文章编号 1004-924X(2008)09-1738-08

三维可逆混沌映射图像加密及其优化算法

李 娟,冯 勇,杨旭强,黄 峰
(哈尔滨工业大学 电气工程及自动化学院,黑龙江 哈尔滨 150001)

摘要:利用混沌拉伸和折叠的原理,提出了一种三维可逆混沌映射图像加密方法及其优化算法。该方法用一个三维数据矩阵描述灰度图像,用提出的算法将该三维数据矩阵映射为二维数据矩阵。然后,应用拉伸和折叠算法对此二维数据矩阵实现图像像素的置乱处理。最后将置乱后的二维数据矩阵还原为三维数据矩阵,得到加密图像。该加密方法是可逆的,亦可用于图像解密。推导了加密和解密算法完整的数学表达式。由于图像数据量大,利用推导的数学表达式实现图像加密和解密时计算量较大,加密时间长,因此,提出了一种优化算法。仿真结果表明,该加密方法同时实现了像素置乱和像素混淆,其优化算法将加密速度提高了 3～4 倍。该加密算法抵御统计攻击的能力较强,密钥敏感度高,加密速度快,安全性高。

关 键 词:图像加密;三维可逆映射;混沌;优化算法
中图分类号:TP309.7 **文献标识码**:A

Invertible chaotic 3D map based image encryption and its optimized algorithm

LI Juan, FENG Yong, YANG Xu-qiang, HUANG Feng

(*Department of Electrical Engineering, Harbin Institute of Technology, Harbin* 150001, *China*)

Abstract: In order to ensure the security of transmitted digital image effectively, an invertible chaotic 3D map based image encryption approach and its optimized algorithm are proposed based on the stretching and folding mechanisms of chaos. A gray-level image is depicted as a 3D matrix and mapped to a 2D image matrix according to proposed algorithm. Then, stretching and folding maps are used to permute the pixel positions of the 2D matrix. The stretching process is to transform the 2D image matrix to an array, and the folding process is to fold the array to another 2D image matrix with the same size as the original 2D matrix. Finally, the permuted 2D matrix is mapped back to a 3D matrix to obtain a cipher image. This proposed approach is invertible, it could be used for image encryption and decryption. The encryption and decryption algorithms are formulated, by which image encryption and decryption will do a large of calculation and consume a lot time for the image has large data quantity. In order to solve this problem, an optimized algorithm is proposed. Simulation results indicate that proposed optimized algorithm can increase image encryption speed, which is 3～4 times faster than that of the deduced formulas, proposed image encryption approach also can realize pixel permutation and sub-

收稿日期:2008-01-23;**修订日期**:2008-03-13.
基金项目:国家自然科学基金资助项目(No. 60474016;No. 60774040)

stitution at the same time via one iteration map for the histogram information of the plain image, and can enhance the capability of resisting statistic attack.

Key words: image encryption; invertible 3D map; chaos; optimized algorithm

1　引　言

随着计算机网络技术、信息存储技术的迅速发展，越来越多的数字图像在网络上传输。有些图像信息可能涉及到个人隐私、商业机密和军事机密等，如何保证这些图像的安全性是当前国内外学者研究的主要方向之一。目前主要有两种保护图像信息的技术：数字水印技术和图像加密技术。数字水印技术是在图像中嵌入数字水印信息而不改变图像的可见性，主要用于票证防伪、保护版权等。数字图像加密技术是通过对数字图像的像素进行位置置乱和灰度变换，改变图像的可见性，使图像变为类似于信道随机噪声的信息，从而有效地保证传输中数字图像的安全性。

目前常用的图像加密技术有基于矩阵变换/像素置换的图像加密算法、基于密钥分割与秘密共享的图像加密算法、基于现代密码体制的图像加密算法和基于混沌理论的图像加密算法。

基于混沌理论的图像加密技术是近年来发展起来的。一个良好的密码系统应该满足如下要求：把明文变为尽可能随机的密文；对秘钥非常敏感等。而混沌系统具有良好的伪随机性、对初始状态的敏感性等，这些特性很好地满足了密码系统的要求，非常适合于加密技术[1-2]。针对图像信息数据量大、相邻像素间相关性强等特点，国内外学者提出了一系列混沌图像加密方法[3-8]。Fridrich 研究了 Baker 映射和 Cat 映射，并分析了两种映射的密钥空间和安全性[3]。Mazleena Sallehd 等提出了一种混沌图像加密方法，将原来针对正方形图像的 Baker map 扩展到可用于矩形图像，并采用密码绑定和像素混淆等技术增强了密图的安全性[9]。茅耀斌、陈关荣等人在 Fridrich 方法的基础上将二维 Baker map 扩展到了三维[4,6]。冯教授等利用混沌拉伸和折叠的原理提出了 line map 图像加密算法[10]，后来又利用图像分割的思想提出了一种混沌映射图像加密算法[11]。

