了比较. 取 Arnold 迭代算子为

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

其中 $N=256$，迭代次数为 194. 与本文算法相比较，Arnold 算法具有确定的解析迭代公式，同时具有一定的周期性，图象解密与周期有关，而不同的 N，周期各不相同，且没有一个统一的求解周期算法，同时不同的迭代次数，置乱效果相差较大，N 的取值受图象大小限制；而本文算法不仅没有统一的迭代公式，属于随机加密算法，且不具有周期，加密过程不受任何限制，加密完全依赖于密钥 x_0 和 μ，密钥 x_0 可以是[0, 1]区间任意一个实数，$3.569\,945\,6\cdots<\mu\le4$，其可选空间很大. 图 1(a)为原始图象，图 1(b)为采用本文算法所得的置乱图



(a) 原始图象 $\sigma^2_{org}=209.1$　(b) 本文算法的置乱图象 $\sigma^2_{new}=4\,007.8$　(c) Arnold 算法的置乱图象 $\sigma^2_{new}=2\,223.1$　(d) 错误密码解密图象

图 1　实验结果

象,图 1(c)为采用 Arnold 算法所得置乱图象,不论从视觉效果,还是从图象置乱度大小来看,本文提出的算法均优于 Arnold 算法. 由于混沌序列对初始值非常敏感,即使密钥值有微小的变化也会得到完全不同的解密结果(图 1(d)),如初始值(密钥)$x_0=0.124$,$\mu=4.0$ 时,就无法对图象进行正确解密. 实验证明,本算法具有加密速度快,加密效果好等特点,同时其图象置乱度有效地反映了人类视觉系统的特性,能够用来衡量置乱算法的效果. 此外,对于生成的混沌序列,最好不选用初始段部分序列,因为这样能加强加密效果.

参 考 文 献

1 卢朝阳,周幸妮. 一种新的数据信息值乱算法[J]. 计算机工程与科学,1998,20(3):28~41..

2 吴昊升,王介生,刘慎权. 图象的排列变换[J]. 计算机学报,1998,21(6):514~519.

3 Voyatzis G, Pitas I. Application of toral automorphisms in image watermarking[J]. IEEE Int. Conf. on Image Processing, 1996,2:237~240.

4 丁玮,齐东旭. 数字图象变换及信息隐藏与伪装技术[J]. 计算机学报,1998,21(9):838~843.

5 柏森,黄长修. 图象置乱度研究[A]. 见:全国第三届信息隐藏学术研讨会论文集[C], 西安:西安电子科技大学,2001:75~81.

张小华 1974 年生,西安电子科技大学博士研究生. 研究方向为图象处理、信息安全、进化算法、小波分析.

刘 芳 1963 年生,副教授. 研究方向为智能信息处理、模式识别、电子商务.

焦李成 教授,博士生导师. 研究方向为智能信息处理、非线性理论、信息安全.