Journal of Image and Signal Processing 图像与信号处理, 2016, 5(3), 88-94
Published Online July 2016 in Hans. http://www.hanspub.org/journal/jisp
http://dx.doi.org/10.12677/jisp.2016.53012

Hans汉斯

Research on Bit-Level Digital Image Encryption Algorithm Based on Logistic Chaotic System

Jingjing Huang, Qinghua Wang, Zhenhua Li

Nanjing University of Science and Technology, Nanjing Jiangsu
Email: 823223165@qq.com

Received: Jun. 25th, 2016; accepted: Jul. 10th, 2016; published: Jul. 13th, 2016

Abstract

A bit-level digital image encryption method based on Logistic chaotic system is proposed. Each pixel value of a grayscale image uses eight-bit binary numbers, and the two-dimensional gray image is converted to a one-dimensional string containing 0 and 1. We generate the Logistic chaotic sequence with the given initial value, and then sort the chaotic sequence to obtain a location index. According to the location index, the original image is scrambled in bit-level. The pixels fusion and pixel scrambling encryption of an image are realized simultaneously. Experiments show that the algorithm is simple, safe and efficient.

Keywords

Chaos, Scrambling, Image Encryption

基于Logistic混沌映射的比特级数字图像加密算法研究

黄晶晶，王清华，李振华

南京理工大学，江苏 南京
Email: 823223165@qq.com

文章引用: 黄晶晶, 王清华, 李振华. 基于 Logistic 混沌映射的比特级数字图像加密算法研究[J]. 图像与信号处理, 2016, 5(3): 88-94. http://dx.doi.org/10.12677/jisp.2016.53012

收稿日期：2016年6月25日；录用日期：2016年7月10日；发布日期：2016年7月13日

摘　要

提出一种基于Logistic混沌映射的比特级数字图像加密方法。灰度图像的每个像素值采用八位的二进制数来表示，将二维灰度图转换为一维的0和1的数码串来处理。根据给定的初始值由Logistic映射及生成混沌序列，对混沌序列进行排序，得到位置索引，根据位置索引对原始图像进行比特级的置乱操作，可以达到集像素融合和像素置乱于一体的图像加密结果。实验表明，该算法简单易行，安全高效。

关键词

混沌，置乱，图像加密

1. 引言

信息时代的飞速发展让信息传递更加迅速和便捷，数字图像信息因其具有形象直观传递信息的特点，在日常的数据通信中运用得尤为广泛。因此，数字图像在传递过程中的安全问题也更加值得我们关注。

由于数字图像数据量庞大，冗余性严重，且数据存储结构呈二维空间分布，用传统的加密方式加密效率非常低，需要一种适合数字图像的新的加密方式来提高加密效率[1]。混沌映射与加密系统两者之间的诸多共性，例如：混沌的拓扑传递与混迭特性类似于密码的扩散与混淆特性；混沌对参数的敏感性则对应着密码对密钥的敏感性；混沌映射通过多轮的迭代获得指数分离的轨道，加密系统则通过多轮的置乱与替换将明文打乱[2]。基于混沌映射的图像加密算法受到了许多学者的青睐[3]。本文在前人研究基础上，探讨基于 Logistic 混沌映射的比特级数字图像加密方法的可行性，设计了图像的比特级置乱步骤。

2. Logistic 映射

Logistic 映射是一种应用十分广泛的动力系统，其一般定义形式如下[4]：

$$x_{n+1} = \mu x_n \left(1 - x_n\right) \tag{1}$$

图 1 为 Logistic 映射的分岔图。其中，分岔系数 $\mu \in (0,4)$，状态 $x_n \in (0,1)$。由图示可知当 $\mu \in (3.5699456,4]$ 时，Logistic 映射的输入输出都分布在(0,1)上，Logistic 映射工作于混沌状态。

3. 加密解密算法

一般的加密过程分为两个模块，一部分是像素融合模块，一部分是像素置乱模块。两模块之间相互独立，均可单独对图像进行有效的加密操作。为了提高加密的安全性，通常将两种加密方式结合起来使用[5]。本文采取的是比特级的加密方式，这种加密方式可以只进行一步置乱操作，但在效果上却可以达到像素融合的目的。下面是具体算法：

