基于三维空间的图像加密算法①

农盛功 周满元 (桂林电子科技大学 计算机与控制学院 广西 桂林 541004)

摘 要: 为了实现图像安全，快速加密，利用了图像像素可以插入到相邻像素之间以及拉伸折叠的思想设计了一种基于三维坐标的图像加密算法。算法首先将二维十进制矩阵转化为三维二进制矩阵，再根据图像像素可以插入到相邻像素之间，即左映射或者右映射，和拉伸方法，把三维矩阵转化为二维二进制矩阵。然后用置乱算法把二维二进制矩阵进行置乱，接着根据折叠方法把二维二进制矩阵转化为三维二进制矩阵，最后再把三维二进制矩阵转化为二维十进制矩阵以达到加密的效果。实验表明，该算法是一个安全有效的加密算法，加密本身还可以改变图像的像素值。

关键词: 混沌；映射；置乱；加密；折叠

Image Encryption Based on Three-Dimensional Space

NONG Sheng-Gong, ZHOU Man-Yuan

(College of Computer Science and Control, Guilin University of Electronic Technology, Guilin 541004, China)

Abstract: To make the image secure and encryption faster, this paper proposes a simple three-dimensional chaotic mapping based on the idea that the image's pixels can insert the adjoining pixels and the thought of stretching and folding the image. First of all, the algorithm changes the two-dimensional decimal matrix into a three-dimensional binary matrix. Second, based on the thought that the image's pixels can insert the adjoining pixels, that is left mapping or right mapping, and the thought of stretching and folding the image, it changes the three-dimensional binary matrix into two-dimensional binary matrix. Third, the compound chaotic algorithm is used to scramble the decimal matrix, and the folding algorithm is used to change the two-dimensional binary matrix into three-dimensional binary matrix. At last, it changes the three-dimensional binary matrix into a two-dimensional decimal matrix, and the decimal matrix is the encryption image. Experiments show that the image encryption is rapid and highly secure, and it can change the value of pixels element.

Keywords: chaotic; mapping; compound; encryption; fold

随着数字技术，因特网和多媒体技术的飞速发展，图像、视频等多媒体在网络上传输越来越密集。其安全性也受到了普遍的关注，成为了热点问题，因此其加密技术得到了飞速发展，由于其数据本身具有高冗余性、数据量大，相邻像素相关性强等特点。对其加密有着特殊的要求。传统的加密算法 DES、IDEA、RSA 等技术已经成熟，并且在很多方面已经成功应用[1]。传统的加密算法是针对文本文件的特点来设计，在对图像加密时，由于图像自身具有的区别于文本文件的特点，加密往往达不到所求的效果。

由于混沌系统本身具有伪随机性，对系统参数和初始值的敏感性，奇异吸引子，难以分析性的特性，所以混沌系统可以提供大量的具有良好随机性，非相关性和复杂性的伪随机序列，非常适合用于图像加密。混沌加密主要分为把图像像素置乱以达到加密效果的置乱加密技术[2]和改变图像像素值来达到加密效果的置换加密技术[3]。

