第 59 卷 第 3 期 2010 年 3 月
1000-3290/2010/59(03)/1507-17

物 理 学 报
ACTA PHYSICA SINICA

Vol. 59, No. 3, March, 2010

基于 Z 矩阵映射和选择加密的彩色图像退化算法研究*

赵 亮† 廖晓峰 向 涛 肖 迪

(重庆大学计算机学院,重庆 400044)

(2009 年 4 月 8 日收到;2009 年 7 月 14 日收到修改稿)

首先提出了一种可应用于加密的三维 Z 矩阵映射,并从理论上证明了其良好的密码学特性,其次提出了两种基于不同选择加密模板的彩色图像退化算法并进行了仿真实验. 最后,对所提出的两种退化算法从性能和安全性上进行了有效的分析,证明了算法的可靠性.

关键词: Z 矩阵, 选择加密, 混沌加密, 彩色图像退化

PACC: 0545

1. 引 言

人类与外界世界的交流主要是通过各种感觉器官不断接受信息传递给大脑,然后做出各种相应的反应,而通过视觉所获得的信息就占了绝大部分. 据统计表明,视觉信息约占人类从外界获得信息的 2/3[1],其中主要以照片和图画等静止图像为主. 而近年来,随着计算机技术和网络技术的不断发展,数字图像在我们的生活中就有着越来越广泛的应用,尤其是彩色图像,它对我们的生活产生了许多直接的影响. 而此时,通过网络传输图像的安全性就变得尤为重要了,这其中主要以图像的版权保护,认证以及图像的保密等方面作为数字图像安全性的主要内容,文献[2—10]列出了近年来一些图像版权保护和保密加密方面的主要算法和思路. 虽然在网络中传播的许多图像均需要防止黑客的攻击,但随着 Web2.0 技术的问世,许多商业用途的图像并不需要对其进行完全加密,以使其识别不出,而只需要降低图像本身的清晰度,使需要的用户阅览降低了视觉质量的数字图像,当用户进行付费之后才能完全欣赏到具有高质量的数字图像,在这种背景下,出现了图像退化(Degradation)加密模式,而在这种应用模式下,加密后的数字图像仍保留有原清晰图像的部分信息,可反映出原图像的主要内容,但是与原图像相比显得更粗糙、更模糊. 这种人为主动降低图像的视觉模式的方式主要用于电子消费品的销售,当图像的所有者先将退化后的图像发送给潜在的消费者进行试用,消费者在对退化图像进行预览后决定是否购买. 文献[11]首次提出了基于灰度图像的退化加密算法,作者建议把灰度图像分成 8 个位平面,而对最低的 4 个或 5 个位平面 LSB(least significant bit-plane)进行加密以达到较好的退化效果.

虽然文献[11]中提出的选择位平面加密算法可以在加密最低 4—5 个位平面后取得数字图像视频质量上的下降,但是对于退化后的数字图像来说,我们依然可以看清整个图像的轮廓和重要信息(见文献[11]中 Table 1),这时,只要达到用户的要求,即使用户不提出购买图像,也能从图像中获取所需要的信息. 同时,对于彩色数字图像来说,如果分别对其中的 3 个颜色分量(R, G, B)按照文献[11]中的方法进行选择加密,则加密所需的时间必然为对灰度图像进行加密所花开销的 3 倍,而如果仅仅进行简单的异或(XOR)操作,此时在安全性上也无法得到保障. 本文根据网络环境下数字彩色图

* 国家自然科学基金(批准号:60703035),新世纪优秀人才支持计划(批准号:NCET-08-0603),中国博士后科学基金(批准号:20080430741),重庆市自然科学基金(批准号:2008BB2182, 2008BB2193),重庆市自然科学重点基金(批准号:CSTC2009BA2024),重庆大学研究生科技创新基金(批准号:200903A1B0010303)资助的课题.

† 通讯联系人. E-mail: zhaoliang@cqu.edu.cn; zhaoliang_916@163.com

像的特点,提出了利用一种新型的三维 Z 矩阵和三维 Chen 系统的选择加密来退化彩色图像的方法,其中本文对彩色图像加密像素的选取提供了两种方式:随机模板方式和基于信息熵的模块划分方式.文章的最后分别对这两种方式给出了相应的分析和比较.

2. 三维 Z 矩阵映射

2.1. 三维 Z 矩阵映射及其构造

三维 Z 矩阵是一类带两个变量参数 a 和 b 的矩阵(a 和 b 为正整数),其具体的定义形式如下:

$$Z_{3\times3}=\begin{bmatrix}1 & a & a\\ b & ab+1 & ab+1\\ b & ab+2 & ab+3\end{bmatrix},$$

其中当用来进行加密时,参数 a 和 b 可以看作密钥进行管理,如果系统参数 a 和 b 置为 $a=1$, $b=1$,则对应的 Z 矩阵就类似于三维 Arnold 猫矩阵:

$$A=\begin{bmatrix}1 & 1 & 1\\ 1 & 2 & 2\\ 1 & 2 & 3\end{bmatrix},$$

$$Z_{3\times3}=\begin{bmatrix}1 & 1 & 1\\ 1 & 2 & 2\\ 1 & 3 & 4\end{bmatrix},$$

A 矩阵为文献[12]中所提出的标准三维 Arnold 猫矩阵,它是 V. I. Arnold 所提出的标准二维 Arnold 猫矩阵在维数上的扩展,而 $Z_{3\times3}$ 矩阵则是当 $a=1$, $b=1$ 时的 Z 矩阵.而对于三维 Z 矩阵来说,其对应的映射如下:

$$\begin{bmatrix}x'\\ y'\\ z'\end{bmatrix}=\begin{bmatrix}1 & a & a\\ b & ab+1 & ab+1\\ b & ab+2 & ab+3\end{bmatrix}\begin{bmatrix}x\\ y\\ z\end{bmatrix}\bmod1, \quad (1)$$

即对应的相空间限制在[0,1]×[0,1]×[0,1]内.由于在图像处理中时常是对有限集进行操作,因此,对以上映射((1)式)进行扩展并广义化处理,有以下等式:

$$\begin{bmatrix}x'\\ y'\\ z'\end{bmatrix}=\begin{bmatrix}1 & a & a\\ b & ab+1 & ab+1\\ b & ab+2 & ab+3\end{bmatrix}\begin{bmatrix}x\\ y\\ z\end{bmatrix}\bmod N. \quad (2)$$

这样,得到离散化后的有限集是{0,1,2,…,$N-1$}×{0,1,2,…,$N-1$}×{0,1,2,…,$N-1$},即只取0到 N−1 的正整数.下面我们将就以上映射的性质进行证明和分析.

2.2. 三维 Z 矩阵映射的特性

定理1 三维 Z 矩阵映射的最大 Lyapunov 特征指数大于0.

证明 对于三维 Z 矩阵映射,其 Lyapunov 特征指数与对应矩阵的特征值有直接关系.根据矩阵相关理论,由于三维 Z 矩阵是满秩矩阵,因此这里必然存在三个特征值 λ_1, λ_2, λ_3,从而,我们可以根据如下特征多项式讨论特征值的情况:

$$\begin{vmatrix}\lambda-1 & -a & -a\\ -b & \lambda-(ab+1) & -(ab+1)\\ -b & -(ab+2) & \lambda-(ab+3)\end{vmatrix}=0$$

$$\Rightarrow\begin{vmatrix}\lambda-1 & 0 & -a\\ -b & \lambda & -(ab+1)\\ 0 & 1-2\lambda & \lambda-2\end{vmatrix}=0$$

$$\Rightarrow\lambda^3-(5+2ab)\lambda^2+(5+ab)\lambda-1=0,$$

通过以上变换,我们可以看出,三维 Z 矩阵特征值的讨论可以转化为讨论有关一元三次方程的解(a 和 b 可看成常量),同时,由于 λ^3 前的实系数为1,因此,可以根据 Cardan 公式[13,14]中有关一元三次方程根的判别式来判别特征值 λ 的情况,其过程如下:

首先,确定判别式[13]

$$D=\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3$$

中 q 和 p 的值,根据 Cardan 公式可得到

$$q=-\frac{2}{27}(5+2ab)^3+\frac{1}{3}(5+2ab)(5+ab)-1,$$

$$p=(5+ab)-\frac{(5+2ab)^2}{3},$$

同时,对以上 q 和 p 进行变换得到以下等式:

$$q=\frac{-(52+165ab+102a^2b^2+16a^3b^3)}{27},$$

$$p=\frac{-(10+17ab+4a^2b^2)}{3}.$$

从以上等式可以看出,由于 a 和 b 均为正整数,因此,可得到 $q<0$, $p<0$.把 q 和 p 代入 D 中进行计算,其过程如下(令 $l=ab$, l 为正整数):

$$D=\frac{(52+165l+102l^2+16l^3)^2}{27^2\times4}-\frac{(10+17l+4l^2)^3}{27^2}$$

$$=\frac{(52+165l+102l^2+16l^3)\times(52+165l+102l^2+16l^3)}{27^2\times4}$$

$$-\frac{(10+17l+4l^2)\times(10+17l+4l^2)\times(10+17l+4l^2)}{27^2}$$

$$= -\frac{1296 + 3240l + 1647l^2 + 648l^3 + 108l^4}{27^2 \times 4}.$$

由此,我们可以得出,在 l 为正整数时,D 恒小于 0. 因此,根据文献[14]中的根的判别式,当 $D<0$ 时,一元三次方程

$$\lambda^3 - (5 + 2ab)\lambda^2 + (5 + ab)\lambda - 1 = 0$$

有三个互异的实根,即我们所讨论的三维 Z 矩阵有 3 个互不相等的实特征值 $\lambda_1 \neq \lambda_2 \neq \lambda_3$,从而可得出三维 Z 矩阵有三个线性无关的特征向量. 因此,三维 Z 矩阵是可对角化矩阵,则 Z 矩阵可表示为正交矩阵 Q 和对角矩阵 E 的乘积:$Z = QEQ^{-1}$(其中 Q 为 Z 矩阵对应特征向量所组成的矩阵,E 中非零元素为特征值),

$$Q = [q_1, q_2, q_3],$$

$$E = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix}.$$

因为矩阵特征值的乘积等于它相应的行列式的值,所以可以得到 $\lambda_1 \times \lambda_2 \times \lambda_3 = |Z_{3\times3}| = 1$. 1) 如果特征值 $\lambda_1 = 1$, $\lambda_2 = 1$, $\lambda_3 = 1$,则 $Z = QEQ^{-1} = QQ^{-1} = I$,其中 I 是三维的单位矩阵. 然而,对于任意的正整数 a 和 b,$Z \neq I$. 2) 如果特征值 $\lambda_1 < 1$, $\lambda_2 < 1$ 同时 $\lambda_3 < 1$,则乘积 $\lambda_1 \times \lambda_2 \times \lambda_3 < 1$. 因此,这里至少存在一个特征值 $\lambda_i > 1$,这说明了最大 Lyapunov 特征指数大于 0,由此可以得出连续三维 Z 矩阵映射的运动是混沌的. 表 1 列出了(1)式中 a 和 b 取不同值的三个 Lyapunov 特征指数所对应的矩阵特征值.

表 1　a 和 b 取不同值的三个 Lyapunov 特征指数所对应的矩阵特征值

$[a, b]$	LCE(1)	LCE(2)	LCE(3)
[1, 1]	6.0329	0.7444	0.2227
[7, 3]	46.4406	0.0416	0.5178
[5, 9]	94.4708	0.0208	0.5083
[13, 19]	498.4945	0.0040	0.5015

对于 Z 矩阵映射(1)式来说,由于广义化后的映射((2)式)改变了原有映射的某些性质,因此,我们对其进行特别的分析.

定理 2　当系统参数 a 和 b 取任意正整数时,广义三维 Z 矩阵映射为 1 - 1 映射.

证明　对于三维 Z 矩阵来说,有

$$|Z_{3\times3}| = \begin{vmatrix} 1 & a & a \\ b & ab+1 & ab+1 \\ b & ab+2 & ab+3 \end{vmatrix}$$

$$= \begin{vmatrix} 1 & a & a \\ b & ab+1 & ab+1 \\ 0 & 1 & 2 \end{vmatrix}$$

$$= \begin{vmatrix} 1 & a & 0 \\ b & ab+1 & 0 \\ 0 & 1 & 1 \end{vmatrix}$$

$$= \begin{vmatrix} 1 & a & 0 \\ b & ab+1 & 0 \\ 0 & 0 & 1 \end{vmatrix} = 1,$$

则有当 a 和 b 取任何正整数,三维 Z 矩阵的行列式均等于 1,因此,这保证了广义三维 Z 矩阵映射是 1 - 1 映射.

定理 3　广义三维 Z 矩阵映射具有周期性.

证明　根据文献[12]中关于周期性的定理,对于任何正整数 N,映射 $r_m = Ar_0 (\mathrm{mod}N)$ 具有周期性的充分必要条件是映射矩阵 A 的行列式和 N 互素,其中 $r_m = (x_m, y_m, z_m)$, $r_0 = (x_0, y_0, z_0)$. 而对于三维 Z 矩阵来说,由于当系统参数 a 和 b 取任意正整数时,其所对应的行列式均等于 1,而 1 和任意的正整数 N 均互素,所以广义三维 Z 矩阵映射满足充分必要条件,因此,广义三维 Z 矩阵映射具有周期性.

定理 4　广义三维 Z 矩阵映射与其逆矩阵映射具有相同的周期性.

证明　根据文献[15]中的命题,广义三维 Z 矩阵映射与其逆矩阵映射具有相同的周期当且仅当映射 $r_m = Ar_0 (\mathrm{mod}N)$ 可以推导出逆映射 $r_0 = A^{-1}r_m (\mathrm{mod}N)$. 因此,根据广义三维 Z 矩阵映射的构造((2)式)得到以下线性方程组:

$$\begin{aligned} x' &= x + ay + az - k_1 N, \\ y' &= bx + (ab+1)y + (ab+1)z - k_2 N, \\ z' &= bx + (ab+2)y + (ab+3)z - k_3 N, \end{aligned} \quad (3)$$

其中 k_1, k_2, k_3 是三个整数. 同时,根据三维 Z 矩阵的形式,推导出其逆矩阵结构

$$Z_{3\times3}^{-1} = \begin{bmatrix} 1 & a & a \\ b & ab+1 & ab+1 \\ b & ab+2 & ab+3 \end{bmatrix}^{-1}$$

$$= \begin{bmatrix} ab+1 & -a & 0 \\ -2b & 3 & -1 \\ b & -2 & 1 \end{bmatrix}. \quad (4)$$

然后用(3)式与(4)式相乘,

$$Z_{3\times3}^{-1}\begin{bmatrix}x'\\y'\\z'\end{bmatrix}=\begin{bmatrix}ab+1 & -a & 0\\ -2b & 3 & -1\\ b & -2 & 1\end{bmatrix}\begin{bmatrix}x+ay+az-k_1N\\ bx+(ab+1)y+(ab+1)z-k_2N\\ bx+(ab+2)y+(ab+3)z-k_3N\end{bmatrix}$$

$$=\begin{bmatrix}(ab+1)(x+ay+az-k_1N)-a(bx+(ab+1)y+(ab+1)z-k_2N)\\ -2b(x+ay+az-k_1N)+3(bx+(ab+1)y+(ab+1)z-k_2N)\\ -(bx+(ab+2)y+(ab+3)z-k_3N)\\ b(x+ay+az-k_1N)-2(bx+(ab+1)y+(ab+1)z-k_2N)\\ +(bx+(ab+2)y+(ab+3)z-k_3N)\end{bmatrix}$$

$$=\begin{bmatrix}x+(-(ab+1)k_1+ak_2)N\\ y+(2bk_1-3k_2+k_3)N\\ z+(-bk_1+2k_2-k_3)N\end{bmatrix}.$$

由此可以看出可逆变换为

$$Z_{3\times3}^{-1}\begin{bmatrix}x'\\y'\\z'\end{bmatrix}(\mathrm{bmod}N)=\begin{bmatrix}x\\y\\x\end{bmatrix}\Rightarrow\begin{bmatrix}x\\y\\x\end{bmatrix}=\begin{bmatrix}ab+1 & -a & 0\\ -2b & 3 & -1\\ b & -2 & 1\end{bmatrix}\begin{bmatrix}x'\\y'\\z'\end{bmatrix}\mathrm{bmod}N.$$

综上所述,广义三维 Z 矩阵映射与它的逆矩阵映射具有相同的周期性.

2.3. 广义三维 Z 矩阵映射的周期性分析

在文献[2, 12]中分别提出了两种基于二维 Arnold 猫变换的高维猫矩阵,2.1 节列出了标准三维 Arnold 猫变换的矩阵形式,而三维 Chen 猫变换的矩阵形式如下:

$$A=\begin{bmatrix}1+a_xa_za_y & a_z & a_y+a_xa_z+a_xa_ya_zb_y\\ b_z+a_xb_y+a_xa_zb_yb_z & a_zb_z+1 & a_ya_z+a_xa_ya_zb_yb_z+a_xa_zb_z+a_xa_yb_y+a_x\\ a_xb_xb_y+b_y & b_x & a_xa_yb_xb_y+a_xb_x+a_yb_y+1\end{bmatrix},$$

其中 a_x, a_y, a_z, b_x, b_y和 b_z 是矩阵的可控参数,当这些参数均设置为 1 时,矩阵的形式如下:

$$A=\begin{bmatrix}2 & 1 & 3\\ 3 & 2 & 5\\ 2 & 1 & 4\end{bmatrix}.$$

由于周期的长短是测试一个映射变换优劣的重要标准,特别是对于图像加密来说,当映射的周期越长,其加密的安全性越高. 所以,我们分别测试了广义 Z 矩阵、标准三维 Arnold 猫矩阵和 Chen 猫矩阵映射的周期,并列于表 2,其中所有的控制参数均设置为 1,并且为了适应一般的图像处理,$N=2^\beta$ (β 是个正整数). 从表中可以看出,Z 矩阵对应最长的周期,特别的,Z 矩阵映射的周期是标准三维 Arnold 猫映射周期的 2 倍,这对于图像处理,尤其是图像加密来说非常重要.