本文提出了一种具有混沌性质的三维可逆映射图像加密方法及其优化算法。将灰度图像用一个三维矩阵来描述，按照本文提出的方式将其映射为二维图像矩阵后，利用拉伸和折叠算法对二维图像数据矩阵进行置乱处理，再将置乱后的图像还原为三维图像矩阵，实现图像加密。针对图像数据量大，加密时计算量大、加密时间长等问题，提出了一种优化算法，缩短了加密时间。

2　三维数据矩阵映射为二维数据矩阵的算法设计

提出的三维可逆混沌加密算法用一个三维数据矩阵描述灰度图像。对于本文所采用的灰度为 256、维数为 $N\times M$ 的图像，每个十进制像素值可以用 8 个二进制位表示，因此可用 $N\times M\times 8$ 的三维数据矩阵描述 $N\times M$ 的灰度图像。这里假设 $N\leqslant M$，如果 $N>M$，需对原图像矩阵进行一次转置变换。

假设由灰度图像得到的 4×4 二维数据矩阵为

$$\boldsymbol{A}=\begin{bmatrix}15 & 34 & 123 & 15\\ 178 & 143 & 57 & 45\\ 74 & 103 & 66 & 86\\ 0 & 23 & 234 & 1\end{bmatrix}. \tag{1}$$

每一个十进制像素值用 8 个二进制位表示，则原灰度图像可用一个 4×4×8 的三维图像矩阵描述，如图 1 所示。

对于得到的三维数据矩阵，再将其映射为二维数据矩阵，以公式(1)中的十进制二维图像数据矩阵 $\boldsymbol{A}$ 为例说明将三维数据矩阵 $\boldsymbol{C}$ 映射为二维数据矩阵 $\boldsymbol{E}$ 的过程。先将数据矩阵 $\boldsymbol{A}$ 映射为 4×4×8 的三维数据矩阵 $\boldsymbol{C}$。将组成三维矩阵 $\boldsymbol{C}$ 的 7 个平面依次展开的顺序为：$i=1$ 所在的维数为 8×4 的平面，$j=4$ 所在的维数为 8×3 的平面，$i=4$ 所在的维数为 8×3 的平面，$j=1$ 所在的维数为 8×2 的平面，$i=2$ 所在的维数为 8×2 的平面，$j=3$所在的维数为 8×1 的平面，$i=3$ 所在的维数为 8×1 的平面。将这 7 个平面按上述顺序排列