1 把二维十进制矩阵转化为三维二进制矩阵

对二维图像的处理一般是把数字图像读成 N×M

① 收稿时间:2009-11-24;收到修改稿时间:2009-12-26

分别为原二维矩阵的长和宽，K 为十进制数转化为二进制数后的二进制位数。如下图 1 所示：

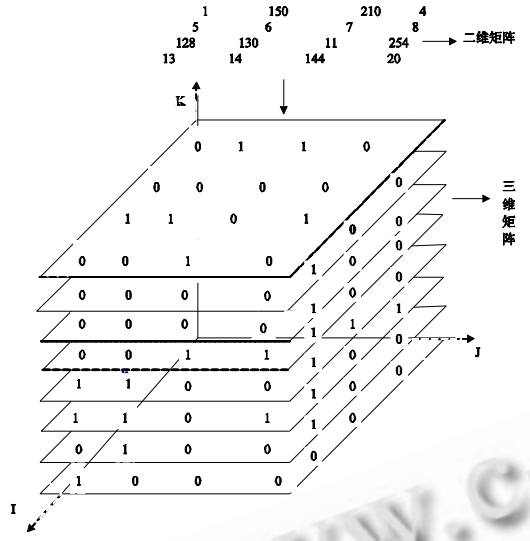

图 1　8×4×4 的三维矩阵

2　映射思想

设三维矩阵在在 IJ 坐标的投影上一个 N×N 二维矩阵(当投影不是 N×N 的方阵时，可以用插补法把它补成投影时是方阵)，新映射方法就是根据图像像素能够插入到其他相邻的像素之间的性质。根据方向的不同，映射分为左映射跟右映射。首先把三维矩阵沿平行于 K 轴，沿着 IJ 平面的对角先把三维矩阵切开，分成左右两部分。左映射就是在 IJ 平面上，把左半边矩阵从左到右第一行的所有元素依次插入右半边矩阵从上到下的第一行两个元素之间，并且保持 K 轴坐标不变。然后再把左半边矩阵从左到右第二行的所有元素依次插入右半边矩阵从上到下的第二行矩阵中，并且保持 K 轴坐标不变…重复以上过程，直到取完左半边的数据，如图 2 所示。第 2 步就是把在 IJ 平面上第二，三，…N 行的对应的平行于 K 轴平面依次添加到第一行的平行于 K 轴的平面后面，这样三维矩阵就转化成为了一个的二维矩阵，如图 3 所示。最后对二维矩阵进行置乱，然后把矩阵还原为原来的 8×N×N 矩阵。其中除了最后一步对二维矩阵进行置乱之外，前两步中，数据保持 K 轴不变。右映射与左映射相似，而且是相对称的。就是首先把右半边 IJ 平面上第一行的元素分别插入到左半边第一列的两个元素之间，然后是第二行…，第三行…。第 2 步就是把平行于 K 轴的，第 2，3，…列所在的平面的二维矩阵沿 K 轴依次添加到第一行所在的平面的矩阵后面。最后就是对生成的二维矩阵进行置乱，并且把矩阵还原为原来的 8×N×N 矩阵。

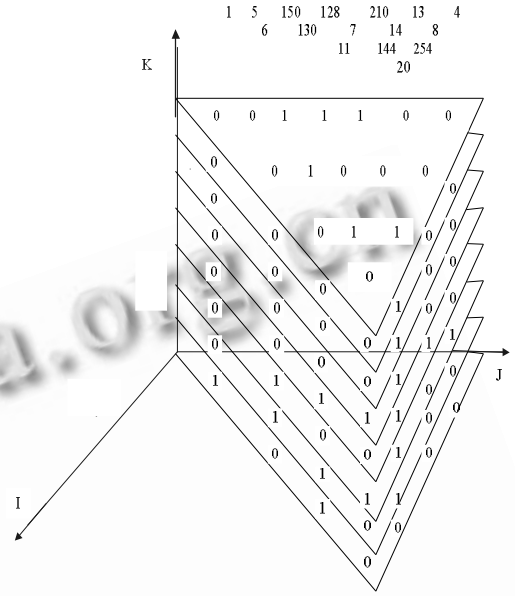

图 2　左映射第一步插入后的图像

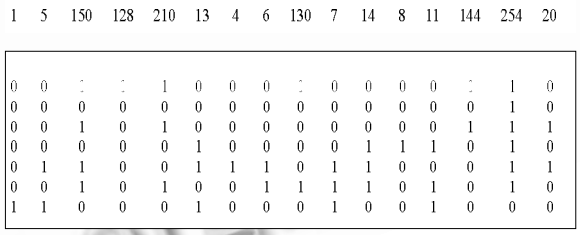

图 3　8×16 的二维矩阵

2.1 映射的计算算法

设图像读成 8×N×N 的三维矩阵 A(k,i,j)，i,j=0,1,…,N−1，k =0,1,…,7，P(k,m)，m=0,1,…,N^2-1，k =0,1,…,7;为将 A(k,i,j)拉伸为一个平面后的二维矩阵。(下文的 k,i,j,m 取值范围同上)

左映射计算算法如下：

当 i>j 时，有

$$P(k,(2N-j)\times j+2(i-j)-1)=A(k,i,j) \quad (1)$$

当 i<=j 时，有

$$P(k,(2N-i)\times i+2(j-i))=A(k,i,j) \quad (2)$$

右映射计算算法为：

当 i>j 时，有

$$P(k,(2N-j)\times j+2(i-j)-1)=A(k,i,N-1-j) \quad (3)$$

当 i<=j 时，有

P(k,(2N-i)×i+2(j-i))=A(k,i,N-1-j)　　(4)

把二维矩阵 P(k，m)折叠成为三维矩阵 B(k,i,j)的折叠算法为：

B(k,i,j)= p(k,i×N+j)　　(5)

3　图像加密和解密

将左映射和右映射的映射次数设计为密钥 Key，其中当取 Key 的值是第奇数位时，映射为左映射，且映射次数为 Key 的位数数字的值，同理，当取 Key 的值是第偶数位时，映射为右映射，且映射次数为 Key 的位数数字的值。例如 Key=2345 表示先左映射 2 次，然后右映射 3 次，再左映射 4 次，最后右映射 5 次。

