基于双 Logistic 混沌映射的数字图像加密算法研究

李繁[1,3]，林才寿[2]，王小敏[3]

（1. 成都纺织高等专科学校电气信息工程学院，四川 成都 611731；2. 中国地质科学院矿产综合利用研究所，四川 成都 610041；3. 西南交通大学信息科学与技术学院，四川 成都 610000）

摘要：本文提出了一种基于双 Logistic 混沌映射的数字图像加密方案。在双混沌数字图像加密方案中主要利用了两级 Logistic 混沌映射来进行伪随机序列数的创建和生成，并通过两次创建过程来得到图像扩散和置乱的随机序列数。在加密和解密处理过程中，双混沌数字图像加密方案采用的密钥为一级 Logistic 混沌映射的计算参数和二级 Logistic 混沌映射的初值，加密过程采用先扩散后置乱的顺序进行，解密过程按照相反顺序进行处理。通过对加密方案在 .NET 平台下进行试验仿真，可以得到方案的加密效果是比较好的，同时也可以基本正确完成图像的解密处理。最后，在方案试验仿真工作的基础上，对方案的密钥空间大小、方案对密钥的敏感性、加密图像的像素关联性以及信息熵等方面进行了详细分析和研究，证明了方案的安全性和执行效率。结果表明，该算法安全高效，在图像保密通信中具有较大的应用潜力。关

关键词：数字图像；混沌系统；混沌加密；Logistic 混沌映射

doi:10.3969/j.issn.1000-6532.2018.03.033

中图分类号：TD989　**文献标志码**：A　**文章编号**：1000-6532（2018）03-0151-07

近年来，伴随着网络技术和数字通信技术在全球范围内的快速推广与普及，在民用和军用领域中，数字图像以及基于数字图像的数字视频已经成为计算机网络中进行信息存储和传输的重要媒介[1]。图像发行者为了保护自身的利益，就需要可靠的图像数据加密技术。而且，在某些情况下，对于某些图像数据必须要采用可靠的加密技术，在诸如矿产资源环境下的图像信息保密存储以及工业协同设计、场景监控、矿产数据信息分析等传输系统中，需要可靠的图像加密技术。

1　混沌数字图像加密算法

随着信息技术和数字图像加密技术的快速发展，混沌加密技术凭借着良好的随机性和流加密特点，在数字图像加密技术中的应用越来越广泛。数字图像混沌加密技术就是利用混沌映射来对数字图像进行加密保护，并设计对应的解密方法，目前基于混沌系统的数字图像加密技术或者方案主要是利用了混沌映射来进行伪随机序列的创建，相比传统的利用计算机软件的方式进行伪随机数创建的方式，其序列的随机性更好。另外一种数字图像混沌加密算法主要是利用了混沌系统的参数与初值敏感性特征来进行，可以将加密过程中的密钥设置为混沌系统的控制参数，同时利用原始数字图像作为混沌系统的初始条件，通过循环迭代计算的方式来对图像进行加密，解密过程执行逆操作即可[2]。在加密解密处理过程中，这种方式与第一种方式相比，在执行速度方面要更快。近年来还出现了一种基于二维混沌分组密码的数字图像加密方案，其核心是通过利用二维混沌系统来对数字图像进行更为复杂的变换处理，其密钥长度不定，并且在加密速率和安全性方面也比较好[3]。但是由于传统的密码系统和混沌系统分别工作在有限离散集和连续实数集上，这种差异导致在混沌加密技术的应用过程中需要进行比较复杂的映射处理[4]。

收稿日期：2017-04-25；**改回日期**：2017-05-15

作者简介：李繁（1983-），女，硕士研究生在读，研究方向为信息安全。

为了获得高安全与高效率的图像加密方案，本文提出了一种基于双 Logistic 混沌映射的数字图像加密方案。主要利用了两级 Logistic 混沌映射来进行伪随机序列数的创建和生成，并通过两次创建过程来得到图像扩散和置乱的随机序列数。通过对加密方案在 .NET 平台下进行试验仿真，可以得到方案的加密效果是比较好的，同时也可以基本正确完成图像的解密处理。