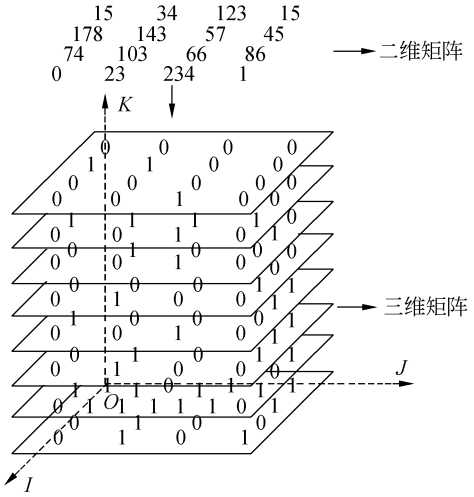


图 1　用三维数据矩阵描述 4×4 的灰度图像

Fig. 1　4×4 gray-level image depicted by a 3D matrix

可组成一个维数为 8×16 的平面，从而完成三维矩阵 $\boldsymbol{C}$ 二维矩阵 $\boldsymbol{E}$ 的映射，如图 2 所示。

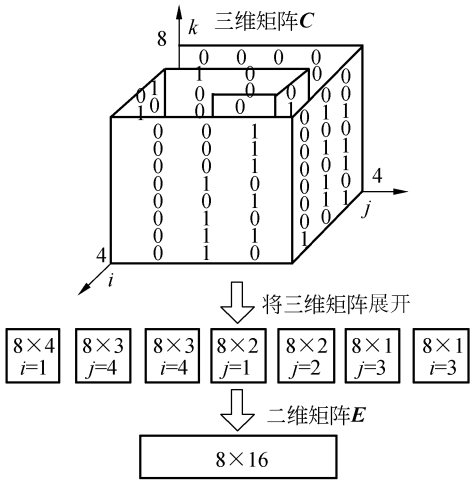


图 2　将三维矩阵映射为二维矩阵的过程

Fig. 2　Process of mapping 3D matrix to 2D matrix

三维矩阵 $\boldsymbol{C}$ 映射为二维矩阵 $\boldsymbol{E}$ 的算法如下：

$m=i-1$，

$$\boldsymbol{E}(k,2m(M+N-2m)+j-m)=\boldsymbol{C}(i,j,k)$$
$$i=1,2,\cdots,\mathrm{ceil}(N/2);$$
$$j=i,i+1,\cdots,M-i+1, \tag{2}$$

$m=M-j$，

$$\boldsymbol{E}(k,2m(M+N-2m)+M-3m+i-1)=\boldsymbol{C}(i,j,k)$$
$$j=M-\mathrm{ceil}(N/2)+1,M-\mathrm{ceil}(N/2)+2,\cdots,M;$$
$$i=M-j+2,M-j+3,\cdots,N-(M-j), \tag{3}$$

$m=N-i$，

$$\boldsymbol{E}(k,2m(M+N-2m)+2M+N-5m-j-1)=\boldsymbol{C}(i,j,k)$$
$$i=N-\mathrm{floor}(N/2)+1,N-\mathrm{floor}(N/2)+2,\cdots,N;$$
$$j=N-i+1,M-(N-i)-1,\cdots,M-(N-j)-1, \tag{4}$$

$m=j-1$，

$$\boldsymbol{E}(k,2m(M+N-2m)+2M+2N-5m-2j-i)=\boldsymbol{C}(i,j,k)$$
$$j=1,2,\cdots,\mathrm{floor}((N-1)/2);$$
$$i=j+1,j+2,\cdots,N-j. \tag{5}$$

3　拉伸和折叠算法设计

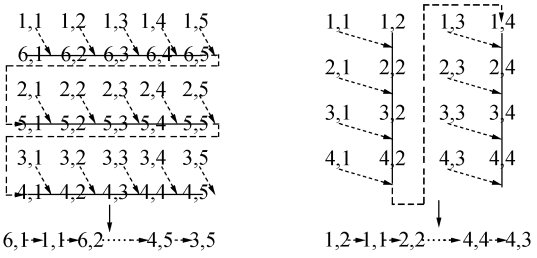
按照第 2 节所述算法将图像的三维数据矩阵 $\boldsymbol{C}$ 映射为二维数据矩阵 $\boldsymbol{E}$ 后，对矩阵 $\boldsymbol{E}$ 的像素进行置乱处理。置乱处理包括对像素的拉伸和折叠。拉伸算法将二维数据矩阵的像素按照一定顺序进行拉伸得到一个数据向量；折叠算法将拉伸得到的数据向量按原图大小进行折叠，得到置乱后的数据矩阵。

3.1　拉伸算法设计

提出了行、列非邻的拉伸算法，就是将二维数据矩阵行、列中的像素插入到非相邻的其它行、列的像素中，实现像素的拉伸。对于维数为 $N\times M$ 的图像，行(列)非邻拉伸算法是将第 1 行(列)中的像素插入到第 N 行(列)，第 2 行(列)的像素插入到第 $N-1$ 行(列)，后面各行(列)的像素按照该顺序依次进行拉伸。当 N 为偶数时，中间的两行(列)的元素互相插入，当 N 为奇数时，中间一行(列)不经过互插拉伸直接添加到向量尾。每两个非相邻行(列)中的像素互相插入可得到一个数据向量，将得到的各向量首尾相接实现对二维数据矩阵的拉伸处理。图 3(a)给出了维数为 65 的图像数据矩阵的行非邻拉伸过程，图 3(b)为维数为 4×4 的图像数据矩阵的列非邻拉伸过程。

设 $\boldsymbol{A}(i,j)$，$i=1,2,\cdots,N$；$j=1,2,\cdots,M$ 为图像的二维数据矩阵中的任意像素点，$\boldsymbol{l}(i)$，$i=1,\cdots,NM$ 为将 $\boldsymbol{A}(i,j)$ 拉伸得到的数据向量中的像素。

