数字图像的混沌加密方案

北京中国科技大学研究生院(100039)　王　军

摘　要：基于变参数复合混沌系统生成更复杂、更长周期的混沌序列，通过该混沌序列打乱数字图像象素值和位置的混沌加密方案。

关键词：混沌　混沌序列　数字图像　加密

混沌系统是一种高度复杂的非线性动态系统，具有对初始条件和混沌参数非常敏感以及生成的混沌序列具有非周期性和伪随机性的特性。因此，混沌系统近年来被应用于通信保密领域，混沌密码学方法也得到了大量研究。本文在考虑数字图像数据存储特点的基础上，应用新发展起来的混沌动力学加密方法，设计了一种图像加密方案。分析和仿真结果表明，本文所提出的加密/解密方案能够有效地实现对数字图像数据的加密/解密。

1　数字混沌系统的实现

利用传统的差分方程在计算机上实现混沌序列时，由于实现精度是有限的，所产生的混沌序列周期与理论上周期无限的性质相差很远。而利用增大实现精度的方法无法避免混沌序列在迭代过程中退化为周期序列的问题。因此混沌序列的有限精度实现是决定它能否在实际中应用的关键。解决混沌周期的退化问题有2种方法：级联多个混沌系统和通过伪随机序列加入扰动。本文通过级联2个混沌系统来构造一种变参数复合混沌系统(Variable Parameter Compound Chaotic System，VPCCS)，然后利用VPCCS来生成更复杂、更长周期的数字混沌序列。所选2个混沌子系统是抛物线映射和与它非常接近的人字映射。

抛物线映射的形式如下：

$x_{n+1}=1-\mu x_n^2 \quad \mu\in(0,2];\ x\in[-1,1]$

人字映射的形式如下：

$$y_{n+1}=\begin{cases}\mu y_n & y_n\leqslant 0.5\\ \mu(1-y_n) & y_n>0.5\end{cases}\quad \mu\in(0,2];\ y\in[0,1]$$

研究表明，当$1.4011<\mu<2$时，这2个映射是混沌的。变参数复合混沌系统的结构框图如图1所示。由于该系统框图具有对称性，因此只给出了左半部分。

在VPCCS中，引入了参数切换条件来控制混沌系统的参数在不同的值之间进行切换。例如，设定切换条件为：x_i小数点后面第3位是否为2来控制μ值在μ_1和$\mu_2$2个数上相互切换。μ_1和μ_2是(1.4011，2)之间的任意2个实数，可以作为密钥的一部分由用户输入。组成系统的某一子混沌系统通过自身的输出状态来改变另一个子混沌系统的参数，从而实现了2个子混沌系统之间的相互作用。

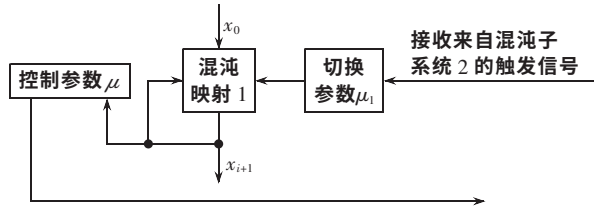


图1　变参数复合混沌系统的结构框图

输入(x_0,y_0)到VPCCS，就可以产生2个混沌序列x_k和y_k。实验表明，通过VPCCS产生的混沌序列的特点为：功率谱平坦，相邻轨道分离速度快，自相关函数近似理想冲击函数$\delta(x)$，互相关接近0。而且由于混沌映射对初始条件的敏感性，从而可以方便地获得大量具有良好自相关特性和互相关特性的混沌序列。

2　基于混沌序列的图像加密算法

2.1　算法思想

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，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，而与密钥无关。这个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，只改变象素点的位置，而不改变象素点灰度值，使得置乱后的图像依然呈某种规律性，从而很容易引起攻击者的注意，增加受攻击的概率。

基于密钥的排列可以在频域或空域进行。排列变换可以是局部的或全局的。空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，本文选择利用混沌序列的随机性来随机扰动象素点的灰度值，然后在空域内全局置乱图像，

以此达到加密的目的，具体算法如下。

假设一幅大小为 $M\times N$ 和灰度级为 L 的图像，$I(i,j)$为(i,j)坐标处图像的象素值，其中 $0\leqslant i\leqslant M-1,0\leqslant j\leqslant N-1$。