2 双混沌数字图像加密算法设计

2.1 双混沌图像加密的体系结构

本文中采用双混沌系统进行图像的加密和解密处理，其优点在于能够将加密处理过程与图像的压缩过程相互独立，并且加密效果不会存在明显差异。本文提出的双混沌图像加密体系的整体功能结构如图 1 所示。

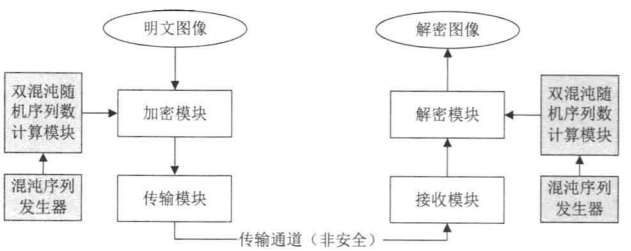


图 1 双混沌图像加密体系结构

Fig .1 Double chaotic image encryption system structure

在图 1 中所包含的两个混沌序列发生器是本加密系统的关键模块，负责系统的图像加密算法的实现，分别采用一个混沌映射来实现，所以称为双混沌数字图像加密系统，其他的模块则主要包括了加解密模块和传输模块。

2.2 随机序列产生模块

本文直接采用了最简单的 Logistic 映射，主要原因是因为如下几点：

1. Logistic 映射的形式比较简单，在具体实现过程中难度比较低。

2. 陈尔东（2004）对多种混沌映射的伪随机性进行了量化分析和研究，并采用美国 NIST 国家标准技术研究局的随机序列检验标准，对包涵 Logistic 映射在内的混沌序列进行了检验，Logistic 映射的通过率达到了 93.75%，在所选的混沌映射中属于最优。

按照 Timm 和 Sopniklus（2005）的研究，如果 Logistic 映射中的参数 μ 满足条件 $3.5669 < \mu \leqslant 4$，那么 Logistic 映射得到的混沌序列的随机性是非常高的，而当参数 μ 满足条件 $3.9 < \mu \leqslant 4$ 时，Logistic 映射满足遍历性特征，混沌序列的随机性更为明显，所以对于数字图像加密体系中的随机性要求是完全可以应对的。

在具体的随机序列产生模块中，本文设置了两个 Logistic 映射（L1 和 L2）来进行伪随机序列的迭代创建，其中的 L1 用于一级伪随机序列的创建，L2 进行二级伪随机序列的创建，按照初值的设置自动生成对应的随机数序列，用于数字图像的流加密处理，具体的功能结构如图 2 所示。

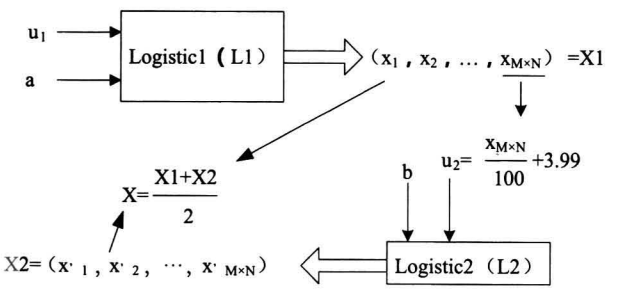


图 2 随机序列产生模块的功能结构

Fig . 2 Random sequence to produce the function of the module structure

按照图 2 中的双混沌图像加密体系中的随机序列产生模块的功能结构，其中的初值包括了一级 Logistic 混沌映射 L1 的 $u1^{u1}$ 和 a，以及二级 Logistic 混沌映射 L2 的 b，其中 L2 的 $u1^{u2}$ 采用 L1 计算得到的最后一个随机数 $XM\times N^{XM\times N}$ 乘以 1/100 再加上 3.99 来得到，即 L2 中的 u2 是通过 L1 的计算结果来确定的，其中的 M 和 N 分别表示数字图像的像素宽度和像素高度。

