基于三维混沌系统的彩色图像加密新算法

张 燕,黄贤武,刘家胜
ZHANG Yan,HUANG Xian-wu,LIU Jia-sheng

苏州大学 电子信息学院,江苏 苏州 215021
School of Electronics and Information Engineering,Soochow University,Suzhou,Jiangsu 215021,China

ZHANG Yan,HUANG Xian-wu,LIU Jia-sheng.New encryption scheme for color images based on 3D chaotic system. Computer Engineering and Applications,2008,44(20):202-205.

Abstract: The 1D chaotic image encryption method is reported with appropriate performances by using the appropriate complexity,pseudo-randomness and extreme parameter sensitivity of chaotic sequences but with smaller key space as its serious drawback compared with others.So,a new image encryption method based on 3D chaotic system is proposed in this paper, which can not only increase secret key space,but also tone up ability to deciphering.And in this paper,the pixel value of cipher-image used to get secret key and the feedback used in encryption process improve greatly the performances of the diffusion function.The method is proved to work well by the result,because of its larger secret key space and high speed of encryption and so on.

Key words: 3D chaotic system;chaotic sequence;image encryption

摘 要:一维混沌加密算法由于利用了混沌序列的良好复杂性、伪随机性和对初值的敏感特性而具有较好的加密性能,但与其它方法比较,其缺点是密钥空间较小。为此,提出了一种基于三维混沌系统的图像加密新方法,扩大了密钥空间,提高了加密系统的抗破译强度。通过在密钥发生器中嵌入密文像素值,在加密过程中引入反馈加密法,使得扩散函数的影响得到了进一步的加强。实验结果表明,算法具有密钥空间大,加密速度快及效果好等优点。

关键词:三维混沌系统;混沌序列;图像加密
DOI:10.3778/j.issn.1002-8331.2008.20.061 **文章编号:**1002-8331(2008)20-0202-04 **文献标识码:**A **中图分类号:**TP391

1 引言

随着计算机、网络和通信技术的飞速发展,特别是 Internet 的普及,数字图像加密技术[1]越来越受到人们的重视。但由于传统的对称和非对称加密算法(比如 DES[2]、3DES 和 RSA 算法)主要针对文本信息,在设计算法时不考虑数据的膨胀,不适合用来加密数字图像。因此,许多新的数字图像加密方案(比如秘密共享[3]、双随机相位编码和混沌图像加密方案[4,5]等)得到了广泛的研究和应用。

目前,对彩色图像的加密大多都采用基于(k,n)秘密共享的加密算法($1\leqslant k\leqslant n$),其主要思想是将原始图像加密分解成 n 份同样尺寸、类似噪音一样的子图像,然后把这 n 份子图像通过网络传输到接收端,在接收端则至少需要 k 份这样的加密子图像才能恢复原始图像。这种算法的优点在于个别子图像的泄漏不至于引起原始图像的泄漏,而个别子图像的损失也不至于影响原始图像的恢复,算法简单直观,安全性好,具有较好的抗干扰性能,因此,采用这种加密方法加密彩色图像理论上是可行的。而实际上这种算法存在着一个很严重的缺点,就是会使得图像数据量发生膨胀,这在图像数据本来就很大的情况下给图像的网络传输带来了巨大的困难,限制了这种加密算法在实际中的应用。所以本节在考虑到这个问题的基础上,提出了一种基于三维混沌系统的彩色图像加密新算法,既能扩大密钥空间,提高加密系统的抗破译强度,又能弥补基于秘密共享加密算法的缺陷。

2 基于三维混沌系统的彩色图像加密/解密算法设计

2.1 算法思想

一幅 24 位的真彩色图像由 RGB 三原色组成,可以表示为 $M\times N\times 3$ 三维数组的形式,且相邻像素的三原色值在空间域上具有很强的相关性。所以,本文所采用的方法就是利用混沌系统产生的密钥序列分别作用于 RGB 三原色,扰乱三原色在空间域中的相关性,从而使得原彩色图像变成一幅杂乱无章的图像,达到良好的加密效果。

2.2 密钥产生

目前被广泛研究的一维混沌系统为 Logistic 映射,即

$$f_{k+1}=uf_k(1-f_k) \tag{1}$$

其中,$0\leqslant u\leqslant 4$ 称为分枝参数,$f_k\in(0,1)$。混沌动力系统的研究

作者简介:张燕(1982-),女,硕士研究生,主要研究方向:图像处理,视频处理;黄贤武,男,教授,博导,主要研究方向:数字图像处理,模式识别等;刘家胜,男,博士,主要研究方向:信息安全,小波分析等。