3.1 图像加密过程如下：

①把二维图像读成三维二进制矩阵，设置好密钥 Key；

②取出 Key 的一位数字，并根据数字位置跟数字和式(1) ~ (4)将图像三维 A(k,i,j)转化成二维图像 p(k,m)；

③用图像置乱算法将二维图像 p(k,m)置乱；

④根据折叠法(式(5)把二维矩阵 p(k,m)折叠成为三维矩阵 A(k,i,j)，继续取出 Key 的一位数，重复①，③步直到取完 Key 的位数；

⑤把最后生成的三维二进制矩阵读成二维十进制矩阵；

3.2 解密过程如下：

①从末位读起读取 Key 的一位数字，并且把二维矩阵图像读成三维 A(k,i,j)；

②把三维矩阵 A(k,i,j)拉着一个二维矩阵 p(k,m)：

p(k,i×N+j) = A(k,i,j)　　(6)

③根据图像置乱算法的解密算法把 p(k,m)解密，并且根据读取的是 Key 的第几位数值和数值的大小，来判断加密是左映射还是右映射和解密次数。如果加密时是左映射，则解密方法如下：

当 i>j 时，有

A(k,i,j) = p(k,(2N-j) ×j+2(i-j)-1)　　(7)

当 i<=j 时，有

A(k,i,j) = p(k,(2N-i)×j+2(j-i))　　(8)

如果加密时是右映射，则解密方法如下：

当 i>j 时，有

A(k,i,N-1-j) = p(k,(2N-j)×j+2(i-j)-1)　　(9)

当 i<=j 时，有

A(k,i,N-1-j) = p(k,(2N-i)×i+2(j-i))　　(10)

④继续读取 Key 的数值，重复(2)，(3)步，知道读取完 Key 的位数。

⑤把最后生成的三维二进制矩阵转化为二维十进制矩阵，则其对应的图像为所求的解密图像。

4　图像加密和解密

4.1 图像加密

本文在加密过程中的第 3 步对二维图像 p(k,m)是基于改进的 Logistic 映射（其动力学方程为：$x_{n+1}=(\beta+1)(1+\frac{1}{\beta})^{\beta}x_n(1-x_n)^{\beta}$，式中：$\beta$ 为[1,4]之间的实数，$x_0\in(0,1)$ ）。

对 L = 256 的 Lena 灰度图进行加密。当 Key_1 =1，Key_2 =01，Key_3=123456778 和 Logistic 映射中 x_0 =0.556465656，β =3.943534534534 时，加密效果如下图所示。

图4　原图像

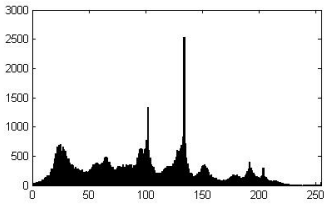

图5　原图像的直方图

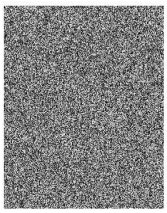

图6 Key1=1的密图

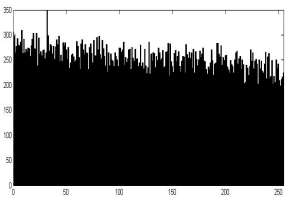

图7 Key1=1的密图的直方图

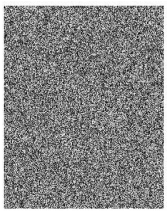

图8 Key2=01的密图

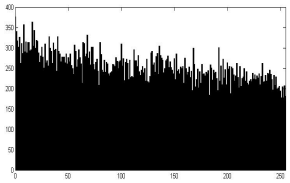

图9 Key2=01的密图的直方图

由图 5，图 7，图 9,图 11 可以看出，利用本文提出的加密算法加密的密图的直方图与原图的直方图

是不同的，这说明这种加密算法不仅改变了像素的位置还达到了改变图像像素的效果，隐藏了直方图信息，可以有效的抵御已知(选择) 明文攻击，提高了加密算法的安全性。

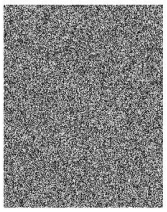

图10 Key_3=123456778 密图

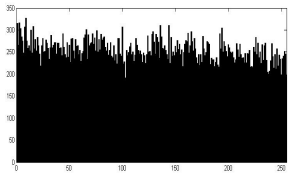

图11 Key_3=123456778 密图的直方图

4.2 安全性能分析

本算法中涉及了左右映射跟改进的 Logistic 映射，其中左右映射的密钥空间只与密钥长度大小有关他们之间的关系如下表 1：

表 1　密钥长度(位)和密钥空间

长度	64	128	256	512
空间	1.84×10^{19}	3.4×10^{38}	1.16×10^{77}	1.34×10^{154}

密钥敏感性分析。对用 Key = 123456778 对图像进行加密，然后分别用 Key_1= 123456777，Key_2= 123456779 和正确的 Logistic 映射密钥进行解密，如图 12，13 所示。即使加密密钥和解密密钥仅有非常小的差异，也无法解密图像，加密算法对密钥变化非常敏感。