(1)输入初始值(x_0,y_0,μ_1,μ_2)到 VPCSS 系统，产生 2 个混沌实数值序列 x_k 和 y_k。

(2)利用 x_k 和 y_k 分别生成灰度矩阵 $G_1(i,j)$和 $G_2(i,j)$，$0\leqslant i\leqslant M-1,0\leqslant j\leqslant N-1$。

(3)利用 $G_1(i,j)$和 $G_2(i,j)$，并通过替代变换规则 S 来改变图像 I 中每个象素点的灰度值，得到图像 $I'(i,j)$。

(4)再次利用 x_k 和 y_k 分别生成一个整数值序列和一个二值序列，将它们作为置乱变换规则 P 的一部分。

(5)将图像 $I'(i,j)$按置乱变换规则 P 进行置乱，得到最终加密的图像 $I''(i,j)$。

2.2 算法设计

2.2.1 替代变换规则 S 的设计

对于一幅大小为 $M\times N$ 和灰度级为 L 的图像，设 $I(i,j)$为(i,j)坐标处图像的象素值，$0\leqslant i\leqslant M-1,0\leqslant j\leqslant N-1$。$I'(i,j)$为$(i,j)$坐标处替代操作后图像的象素值，即要求设计映射 f，$f:I(i,j)\rightarrow I'(i,j)$。

为了使替代操作后的象素值 $I'(i,j)$ 具有不可预测性，本文采用混沌映射来达到这个目的，其替代变换可用公式表示为：

$$I'(i,j)=G_1(i,j)\oplus[(G_2(i,j)+I(i,j))\bmod L] \qquad (1)$$

其中$\oplus$代表异或运算，+代表模 L 相加。$G_1(i,j)$和 $G_2(i,j)$二个灰度矩阵由 VPCCS 生成的序列 x_k 和 $y_k(0\leqslant k\leqslant M\times N-1)$通过下列公式变换而来：

$$g_k=round(z_k\times(L-1)) \qquad (2)$$

其中 $round(a)$函数表示取与 a 最接近的整数值。将 x_k 和 y_k 分别替换(2)式中的 z_k，即可得到 2 个整数序列，其值范围是$[0,L-1]$，然后按行扫描顺序排列成 $M\times N$ 矩阵形式，即可形成 $G_1(i,j)$和 $G_2(i,j)$二个灰度矩阵。这样就完成了替代变换的设计。解密时，其相应的逆运算是：

$$I(i,j)=[(I'(i,j)\oplus G_1(i,j))-G_2(i,j)]\bmod L \qquad (3)$$

2.2.2 置乱变换规则 P 的设计

一般地，置乱并没有多大的密码作用（因与密钥无关，如 DES），但它可以有效地打乱输入明文(或中间密文)的次序，进而能有效地掩盖明文(中间密文)的统计特性，因而能有效地抵御统计及预测分析。本文利用的置乱规则如下：

对于 $M\times N$ 大小的图像，将此图像中的每一行象素沿着某个方向循环移动 p 位，移动方向 q 和位移变量 p 可由特定的算法来确定。图像矩阵的各列可以做同样的处理。当每一行和每一列都进行了一次循环移位之后，就完成了一次置乱变换。其中，设 $q=0$ 时，行向左循环或列向上循环；设 $q=1$ 时，行向右循环或列向下循环。

本文利用混沌序列来产生位移方向 q 和位移变量 p。这里继续使用 VPCCS 系统生成的混沌序列 x_k 和 y_k。对于位移变量 p，最简单的方式是选取 x_k 小数点后第 4 和第 5 位有效数字。对于移动方向 q，可以通过一个二值序列 $sign_k$ 来确定，通过选取门值并对 y_k 进行量化即可获得二值序列 $sign_k$。

$$sign_k=\begin{cases}0 & s_k\leqslant 0.5\\ 1 & s_k>0.5\end{cases}$$

令 $q=sign_k$，即完成了置乱变换的设计。

整个系统所用的密钥为 $Key=(x_0,y_0,\mu_1,\mu_2,n)$，其中 n 是置乱变换时的迭代次数。

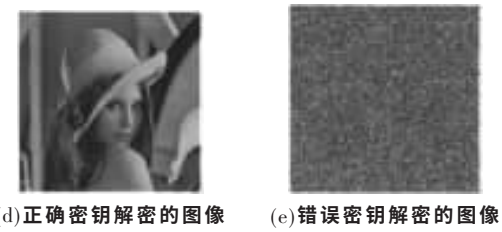
最终的加密算法由替代变换和置乱变换构成，这类似 AES 中 Safer+及 Shake 算法中的替代和置乱(Substitution and Permutation，SP)结构。其中 S 部分主要起到混淆作用，而 P 部分主要起扩散作用。这样，不但应用混沌动力系统产生了替代和置乱变换，而且应用混沌动力系统产生了各部分所需要的密钥。