收稿日期:2007-10-09 **修回日期:**2008-01-15

工作指出，当 3.569 945 6 时，Logistic 映射处于混沌状态。

本文所采用的三维混沌系统[8]的形式如下：

$$\begin{cases}\dot{x}=a(y-x)\\ \dot{y}=(c-a)x-xz+cy\\ \dot{z}=xy-bz\end{cases}\tag{2}$$

其中，a、b、c 为参数。当 a=35，b=3，$c\in$[20，28，4]时，系统处于混沌状态，如图 1 所示。即初始条件 x_0、y_0、z_0在三维混沌系统的作用下所产生的序列$\{x_k,y_k,z_k;k=0,1,2,\cdots\}$是非周期的、不收敛的，并对初始值非常敏感。实验结果表明，由此产生的混沌序列值随着重复次数的增加而增加，最后会超出计算机的精度范围。由于从彩色图像中提取出的 R 色、G 色和 B 色的取值范围都是 0~255。因此，就需要对所产生的密钥作适当的修正。所采用的方法为：

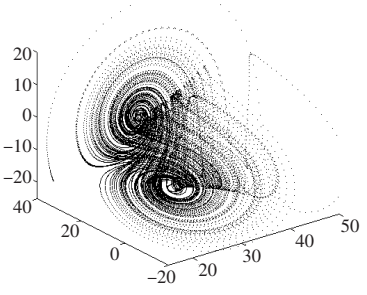


图 1　三维超混沌吸引子

$$\begin{cases}x=fabs(x)-round(fabs(x))\\ y=fabs(y)-round(fabs(y))\\ z=fabs(z)-round(fabs(z))\end{cases}\tag{3}$$

其中，$fabs(x)$是 x 的绝对值，$round(x)$是取 $fabs(x)$靠近零的整数。经过这样处理后，所产生的混沌序列值$\{x_k,y_k,z_k;k=0,1,2,\cdots\}\in(0,1)$。

另外，本文为了增强抗破译强度还将扩散函数的思想应用到密钥当中，将密文中的像素值嵌入到密钥发生器当中，其具体的形式为：

$$\begin{cases}x=(fabs(x)-round(fabs(x))+(K_R\oplus(256*f_{k+1}))/256)\bmod 1\\ y=(fabs(y)-round(fabs(y))+(K_G\oplus(256*f_{k+1}))/256)\bmod 1\\ z=(fabs(z)-round(fabs(z))+(K_B\oplus(256*f_{k+1}))/256)\bmod 1\end{cases}\tag{4}$$

其中，K_R、K_G和 K_B分别表示密文中一个像素的 R、G 和 B 分量值，是 Logistic 映射(式(1))所产生的混沌序列值。由式(4)可见，通过将密文当中的像素分量 R、G 和 B 值嵌入到密钥发生器中，可以达到大大增强扩散函数影响的目的，将密文当中每一位像素的影响扩散到整个密文当中去。

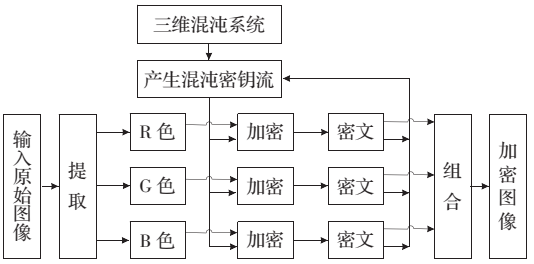
2.3　加密/解密算法

对一幅大小为 $M\times N\times 3$ 的 24 位真彩色图像进行加密/解密处理的统框图如图 2 所示，具体过程描述如下：

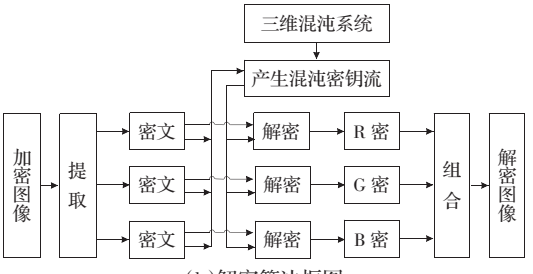
2.3.1　加密过程

步骤 1　输入原始图像 $I'_{M\times N}$，混沌系统初始值 x_0、y_0和 z_0。

步骤 2　利用三维混沌系统生成混沌序列$\{x_k,y_k,z_k;k=0,1,2,\cdots\}$，取该序列的某连续片断(如 1 000<$k\leqslant$1 000+3$MN$)，该片断元素个数为 3$MN$。同时利用上述(式(4))密钥产生法生成最终用来加密图像的混沌序列$\{x_k,y_k,z_k\}$。