定义奇偶识别函数：



(a) 行非邻拉伸　(b) 列非邻拉伸

(a) Stretching map of nonadjacent rows　(b) Stretching map of nonadjacent columns

图 3　行非邻和列非邻拉伸过程

Fig. 3　Stretching map process of nonadjacent rows and columns

$$f(x)=\overline{g(x)};g(x)=x\%2\ . \tag{6}$$

当 x 为奇数时，$f(x)=0,g(x)=1$；当 x 为偶数时，$f(x)=1,g(x)=0$。则行非邻拉伸算法为：

$$\alpha(x,y)=g(N)\mathrm{floor}((N+1)/2)+f(N)(g(y)(N+1-x)+f(y)x),$$

$$\beta(x)=g(N)x+f(N)\mathrm{floor}((x+1)/2)\ , \tag{7}$$

$$\boldsymbol{l}((i-1)2M+j)=\boldsymbol{A}(g(j)(N+1-i)+f(j)i,\mathrm{floor}((j+1)/2))$$

$$j=1,2,\cdots,2M;i=1,2,\cdots,\mathrm{floor}(N/2)\ , \tag{8}$$

$$\boldsymbol{l}((i-1)2M+j)=\boldsymbol{A}(\alpha(i,j),\beta(j))$$

$$j=1,2,\cdots,m;i=\mathrm{floor}((N+2)/2)\ . \tag{9}$$

列非邻拉伸算法与行非邻拉伸算法类似，不再详述。

3.2　折叠算法设计

折叠算法是将拉伸得到的向量按照斜向蛇形线的顺序进行折叠，得到与原图像大小相同的二维数据矩阵。

对于一个 $N\times M$ 的二维数据矩阵，从 45°方向看去，该矩阵是由 $M+N-1$ 个斜行组成的。将拉伸算法得到的数据向量中的像素沿着斜向蛇形顺序折叠，就得到一个 $N\times M$ 的二维数据矩阵。图 4 给出了起点为(1,1)和(1,M)的斜向折叠过程。

仅给出起点为(1,1)的斜向蛇形线折叠算法，如公式(10)、(11)和(12)所示。

$$\boldsymbol{B}(1+(j-1),i-(j-1))=\boldsymbol{l}\left(\sum_{k=0}^{i-1}k+j\right)$$

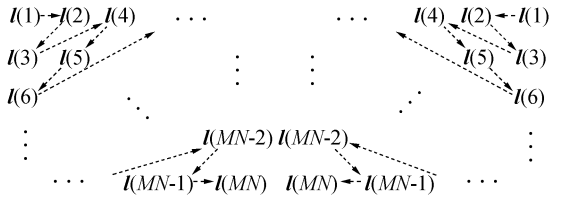
$$j=1,2,\cdots,i;i=1,2,\cdots,l_{\min}, \tag{10}$$

$$\boldsymbol{B}(j,i-(j-1))=\boldsymbol{l}\left(\sum_{k=0}^{l_{\min}}k+(i-l_{\min}-1)l_{\min}+j\right)$$

$$j=1,2,\cdots,l_{\min};i=l_{\min}+1,\cdots,l_{\max}, \tag{11}$$

$$\boldsymbol{B}(i-l_{\max}+j,l_{\max}-(j-1))=\boldsymbol{l}\left(MN-\sum_{k=0}^{l_{\max}+l_{\min}-i}k+j\right),$$

$$j=1,2,\cdots,l_{\max}+l_{\min}-i;i=l_{\max}+1,\cdots,l_{\max}+l_{\min}-1\ . \tag{12}$$



(a) 起点为(1,1)　(b) 起点为(1,M)

(a) Start point of (1,1)　(b) Start point of (1,M)

图 4　起点为(1,1)和(1,M)的斜向蛇形线折叠过程

Fig. 4　Folding process along diagonal snake line at start points (1,1) and (1,M)

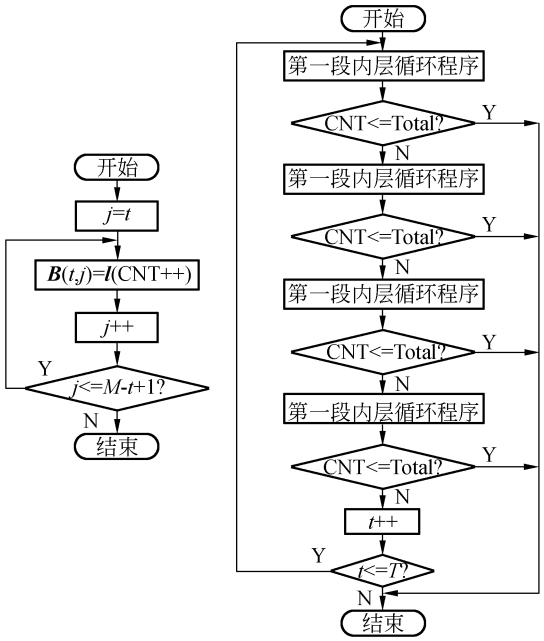
4　三维可逆混沌映射的优化算法

由于数字图像的数据量十分庞大，如果加密图像时采用推导的算法公式，计算量会很大，相应地加密时间也比较长。为了降低该加密算法的复杂性，分析了将三维数据矩阵映射为二维数据矩阵的过程中各相邻平面、平面内各相邻列向量系，以及二维数据矩阵的拉伸和折叠过程中各相邻像素之间的关系，提出了一种用简单加减运算代替复杂的算法公式的优化算法，大大缩短了加密时间。