表 2 3 种矩阵映射周期性比较

N	16	32	64	128	256	512	1024
Z-matrix	56	112	224	448	896	1792	3584
Standard Arnold	28	56	112	224	448	896	1792
Chen's Arnold	24	48	96	192	384	768	1536

为了测试当 a 和 b 取不同的数字时,广义 Z 矩阵映射也具有这样的长周期效应,我们把[a, b]进行划分,分别为[$2m+1$, $2m$],[$2m+1$, $2m+1$]和[$2m$, $2m$](其中 m 为任意正整数),并求出对应的周期数($N=2^4=16$),如表 3 所示.

表 3　a 和 b 取不同值所对应的周期($N=16$)

$[a, b]$	周期数	$[a, b]$	周期数	$[a, b]$	周期数
[12, 68]	8	[6, 95]	32	[31, 41]	56
[38, 16]	8	[76, 15]	16	[53, 75]	56
[58, 84]	8	[90, 97]	32	[33, 13]	56
[98, 6]	16	[26, 87]	32	[3, 69]	56
[440, 254]	8	[126, 121]	32	[55, 269]	56
[516, 202]	8	[512, 75]	16	[473, 593]	56
[410, 34]	16	[338, 315]	32	[287, 543]	56
[214, 300]	8	[192, 73]	16	[273, 485]	56
[262, 338]	16	[226, 463]	32	[499, 101]	56
[370, 70]	16	[522, 227]	32	[239, 315]	56
[540, 454]	8	[224, 497]	16	[433, 343]	56
[984, 130]	8	[1330, 299]	32	[1195, 1065]	56
[1176, 634]	8	[144, 943]	16	[1145, 1396]	56
[1340, 208]	8	[92, 1343]	16	[313, 987]	56
[1218,1078]	16	[330, 1075]	32	[733, 1309]	56
[622, 870]	16	[1308, 935]	16	[1001, 321]	56
[1334, 898]	16	[90, 185]	32	[631, 243]	56

从表中可以得到如下重要信息:a,b 和 N 之间具有非常密切的关系,如果 a 和 b 都是奇正数,映射的周期最大,并且是最大周期;否则,周期数是个变化的值,且小于最大周期. 表 3 中给出了具体的实例,当 a 和 b 均是奇正数时,周期数是 56,而其他情况下周期数可能是 8, 16 或者 32. 因此,我们可以得到以下结论:当 $N=2^{\beta}$(β 为正整数),广义三维 Z 矩阵映射的最大周期满足以下关系式:

$$\begin{aligned} &\mathrm{MP}(N) = f(a,b),\\ &\mathrm{mod}(a,2) \neq 0,\\ &\mathrm{mod}(b,2) \neq 0, \end{aligned}$$

其中 MP(N)是对应不同 N 的最大周期数,$f(\cdot)$表示 MP(N)和 a,b 之间的关系式.

3. 基于选择加密的并行彩色图像退化算法

与一些常用的矩阵映射相比,对于广义三维 Z 矩阵映射来说,由于它具有结构简单,周期长等显著特点,因此非常适合于普通图像的加密. 特别地,对于彩色图像来说,应用三维 Z 矩阵映射可以并行完成对同一个点的三个对应像素值(R,G,B)的加密,因此,这可以提高彩色图像加密的速度. 以下首先介绍一种基于三维 Z 矩阵的彩色图像加密方法,然后将分别应用两种选择加密模板对彩色图像进行退化研究. 而本文提出的彩色图像退化算法至少应该满足以下三点要求:

1)退化算法是可逆的,用户可以利用密钥恢复出原彩色图像.

2)对通用的图像增强算法应有较强的抵御能力.

3)退化算法应尽量简单快速,利于实际应用.

3.1. 基于 Z 矩阵映射和 Chen 系统的混沌加密算法

Chen 混沌系统由陈关荣在 1999 年提出,它是一个带有三个控制参数 p, q 和 r 的连续三维混沌系统,其动力学方程表示如下:

$$\begin{aligned} \dot{x} &= p(y-x),\\ \dot{y} &= (r-p)x - xz + ry,\\ \dot{z} &= xy - qz. \end{aligned} \tag{5}$$

当参数 $p=35$, $q=3$, $r=28$ 时,系统会产生混沌吸引子,对其应用步长为 0.001 的四阶 Runge – Kutta 算法进行离散化处理,Chen 系统的混沌特性如图 1 所示.

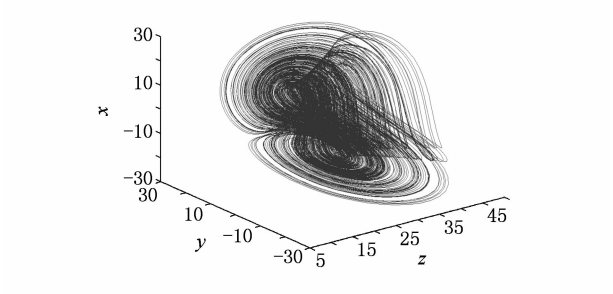

图 1 Chen 系统的混沌行为

与著名的 Lorenz 系统比较,Chen 混沌系统的动力学特征更加复杂,因此其更适用于安全通信的应用.

在我们的加密算法中,三维 Chen 混沌系统被用来加密彩色图像的 3 个颜色分量的像素值,整个加密的过程包括以下 4 个步骤:

1)把 $N\times N$ 大小的彩色图像按从左到右,从上到下的顺序排列成 $3\times N^2$ 的矩阵 T,其中每一列对应一个坐标位置上的(R,G,B)三个分量的像素值.

2)为了使 Chen 系统能进入混沌状态,首先对其进行初始迭代 N_0 次.

3)继续迭代混沌 Chen 系统 N^2 次,对于每次迭代产生的 3 个迭代值,我们可以应用以下方式对其进行转换使其成为 3 个 3 位正整数.

$$\begin{aligned} M_{x_x} &= \mathrm{floor}((\mathrm{abs}(\mathrm{ceil}(x_i))\\ &\quad -\mathrm{abs}(x_i))\times 10^3),\\ M_{y_i} &= \mathrm{floor}((\mathrm{abs}(\mathrm{ceil}(y_i))\\ &\quad -\mathrm{abs}(y_i))\times 10^3),\\ M_{z_i} &= \mathrm{floor}((\mathrm{abs}(\mathrm{ceil}(z_i))\\ &\quad -\mathrm{abs}(z_i))\times 10^3), \end{aligned} \tag{6}$$

其中函数 floor(·)表示向下取整;函数 abs(·)表示取对应数字的绝对值;函数 ceil(·)表示向上取整.

4)按列提取矩阵 T 中对应的 3 个像素值,并应用广义三维 Z 矩阵映射和 Chen 系统产生的迭代值对每个像素进行加密:

$$\begin{bmatrix} C_{\mathrm{R}_i}\\ C_{\mathrm{G}_i}\\ C_{\mathrm{B}_i} \end{bmatrix} = \begin{bmatrix} 1 & a & a\\ b & ab+1 & ab+1\\ b & ab+2 & ab+3 \end{bmatrix} \begin{bmatrix} T_{\mathrm{R}_i}\\ T_{\mathrm{G}_i}\\ T_{\mathrm{B}_i} \end{bmatrix} + \begin{bmatrix} M_{x_i}\\ M_{y_i}\\ M_{z_i} \end{bmatrix} \mathrm{mod}256, \tag{7}$$

其中 $i=1,2,3,\cdots,N^2$,不断利用迭代 Chen 系统产生的值按以上步骤继续进行,则最终产生的 C_{R}, C_{G}, C_{B} 就是所需的图像密文.

3.2. 基于随机选择模板的彩色图像退化算法

图像退化的目的是通过降低图像的视觉质量来达到隐藏图像的部分重要信息或者是图像的某些细节信息.这样,即使是用户收到退化图像后,依然可以通过一些残留部分对原有的图像进行理解.基于此思想,我们提出应用随机选择模板的方式来退化彩色图像,其具体过程如下:

1)随机生成一个与图像尺度相同的可控二值选择模板(0 和 1),如图 2 所示.

2)把此模板对应于要进行退化的彩色图像,如果彩色图像位置(i,j), $i,j=0,1,\cdots,N$ 所对应的模板位置的值为 1,则提取出此像素,否则跳过.

3)对提取出的像素按 3.1 节中的方式进行加密,得到最终的退化图像.

0	1	0	0	1	1
0	1	0	1	1	1
0	0	1	0	1	0
1	1	0	1	0	0
1	0	1	0	1	0

图 2 随机选择模板

从算法的思路可以看出,图像退化的强度主要依赖于加密像素的数量,及随机选择模板中 1 的个数.如果加密的像素个数越多,图像的退化程度越大,因此,这里我们可以对所选像素的百分比进行控制,例如可选取其中 30% 或者 50% 的像素进行加密,并认为此百分比为图像退化程度的阈值.如果我们假设图像加密的像素值占全部像素的比例为 Q,则图像的视觉质量退化程度可定义如下:$Q\times\sigma^2$.其中 σ^2 为图像的平均功率,特别地,对于彩色图像,其平均功率的定义如下(这里根据 R,G,B 的线性组合[16]来定义平均功率):

$$\sigma_{\mathrm{R}}^2 = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[S_{\mathrm{R}}(i,j)]^2,$$

$$\sigma_{\mathrm{G}}^2 = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[S_{\mathrm{G}}(i,j)]^2,$$

$$\sigma_B^2 = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[S_B(i,j)]^2,$$

$$\sigma^2 = 0.301 \times \sigma_R^2 + 0.586 \times \sigma_G^2 + 0.113 \times \sigma_B^2. \quad (8)$$

有关此图像退化算法的性能将在第 5 节中进行分析.