从图 2 可以看到，随机序列数的计算过程是首先通过 L1 来计算一个随机数序列 $X1=(x_1,x_2,...,x_{M\times N})$，随后将 X1 中的元素 XM×N 通过 XM×N/100+3.99 计算作为 L2 的参数，并随机选择一个位于区间（0，1）的浮点数，作为 L2 的计算初值，再次计算得到一个随机数序列

$X2=(x'_1,x'_2,...,x'_{M\times N})$，最后图像加密使用的随机数序列 X 通过式（5）来计算：

$$X=\frac{X1+X2}{2}=\left(\frac{x_1+x'_1}{2},\frac{x_2+x'_2}{2},...,\frac{x_{M\times N}+x'_{M\times N}}{2}\right) \quad (5)$$

在具体的计算过程中，约定 L1 的参数 u1 值为 3.99，可以确保 L1 完全进入混沌状态，而通过 XM×N/100+3.99 得到的 u2 同样满足条件 $3.9<\mu<4$，所以 L2 也完全进入混沌状态。通过双混沌技术，以线性计算的方式进行随机序列数确定，按照 Rowlands 的轨道跳跃理论，可以至少确保双混沌技术得到的随机数序列的随机性不低于单个 Logistic 混沌映射得到伪随机数序列的随机性，从而提高加密算法的安全性和可靠性。

另外，在伪随机序列数的选择过程中，为了避免 Logistic 映射初期得到的序列数随机性不强的问题，在双混沌模型中约束在 1000 次迭代之后才开始取值，即从第 1001 个迭代结果起，再连续迭代 M×N 次，最后使用得到的 M×N 个序列数作为数字图像加密密钥。

2.3　加密解密处理模块

本文的双混沌数字图像加密体系的图像加密过程包括了扩散处理和置乱处理两个过程，具体的操作以及用于加密的伪随机序列数的获取方法如下：

1. 数字图像扩散处理

基本流程如下：

（1）在图 2 中所示的伪随机序列数计算模型中提交初值 a 和 b，并设置 L1 的计算参数 u_1 为 3.99，按照图 2 中的计算流程得到用于扩散处理的伪随机序列数 X。

（2）将伪随机序列数 X 中的所有元素按 $(x_i\times 256)\bmod 256$ 进行计算，再将计算得到的结果转化为二进制，从而得到一个二进制的 M×N 长的序列数 X'。

（3）获取待加密数字图像 I 的像素灰度或者颜色分量序列，得到数字图像的灰度或者颜色分量序列向量 G，其中 $G=(g_1,g_2,...,g_{M\times N})$。

（4）对于 G 中的第一个元素 g_1 按照 $X'\oplus g_1$ 进行异或运算，对于 G 中的后续元素，按照式（6）进行处理[5]：

$$I'(k)=X'(k)\oplus\{[X'(k)+g_k]\bmod N\}\oplus I'(k-1) \quad (6)$$

其中的参数 $I'(k)$ 表示加密之后的密文，N 取 256，表示数字图像灰度空间或者颜色分量的空间取值范围，从而得到扩散处理之后的加密图像 I'。

（5）对第四步中扩散得到的像素序列进行逆序操作，将原来的第 M×N 个元素调整到第 1 个位置，将原来的第 M×N-1 个元素调整到第 2 个位置等，再按照式（6）进行二次扩散处理。

进行多次扩散，不仅能够利用 Logistic 混沌映射产生的伪随机序列数的随机性，还将数字图像中各像素与其前序像素之间的颜色进行了关联，在扩散过程中增加像素集合内部元素之间的关系，可以提高加密算法的复杂性和安全性。

