基于 m 序列变换和混沌映射的图像加密算法

刘家胜[①②]　黄贤武[②]　朱灿焰[②]　吕皖丽[①]
[①](安徽大学计算机科学技术学院　合肥　230039)
[②](苏州大学电子信息学院　苏州　215021)

摘　要：该文利用 m 序列发生器中移位寄存器状态的遍历性(全零状态除外)，首次提出一种“ m 序列变换”用于图像位置置乱的方法。并利用混沌映射系统具有初值敏感性，参数敏感性和类随机性的特点，设计了一种基于“ m 序列变换”与混沌映射相结合的图像加密算法，与其它图像加密算法相比，该算法的密钥空间非常巨大，具有更好的安全性。

关键词：图像加密； m 序列变换；混沌映射
中图分类号：TP391　　**文献标识码**：A　　**文章编号**：1009-5896(2007)06-1476-04

Image Encryption Algorithm Based on m-Sequence Transform and Chaos Map

Liu Jia-sheng[①②]　Huang Xian-wu[②]　Zhu Can-yan[②]　Lü Wan-li[①]
[①](*School of Computer Science & Technology*, *Anhui University*, *Hefei* 230039, *China*)
[②](*School of Electronics & Information Engineering*, *Soochow University*, *Suzhou* 215021, *China*)

Abstract: Based on the ergodicity of the shifters (except for all zero-states) in m-sequence generator, in this paper a new “m-sequence transform” method is first proposed to apply to image position permutation. Combining this method with chaotic map, a novel image encryption approach is presented, and some simulating results are shown in this paper. Comparing with the existing encryption methods, the approach is not only of the characteristics of chaotic map with initial value sensitivity, parameter sensitivity and random sensitivity, but also of more larger secret key space. Thus the approach is more security than other encryption methods.

Key words: Image encryption; m-sequence transform; Chaos map

1　引言

随着网络技术与多媒体技术的飞速发展，信息的安全问题受到使用者和学者们的关注和研究，其中数字水印[1,2]和图像加密[3,4]是目前研究最为广泛的领域。

图像加密主要包括图像置乱和图像替代两种技术。其中图像置乱是改变图像像素的位置关系，降低图像的相关性。常用的图像置乱方法主要有：Arnold 变换[3]、面包师变换[5]、Standard 映射、魔方变换等。 m 序列由于其良好的伪随机特性受到广泛的应用。许多文献就是利用 m 序列的伪随机特性进行信息加密的，如文献[6]是利用 m 序列的伪随机特性对视频图像加密。笔者在分析 m 序列的原理时发现， m 序列发生器中移位寄存器具有遍历性(全零状态除外)，利用这一特性，本文提出一种新的图像置乱方法，称之为“ m 序列变换”。因此， m 序列变换与其它文献采用 m 序列进行图像加密有很大的不同，它是利用 m 序列发生器中移位寄存器状态的遍历性进行位置置换；同时，也利用了 m 序列的伪随机特性能很好地实现图像位置置乱。图像替代是改变图像每个像素点的值，使替代后的图像直方图近似于由随机序列组成的图像的直方图。这种方法可以有效地紊乱图像，使经替代处理后图像的相关性进一步降低，从而更好地保护图像数据。考虑到上述两个因素，本文设计一种基于 m 序列变换与混沌映射相结合的图像加密算法。

2005-11-07 收到，2006-05-15 改回
江苏省自然科学基金(BK2001137)和安徽省高校青年教师基金(2004jq107)资助课题

2　Logistic 混沌映射

Logistic 混沌映射是一个源于人口统计的动力学系统，其系统方程为

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

其中 x_k 为映射变量， μ 为系统参量，它们的取值范围分别为： $-1 < x_k < 1, 0 < \mu \le 2$ 。Logistic 映射是一个非常简单，却又具有重要意义的非线性迭代方程，当 $1.401155 \le \mu \le 2$ 时，系统处于混沌状态[7]，此时系统对初始值 x_0 和参数 μ 具有敏感依赖性，可用来提供数量众多，非相关，类随机而又确定的可再生信号，便于图像的加密和解密使用。