3.3. 基于信息熵划分的彩色图像退化算法

3.3.1. 基于信息熵的图像划分

信息熵在信息论中是用来描述信源所能发出的平均信息量,当信息熵越大时,表明信源所发出的信息量越多. 对于图像来说,我们可以利用信息熵来衡量一幅图像的复杂程度,当熵值越大时,所包含的信息量越多,则这时的图像变化越复杂;当熵值越小时,所包含的信息量越少,则这时的图像越平滑. 因此,我们可以利用以上原理对图像进行划分,对于灰度图像的一个像素来说,一般情况下有 0, 1, 2,…,255 共 256 个灰度值,其对应的出现概率分别为 p_0, p_1, p_2,…, p_{255},则一幅灰度图像信息源所对应的熵值[1]为

$$H = -\sum_{i=1}^{256} p_i \log_2 p_i. \quad (9)$$

而对于彩色图像来说,由于其所对应的三个颜色分量(R,G,B)之间具有相关性,因此,不能单一的应用三个颜色分量信息熵的平均值作为彩色图像的信息熵,而是应该根据 R,G,B 的线性组合来定义,因此,我们有

$$H_R = -\sum_{i=1}^{256} p_i^R \log_2 p_i^R,$$

$$H_G = -\sum_{i=1}^{256} p_i^G \log_2 p_i^G,$$

$$H_B = -\sum_{i=1}^{256} p_i^B \log_2 p_i^B,$$

$$\overline{H} = 0.301 \times H_R + 0.586 \times H_G + 0.113 \times H_B, \quad (10)$$

则这时相应的彩色图像划分算法如下.

1)把彩色图像按 $n \times n$ 进行分块,例如可以分成 4×4,8×8 的图像块,同时分成 R,G,B 三个颜色分量所对应的灰度图像.

2)统计三个颜色分量的各个图像块内各种像素值出现的概率 p_i, $i = 0, 1, 2, \cdots, 255$.

3)根据(10)式先分别求出 R,G,B 图像块的对应熵值,然后再求彩色图像对应块的熵值.

4)设定阈值 H_s,根据每个图像块的熵值来划分一幅彩色图像,当 $H_i \geqslant H_s$ 时,图像块被划分在一类,当 $H_i < H_s$ 时则划分在另一类.

其中阈值 H_s 的大小由人为设定,这样可以控制图像区域的划分. 例如,对于 8×8 的图像块来说,可以取信息熵阈值 H_s 为 4.5(最大信息熵的 75%),则信息熵大于等于 4.5 的像素块为一个区域,而小于 4.5 的为另一个区域.

3.3.2. 应用信息熵划分的彩色图像退化算法

基于以上分析,我们可以根据一幅图像中像素块的信息熵大小来划分图像的区域,并对选取出的某个区域进行加密. 由于信息熵越大,图像所包含的信息量越多,而信息熵越小,图像中所包含的信息量越少,因此我们选择信息熵 H 小于某个阈值的区域进行加密,这样可以有效地保留图像中主要的部分,而隐藏掉图像的平滑区域和次要部分,达到退化的目的. 因此,我们定义的算法如下.

1)对于一幅彩色图像,按 3.3.1 节中的方法先对图像进行划分,把图像分成两个区域.

2)把信息熵小于阈值 H_s 的区域中的像素提取出来.

3)按照 3.1 节中的方式对提取出的像素进行加密,得到最终的退化图像.

应用此彩色图像退化算法可以很好地退化一幅图像中不重要的部分,而保留住图像中主要的信息,其中阈值 H_s 的选取特别关键,同时,对于选取不同的阈值,得到的退化图像也不相同. 有关算法的性能分析将在第 5 节中讨论.

4. 两种退化算法的具体实现及其结果

根据 3 节中有关基于选择加密的并行彩色图像退化算法的具体设计,我们对两种方法进行仿真实验,其中需要退化的测试图像选择标准的 USC-SIPI 图像数据库(http://sipi.usc.edu/database/)中的彩色图像(图 3, 128×128),密钥设置如 $p = 7$, $q = 3$, $a = 35$, $b = 3$, $c = 28$, $x = -10.058$, $y = 0.368$, $z = 37.368$. 同时,对于基于随机选择模板的彩色图像退化算法,百分比阈值设为 50%,而对于基于信息熵划分的彩色图像退化算法,信息熵阈值设为图像块最大信息熵的 90%(4×4 分块). 则算法仿真结果如图 4 和图 5 所示.

图 3 退化测试用标准图像(源自 USC-SIPI 图像数据库)

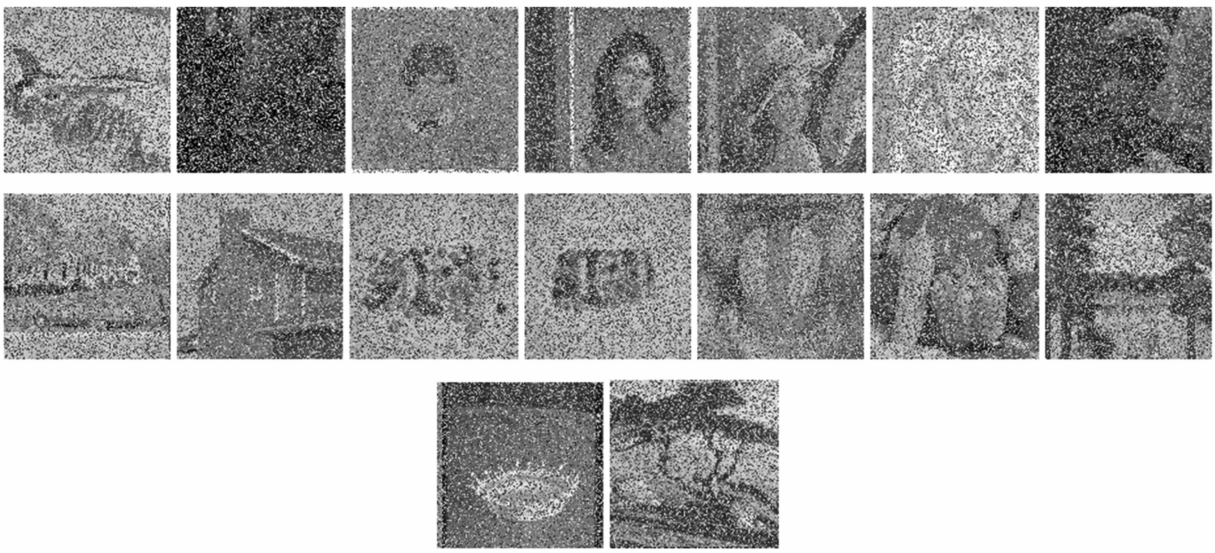

图 4 基于随机选择模板算法的退化图像

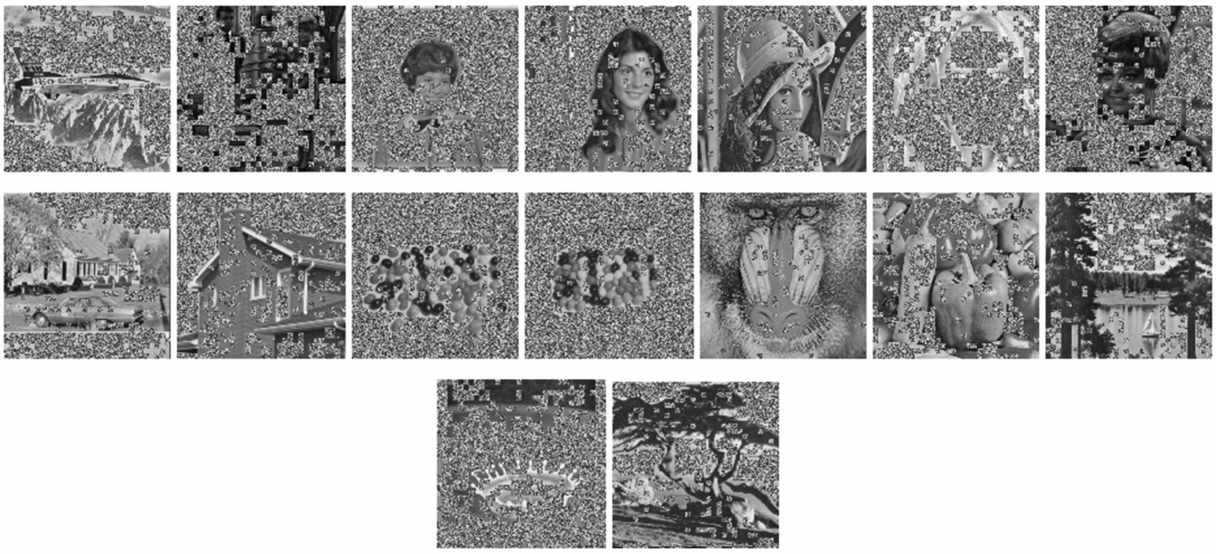

图 5 基于信息熵划分算法的退化图像

从图 4 和图 5 中可以看出,由于根据不同的方式选择了加密的区域,因此图像都出现了不同程度的退化. 基于随机选择模板的彩色图像退化算法使彩色图像看起来像嵌入了随机的噪声,而基于信息熵划分的彩色图像退化算法则加密了图像的部分区域,保留了图像的重要信息. 因此,两种退化算法都能达到商业退化的目的,即在保留数字图像的主要信息后,使图像变的粗糙、模糊,而只有当获得对应的密钥后才能看到清晰的图像(如图 6).