4.1　三维矩阵映射为二维矩阵的优化算法

将三维数据矩阵映射为一个二维数据矩阵时不采用公式(2)～(5)来实现，而是将原图像的三维数据矩阵看作是 $2N-1$ 个平面，每个平面是由若干个列向量组成，每 4 个相邻的平面组成一个闭合矩形曲面，如图 3 所示。提出的优化算法的程序由外循环和内循环组成，每个平面对应一段内循环程序，内循环是将平面内的各列向量依次展开。根据平面方向的不同，内循环可分为 4 段，平面为水平方向时，用 $j++$ 或 $j--$ 来控制内循环的走向，当平面为垂直方向时用 $i++$ 或 $i--$ 来控制内循环的走向。则通过 $2N-1$ 次内循环可将组成三维数据矩阵的 $2N-1$ 个平面展开。

外循环是将内循环得到的 $2N-1$ 个平面按展开的顺序排列，构成一个 $8\times(NM)$ 的二维数据矩阵。优化算法程序的流程图如图 5 所示，仅给出其中一段内循环的流程，其余 3 段类似。程序中定义循环变量 $t=1$，计数变量 CNT=1，总数变量 Total=$N\times M$，$\boldsymbol{B}(i,j)$ 表示展开三维矩阵得到的二维数据矩阵。



(a) 第一段内层循环　　(b)外层循环

(a) First inner iteration　　(b)Exterior iteration

图 5　优化程序的内层和外层循环流程图

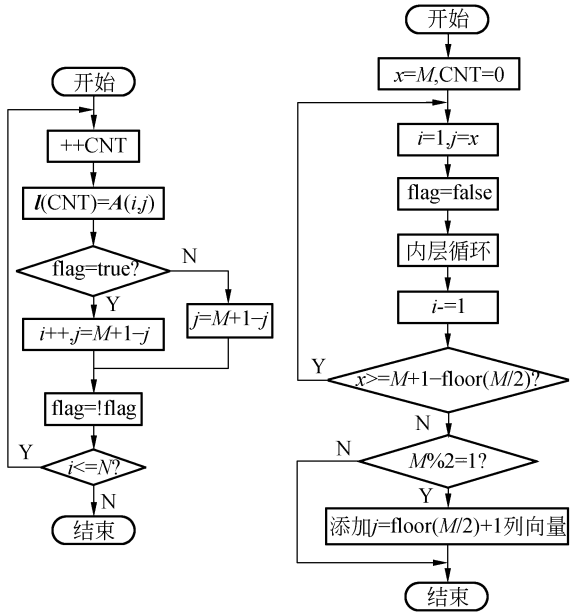
Fig. 5　Flowcharts of inner and exterior iterations of optimized program

4.2　图像拉伸算法优化

对于行(列)非邻拉伸算法，从图 3(b)中可以看出，首先将二维数据矩阵的行(列)向量重新排列，再进行拉伸处理，拉伸得到的各向量首尾相接完成行(列)非邻拉伸映射。

行(列)非邻拉伸映射优化算法的程序也包括内循环和外循环。内循环对应行(列)向量重新排列后的二维数据矩阵两个相邻的行(列)向量。内循环的实现过程是，首先找到每个行(列)向量的起点，那么行(列)向量的下一个点就在上一个点的下(左)方或者右下方，一直到行(列)向量拉伸结束；外循环是将内循环拉伸得到的各行(列)向量首尾相接得到一个行(列)向量，实现行(列)非邻拉伸映射。

图 6 给出了列非邻拉伸算法优化程序的内层和外层循环的流程，行非邻拉伸算法的优化程序与此类似。其中定义标志变量 flag，并赋初值 flag=false；定义计数变量 CNT。外部循环要判断 M 的奇偶，当 M 为奇时原矩阵的中间一列直接添加到向量中去。