3　m 序列变换

3.1　m序列原理[8]

伪随机序列可以通过一个 n 级线性反馈移位寄存器得

到，如图 1 所示。其中 $a_{n-1},a_{n-2},\cdots a_1,a_0$ 为寄存器的状态，反馈线的连接状态用 c_i 表示，$c_i=1$ 表示反馈线接通(参与反馈)，$c_i=0$ 表示反馈线断开，但是 $c_n=c_0=1$。寄存器的每一级输出经反馈相加后作为最高位的输入 a_n。n 级线性反馈移位寄存器可能产生的最长周期为 2^n-1，称这种最长的序列为 m 序列。线性反馈移位寄存器能产生 m 序列的充要条件是反馈移位寄存器的特征多项式为本原多项式。

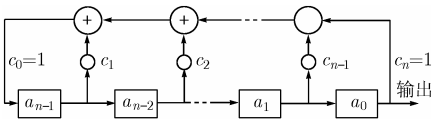


图 1　n 级线性反馈移位寄存器

3.2 m 序列变换

根据 m 序列的理论，本文设计了一种基于 m 序列的图像位置置乱方法，即称之为 m 序列变换，其变换原理如下：

设数字图像为 $\boldsymbol{f}(x,y)$，$x=0,1,\cdots,M-1$，$y=0,1,\cdots,N-1$，若 M 和 N 满足 $2^{k_x-1}<M\le 2^{k_x}$ 和 $2^{k_y-1}<N\le 2^{k_y}$，取一个 $k=k_x+k_y$ 级线性反馈移存器的本原多项式 $f(x)$ 作为其特征方程，且移位寄存器的初始状态为非零状态。则数字图像 $\boldsymbol{f}(x,y)$ 的水平坐标 x_r 和垂直坐标 y_r 可分别用前 k_x 个和后 k_y 个移位寄存器的状态来表示，其对应关系如式(2)：

$$\left.\begin{aligned} x_r&=\sum_{i=1}^{k_x}a_{k_x+k_y-i,r}\cdot 2^{k_x-i}\\ y_r&=\sum_{j=1}^{k_y}a_{k_y-j,r}\cdot 2^{k_y-j}\end{aligned}\right\} \tag{2}$$

其中 r 表示 m 序列由第 0 时刻开始的移位次数，$r\in\{0,1,2,\cdots,2^k-2\}$。而 $a_{k_x+k_y-i,r}$ 和 $a_{k_y-j,r}$ 表示前 k_x 个和后 k_y 个移位寄存器在 r 时刻的状态。根据 m 序列原理可知 $x_r\in\{0,1,\cdots,2^{k_x}-1\}$ 和 $y_r=\{0,1,\cdots,2^{k_y}-1\}$，但 x_r 和 y_r 不能同时为零。在图像位置置乱中，x_r 和 y_r 可作为原图像经过 m 序列变换后的水平和垂直坐标。显然，m 序列在移位时得到的 x_r 和 y_r 有些超出了图像的尺寸界限，在 m 序列变换中对这些点要作舍弃处理。

设 $\boldsymbol{f}'(x',y')$ 表示 $\boldsymbol{f}(x,y)$ 经 m 序列变换后图像，其中 $x'=0,1,2,\cdots M-1$; $y'=0,1,2,\cdots N-1$，则 m 序列变换算法描述如下：

(1) 设 $\boldsymbol{f}(x,y)$ 的第 1 个像素点 $(0,0)$ 映射到 $\boldsymbol{f}'(x',y')$ 的除 $(0,0)$ 外的任意一点 (x_0',y_0')，x_0' 和 y_0' 分别对应前 k_x 个和后 k_y 个移位寄存器的状态，其对应关系参照式(2)。