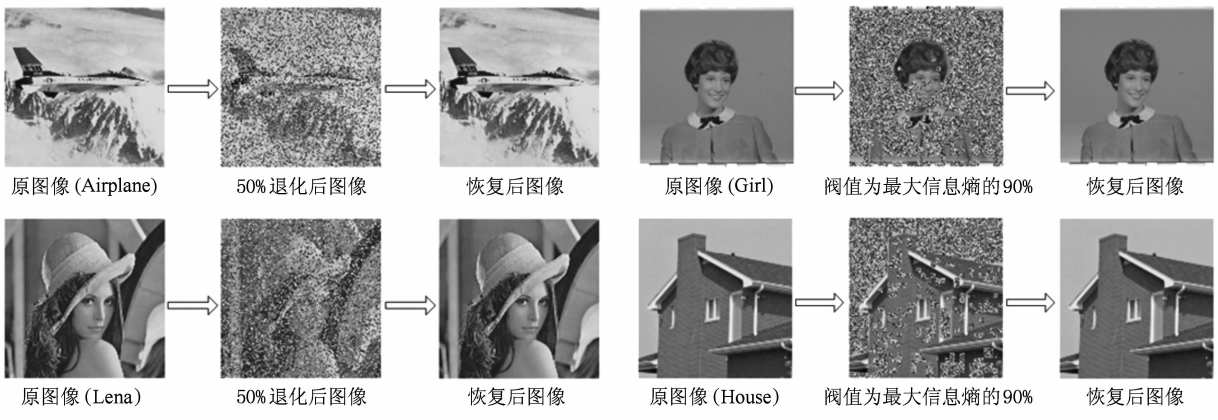

图 6　退化图像及其所对应的恢复图像

5. 两种退化算法的性能分析

5.1. 退化算法阈值选取分析

对于基于随机选择模板的退化算法来说,阈值即为选择加密所占像素的比例,我们可以随机选择图像中 20% ,40% ,50% 和 60% 的像素进行退化加密,并求得其对应的 Power Signal-to-Noise Ratio(PSNR)值,结果如下,其中 PSNR 的求解应该考虑为三个颜色分量的线性组合(R,G,B):

$$\mathrm{PSNR} = 10 \times \log\left(\frac{255^2}{\mathrm{MSE}}\right),$$

$$\mathrm{MSE}(\mathrm{R}) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[S(\mathrm{R})(i,j) - S'(\mathrm{R})(i,j)]^2}{\mathrm{framesize}(MN)},$$

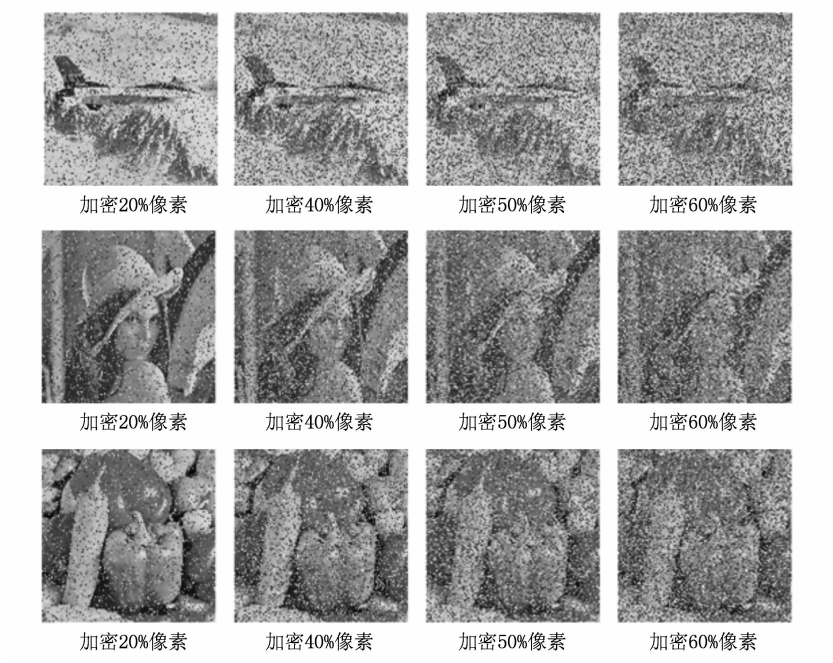

图 7　不同阈值下的退化图像(基于随机选择模板的退化算法)

$$\mathrm{MSE(G)} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[S(\mathrm{G})(i,j) - S'(\mathrm{G})(i,j)]^2}{\mathrm{framesize}(MN)},$$

$$\mathrm{MSE(B)} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[S(\mathrm{B})(i,j) - S'(\mathrm{B})(i,j)]^2}{\mathrm{framesize}(MN)},$$

$$\mathrm{MSE} = 0.301 \times \mathrm{MSE}(R) + 0.586 \times \mathrm{MSE(G)} + 0.113 \times \mathrm{MSE(B)}. \quad (11)$$

从表4中可以看出,当加密彩色图像的像素越多时,图像对应的PSNR值越小.特别地,通过计算每幅图像PSNR所对应的差值(ΔPSNR),我们可以发现当加密40%以下像素时,ΔPSNR > 1dB,而加密40%以上像素时,ΔPSNR < 1dB,同时,从图7中也可以观察到,当加密40%以上像素时,图像出现严重的退化效果,图像变的非常粗糙.因此,加密百分比至少设置在40%左右可以认为是较为合理的阈值.

对于基于信息熵划分的退化算法来说,阈值即为图像块最大信息熵的比例,在此我们设定测试阈值为图像最大信息熵的65%,70%,75%,80%和90%,同时,应用(11)式分别计算对应的PSNR值,测试结果如图8所示.

表4 不同阈值下三幅图像(Airplane, Lena, Peppers)退化后所对应的PSNR值(基于随机选择模板的退化算法)(dB)

	10%	20%	30%	40%	50%	60%	70%	80%
Airplane	17.8925	15.0089	13.1997	11.9213	10.9841	10.2205	9.5261	8.9531
Lena	18.3338	15.4334	13.5790	12.3906	11.4202	10.6183	9.9313	9.3591
Peppers	18.1259	15.0167	13.1556	12.0063	11.0559	10.2370	9.5697	8.9927

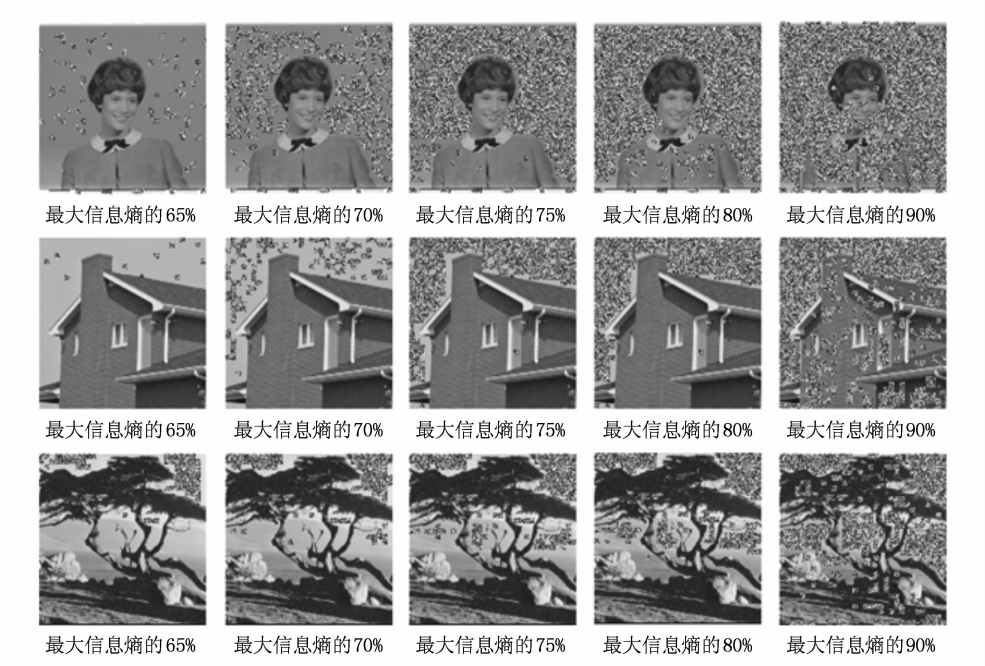

图8 不同阈值下的退化图像(基于信息熵划分的退化算法)

表5 不同阈值下三幅图像(Girl, House, Tree)退化后所对应的PSNR值(基于信息熵划分的退化算法)(dB)

	65%	70%	75%	80%	85%	90%
Girl	21.4827	14.9737	12.8575	12.3442	11.8516	11.2746
House	28.4535	17.8806	14.1713	13.7806	13.3135	11.6569
Tree	18.3262	16.9374	15.6140	14.7910	13.9086	11.9623

从表5中我们可以得出这样的结论,当信息熵阈值设定越大时,即我们所设定的阈值为最大信息熵的比例越大时,彩色图像所对应的PSNR值越小.特别地,通过计算每幅图像PSNR所对应的差值(ΔPSNR),我们可以发现当信息熵阈值小于最大信息熵的75%时,ΔPSNR > 1dB,而当信息熵阈值大于

最大信息熵的 75% 时,一般来说,$\Delta PSNR < 1dB$,同时,通过观察图 8 中的退化变化,我们也可以发现同样的现象,即所设定的信息熵阈值大于最大信息熵的 75% 时,退化图像除主要信息外其他部分变得非常模糊和粗糙. 所以,信息熵阈值至少设定为最大信息熵的 75% 左右可以认为是比较合理的选择.