(a)内层循环　　(b)外层循环

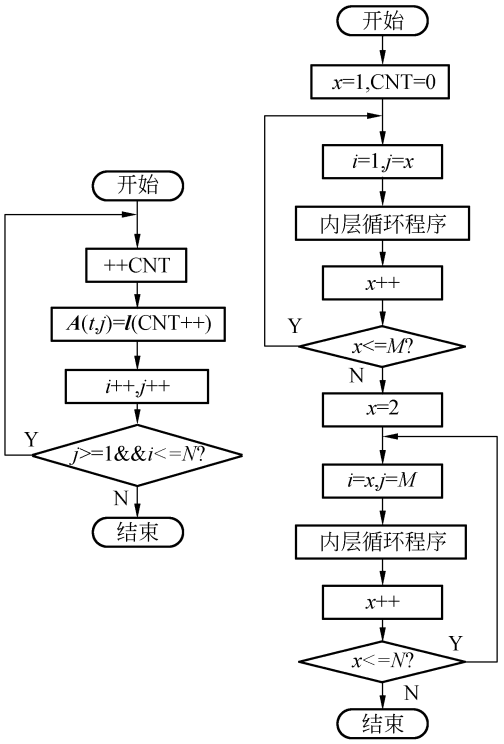
(a) Inner iteration　　(b)Exterior iteration

图 6　列非邻插拉伸优化算法的流程图

Fig. 6　Flowcharts of optimized stretching maps of nonadjacent columns

4.3　图像折叠算法优化

以起点为(1,1)的斜向蛇形线折叠过程为例说明折叠映射的优化算法。如图 4 所示，二维数据矩阵可看作是由 $N+M-1$ 个斜行组成，由拉伸算法得到的数据向量中的像素按照图 4 所示的顺序排列可得到置乱后的数据矩阵。折叠映射的优化算法程序包括内循环和外循环，每一个斜行对应一段内循环程序，所有的斜行对应一个外循环。对于内循环，每次向斜行中添加一个像素时，就让 $i=i+1$，$j=j-1$，当 $j<1$ 或 $i>N$ 时就跳到下一个斜行；这样经过 $N+M-1$ 次内层循环完成折叠过程。$N+M-1$ 个斜行对应的 $N+M-1$ 内层循环构成一个外层循环。内、外层循环流程如图 7 所示，程序中定义变量 CNT，x。



(a)内层循环　　(b)外层循环

(a) Inner iteration　　(b) Exterior iteration

图 7　斜向蛇形线折叠流程图

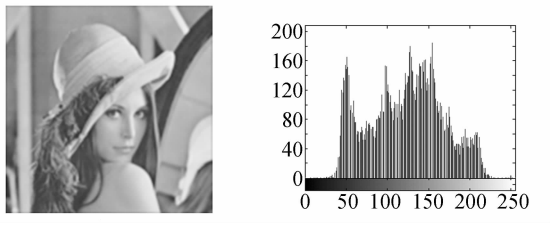
Fig. 7　Flowcharts of snake diagonal maps

5　图像加密方案和仿真结果

对于一个灰度图像,首先按照第 2 节提出的算法将图像的三维数据矩阵映射为二维数据矩阵,然后利用第 3 节提出的拉伸和折叠算法对二维数据矩阵的像素进行置乱处理,再将置乱后的二维数据矩阵还原为三维数据矩阵,这一过程称为一次循环映射。其中,对二维数据矩阵的置乱处理有两种算法:一种是将行非邻拉伸算法和起点为(1,1)的斜向蛇形线折叠相结合,另一种是将列非邻拉伸算法和起点为(1,M)的斜向蛇形线折叠算法相结合,分别称为置乱算法 1 和置乱算法 2。采用置乱算法 1 对二维数据矩阵进行置乱处理的映射算法称为映射算法 1,采用置乱算法 2 的称为映射算法 2。密钥设计为循环映射的次数,密钥的奇数位对应映射算法 1 的循环映射次数,偶数位对应映射算法 2 的循环映射次数。假设秘钥 Key=3 465,则首先应用映射算法 1 对图像的三维数据矩阵进行 3 次循环映射,应用映射算法 2 进行 4 次循环映射,应用映射算法 1 进行 6 次循环映射,应用映射算法 2 进行 5 次循环映射,完成图像加密,图像解密是图像加密的逆过程。

