基于离散数字混沌序列的图像加密

陈 帅[①②] 钟先信[①] 石军锋[①] 朱士永[②]
[①](重庆大学光电技术及系统教育部重点实验室 重庆 400030)
[②](淮南师范学院物理系电子教研室 淮南 232001)

摘 要：由幅值连续的 Logistic 混沌公式研究了一种幅度值离散数字混沌序列的产生方法，可方便用于硬件实现图像加密。采用函数运算方法由 3 个不同周期的离散数字混沌序列“异或”运算获得长周期图像加密序列，将图像加密序列与原始图像“异或”加密图像。加密和解密仿真对比可见，该方法对初始值具有敏感性。分析表明，所获得的幅度离散数字混沌序列产生方法具有算法简单，信息安全可靠性高，便于硬件实现的特点。

关键词：图像加密；幅度离散；混沌序列；异或运算
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2007)04-0898-05

Image Encryption through Discrete Digital Chaotic Sequence

Chen Shuai[①②] Zhong Xian-xin[①] Shi Jun-feng[①] Zhu Shi-yong[②]
[①](*Key Laboratory of Optoelectronic Technology & System under State Ministry of Education, Chongqing University, Chongqing* 400030, *China*)
[②](*Electronic Staff Room in Physics Department, Huainan Normal university, Huainan* 232001,*China*)

Abstract: Study a new formula for amplitude discrete chaotic sequence to encrypt images under hardware devices conveniently from Logistic mapping formula for continuous amplitude, and generate a longer period sequences by exclusive OR algorithm with three amplitude discrete digital chaotic sequence in different periods. The image is encrypted by exclusive OR algorithm with the longer period image encrypting sequence and original image. The method is sensitive to initial values through simulation of encrypting and decrypting image. The result shows that the manner to generate amplitude discrete chaotic sequence is simple and more secure for information security, more convenient for hardware to encrypt images.

Key words: Image encryption; Amplitude discrete; Chaotic sequence; Exclusive OR algorithm

1 引言

采用混沌序列的保密通信仅仅只需要传递少数参数。馄饨序列的特性类似随机的过程[1]，等同于白噪声，对初始值极其敏感[2]。因此，将混沌序列运用于图像加密，将具有极大的方便。

文献[3,4]采用了时间离散而幅度连续的混沌序列加密图像，但这不方便图像加密的硬件实现。如果混沌序列计算不但在时间上离散，且在幅度上也离散化，这将大大方便图像加密的硬件芯片实现。但由于硬件中一般采用有限位精度进行计算，就使得按照混沌计算公式所得序列具有周期性。如果序列最小周期足够大，就可以将该序列用于信息安全[5]。文献[6,7]产生的混沌序列得到了周期延长，但序列在时间上离散化，而幅度仍然连续。

本文推导并改进了基于 Logistic 映射的幅度离散数字混沌的通用计算公式，进而采用了“异或”函数由 3 个幅度离散数字混沌序列获得有关图像加密序列，最后将图像加密混沌序列用于数字图像的加密和解密仿真。并分析了结果。

2 离散数字混沌计算原理

根据Logistic映射[1]：

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

其中 $0 \leqslant \mu \leqslant 4$，称为分支参数。$x_k \in (-1,1)$。

经过简单的变量代换，Logistic 映射可以在区间(–1，+1)上定义如下：

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

其中 $\lambda \in [0, 2]$，当 $\lambda = 2$ 时称为满映射。

对式(2)两边乘以 a^2 得：

$$a^2 x_{k+1} = a^2 - \lambda(a x_k)^2 \tag{3}$$

令 $z_k = a x_k + a$，则

$$x_k = z_k / a - 1 \tag{4}$$

2005-08-23 收到，2006-01-25 改回
国家 973 项目(G1999033105)，重庆市自然科学基金(2005BB2198)，重庆市科技计划项目(8673)，安徽省高等学校自然科学研究项目(2005KJ092)和淮南师范学院青年教师自然科学研究项目(2004 LKQ01)资助课题

将式(4)代入式(3)，取 $\lambda=2$，化简得[8]：

$$z_k = 4z_{k-1} - (2/a)z_{k-1}^2 \tag{5}$$

令式(5)左边为零，得到两个稳定解：

$$\begin{cases} z_k = 0 \\ z_k = 2a \end{cases} \tag{6}$$

在有限二进制位离散数字计算中，由于量化误差的存在，即使初始值不为零值或 $2a$，则由式(5)经过多次的迭代计算，只要某次迭代中间得到值 $2a$，则以后再次迭代的值就保持为零值。如参数 $a=2^{15}=32768$，初始值取 9，则经过 120 次的迭代后将保持为零值。为了消除这种现象，将式(5)改写为：