第一步，先将原始图像的像素值二维矩阵由 L 行 R 列转换成 L × R 行一列的形式，每一行有一个十进制数，表示一个像素值。

第二步，既然要做比特级的操作，我们就要把原始图片的每一位像素值由十进制化成二进制形式，像素值在区间(0,255)上，所以每个十进制像素值由八位二进制数表示，不足八位的高位由 0 补齐。具体换算公式为：

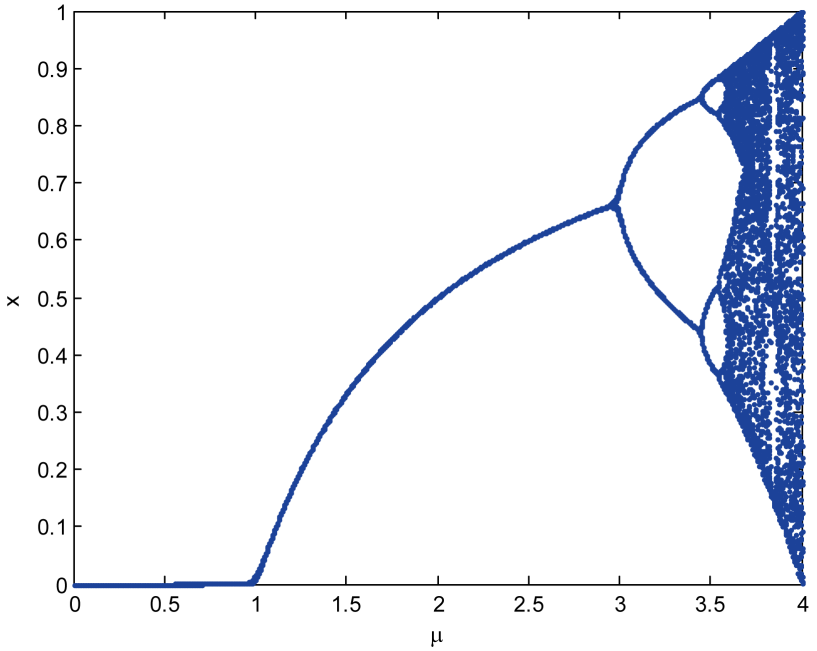


Figure 1. The bifurcation diagram of Logistic mapping
图 1. Logistic 映射的分岔图

$$\begin{cases} x_i = y_i \bmod 2 \\ y_{i+1} = \left[y_i / 2 \right] \end{cases} \tag{2}$$

其中 $i = 1,2,\cdots,8$， x_i 表示二进制数的第 i 位(第一位为最低位)， y_i 是原始像素值， $\left[y_i / 2 \right]$表示除以 2 再取整。

我们把每一位二进制数看成是一个数，换算过后由十进制数表示的 L × R 行一列的矩阵就变成了 L × R 行八列的形式。

第三步，将 L × R 行八列的矩阵继续整形成 L × R × 8 行一列的形式。

第四步，利用式(1)及初始值生成混沌序列，即迭代 Logistic 映射直到产生 L × R × 8 个完全不同的值为止，记作 $\{A_i, i = 1,2,\cdots, L \times R \times 8\}$，其中 L × R 是需要加密的图像的大小。