5.2. 视觉影响测试

为了测试退化图像对用户视觉的直接影响,我们随机找到 22 名高中程度以上的用户进行主观评价,即在不告诉原图像的情况下,对被测图像进行主观视觉判断. 其中被测图像为图 7 和图 8 中的彩色退化图像,而评价标准为国际上通行的 5 级评分尺度,如表 6,则我们可以得到表 7 和表 8 所示的测试结果.

表 6　主观评价标准

妨碍尺度	得分	品质尺度
无察觉	5	非常好
刚察觉	4	好
察觉但不讨厌	3	一般
讨厌	2	差
难以观看	1	非常差

表 7　对图 7 中退化图像的主观评价

	Airplane				Lena				Peppers			
	20%	40%	50%	60%	20%	40%	50%	60%	20%	40%	50%	60%
非常好												
好	5				11				11			
一般	11	5			8	11			11	16		
差	6	15	5		2	11	14	4		6	13	3
非常差		2	17	22			8	18			9	19
得分	65	47	27	22	69	55	36	26	77	60	35	25

表 8　对图 8 中退化图像的主观评价

	Gir					House					Tree				
	65%	70%	75%	80%	90%	65%	70%	75%	80%	90%	65%	70%	75%	80%	90%
非常好	11					20	3				13	8			
好	9	16	5			2	15	9	4	1	5	9	10	2	1
一般	2	6	14	7	3		4	13	8	7	4	5	10	10	7
差			3	15	15				10	4			2	10	11
非常差					4					10					3
得分	97	82	68	51	43	108	87	75	60	43	97	91	74	58	50

从表 7 中可以看到,对于基于随机选择模板的退化算法来说,当加密百分比设置在 40% 左右时,退化图像会给测试人员带来一定的视觉影像,但一般情况下,测试人员依然可以观察出图像的主要信息,而当退化百分比逐渐增大时,视觉影响会越来越强. 而从表 8 中可以看出,对于基于信息熵划分的退化算法来说,当信息熵阈值设定在最大信息熵的 75% 左右,特别是 70%—75% 时,视觉影响比较合适,可以认为此时退化出的图像是令人满意的退化图像. 因此,从以上数据可以看出,5.1 节中的分析是符合退化应用的.

5.3. 退化算法的密码学分析

从两种退化算法的结构可以看出,退化算法的安全性主要依赖于所应用的 Z 矩阵和三维 Chen 系统. 对于广义 Z 矩阵映射来说,由于它具有较好的周期性,因此能够很好地应用于图像加密. 特别地,由于是三维矩阵,所以 Z 矩阵映射可以对彩色图像的三个颜色分量实现并行处理,这样可以提高加密的效率. 而 Chen 系统则是近年来应用较为广泛的一种混沌系统,它可以被利用来产生加密所需要的混沌序列,由于 Chen 系统具有良好的动力学特征,因此它可以有效地保证所产生序列的随机性.

同时,从密钥空间的大小来考虑,假设只设定 Chen 系统的初始值为退化密钥,且数字的精度为 10^{-15},则密钥空间大小为 10^{45},而此时的这个密钥空间已经非常大. 当把 Chen 系统和 Z 矩阵的参数 (p, q, a, b, c) 均看作密钥时,则这时的密钥空间足以抵抗任何暴力攻击和密钥空间穷举搜索.

5.4. 彩色图像滤波攻击测试

对于应用了以上两种退化算法的退化图像来说,由于只是在图像空间中选择了部分像素进行加密退化,因此可以把其看成是加入了噪声(尤其是第一种退化方式),而对于噪声的成熟攻击方法就是去噪技术,文献[17—19]分别介绍了三种常用的图像滤波方法:均值滤波、中值滤波和维纳滤波. 图 9和图 10 分别给出了两种退化算法被三种滤波攻击后的效果图,表 9 和表 10 利用(11)式给出了对应的 PSNR 值,其中退化图像取自图 4 和图 5.

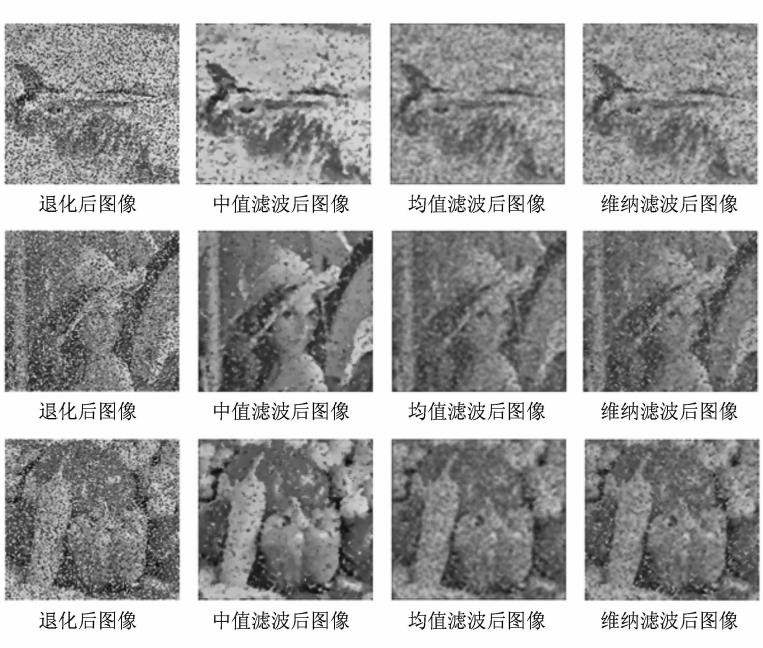

图 9 对退化后图像的滤波攻击(基于随机选择模板的退化算法)

表 9 各种滤波攻击所对应的 PSNR 值(基于随机选择模板的退化算法)(dB)

	退化后	中值滤波后	均值滤波后	维纳滤波后
Airplane	10.9841	16.4476	14.7841	14.6213
Lena	11.4202	17.6604	15.8734	15.3620
Peppers	11.0559	17.1742	15.2130	14.8389

对于基于随机选择模板的退化算法来说,从图 9 和表 9 中可以看出,三种滤波方式对于退化图像来说有一定的平滑效果,PSNR 值也有一定的提高,特别是中值滤波方式可以得到相对理想的滤波效果. 但是图像的整体质量并没有得到明显的提高,图像的细节和边缘信息也有不同程度的丢失,因此,可以认为此退化算法可以相对有效地抵抗滤波攻击.

而对于基于信息熵划分的退化算法来说,从图 10 和表 10 可以得到如下结论:三种滤波攻击对退化后的图像都能产生平滑效果,但平滑的作用微乎其微,这主要是因为此退化算法是对部分区域进行加密退化,而不是对单个像素进行处理. 同时,我们可以看出,三种滤波攻击后的效果几乎相同,即通过任何一种攻击都不会明显提高图像的质量. 因此,基于信息熵划分的退化算法能更加有效地抵抗滤波攻击.

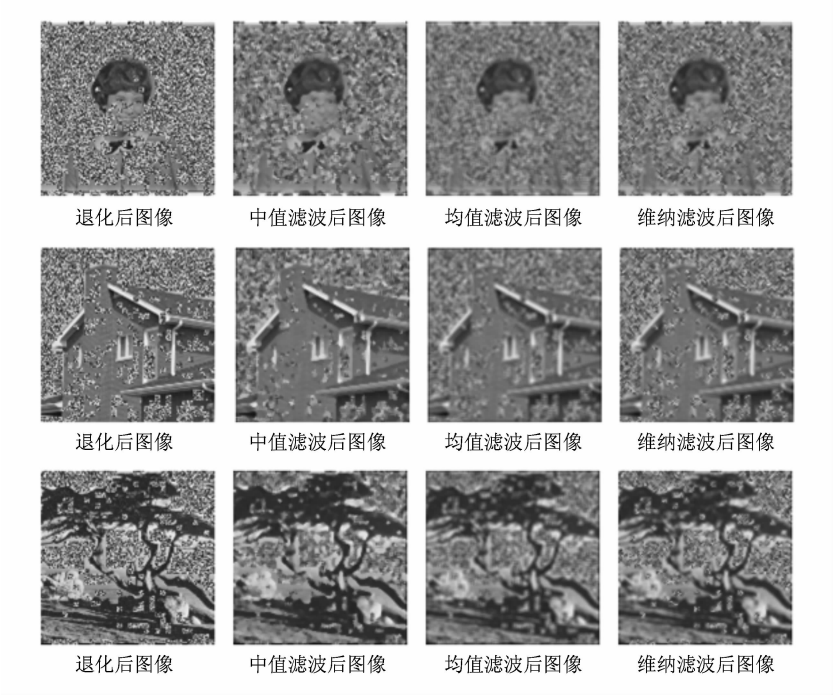

图 10　对退化后图像的滤波攻击(基于信息熵划分的退化算法)