解密算法和加密算法较为相似，差别在于：在加密算法中，先进行替代变换，然后进行置乱变换；而解密时其顺序相反，先要进行逆置乱变换，然后进行逆替代变换。在替代和置乱变换的每一部分，其加密和解密在结构上类似，这样的结构有利于模块化实现。

3 仿真结果与分析

采用本文方法对多幅图像进行实验。取密钥参数分别为 $x_0=0.731$，$y_0=0.342$，$\mu_1=1.7498$，$\mu_2=1.5438$，$n=1$，原始图像为 256×256 的标准 Lena 图像，则图像加密/解密的仿真结果如图 2 所示。

(a)原图像　(b)替代运算后的图像　(c)置乱运算后的图像



(d)正确密钥解密的图像　(e)错误密钥解密的图像

图 2　图像加密/解密仿真结果

可以看出，本文方法能够有效地加密/解密图像。由于混沌序列对初始值的敏感性，即使密钥值有微小的变化也会得到完全不同的解密结果。如图 2(e)中只改变 $x_0=0.732$，而密钥其他部分保持不变。

本文提出的方案有以下几个特点来确保高安全性：(1)使用变参数混合混沌系统(级联 2 个混沌系统)来生成

混沌序列。这不仅增强了混沌序列的复杂性,而且解决了混沌序列周期的退化问题。(2)混沌序列对初始条件具有极其敏感的依赖性,在状态空间中其轨迹既非周期又不收敛,这种类随机特性使得混沌序列是不可预知的,难以分析和预测。本方案中各部分所采用的密钥都是由混沌序列产生的,因此除非确切知道初始值,否则不可能有效解密。(3)在该方案中,密钥由4个初始值和1个迭代参数组成,其中 x_0 和 y_0 分别是[-1,1]和[0,1]之间的任意实数值,而 μ_1 和 μ_2 是(1.4011,2)之间的任意实数值。这使得密钥量比较大。这样的选择使得算法有着几乎一次一密特性的安全性。(4)从(1)式可知,即使攻击者截取了信道中密文,并且他可以选择明文,他也不能由式(3)有效地计算出灰度矩阵 $G_1(i,j)$ 和 $G_2(i,j)$。因此该方案不但能够对惟密文攻击免疫,而且也能够很好地抵御选择明文攻击。

本方案同时具有良好的执行效率。首先,本方案选择的是比较简单的一维混沌映射来产生混沌序列。其次,对图像数据仅在空域处理、替代运算中采用的是异或和模运算,这些都适合计算机快速处理;而在置乱变换中,不需要多次迭代即可达到面目全非的效果。本方案的测试环境是:Intel Pentium 4 1.6A CPU,256MB 内存,Windows 2000 Server。对于一幅大小为256×256的Lean图像,加密时间只需要0.75秒左右。

4 结 论

本文提出了一种基于变参数复合混沌系统的图像加密方案。在该方案中,首先利用VPCCS生成混沌序列,这不仅增大了单纯依靠差分方程产生混沌系列的复杂性,而且延长了混沌序列的周期。然后利用混沌序列的随机性来扰乱图像的象素值(替代变换)和打乱象素的位置(置乱变换)。理论和实验证明了该方案具有加密算法容易实现、加密速度快和安全性高等特点。对于生成的混沌序列,最好不要选取初始段部分序列,这样能够加强加密效果。

参考文献

1 黄润生.混沌及其应用.武汉:武汉大学出版社,2000

2 Wheeler D D.Problems with Chaotic Cryptosystems. Cryptologia,1989;13(3)

3 张巍,胡汉平,李德华.一种新的混沌序列生成方式.华中科技大学学报,2001;29(11)

4 孙克辉,刘巍,张泰山.一种混沌加密算法的实现.计算机应用,2003;23(1)

5 李昌刚,韩正之,张浩然.一种基于随机密钥及"类标准映射"的图像加密算法.计算机学报,2003;26(4)

(收稿日期:2003-11-10)