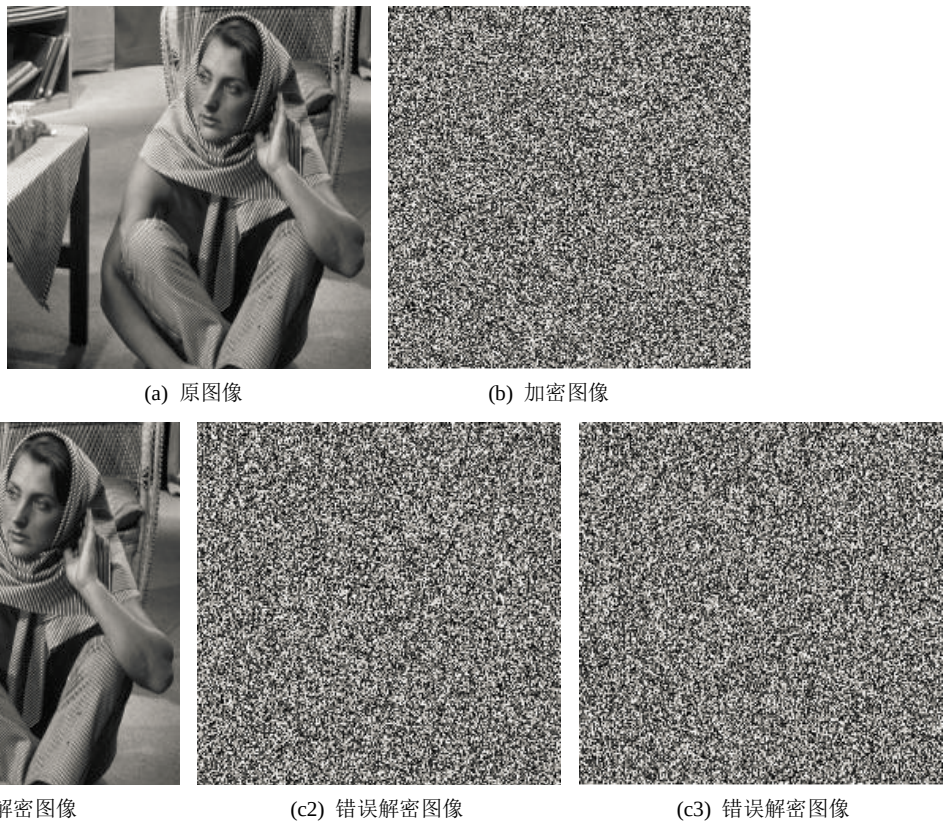
第五步，对混沌序列 $\{A_i, i = 1,2,\cdots, L \times R \times 8\}$ 进行排序，得到位置索引，根据位置索引对上述 L × R × 8 行一列形式的矩阵进行置乱。

第六步，对置乱后的 L × R × 8 行一列形式的矩阵做第一步到第三步的逆操作。即先由 L × R × 8 行一列形式整形成 L × R 行八列的形式；再把 L × R 行八列矩阵每一行的八个数看成是二进制的每一位合并成一个二进制数，将这个二进制数换算成一个十进制数，L × R 行八列的矩阵变成 L × R 行一列；最后将 L × R 行一列的矩阵还原成 L 行 R 列的形式成为加密图像。

解密过程是加密过程的逆运算。

4. 加密解密数值实验

如下图 2 所示，对原图像(a)用密钥 $X_0 = 0.1$， $\mu = 3.8$ 进行加密，得到加密图像(b)。再分别用密钥 $X_0 = 0.1$， $\mu = 3.8$ 、密钥 $X_0 = 0.10001$， $\mu = 3.8$ 和密钥 $X_0 = 0.1$， $\mu = 3.80001$ 对加密图像进行解密，得到解密图像(c1) (c2) (c3)，由三个解密图像可以看出，只有当使用正确的密钥解密时才能恢复出原图像，否则会得到杂乱无章的图像。



(a) 原图像 (b) 加密图像

(c1) 正确解密图像 (c2) 错误解密图像 (c3) 错误解密图像

Figure 2. Encrypted image obtained with a different key to decrypt
图 2. 对加密图像用不同密钥进行解密

5. 实验结果及安全性分析

5.1. 密钥空间和雪崩效应分析

5.1.1. 密钥空间分析

密钥主要是由 Logistic 映射的控制参数 μ 和初始值 X_0 组成[6]。由 Logistic 映射的特点可知，$\mu \in [3.5699456,4]$，$x_0 \in (0,1)$，所以密钥 μ 可以取区间[3.5699456,4]上的任意浮点数，而密钥 X_0 则可以取区间(0,1)上的任意浮点数，可见密钥空间相当大。

5.1.2. 密钥雪崩效应分析

从密钥更换的有效性考虑，一个秘密算法对密钥的变化应该是敏感的，即密钥具有所谓的雪崩现象。我们分别改变 μ 和 X_0 的值，观察加密图像，考察算法对密钥的敏感度。

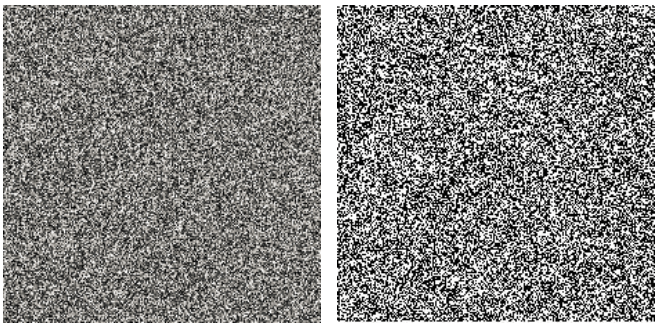
图 3 和图 4 示当参数 X_0，μ 分别改变 0.00001 的情况下，不能从密文中提取更多的信息，这表明算法对密钥非常敏感。