(2) m 序列移位一次，并由移位寄存器状态用式(2)计算 x_1 和 y_1，检查 x_1 和 y_1 是否满足式(3)：

$$\left.\begin{aligned} 0\le x_r\le M-1\\ 0\le y_r\le N-1\end{aligned}\right\} \tag{3}$$

若不满足，m 序列继续移位，并由移位寄存器状态用式(2)计算 x_2 和 y_2，检查 x_2 和 y_2 是否满足式(3)，直到寻找到满足式(3)的 x_r 和 y_r 为止，并把此时的 x_r 和 y_r 记为 x_1' 和 y_1'，将 $\boldsymbol{f}(x,y)$ 的第 2 个像素点 $(0,1)$ 映射到 $\boldsymbol{f}'(x',y')$ 的点 (x_1',y_1')。

(3) m 序列继续移位，按照步骤(2)方法对 $\boldsymbol{f}(x,y)$ 其它像素点映射到 $\boldsymbol{f}'(x',y')$ 中，m 序列经过一个周期后，正好将 $\boldsymbol{f}(x,y)$ 除 $(M-1,N-1)$ 一点外的其它所有像素点都映射到 $\boldsymbol{f}'(x',y')$ 的对应点，最后将 $\boldsymbol{f}(x,y)$ 的 $(M-1,N-1)$ 点映射到 $\boldsymbol{f}'(x',y')$ 的 $(0,0)$ 点。

上述过程实现了图像的 m 序列变换。当 $f(x)$ 为本原多项式时，$k=k_x+k_y$ 级线性反馈移位寄存器的周期为 $2^{k_x+k_y}-1$，舍弃不同时满足 $0\le x_r\le M-1$ 和 $0\le y_r\le N-1$ 的映射点，再把移位寄存器的全零状态补上，上述 m 序列变换显然是一一映射，用它可实现图像的位置置乱。其图像置乱的结果取决于任意选定的 x_0' 和 y_0'，因此 x_0' 和 y_0' 可作为图像加解密的密钥。其中 x_0' 和 y_0' 的密钥空间分别是 $x_0'\in\{0,1,\cdots,M-1\}$ 和 $y_0'=\{0,1,\cdots,N-1\}$，但是 x_0' 和 y_0' 不能同时为零。所以，x_0' 和 y_0' 总的密钥空间大小为 $M\times N-1$。

m 序列变换对图像位置置乱非常有效，它具有映射的随机性，且取决于 x_0' 和 y_0'。采用 m 序列变换对尺寸大小为 207×250 灰度图像进行位置置乱加密处理的实验结果如图 2 所示，在本文实验中取 $x_0'=10$ 和 $y_0'=21$。

(a) 原始图像　　(b) m序列变换后图像

图 2　位置置乱图像加密

很遗憾，在仅用 m 序列变换进行图像位置置乱的图像加密中，如果公布图像位置置乱的加密算法，此时 x_0' 和 y_0' 将失去密钥作用。图 3 是 x_0' 和 y_0' 取不同值得到的解密图，尽管与原图像不尽相同，但经过简单的裁剪和拼接，就可恢复出原图像。因此，这类算法是不能公开的，其秘密不是完全寓于密钥，这不符合现代密码体制的规范。这是 m 序列变换的一个缺点。

为了使得 m 序列变换适用于现代密码体制，本文设计了一种基于 m 序列变换与 Logistic 混沌映射相结合的图像

(a) 解密图像 x_0'=11　　(b) 解密图像 y_0'=20

图 3　图像解密

加密算法，该算法能很好地避免上述问题，其加解密算法步骤如下。

4 基于 m 序列变换与混沌映射相结合的图像加解密算法

加密算法描述如下：

步骤 1 输入待加密图像，用矩阵表示为 $\boldsymbol{f}_0(i,j), i=0,1,\cdots,M-1; j=0,1,\cdots,N-1$。设定图像加密的迭代次数 r。