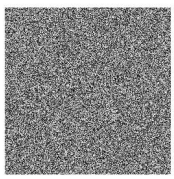

图12 Key_1=123456777 解密图

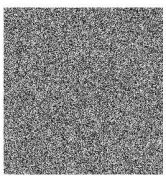

图13 Key_2=123456779的解密图

统计分析：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，对图像中像素点相邻点进行相邻点分析[4,5]。文献[6]介绍了相关系数的计算方法。

经过文献[6]介绍的相关系数的计算方法计算,相邻点的相关系数如表2。显然，加密后，密图像素值与相邻点像素值之间的相关系数非常小，解密算法很难利用统计方法从密图中恢复原图。

表 2　加密前后，像素点(x, y)与其相邻点的相关系数

	原图	密图
水平方向	0.9423	0.0034
垂直方向	0.9618	0.0029
对角线方向	0.9561	0.0051

最后计算分析原图和密图的不动点比。原图像 A 的像素点 A(i,j)，在加密后其图像灰度值没有发生变化，则称该像素点为不动点。图像中不动点占有像素的百分比称为该图像的不动点比。在 Key=1 时，即图 6 跟图 4 的不动点比为 0.404%；Key=01，即图 8 跟图 4 的不动点比为 0.407%。这说明只在一次左映射或者右映射的情况下，不动点的数目很少，99.5% 以上的像素点都发生了改变，置乱效果很明显。

最后计算分析原图和密图的不动点比。原图像 A 的像素点 A(i,j)，在加密后其图像灰度值没有发生变化，则称该像素点为不动点。图像中不动点占有像素的百分比称为该图像的不动点比。在 Key=1 时，即图 6 跟图 4 的不动点比为 0.404%；Key=01，即图 8 跟图 4 的不动点比为 0.407%。这说明只在一次左映射或者右映射的情况下，不动点的数目很少，99.5% 以上的像素点都发生了改变，置乱效果很明显。

5　新映射与其他混沌映射比较

Baker map 是最典型、应用最广的混沌映射之一，在图像加密领域得到广泛的应用。新映射和 Baker map 比较:

①密钥空间更大。文献[4]介绍了 Baker map 的两种形式,但即使是 Baker map 的一般形式(即密钥不是图像大小的因数的情况),Baker map 的密钥空间最大仅为 2N-1(N 为图像的宽),而新映射的密钥空间只和密钥本身长度和改进的 Logistic 映射有关。只要计算速度允许,密钥长度没有限制。

②对密钥变化更加敏感。新映射只要密钥稍有变化,密图就会截然不同。因此,用相似但不相同的密钥无法对密图解密。而使用相似的密钥也可以对 Baker map 加密密图进行解密。

③改变图像的像素值，由图 5，图 7，图 9，图 11 可知，本算法可以改变原图像的直方图，即本算法可以改变图像的像素值，这样可以有效的隐藏直方图信息，从而抵御已知(选择)明文攻击，提高加密算法的安全性。

6 结语

本文提出了一种基于三维空间下的图像加密算法，算法具有如下优点：

①公式非常简单,容易编程实现。

②映射是可逆的。

③在加密/解密过程中没有信息损失。

④加密的密钥基本没有限制。

⑤密图和原图大小一致,没有大小差异。

⑥能满足实时需要,适合大尺寸图像加密。

⑦经过映射后，可以改变原图像的直方图。

⑧加密算法简单,容易硬件实现。

参考文献

1 Ruces. Appied cryptography-protocols,algorithms,and source code in C. second edition ,New York. John Wiley & Sons, Inc, 1996

2 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.

3 陶栋,李之棠.混沌加密图像算法.计算机工程与科学,2003,25(4):7－9.

4 Mao Y, Chen G, Lian S. A novel fast image encryption scheme based on 3D chaotic Baker maps. Int Bifurc Chaos,2004,14(10):3612－3624.

5 Chen GR, Mao YB, Chui CK. A symmetric image encryption scheme Based on 3D chaotic Cat maps. Chaos, Solitons&Fractals, 2004,21(3):749－761.

6 刘家胜.基于混沌的图像加密技术研究[博士学位论文].合肥:安徽大学,2007.55－56.