5.2. 抗统计攻击

5.2.1. 直方图分析

图 5 给出了原始图像和加密图像的灰度值统计直方图，由比较可知，变化前后的直方图有明显的变化，原图像的统计直方图分布不均匀，而加密后的统计直方图呈均匀分布，一定程度上掩盖了变换前原图的分布规律。而传统的置乱加密算法只改变像素点的位置，不改变直方图的分布。

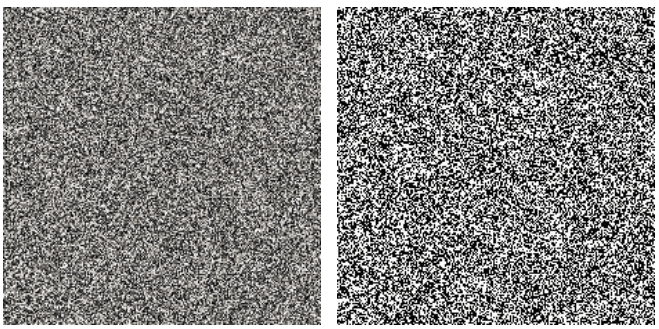
原图像 $X_0=0.1$， $\mu=3.8$ 的加密图像



$X_0=0.10001$， $\mu=3.8$ 的加密图像加密图像差

Figure 3. Ciphertext sensitivity to key X_0
图 3. 密文对密钥 X_0 的敏感度

原图像 $X_0=0.1$， $\mu=3.8$ 的加密图像



$X_0=0.1$， $\mu=3.80001$ 的加密图像加密图像差

Figure 4. Ciphertext sensitivity to key μ
图 4. 密文对密钥 μ 的敏感度

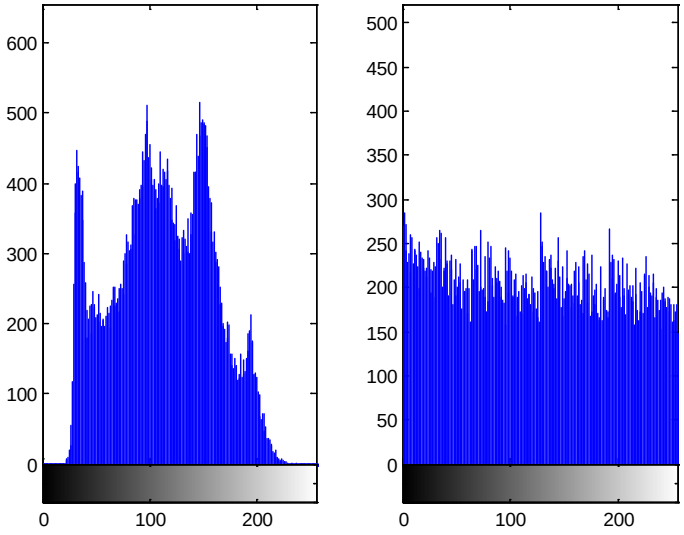


Figure 5. The gray value histogram of the images encrypted before and after
图 5. 加密前后图像灰度值直方图

5.2.2. 相关性分析

在测试图像中，随机选取 1000 对相邻(包括水平、垂直和对角方向相邻)的像素点对，记为(x_i, y_i)，其中 x_i， y_i 分别代表第i对像素的两个像素值。按如下定义的相关系数，计算这 1000 对像素灰度值之间的线性相关系数。

$$Cov(x,y)=E\left[\left(x-E(x)\right)\left(y-E(y)\right)\right] \tag{3}$$

$$r_{xy}=\frac{\left|Cov(x,y)\right|}{\sqrt{D(x)}\ \sqrt{D(y)}} \tag{4}$$

式中，x，y 表示两个相邻的像素灰度值。在实际测试中用如下离散化的计算公式[7] [8]：

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{5}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)^2 \tag{6}$$

$$Cov(x,y)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)\left(y_i-E(y)\right) \tag{7}$$