2. 数字图像置乱处理

具体的流程如下：

（1）使用扩散处理的伪随机序列数 X 作为最终的置乱伪随机序列数集合，同时设置一个空的 M×N 大小的向量 Y，按照 X 元素的均匀化处理结果，将 X 对应元素扩充到 [0，M×N] 的整数域空间中，并将结果写入到向量 Y 中。

（2）利用上一步中得到的向量 Y 和扩散处理之后的加密图像 I'，对 I' 进行像素点的置乱处理，即将 I' 中的第 i 个像素的灰度值和第 y_I 个像素的灰度值进行交换。

（3）对置乱得到的结果再次按照扩散过程中的第四步和第五步进行一轮正序扩散和逆序扩散，从而得到最终的加密图像 I''。

按照上述扩散和置乱处理流程，双混沌数字图像加密体系采用了先扩散后置乱的方式来进行图像加密，图像解密的过程采用先置乱再扩散的方式进行，所做的运算为上述处理流程逆运算，在扩散逆处理时采用式（7）来进行处理：

$$g_k=\{X'(k)\oplus I'(k)\oplus I'(k-1)-X'(k)\}\bmod N \quad (7)$$

上式中所有参数和式（6）中相同，从而能够利用两次异或结果相同的特性，以及 Logistic 混沌映射在相同初值下能够得到相同伪随机序列数的

特性来对图像进行解密处理。

2.4 置乱随机序列数优化

按照双混沌图像加密框架中的加密解密处理模块的设计，在对像素图像进行置乱处理过程中是通过对置乱随机序列数进行排序后，对数字图像的像素点进行位置调整来实现的。目前常见的集中排序算法的时间复杂度通常为 $O(n^2)$ 或者 $O(n\log_2 n)$，在本文研究中采用了其中最简单的选择排序算法，该算法的时间复杂度为 $O(n^2)$。

在像素置乱处理过程中需要进行排序的主要原因是因为 Logistic 混沌映射的概率密度分布函数是非均匀的，即无法将序列数 $(x_1,x_2\cdots x_n)$ 等概率地映射到区间 (1,2⋯n) 上，所以也就无法简单地通过对 Logistic 混沌映射产生的伪随机序列数进行时间复杂度为 $O(n)$ 的映射处理后，得到置乱序列数 $(y_1, y_2\cdots y_n)$，其中 $yi(1 \leqslant i \leqslant n)$ 满足条件 $y_i, y_j \in (1,2,...,n), i \neq j$。为了提高双混沌数字图像加密方案在图像像素置乱处理过程中的效率，需要将直接通过 Logistic 混沌映射得到的置乱序列数进行均匀化处理，使得得到的序列数满足上述条件。在具体的优化处理过程中，本文参照了文献 [6] 中提出的 Logistic 混沌映射均匀化处理方案：

假定存在两个随机变量 X 和 Y，对应的概率密度函数为 $f(x)$ 和 $g(y)$，并且分别在区间 (i,j) 以及 (k,l) 上可积，那么如果满足式（8）：

$$\int_i^x f(t)dt = \int_k^y g(t)dt \tag{8}$$

则按照概率密度函数的基本含义，可以得到在区间 (i,j) 上的任何一个 X，在 (k,l) 中都存在唯一的一个元素 y，使得概率 $p(x)$ 和 $p(y)$ 相等，从而得到一个值域为 (c, d)，定义域为 (i,j) 的单调函数：

$$y=f(x) \tag{9}$$

如果随机变量 y 在区间 $(0, 1)$ 上满足均匀分布条件，那么可以得到式（10）：

$$y = \int_i^x f(t)dt \tag{10}$$

假定 $f(x)$ 对应的随机变量 x 的分布映射为 $y=F(x)$，那么即可得到，从而能够实现将随机变量转换为在 $(0, 1)$ 区间上服从均匀分布的随机变量 $x=F^{-1}(y)$。Logistic 映射产生的伪随机序列的概率分布函数为：

$$\rho(x) = \begin{cases} \dfrac{1}{\pi\sqrt{1-x^2}}, & x \in (0,1) \\ 0, & x \notin (0,1) \end{cases} \tag{11}$$