表 10　各种滤波攻击所对应的 PSNR 值(基于信息熵划分的退化算法)(dB)

	退化后	中值滤波后	均值滤波后	维纳滤波后
Girl	11.2746	15.2891	17.1556	16.4312
House	11.6569	14.3053	14.8301	14.0646
Tree	11.9623	13.7384	13.8360	13.3087

5.5. 彩色图像平均攻击测试

对于退化后的图像来说,我们可以定义如下等式:

$$g(x,y) = f(x,y) + \sigma(x,y), \tag{12}$$

其中 $g(x, y)$ 为退化后图像,$f(x, y)$ 为原始图像,$\sigma(x, y)$ 为加入的退化信息. 这样,我们可以利用平均处理的方式[20]来对退化后的图像进行攻击. 具体到彩色图像来说,即可对 K 幅采用不同密钥退化的彩色图像的各个色彩分量所对应像素进行平均,如下式:

$$\begin{aligned}
\bar{g}(\mathrm{R})(x,y) &= \frac{1}{K}\sum_{i=1}^{K} g_i(\mathrm{R})(x,y),\\
\bar{g}(\mathrm{G})(x,y) &= \frac{1}{K}\sum_{i=1}^{K} g_i(\mathrm{G})(x,y),\\
\bar{g}(\mathrm{B})(x,y) &= \frac{1}{K}\sum_{i=1}^{K} g_i(\mathrm{B})(x,y).
\end{aligned} \tag{13}$$

根据中心极限定理,当采用的退化图像副本(K)足够大时,可得到

$$\begin{aligned}
&\sum_{i=}^{K} g_i(\mathrm{R})(x,y) \sim N(K\mu_{\mathrm{R}}, K\sigma_{\mathrm{R}}^2)\\
\Rightarrow &\bar{g}(\mathrm{R})(x,y) \sim N\left(\mu_{\mathrm{R}}, \frac{1}{K}\sigma_{\mathrm{R}}^2\right),\\
&\sum_{i=1}^{K} g_i(\mathrm{G})(x,y) \sim N(K\mu_{\mathrm{G}}, K\sigma_{\mathrm{G}}^2)\\
\Rightarrow &\bar{g}(\mathrm{G})(x,y) \sim N\left(\mu_{\mathrm{G}}, \frac{1}{K}\sigma_{\mathrm{G}}^2\right),\\
&\sum_{i=1}^{K} g_i(\mathrm{B})(x,y) \sim N(K\mu_{\mathrm{B}}, K\sigma_{\mathrm{B}}^2)\\
\Rightarrow &\bar{g}(\mathrm{B})(x,y) \sim N\left(\mu_{\mathrm{B}}, \frac{1}{K}\sigma_{\mathrm{B}}^2\right),
\end{aligned} \tag{14}$$

即有

$$\begin{aligned}
E\left|\bar{g}(\mathrm{R})(x,y)\right| &= \mu_{\mathrm{R}} = f(\mathrm{R})(x,y),\\
E\left|\bar{g}(\mathrm{G})(x,y)\right| &= \mu_{\mathrm{G}} = f(\mathrm{G})(x,y),\\
E\left|\bar{g}(\mathrm{B})(x,y)\right| &= \mu_{\mathrm{B}} = f(\mathrm{B})(x,y).
\end{aligned} \tag{15}$$

以上理论分析表明,当退化图像副本(K)足够大,原图像是可以完全恢复出. 因此,对于两种彩色图像退化算法,我们分别随机选择不同的退化加密

密钥对图像进行退化,其中对于基于随机选择模板的退化算法,我们选择 USC-SIPI 图像数据库中的标准 Lena 彩色图像,而对于基于信息熵划分的退化算法,我们选择 USC-SIPI 图像数据库中的标准 Girl 彩色图像,测试结果如图 11 所示.

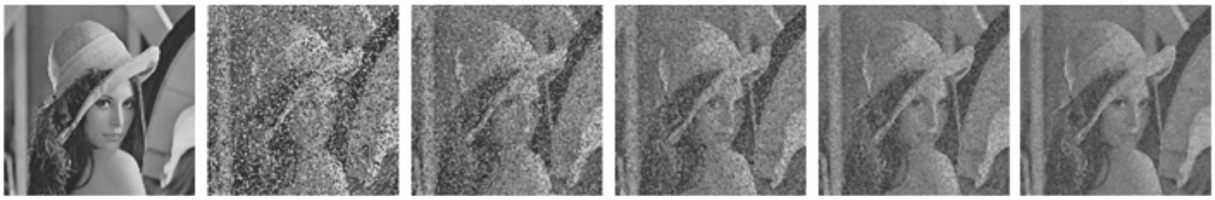

图 11 对退化后图像的平均攻击(基于随机选择模板的退化算法)

表 11 平均攻击所对应的 PSNR 值(基于随机选择模板的退化算法)(dB)

一次退化	两次退化平均	四次退化平均	八次退化平均	十六次退化平均
11.4202	13.6898	15.1459	16.4615	17.2653

从图 11 中可以看出(百分比阈值设为 50%),当对于同一幅原始图像进行平均攻击时,只要有足够的退化图像副本,就可以恢复出相对清晰的图像.但也可以看出,恢复出的图像相对于原始图像来说,变的更加暗淡,同时,图像的轮廓信息并不能恢复出来.而从表 11 中也可以看出,经过平均处理后的图像,其 PSNR 值也只能缓慢提高,且提高速度(ΔPSNR)越来越小.

从图12中可以看出(信息熵阈值为图像块最大信息熵的 90%),相对于基于随机选择模板的退化算法,应用基于信息熵划分的退化算法所得到的退化图像可以很好地抵抗平均攻击,即当给定一定的退化图像副本后,依然无法恢复出图像.因此,我们可以得出,对于基于信息熵划分的退化算法,即使图像的 PSNR 值得到提升,图像仍然非常粗糙、模糊.

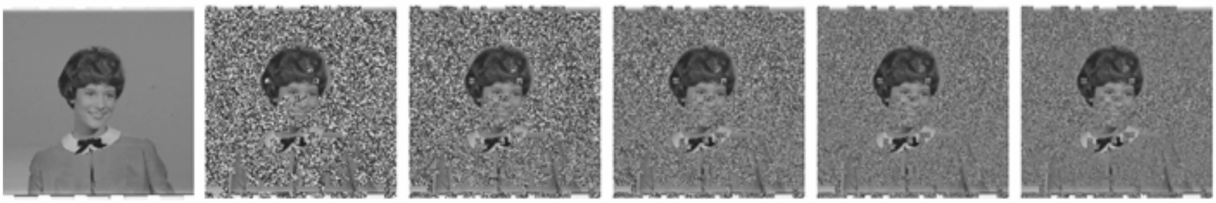

图 12 对退化后图像的平均攻击(基于信息熵划分的退化算法)

表 12 平均攻击所对应的 PSNR 值(基于信息熵划分的退化算法)(dB)

一次退化	两次退化平均	四次退化平均	八次退化平均	十六次退化平均
11.2746	12.8043	14.4969	16.5370	17.6894

5.6. 与 Marc[11] 位平面选择退化算法的比较和分析

Marc 在文献[11]中提出了一种用于退化的位平面选择加密算法.其原理是较高位的位平面包含更多的图像信息,而低位位平面则看起来很随机,因此,可以通过加密低位位平面的方法来实现图像退化,同时,通过实验发现对于灰度尺度的图像来说,至少需要加密 4 到 5 个位平面才能取得较好的退化效果.对于彩色图像,我们把其分成三个单独的色彩分量(R,G,B),然后应用 Marc 图像加密算法分别进行退化.图 13 和表 13 分别给出了 Marc 退化算法的实验效果和 PSNR 值.

从图13和表13中可以看出,当加密后4个bit

图 13　Marc 位平面选择退化算法

表 13　Marc 退化算法对于加密不同位平面所得到的 PSNR 值(dB)

	加密后 4 个平面	加密后 5 个平面	加密后 6 个平面	加密后 7 个平面
Airplane	31.6391	26.0501	19.8720	15.1591
Lena	31.6441	25.6934	19.8794	13.9579
House	31.9066	25.3704	20.0623	14.4029

平面时,由于图像的 PSNR 值依然大于 30 dB,图像不能达到退化的效果[21],而当加密到后 5 个 bit 平面时,通过观察,可以发现彩图图像才具有了较好的退化效果.因此,我们可以认为只有加密到后 5 个 bit 平面才能取得理想的退化,即对于理想退化效果来说,至少需要加密 62.5% 的 bit,而对于本文所提出的基于随机选择模板的退化算法来说(基于信息熵划分的退化算法根据图像的不同,加密 bit 数量也不同,但对于一般的图像,加密 bit 百分比也小于 62.5%),则只需要加密 40% 的 bit 就可以取得较好的退化.同时,对于 Marc 的退化算法,我们从表 13 还可以看出,当加密后 7 个 bit 平面,所得到的 PSNR 值才和基于随机选择模板退化算法加密 40% 的像素以及基于信息熵划分的退化算法所设定的信息熵阈值为最大信息熵的 75% 的 PSNR 值比较接近,而这时加密 bits 所占百分比为 87.5%.因此,我们可以看出 Marc 退化加密算法的效率在应用相同的加密机理的情况下要低于本文所提出的算法.