$$z_k = 4z_{k-1} - (2/a)z_{k-1}^2 - 1 \tag{7}$$

如果初始值不为零，则该式迭代结果不再出现零值。可以证明，只要初始值不取为零，则式(5)的计算范围为：

$$z_k \in [1, 2a-1] \tag{8}$$

3　产生图像加密数字混沌序列

设序列 $x(n)$，$y(n)$，$z(n)$，$u(n)$的最小周期分别为 $p1$、$p2$、$p3$、$p4$，则可以证明函数运算：

$$w(n) = f(x(n), y(n), z(n), u(n)) \tag{9}$$

所得复合序列的最小周期 p 为：

$$p = \mathrm{lcm}(p1, p2, p3, p4) \tag{10}$$

其中运算 lcm 表示求最小公倍数。显然，若 $p1$，$p2$，$p3$，$p4$ 中有一个为∞，则 $p=\infty$。

通过短序列的函数运算，就可以克服有限精度处理的短周期问题，从而获得长周期序列。取函数运算为“异或”运算，由 3 个离散数字混沌序列进行“异或”运算产生的长周期离散数字混沌序列的算法如图 1。其中的离散数字混沌计算是式(7)的迭代计算。采用时钟同步的 3 个离散数字混沌序列“异或”运算函数，可以表示为：

$$w(n) = f(x(n), y(n), z(n)) = x(n) \oplus y(n) \oplus z(n) \tag{11}$$

图 2 为采用 24bit精度(对应的参数$a=2^{23}$)的 3 个混沌序列运算产生的离散数字序列的一个实例，图 3 为它的自相关图，可见序列自相关具有良好的二值性，表明序列具有很好的随机性。

4　数字图像加密

采用 BMP 格式图像进行加密仿真。BMP 格式图像的每一个像素点可以由 R(red)，G(green)，B(blue)各一个字节的值表示。

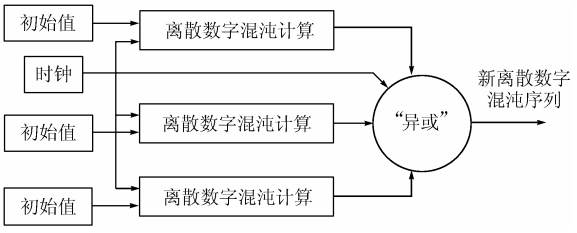

图 1　幅度离散数字 3 混沌序列异或运算产生长周期序列原理图

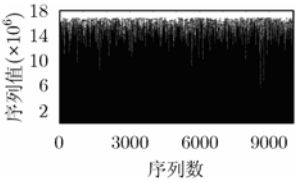

图 2　由 3 个幅度离散数字混沌“异或”所得的数字混沌序列(初始值分别为 10,11,13，24 位整数精度)

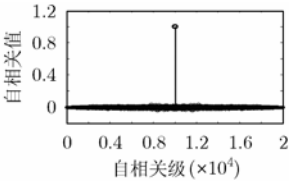

图 3　由 3 个幅度离散数字混沌“异或”所得的数字混沌序列的自相关(初始值分别为 10,11, 13，24 位整数精度)

由图 1 输入 3 个初始值，3 个初始值的每一个都为 24bit 整数，产生一个新的离散数字序列用于图像加解密。密钥序列的长度与图像总像素相等。蜜钥序列的每一个序列值与图像中每一像素对应。每一密钥序列值占 3 个字节(24bit)。加密时分别将这 3 个字节与像素的 R(red)，G(green)，B(blue)各一个字节的值进行“异或”运算。解密是加密的逆运算。

图 4 为加解密仿真对比图。其中图 4(a)为加密前原图，图 4(b)为加密后的图(密钥参数为 3 个离散数字混沌的初始值：10，11，13)，图 4(c)为正确解密后的图，图 4(d)为错误解密后的图(输入的 3 个离散数字混沌的初始值：9，11，13)。