以相邻两像素灰度值为 x，y 坐标，得到加密前后相邻两点的相关性分析结果如图 6 所示。

表 1 列出了对明文图像和密文图像多次随机选取 1000 对像素测试后得到的相关系数。可以看出，加密前的图像像素之间具有较强的相关性，经过加密过后，这种相关性已经基本被破坏了。

6. 结束语

本文提出了一种基于混沌序列进行比特级图像加密的算法，将图像的每一位像素值做二进制转化，形成一维的 0 和 1 的数码串。对二进制数码串进行混沌置乱操作，可同时达到像素融合的目的，实现图像加密。根据数值实验结果可以看出，基于 Logistic 混沌映射的比特级数字图像加密算法的加密效果较好，能很好的去除图像的相关性，用错误的密钥不能解密出原始图像。从安全性分析结果可以看出，密

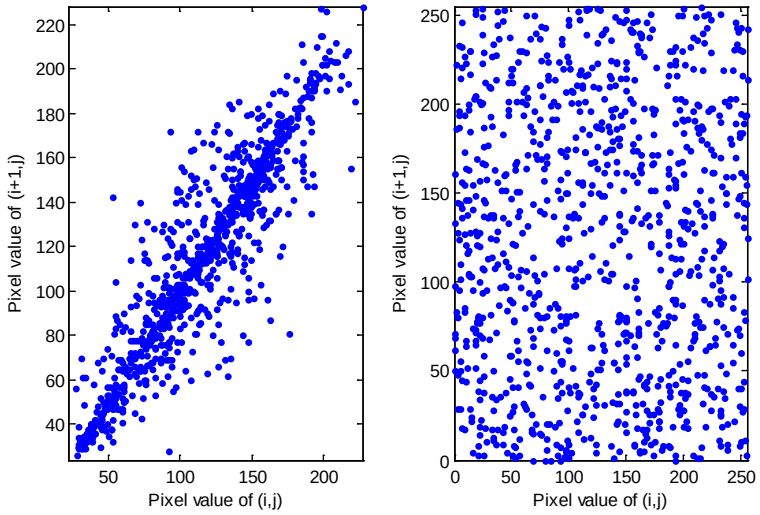


Figure 6. The correlation analysis between adjacent pixels of plaintext and ciphertext
图 6. 明文图像和密文图像相邻两点的相关性分析结果

Table 1. The correlation coefficient between adjacent pixels of plaintext and ciphertext
表 1. 明文图像和密文图像相邻像素间的相关系数

加密前	0.9215	0.9293	0.9225	0.9176	0.9305	0.9235	0.9274	0.9365
加密后	0.0359	0.0366	0.0035	0.0156	0.0479	0.0308	0.0359	0.0183

钥的雪崩效应明显，不同的密钥生产的加密图像差别较大。算法有较强的抗统计攻击能力，能满足安全保密的数据传递。

参考文献 (References)

[1] 王朋飞, 冯桂. 基于混沌动力系统的数字图像加密方法[J]. 计算机工程与应用, 2007, 43(13): 55-57.

[2] 陈关荣. 动力系统的混沌化[M]. 上海: 上海交通大学出版社, 2006.

[3] 张永红, 张博. 基于 Logistic 混沌系统的图像加密算法研究[J]. 计算机应用研究, 2015, 32(6): 1770-1773.

[4] 李彩虹, 李贻斌, 赵磊, 等. 一维 Logistic 映射混沌伪随机序列统计特性研究[J]. 计算机应用研究, 2014, 31(5): 1403-1406.

[5] Chen, J.X., Zhu, Z.L., Fu, C., *et al.* (2013) An Improved Permutation-Diffusion Type Image Cipher with a Chaotic Orbit Perturbing Mechanism. *Optics Express*, **21**, 27873-27890. http://dx.doi.org/10.1364/OE.21.027873

[6] 黄润生. 混沌及其应用[M]. 武汉: 武汉大学出版社, 2000.

[7] Fu, C., Chen, J.J., Zou, H., *et al.* (2012) A Chaos-Based Digital Image Encryption Scheme with an Improved Diffusion Strategy. *Optics Express*, **20**, 2363-2378. http://dx.doi.org/10.1364/OE.20.002363

[8] Wong, K.W., Kwok, S.H. and Law, W.S. (2006) A Fast Image Encryption Scheme Based on Chaotic Standard Map. *Physics Letters A*, **372**, 2645-2652. http://dx.doi.org/10.1016/j.physleta.2007.12.026