该伪随机序列相当于前文的随机变量 x，那么按照式（8）可以得到：

$$y = \int_0^x \frac{1}{\sqrt{\pi(1-t^2)}}dt = \frac{2}{\pi}\arcsin(x^2) \tag{12}$$

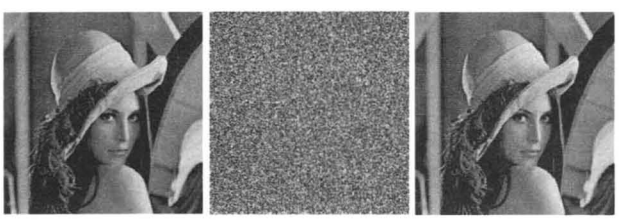
由于随机变量在区间 $(0, 1)$ 上满足均匀分布条件，因此通过式（9）可以将 Logistic 混沌映射生成的伪随机序列数转化为区间 $(0, 1)$ 上满足均匀分布条件的序列数向量。在随后的像素置乱处理过程中，按照 $\frac{2}{\pi}\arcsin(x^2)$ 对原来得到的置乱伪随机数 $(y_1, y_2, ..., y_{N\times M})$ 序列进行均匀化处理，得到随机序列数，再按照下式进行放大处理：

$$Y_i = \text{int}(N \times M \times y_i) + 1 \tag{13}$$

即可得到一个向量 $(y_1, y_2, ..., y_{N\times M})$，其中的元素满足条件 $Y_i \in (1,2,...,N\times M) \cap Y_i \neq Y_j, i \neq j$，从而能够直接用于对数字图像像素点的置乱处理，而不需要对原始的伪随机序列数进行排序处理，上述处理过程的时间复杂度为 $O(n)$，远小于选择排序算法的时间复杂度为 $O(n^2)$，从而可以将本方案的图像加密和解密过程的处理效率提高大约 1/3 左右。

3 实验仿真与性能分析

在仿真试验中使用 256×256 的 Lena 彩色图像和其它经典测试图像，在 .NET 平台下采用 C# 编程技术对方案进行具体实现。选取扩散及置乱参数 u_1 值为 3.99，a、b 值分别为 0.554 和 0.35，进行加密和解密处理，得到的加密图像和解密后的图像分别见图 3（b）和图 3（c）。



（a）原始 Lena 图像　（b）加密 Lena 图像　（c）解密 Lena 图像

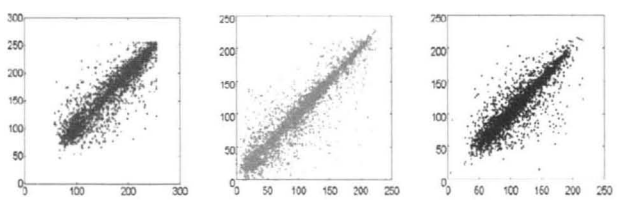
图 3 数字图像加密、解密直观效果

Fig . 3 Digital image encryption and decryption visual effect

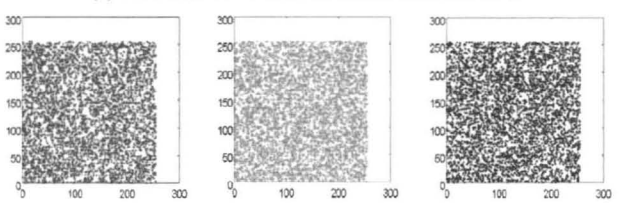
从图 3 中可以看到，本方案在试验仿真中得到的加密图像和原始图像之间凭借人眼观察，完全不存在任何联系，同时解密后的数字图像虽然出现了极少的噪点，但是和原始图像之间的差距并不是特别大，造成解密结果部分噪声存在的主要原因是本方案的试验仿真环境在序列数的计算过程中会出现失真问题。