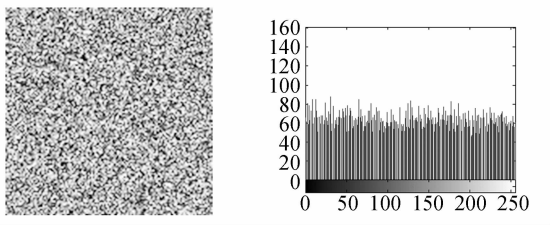
5.1　图像的加密和解密结果

针对灰度为 256、128×128 的 Lenna 图像,利用三维可逆图像加密方法进行了加密和解密。图 8(a)是明文图像,图 8(b)是明文图像的直方图,图 8(c)是加密图像,图 8(d)是密图的直方图,密钥 Key=12 345。



(a)明文图　　(b)明文图像的直方图

(a) Plain image　　(b) Histogram of plain image



(c)密文图　　(d)密文图像的直方图

(c) Cipher image　　(d) Histogram of cipher image

图 8　运用三维可逆映射对 128×128 图加密

Fig. 8　Encrypting 128×128 images by invertible 3D map

由图 8 的(a)和(c)可知,该加密算法较好地置乱了原图像的像素,实现了图像加密。由图 8(b)和(d)可知,原图和密图的直方图不同,这是由于三维可逆映射置乱了图像像素的二进制位的位置,相当于改变了图像的像素值,说明该加密算法同时实现了像素置乱和像素混淆。

5.2　加密时间分析

针对不同大小的图像,分别利用推导的算法公式和提出的优化算法进行加密和解密实验,两种方法所用的时间如表 1 所示。通过将两种算法的加密时间进行对比,可以看出优化算法要比利用公式的算法要快 3～4 倍,说明优化算法明显提高了加密速度。

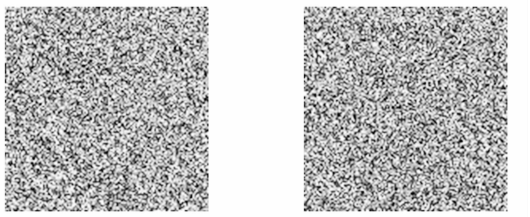
表 1　加密和解密时间

Tab. 1　Time of encryption and decryption

图像大小	利用优化算法		利用算法公式	
	加密	解密	加密	解密
128×128	0.081 1	0.083 9	0.154 3	0.153 8
256×256	0.157 1	0.235 1	0.375 3	0.366 8
512×512	0.293 6	0.407 8	1.335 3	1.286 3
1 024×1 024	1.008 2	1.459 4	5.008 65	4.996 08

5.3　密钥敏感度分析

对于加密密钥为 Key＝12 345 的密文图像 8(c)，用 Key_1＝12 346 和 Key_2＝22 345 对图 8(c)进行解密，结果如图 9 所示。由图可知仅对密钥的最后一位或第一位做微小的变化均不能解密图像，说明该加密算法对密钥非常敏感，安全性较高。



(a) 用 Key_1 解密　(b) 用 Key_2 解密

(a) Decryption with Key_1　(b) Decryption with Key_2

图 9　密钥敏感度测试

Fig. 9　Sensitivity test of security key

5.4　安全性能分析

图像加密的安全性与密钥空间、不动点比、信息熵、相邻像素间的相关系数有关，对这几个参数进行了计算分析。

首先分析了该算法的密钥空间。本算法密钥空间的大小只与密钥的长度有关，它们之间的关系如表 2 所示。理论上，在计算速度允许的情况下，本算法的密钥长度没有限制，密钥空间可以为无限大；实际应用时，密钥长度的选取与安全性的要求有关。

表 2　密钥长度和密钥空间

Tab. 2　Length and space of security key

密钥长度(位)	密钥空间
64	1.84×10^{19}
128	3.4×10^{38}
256	1.16×10^{77}
512	1.34×10^{154}

其次计算分析了原图和密图的不动点比。若原图像 A 中的像素点(i, j)在加密后其灰度值没有发生变化，则称该像素点为不动点。图像中不动点占所有像素的百分比，称为该图的不动点比，用 $BD(A)$表示。根据不动点比的计算公式，计算得到原图 8(a)与密图 8(c)的不动点比为0.37%，这说明不动点的数目很少。利用该加密算法改变了原图 99.6%以上的像素的位置，由该参数看出这种算法的置乱效果很好。

信息熵反映的是图像中的灰度分布情况，分布越均匀，信息熵越大，包含的不确定信息就越多。根据信息熵的计算公式，原图 8(a)的信息熵为 7.369 3，密图 8(c)的信息熵为 7.981 1，密图的信息熵比原图的信息熵大，这说明密图的灰度分布比较均匀，攻击者从灰度分布中得到的图像信息较少，使攻击难度增加，加密安全性高。