步骤 2 输入 Logistic 混沌映射的初始值 $x_{0,1}, x_{0,2}$ 和参数 μ_1,μ_2，采用式⑴迭代 $M\times N+k$ 次生成不同矩阵 $\boldsymbol{g}1(i,j)$ 和 $\boldsymbol{g}2(i,j)$，其中 $0\le i\le M-1, 0\le j\le N-1$（说明：其原因是保证 Logistic 映射的初值敏感性和参数敏感性，矩阵 $\boldsymbol{g}1(i,j)$ 和 $\boldsymbol{g}2(i,j)$ 应该舍弃 Logistic 映射开始迭代 k 次的数据）。由于处理的信号是数字图像，一般要求矩阵 $\boldsymbol{g}1(i,j)$ 和 $\boldsymbol{g}2(i,j)$ 的元素值为正整数(如 $\boldsymbol{g}1, \boldsymbol{g}2\in[0,255]$)，可采用式⑷进行取整操作：

$$\boldsymbol{g}1(i,j) \text{ or } \boldsymbol{g}2(i,j) = \text{round}((x_u+1)\times 255/2) \tag{4}$$

其中 u 表示系统迭代次数，这两个矩阵用于图像灰度值替代操作的随机参数。输入的初始值 $x_{0,1}, x_{0,2}$ 和参数 μ_1,μ_2 即为图像加密的密钥之一。

步骤 3 图像灰度值替代：对图像 $\boldsymbol{f}_0(i,j)$ 逐点按照式(5)进行图像灰度值的替代得到 $\boldsymbol{f}_1(i,j)$：

$$\boldsymbol{f}_1(i,j) = \big(\boldsymbol{f}_0(i,j) + \boldsymbol{g}1(i,j)\cdot i + \boldsymbol{g}2(i,j)\cdot j\big) \bmod L \tag{5}$$

其中 L 为图像的灰度级。

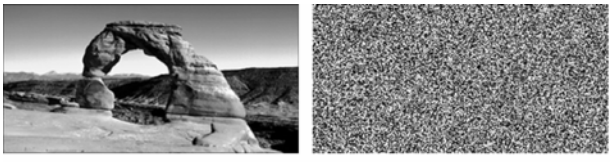
步骤 4 图像置换，随机选择参数 x_0' 和 y_0'，采用上述的 m 序列变换对图像 $\boldsymbol{f}_1(i,j)$ 进行位置置换处理，得到 $\boldsymbol{f}_2(i,j)$。

步骤 5 重复步骤 3 和步骤 4，直至迭代达到 r 次为止。

图像解密是图像加密的逆过程，限于篇幅有限，本文不再介绍。

5 实验结果及其分析

在 Matlab 6.0 编程环境下采用本文算法对大小为 128× 256 的灰度图像进行加解密处理，其中 x_{01}=0.4509, x_{02}=0.87807, μ_1= 1.989, μ_2= 2, $x_0'=10$, $y_0'=21$ 和 $r=1$，其实验结果如图 4 所示。

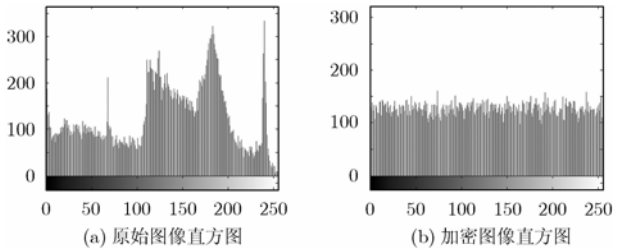


(a) 原始图像 (b) 加密图像

图 4 图像加密

5.1 统计分析

5.1.1 直方图 由图 5 所示实验结果，很清楚表明，与原始图像直方图比较，加密图像直方图有很大的不同，它非常均匀。因此，经本文算法加密后图像在传输中具有更好的隐蔽性。