3.1 像素关联性分析

图 4 分别给出了 Lena 明文图像和密文图像所对应的像素值分布直方图，由图 5(a) 可见，原始图像的像素值分布是不均匀的；但图 4(b) 表明，密文图像的像素值却呈现出平坦而均匀的分布特性，即加密图像的像素值在 [0,255] 范围内出现的概率几乎均等。因此，本文算法将能够有效地抵抗统计攻击。



(a) 明文图像红色、绿色和蓝色分量关联性分布



(b) 加密图像红色、绿色和蓝色分量关联性分布

图 4 数字图像 Lena 加密前后颜色关联性

Fig .4 Color correlation before and after Lena digital image encryption

3.2 信息熵分析

信息熵是反映信息的随机性的重要度量指标。设 s 代表一种信息源，则 s 的信息熵 H(s) 可以用式（17）进行计算：

$$H(s)=\sum_{i=0}^{2^N-1} p(s_i)\log_2 p(s_i) \qquad (17)$$

其中的 *(Si)* 表示一个信息序列或者信息集合、信息源等，N 表示信息序列中各元素的比特长度，*p(Si)* 表示其中第个信息出现的概率值。式（17）中的含义是指一个能发出 $2N$ 个符号的真随机信源，其像素值有 $2N$ 种可能值，其信息熵就是 N，对于目前常见的 256 级的灰度图像而言，将式 (17) 所示的信息熵扩充到 [0,8] 区间中，他的理想信息熵为 8。

通过对图 4 中的本系统加密图像按照式 (17) 进行信息熵计算，得到该图像在红色、绿色和蓝色分量上的矩阵中的信息熵分别为 7.9766、7.9869 以及 7.9871，基本上接近了最大的信息熵，这表明本方案的加密处理过程能够实现加密图像中像素颜色的随机性分布，安全性是比价高的。

3.3 密钥空间分析

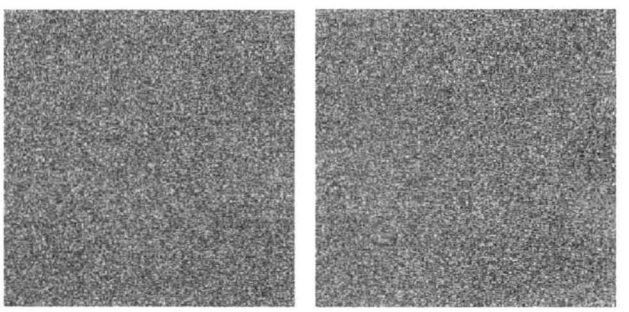
从理论层面来看，本方案的密钥空间是无穷的。但是考虑到实际应用过程中计算机计算性能和精度的限制，在实际取值时会受到精度限制，以本方案试验仿真环境中的计算机为例，实数的计算精度只能够达到的 10^{-15} 水平，本方案的密钥采用了扩散和置乱过程中的 (u^1、a、b) 的密钥，密钥空间可以达到 10^{90} 的范围，其密钥空间是足够抵抗一般的穷举性攻击的。

3.4 密钥敏感性分析

由于混沌映射的初值敏感性，所以本文的方案从理论层面来说是具有很好的密钥敏感性的。在实际仿真中采用的加密密钥为扩散及置乱过程（3.99，0.554，0.35）。

解密过程中需要解密者正确提供 L1 和 L2 在两次迭代计算过程中的初值 a、b，如果将扩散过程中的 a 的值变为 0.5540000001，u^1、b 以及置乱过程参数保持不变，则对图 3 中 Lena 的解密结果如图 6（a）所示，如果将置乱过程参数以及扩散过程中的 u^1、a 保持不变，b 的值改为 0.3499999999，那么对图 3 中的 Lena 解密结果见图 6（b）。