5.7. 其他性能分析

对基于信息熵划分的退化算法来说,由于图像块的信息熵与块的尺度($n \times n$)有直接关系,所以我们所选择的信息熵图像块的大小在整个退化算法中就有非常重要的意义,同时,为了测试 n 的取值与图像退化效果之间的关系,我们选取了 2×2, 4×4 和 8×8 的像素分块对算法进行测试(其中信息熵阈值为图像块最大信息熵的 90%),其结果如图 14 所示.

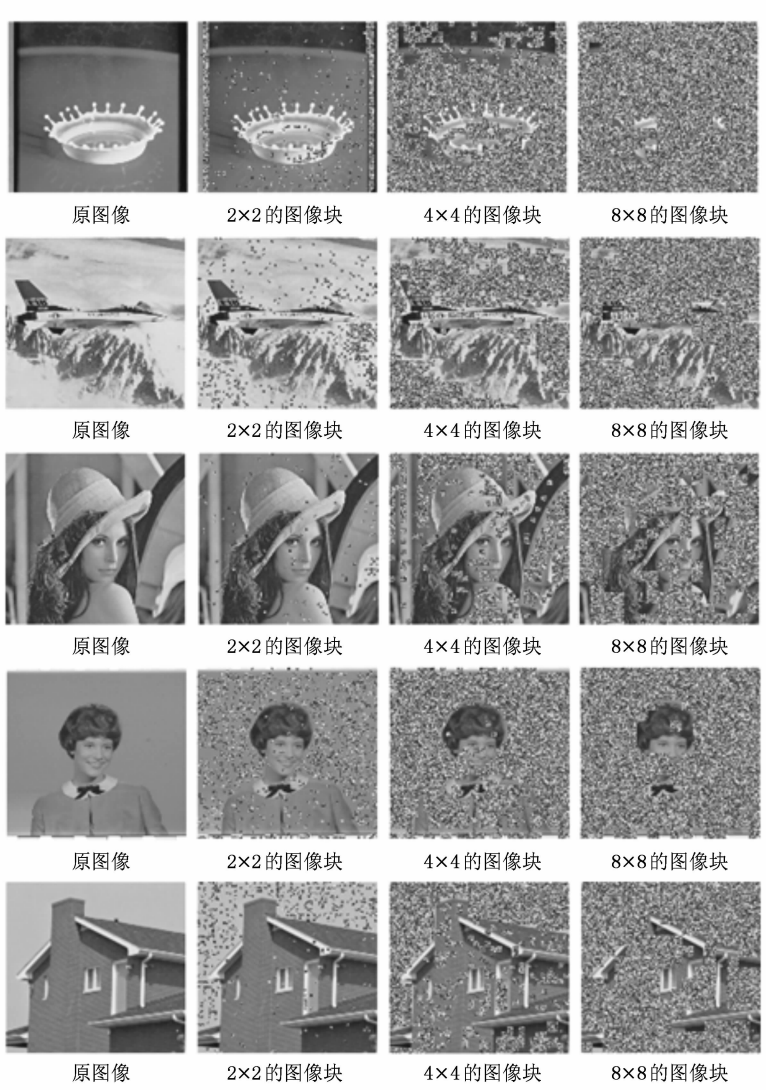

图 14 加密不同图像块所得到的退化图像

从图 14 中可以看出,当以 8 × 8 的图像像素块为单位进行退化加密,则图像大部分像素均被退化,其中许多主要信息都无法获得,这时可以认为图像未能达到退化的效果;而当以 2 × 2 的图像块为单位进行退化时,图像中被退化的部分明显不足,有太多需要加密的部分依然保留,此时,我们也可以认为退化图像仍然不能满足退化的目的. 因此,如果从视觉感和退化效果上进行折中,则应用 4 × 4 (如图 14)的图像块进行退化处理可以认为是比较理想的选择.

6. 结 论

图像退化加密是图像加密中的一个重要分支,尤其是最近几年,图像退化已逐步成为人们的研究热点. 本文首先提出一种三维 Z 矩阵映射,同时从理论和实验上证明了其良好的特性. 然后,根据实际情况提出了两种利用 Z 矩阵映射和选择加密方式的彩色图像退化算法,同时进行了仿真实验. 最后,对两种基于不同选择加密模板的彩色图像退化算法进行了实验分析,结果表明两种退化算法均能有效地抵抗各种攻击并产生良好的退化效果. 但是,我们也应该注意到,对于基于信息熵划分的图像退化算法来说,当退化图像包含的非平滑区较大时,图像退化的效果不是很理想(如图 5 中 Baboon),则我们需要对图像区域再进行细致地划分以确定对于任何图像都能有满意的退化效果,这将是我们后一步的研究工作.

[1] Zhang C T, Su Y T, Zhang J 2006 *Digital Image Compression Code* (Tsinghua University Press) p1 (in Chinese) [张春田、苏育挺、张　静 2006 数字图像压缩编码(清华大学出版社)第 1 页]
[2] Chen G R, Mao Y B, Chui C K 2004 *Chaos Soliton Fract.* **21** 749
[3] Guan Z H, Huang F J, Guan W J 2005 *Phys. Lett.* A **346** 153
[4] Lian S G, Sun J S, Wang Z Q 2005 *Chaos Soliton Fract.* **26** 117
[5] Sun F Y, Liu S T, Lü Z W 2007 *Chin. Phys.* **16** 3616
[6] Zhang X H, Yang Y T 2007 *Acta Electron. Sin.* **1** 34 (in Chinese) [张宪海、杨永田 2007 电子学报 **1** 34]
[7] Wu X Y, Liu H M, Huang J W 2007 *Acta Auto. Sin.* **2** 145 (in Chinese) [吴晓云、刘红梅、黄继武 2007 自动化学报 **2** 145]
[8] Gao L J, Yang X P, Li Z L, Wang X L, Zhai H C, Wang M W. 2009 *Acta Phys. Sin.* **58** 1053 (in Chinese) [高丽娟、杨晓苹、李智磊、王晓雷、翟宏琛、王明伟 2009 物理学报 **58** 1053]
[9] Raphael C W 2008 *Phan. Pattern Recognition* **41** 3493
[10] Wang X Y, Xu Z H, Yang H Y 2009 *Exper. Sy. Ap.* **36** 9056
[11] Droogenbroeck M V, Benedett R 2002 *proceedings of ACIVS* **2002** 90
[12] Qi D X, Zou J C, Han X Y 2000 *Sci. China* E (*China*) **43** 304
[13] Gu Q P 2002 *J. Jianghan University* (*Natura*l *Science*) **19** 28 (in Chinese) [辜青萍 2002 江汉大学学报(自然科学版) **19** 28]
[14] Xing F C 2003 *J. the CUN* (*Natural Sciences Edition*) **12** 207 [邢富冲 2003 中央民族大学学报(自然科学版) **12** 207]
[15] Zou J C, Tie X J 2001 *J. North China University Technol.* **1** 10 (in Chinese) [邹建成、铁小匀 2000 北方工业大学学报 **1** 10]
[16] Jiao H L, Chen G 2003 *Journal of Software* **14** 864 (in Chinese) [焦华龙、陈　刚 2003 软件学报 **14** 864]
[17] Davis L S, Rosenfeld A 1978 *IEEE Trans. Systems, Man and Cybernetics* **SMC-7** 705710
[18] Lee J S 1980 *IEEE Trans. on Pattern Analysis and Machine Intelligence* **4** 286
[19] Zhang Y W 1980 Wiener and Kalman Filtering Theory Introduction (Pearson Education Press) p1 (in Chinese) [张有为 1980 维纳与卡尔曼滤波理论导论(人民教育出版社)第 1 页]
[20] Gonzalez R C, Woods R E 2002 *Digital Image Processing* (*Second Edition*) Pearson Education Asia. p88
[21] Qi X J, Qi J 2007 *Signal Proc.* **87** 1264

Color image degradation algorithms based on *Z*-matrix map and selective encryption*

Zhao Liang†　Liao Xiao-Feng　Xiang Tao　Xiao Di

(*College of Computer Science Chongqing University*, *Chongqing* 400044, *China*)

(Received 8 April 2009; revised manuscript received 14 July 2009)

Abstract

With the development of information technology and network, multimedia protection has become a major concern, in which images are the important research objects. Especially, the image degradation is one of basic fields. This paper introduces a three-dimensional *Z*-matrix map which can be used for encryption, and shows its satisfactory property. Then, two color image degradation algorithms based on different templates for selective encryption are proposed. Finally, the performance and security of them are analyzed. Simulation results indicate the reliability of these schemes.

Keywords: *Z*-matrix, selective encryption, chaotic encryption, color image degradation

PACC: 0545

* Project supported by the National Natural Science Foundation of China (Grant No. 60703035), the Program for New Century Excellent Talents in University of China (Grant No. NCET-08-0603), the National Science Foundation for Post-doctoral Scientists of China (Grant No. 20080430741), the Natural Science Foundation of Chongqing, China (Grant Nos. 2008BB2182, 2008BB2193), the Natural Science Foundation Project of Chongqing, China (Grant No. CSTC2009BA2024), and the Postgraduate Technology Innovation Foundation of Chongqing University, China (Grant No. 200903A1B0010303).

† Corresponding author. E-mail: zhaoliang@cqu.edu.cn; zhaoliang_916@163.com