(a) 原始图像直方图 (b) 加密图像直方图

图 5 图像加密统计直方图

5.1.2 相关性[3] 原始图像中相邻像素的相关性是很大的，为了破坏统计攻击，必须降低相邻像素的相关性。本文采用式(6)–式(10)计算原始图像和加密图像的 $M\times N/2$ 对像素点测试其在水平和垂直方向的相关系数，其测试值如表 1 所示。

$$\text{cov}(x,y) = E(x-E(x))(y-E(y)) \tag{6}$$

$$r_{xy} = \frac{\text{cov}(x,y)}{\sqrt{D(x)}\cdot\sqrt{D(y)}} \tag{7}$$

其中 x 和 y 表示两个相邻的像素灰度值，且在实际数值计算时则采用如式(8)–式(10)的 $E(x)$， $D(x)$ 和 $\text{cov}(x,y)$ 的离散形式：

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{8}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{9}$$

$$\text{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{10}$$

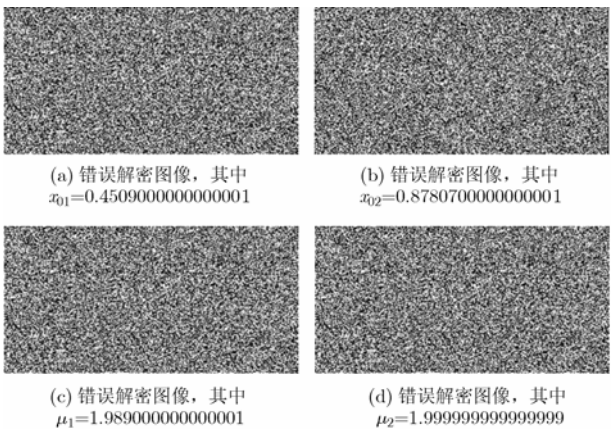
为了描述方便，用 r_f^0, r_f^m 和 r_f^{en} 分别表示原始图像，m 序列变换置乱后图像和本文算法加密后图像的相关系数。其相关系数如表 1 所示。

表 1 原图像与加密图像的相关系数比较

	r_f^0	r_f^m	r_f^{en}
水平方向	0.9593	0.0081	0.0075
垂直方向	0.9177	0.0079	0.0021

5.2 Logistic 映射的敏感性测试

在图 6 实验中，在只改变混沌系统的一个初始值或一个



(a) 错误解密图像，其中 x_{01}=0.4509000000000001 (b) 错误解密图像，其中 x_{02}=0.8780700000000001

(c) 错误解密图像，其中 μ_1=1.989000000000001 (d) 错误解密图像，其中 μ_2=1.999999999999999

图 6　Logistic 映射的敏感性测试

参数而其它参数都相同情况下，均不能正确解密，说明 Logistic 映射对初始值和系统参数具有敏感依赖性。因此，在未知准确密钥时，即使初始值 $x_{0,1},x_{0,2}$ 和参数 μ_1,μ_2 已知，是难以将加密图像正确解密的。

5.3 x_0' 和 y_0' 对图像解密的敏感性测试

在图 7 实验中，若只改变 x_0' 和 y_0' 中一个值情况下，则图像不能正确解密。它说明 x_0' 和 y_0' 可以作为一个图像加密的密钥。与仅用 m 序列变换时使图像位置置乱加密算法 x_0' 和 y_0' 密钥失效相比，其不同在于解密图像尽管几个分块的图像相对位置不变，但我们可以从中理解信息的含义，只是图像的绝对位置改变了。由于我们在像素值替代时，引入了由混沌系统产生的位置参数，使 x_0' 和 y_0' 参数也具有参数敏感性。