从仿真结果来看，虽然只对密钥中的初值进行了 0.0000000001 的改动，而得到的解密结果却相差非常大，完全无法得到和原始图像有关的任何信息，这说明本方案的密钥敏感性是非常强的，也验证了本方案的加密安全性。



(a) 更改 a=0.5540000001　　(b) 更改 b=0.3499999999

图 5　更改扩散及置乱初值的解密结果

Fig .5　Change the decrypt the results of the initial value of diffusion and scrambling

3.5 密文和明文敏感性分析

本算法在图像像素的扩散处理过程中不仅利用了 Logistic 混沌映射得到的序列数的随机性，同时还在处理过程中利用前序像素进行了分组加密处理，在传统的混沌加密算法基础上增加了图像像素之间的关联性构建，因此算法对于密文和明文的敏感性是比较强的，即对密文进行很小的修改，在密钥完全正确的情况下，得到的解密明文都会出现雪崩效益。

同样以图 3 中所示的 256×256 Lena 明文图像为例，加密解密的密钥为 (3.99，0.554，0.35)，对密文进行不同数量像素颜色值的改变得到如下结果：

表 1 密文敏感性检验结果

Table 1 Cipher sensitivity test results

像素改变个数	解密结果像素改变率 /%
1	49.749
10	49.685
50	49.905
100	49.662
200	49.823
400	49.651
500	49.816
1000	49.907

从表 1 中可以看到，在改变了密文中的像素颜色值之后，解密之后的明文中都会有将近 50% 的像素发生变化，出现雪崩效应，同时解密结果中的像素改变率和密文中的像素改变个数没有关系，密文敏感性是非常高的，这说明在本算法中增加的基于前序像素的分组扩散处理之后，和传统的混沌图像加密方法相比，算法出现了密文敏感性，改变密文中少量加密结果后，会出现雪崩效应。

采用同样的方法对明文敏感性进行验证，加密密钥、图像的选择和表 1 相同，考察改变明文像素后得到的加密密文的像素改变率，得到的结果见表 2。

表 2 明文敏感性检验结果

Table 2 Expressly sensitivity test results

像素改变个数	解密结果像素改变率 /%
1	49.749
10	49.685
50	49.905
100	49.662
200	49.823
400	49.651
500	49.816
1000	49.907

从表 2 可以看到，本文提出的数字图像加密方案对于明文的敏感性也是非常高的，在对明文像素进行改变之后，加密的密文会出现雪崩效用。

4 结 论

本文数字图像加密技术进行了研究与分析，并且利用目前在加密领域中比较受关注的混沌加密技术设计和实现了一种基于双混沌随机序列数的数字图像加密方案，在具体工作中通过设置两个具有关联性的 Logistic 混沌映射进行伪随机序列数的创建，并将其应用到图像的扩散和置乱处理中，在扩散处理过程中是通过伪随机序列数和原始图像像素颜色进行异或计算，在置乱操作中则是按照混沌序列数的均匀化结果，直接对图像的像素位置进行更换，免去对序列进行排序的复杂操作。本文在对双混沌数字图像加密方案进行设计和仿真实现的基础上，还针对方案的密钥空间范围、密钥的敏感性、加密前后图像的像素关联性以及像素集合的信息熵进行了探讨和量化分析，论证了本文提出的双混沌数字图像加密方案的安全性和可靠性。因此，本文提出的双 Logistic 混沌映射的数字图像加密算法可以用于矿产资源环境下的保密图像在因特网节点间、云计算核心与节点间的保密通信，以及图像信息保密存储等应用场合。

参考文献：

[1] 程海 . 基于 FPGA 的图像加密关键技术研究 [D]. 黑龙江大学 , 2015.

[2] 范于洪 . 基于分块机制的数字图像快速加密算法及安全性 [J]. 计算机科学 . 2013 (11) : 27-31.