由于图像相邻像素之间具有很强的相关性，如果密图相邻像素之间相关性变小，说明密图安全性变强。计算图 9 的明文图像和密文图像相邻像素的相关系数，结果如表 3 所示。密文图像相邻像素之间的相关系数比原图的小很多，说明该加密方法抵御统计攻击的能力比较强。

表 3　原图和密图相邻点之间的相关系数

Tab. 3　Correlation coefficients of two adjacent pixels in plain image and cipher image

相邻像素的方向	相关系数	
	原图	密图
水平方向	0.890 5	0.005 2
垂直方向	0.947 7	0.011 2
对角线方向	0.853 7	0.003 6

6　结　论

提出了一种三维可逆混沌图像加密算法，推导了该加密算法完整的数学表达式。为提高加密效率，提出了一种优化算法，使该算法更适合于实时加密。三维可逆混沌图像加密方法具有如下优点：(1)通过一次映射同时改变了图像像素的位置和像素值，置乱效率较高；(2)提出的优化算法用简单的加减运算代替复杂的计算公式，将加密速度提高了 3～4 倍；(3)对密钥非常敏感，仅对密钥的第一位或最后一位做微小变化均不能正确解密

图像;(4)原图相邻像素之间的相关系数为 0.8～1,加密后密图的相邻像素之间的相关系数减小到 0.1 以下,明显小于原图。同时分析了该算法的密钥空间,原图与密图的不动点比、信息熵、相邻像素间的相关系数,说明该加密算法具有较高的安全性。

参考文献:

[1] SHANNON C E. Communication theory of secrecy systems[J]. *The Bell System Technical Journal*, 1949, 28(4): 656-715.

[2] LI S J. Some basic cryptographic requirements for chaos-based cryptosystems[J]. *Int. J. Bifurcation and Chaos*, 2006, 16(8): 2129-2151.

[3] FRIDRICH J. Symmetric ciphers based on two-dimensional chaotic maps[J]. *Int. J. Bifurcation and Chaos*, 1998, 8(6): 1259-1284.

[4] CHEN G R, MAO Y B, CHUI C K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. *Chaos, Solitons & Fractals*, 2004, 21(3): 749-761.

[5] SALLEH M, IBRAHIM S, ISNIN I F. Enhanced chaotic image encryption algorithm based on chaotic maps[C]. *In IEEE Conf. Circuits and System*, 2003, 2:508-511.

[6] MAO Y B, CHEN G R, LIAN S. A novel fast image encryption scheme based on 3D chaotic baker maps[J]. *Int. J. Bifurc. Chaos*, 2004, 14(10):3613-3624.

[7] 樊春霞,姜长生. 一种基于混沌映射的图像加密算法[J]. 光学 精密工程, 2004 ,12 (2) :179-184.
FAN CH X, JIANG CH SH. Image encryption based on discrete chaotic maps[J]. *Opt. Precision Eng.*, 2004, 12(2): 179-184. (in Chinese)

[8] 梁士利, 张玲, 王广,等. 一维加法 CA 的同步系统研究光学精密工程[J]. 光学 精密工程,2006 ,14 (3) :495-497.
LIANG SH L , ZHANG L, WANG G, *et al*.. Study on synchronization of 1D additive cellular automata [J]. *Opt. Precision Eng.*, 2006 , 14 (3) : 495-497. (in Chinese)

[9] SALLEH M, IBRAHIM S, ISNIN I F. Enhanced chaotic image encryption algorithm based on baker's map[C]. *Proceedings of the* 2003 *International Symposium on Circuits and Systems*. 2003(2): 508-511.

[10] FENG Y, LI L J , HUANG F. A Symmetric image encryption approach based on line maps[C]. *Proc. of* 1*st International Symposium on Systems and Control in Aerospace and Astronautics*, *Harbin*, *China*, 2006: 1362-1367.

[11] 黄峰,冯勇. 利用图像分割思想的二维混沌映射及图像加密算法[J]. 光学 精密工程,2007,15(7): 1096-1103.
HUANG F, FENG Y. Novel 2D chaotic map based on image segmentation and image encryption approach[J]. *Opt. Precision Eng.*, 2007,15(7): 1096-1103. (in Chinese)

作者简介:李　娟(1982－),女,博士研究生,主要从事图像加密方面的研究。E-mail: lijuan2001422@163.com

冯　勇(1962－),男,教授,博士生导师,主要从事图像加密、混沌控制、滑模控制等方面的研究。E-mail: yfeng@hit.edu.cn