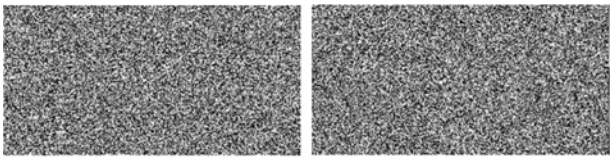


图 7　x_0' 和 y_0' 的敏感性测试

5.4 算法安全性能分析

从上述实验结果及其分析可知，必须正确输入密钥，即初始值 $x_{0,1},x_{0,2}$，参数 μ_1,μ_2，x_0',y_0' 和迭代次数 r 全部正确才能对加密图像正确解密。因此本算法对图像加密的密钥空间在 Matlab 6.0 试验平台上可达到 10^{70}，其中参数 $x_{0,1}$, $x_{0,2}$,μ_1,μ_2 的空间数量级均为 10^{15}，迭代次数 r 空间数量级为 10^5。x_0' 和 y_0' 的密钥空间与图像尺寸大小有关，其总的密钥空间大小为 $M\times N-1$，详见 m 序列变换算法说明。对尺寸大小为 128×256 的图像而言，其空间数量级为 10^5。非授权者若用穷举法进行破密是很难在有限的时间内破密成功。

根据 Kerckhoffs 准则，加密算法要与密钥完全分开是现代密码体制的要求。上述实验结果表明本文提出的算法可以公开，完全符合现代密码体制的要求。

6　结束语

本文首次提出一种基于 m 序列变换与混沌映射相结合的图像加密方案，得到了非常满意的实验结果。概括起来，该算法具有以下优点：

(1) 利用 m 序列产生器中移位寄存器的状态具有遍历性(全零状态除外)，实验证明本文提出的 m 序列变换用于图像位置置换能很快取得非常好的置乱效果。

(2) 当 $1.401155\le\mu\le2$ 时，Logistic 映射进入混沌状态，此时系统对初始值 x_0 和参数 μ 具有依赖敏感性。因此，采用本算法进行图像加密是非常安全的，其密钥空间巨大。

(3) 由于在图像像素值替代中引入了位置参数，使得初始值 x_0' 和 y_0' 具有参数敏感性，克服了 m 序列变换的缺点，使本文设计的图像加密算法符合现代密码体制的要求。

(4) 与 Arnold 变换和 Standard 映射对图像尺寸有特殊要求相比，本文提出的 m 序列变换对图像尺寸没有特别要求。

参 考 文 献

[1] Kumsawat P, Attkitmongcol K, Srikaew A, and Sujitjorn S. Wavelet-based image watermarking using the genetic algorithm. Knowledge-based intelligent information and engineering systems. 8th International Conference, KES 2004. Proceedings (Lecture Notes in Artificial Intelligence Vol.3215), 2004, Vol.3: 643–649.

[2] Bao P and Ma Xiaohu. Image adaptive watermarking using wavelet domain singular value decomposition. *IEEE Trans. on Circuits and Systems for Video Technology*, 2005, 15(1): 96–102.

[3] Chen Guan-rong, Mao Yao-bin, and Chui Charles K. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons and Fractals*, 2004, 21(3): 749–761.

[4] Zhang Lin-hua, Liao Xiao-feng, and Wang Xue-bing. An image encryption approach based on chaotic maps. *Chaos, Solitons and Fractals*, 2005, 24(3): 759–765.

[5] 邹建成，齐东旭，熊昌镇. 基于面包师变换的数字图像加密. 北方工业大学学报, 2003, 15(1): 6–10.

[6] 甘小莺，孙诗瑛，宋文涛. 基于伪随机序列的视频图像加密新算法. 数据采集与处理, 2002, 17(3): 248–251.

[7] 唐秋玲，覃团发，陈光旨. 混沌图像加密. 广西大学学报, 1999, 24(1): 61–64.

[8] 樊昌信，张甫翊等编. 通信原理. 北京: 国防工业出版社, 2001 年 5 月第 5 版: 326–336.

刘家胜：　男，1971 年生，讲师，博士生，研究方向为图像和视频加密.

黄贤武：　男，1941 年生，教授，博士生导师，主要研究方向为数字图像处理、模式识别等.

朱灿焰：　男，1962 年生，教授，硕士生导师，主要研究方向为混沌保密通信.

吕皖丽：　女，1974 年生，讲师，硕士，研究方向为信息安全.