[3]Yong Wang,et al.A chaos-based image encryption algorithm with variable control parameters[J]. Chaos Solitons Fractals. 2009(11) :19-22.

[4] 李璞 . NIST 随机数测试 [N]. 太原理工大学光电工程研究所 . 2011.

[5]Guanrong Chen,Yaobin Mao,Charles K. Chui. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons and Fractals. 2004 (3): 33-36.

[6]Zhi-Hong Guan,Fangjun Huang,Wenjie Guan. Chaos-based image encryption algorithm[J]. Physics Letters A. 2005 (1): 5-9.

[7]Linhua Zhang,Xiaofeng Liao,Xuebing Wang. An image encryption approach based on chaotic maps[J]. Chaos, Solitons and Fractals. 2004 (3): 23-27.

(下转 113)

Effect of Bag Dust and Bentonite on Blast Furnace Top Gas Dechlorinating Agent

Hu Xuewu, Hu Binsheng, Gui Yongliang, Hu Guiyuan
(College of Metallurgy & Energy, North China University of Science and Technology, Tangshan, Hebei, China)

Abstract: Bag ash and bentonite were added for preparing for blast furnace top gas dechlorinating agent in the preparation process of dechlorinating agent. The effects of bag dust content, bentonite content, calcination temperature of blast furnace on the top gas dechlorinating agent was investigated, and the preparation process was obtained. Research shows that the bag dust lime can overcome the single component removal of chlorine disadvantages of low capacity, weaken the adverse impact on the performance of the CO2 removal of chlorine gas in blast furnace gas, dispersion of the appropriate proportion of bentonite can not only improve the active ingredients, chemical dechlorinating agent, but also keep high mechanical strength, the suitable calcination temperature can improve the dechlorinating agent activity, and the pore structure of dechlorinating agent. Blast furnace top gas dechlorinating agent is suitable for the preparation of content: sack dust is about 8%, the content of binder is about 6%, the raw materials are mixed evenly, appropriate amount of distilled water is added for mixing, small cylindrical is extruded, and is dried at 400 ℃ to roast. The test preparation of blast furnace top gas dechlorinating agent in the reaction of 19.25 h after penetrating chlorine capacity reached 17.33%, mechanical strength reached 60.5 N/cm^3, and it has opened up a new field for the comprehensive utilization of the bag ash.

Keywords: Bag dust; Bentonite; Dechlorinating agent; Blast furnace top gas

（上接156页）

Research on digital image encryption algorithm based on double Logistic chaotic map

Li Fan[1,3], Lin Caishou[2],Wang Xiaomin[3]
(1. School of electrical and information engineering, Chengdu Textile College ,Chengdu, Sichuan,China;
2. Institute of Multipurpose Utilization of Mineral Resources, Chengdu, Sichuan,China;3.School of Information Science And Technology, Southwest Jiaotong University, Chengdu, Sichuan, China)

Abstract: A digital image encryption scheme based on double Logistic chaotic map was proposed in this thesis. The two-level Logistic chaotic map was used to create the pseudo-random sequence number in the scheme, and the number of random sequences of image diffusion and scrambling was obtained by two creation processes. The key used in the scheme is the calculation parameters of the first-order Logistic chaotic map and the initial value of the second-order Logistic chaotic map. And in the encryption and decryption process, and the encryption process includes the two steps of proliferation and scrambling. Through the encryption scheme in the. NET platform for experimental simulation, the program encryption effect is good, and it also can complete the correct completion of the image decryption processing. At last, the security and reliability of the scheme were analyzed and studied in detail in this thesis, including the key space size of the scheme, the sensitivity of the scheme to the key, the pixel correlation of the encrypted image and the information entropy, etc. Results suggest that the proposed image encryption scheme is secure and efficient, with high potential to be adopted for the secure image communication applications.

Keywords: Digital Image; Chaotic System; Chaotic Encryption; Logistic Chaotic Map