从图 4(c)和图 4(d)可见，仅仅相差一个 bit 位的错误密钥就不能够正确恢复出原图。从而说明该加密方法对参数具有敏感性。

5　分析

基于离散数字混沌序列的图像加密的安全性取决于密

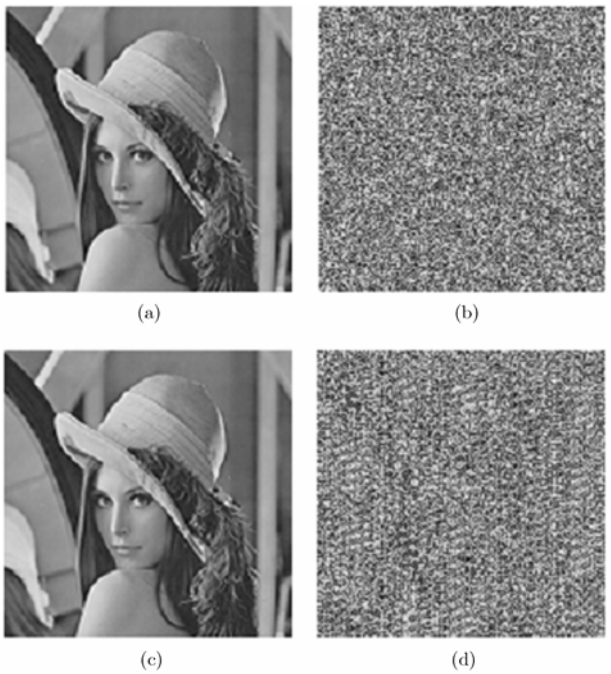

图 4　图像加解密对比图

钥空间大小。

由不同初始值根据式(7)可以获得离散序列。这些离散序列表现为短的周期性。当 $a=2^{24}$，周期为 8，272，716，$2^{24}-1$ 的 4 种序列，表 1 为这 4 种周期对应的初始值数目。

表 1　4 种周期对应的初始值数目($a=2^{24}$)

周期	初始值数目
8	2×10^4
272	1.42×10^6
716	7.5×10^5
$2^{24}-1$	1.459×10^7

将初始值按产生的周期分成 4 个集合，设 $x(n)$，$y(n)$，$z(n)$序列的初始值分别取自周期分别为 272，716，$2^{24}-1$ 的这 3 个集合，作为初始值输入图 1 用以产生图像加密序列。于是产生的新序列的 $w(n)$最小周期 p 为：

$$p=\mathrm{lcm}(272,716,2^{24}-1)=345287401690974960 \tag{12}$$

则新序列的密钥数量为：

$$(1.42\times10^6)\times(7.5\times10^5)\times(1.459\times10^7)\approx1.55\times10^{19} \tag{13}$$

以每秒 100 亿次运算，则约需要 49.27 年才能穷举完所有的可能密钥。令

$$a=2^{r+1} \tag{14}$$

则式(7)可以表示为：

$$z_k=(z_{k-1}<<2)+\text{取补}\{[z_{k-1}\times z_{k-1}]>>r\} \tag{15}$$

可见通过移位、乘法、取补、加法就可以实现离散数字混沌序列，且输入、输出都为离散数字整数值，方法简单，便于硬件实现。

6　结束语

本文在推导出了离散数字混沌计算公式的基础上，采用 3 个由离散数字混沌序列进行“异或”运算获得周期较长的离散数字混沌序列。并将产生的序列用于图像的加密和解密的仿真。仿真结果可见，所产生的离散数字混沌序列对初始密钥敏感，且计算简单，参数较少，安全性非常高。

参 考 文 献

[1] 孙霞, 吴自勤, 黄昀. 分性原理及其应用. 合肥: 中国科技大学出版社, 2003: 1–2.

[2] 王衍波, 薛通. 应用密码学. 北京: 机械工业出版社, 2003: 189–191.

[3] 孙鑫, 易开祥, 孙优贤. 基于混沌系统的图像加密算法. 计算机辅助设计与图形学学报, 2002, 14(2): 136–139.
Sun Xin, Yi Kai-xiang, and Sun You-xian. New image encryption algorithm based on chaos system. *Journal of Computer-Aided Design & Computer Graphics*, 2002, 14(2): 136–139.

[4] 鲍官军, 计时鸣, 张利等. 一种基于位运算的图像加密算法. 浙江工业大学学报, 2003, 31(3): 315–318.
Bao Guan-jun, Ji Shi-ming, and Zhang Li, *et al*.. An image-encrypting algorithm based on bit operation. *Journal of Zhejiang University of Technology*, 2003, 31(3): 315–318.

[5] 章照止. 现代密码学. 北京: 北京邮电大学出版社, 2004: 83–84.

[6] 饶妮妮. 一种数字化混沌扩频序列发生器的设计. 电子与信息学报, 2002, 24(5): 702–706.
Rao Ni-ni. Design for a digital chaotic spreading sequence generator. *Journal of Electronics & Information Technology*, 2002, 24(5): 702–706.

[7] 王相生, 甘骏人. 一种基于混沌的序列密码生成方法. 计算机学报, 2002, 25(4): 351–356.
Wang Xiang-sheng and Gan Jun-ren. A chaotic sequence encryption method. *Chinese Journal of Computers*, 2002, 25(4): 351–356.

[8] Chen Shuai, Zhong Xian-xin, and Shi Jun-feng, *et al*.. Chaos Encryption Algorithm for Wireless Sensor Networks. Seventh International Conference on Electronic Measurement and Instruments(ICEMI2005), Beijing, Aug.16-18, 2005, 8: 468–471.

陈　帅：男，1969 年生，副教授，博士生，研究方向为智能化仪器及嵌入式测控系统、EDA/SOC、信息处理与网络.

钟先信：男，1935 年生，教授，博士生导师，主要研究方向为智能化仪器及嵌入式测控系统、MEMS、图像信息处理.

石军锋：男，1975 年生，讲师，博士生，研究方向为新型网络.

朱士永：男，1976 年生，助教，主要研究方向为图像处理、信息安全.