(a)加密算法框图



(b)解密算法框图

图 2　彩色图像加/解密算法框图

步骤 3　利用生成的混沌序列$\{x_k,y_k,z_k\}$来加密原始图像 $I'_{M\times N}$，具体加密方法如下：

$$\begin{cases}k_x=fabs(x)-round(fabs(x))\\ k_y=fabs(y)-round(fabs(y))\\ k_z=fabs(z)-round(fabs(z))\end{cases}\tag{5}$$

$$\begin{cases}K'_R=((K_R+(K'_{R-1})^2+256*k_x)\bmod 256)\oplus\\ \qquad(256*f_{k+1})\oplus K'_{G-1}\oplus K'_{B-1}\\ K'_G=((K_G+(K'_{G-1})^2+256*k_y)\bmod 256)\oplus\\ \qquad(256*f_{k+1})\oplus K'_{R-1}\oplus K'_{B-1}\\ K'_B=((K_B+(K'_{B-1})^2+256*k_z)\bmod 256)\oplus\\ \qquad(256*f_{k+1})\oplus K'_{G-1}\oplus K'_{R-1}\end{cases}\tag{6}$$

其中，K_R、K_G和 K_B分别表示待加密像素点的 R、G 和 B 分量值，K'_R、K'_G和 K'_B分别表示已加密像素点的 R、G 和 B 分量值，K'_{R-1}、K'_{G-1}和 K'_{B-1}分别表示前一个加密像素点的 R、G 和 B 分量值。

步骤 4　输出加密图像 $I'_{M\times N}$。

2.3.2　解密过程

步骤 1　输入加密图像 $I'_{M\times N}$，与加密过程相同的混沌系统初始值 x_0、y_0和 z_0。

步骤 2　同加密过程的步骤 2，生成与其相同的混沌序列 x_t、y_t和 z_t。

步骤 3　利用生成的混沌序列$\{x_t,y_t,z_t\}$来解密原始图像 $I'_{M\times N}$，具体解密方法如下：

$$\begin{cases}K_R=((K'_R\oplus(256*f_{k+1})\oplus K'_{G-1}\oplus K'_{B-1})-(K'_{R-1})^2-\\ \qquad 256*k_x+256)\bmod 256\\ K_G=((K'_G\oplus(256*f_{k+1})\oplus K'_{R-1}\oplus K'_{B-1})-(K'_{G-1})^2-\\ \qquad 256*k_y+256)\bmod 256\\ K_B=((K'_B\oplus(256*f_{k+1})\oplus K'_{G-1}\oplus K'_{R-1})-(K'_{B-1})^2-\\ \qquad 256*k_z+256)\bmod 256\end{cases}\tag{7}$$

步骤 4 输出解密图像。

3 实验结果及分析

3.1 实验结果

在 VC++6.0 编程环境下利用本文提出的加密算法对一幅 24 位真彩色图像进行了加密和解密实验，设置参数分别为 a=35,b=3,c=28，设置系统初始值分别为 x_0=0.258,y_0=0.368,z_0=0.568,图像加密解密效果如图 3。

由图 3 可见,由于混沌序列对初始值非常敏感,即使初始值有微小的变化也无法对图像进行正确解密。

3.2 分析

3.2.1 密钥空间

一个好的加密方案应该使其密钥空间足够大从而使得强行攻击不可行。在本文提出的加密算法中,三维超混沌系统的初始值用作密钥,其精度为 10^{-16},因此密钥空间可达 10^{48}。另外,在密钥生成算法中还用到了 Logistic 混沌映射,它的初始值也作为密钥的一部分,因此本方案密钥空间得到了进一步增大(可达 10^{54}),可以更加有效地抵抗恶意攻击。

3.2.2 密钥敏感性测试

一个典型的密钥敏感性测试按照下列步骤来执行:

(1)首先,使用混沌初始值 x_0=0.258,y_0=0.368,z_0=0.568 加密一幅 24 位真彩色图像。

(2)然后,分别改变上述三个混沌初始值(在其中两个值保持不变得情况下,对第三个值进行微小的改变,比如x_0=0.258 000 000 000 000 1,y_0=0.368,z_0=0.568)加密同样一幅 24 位真彩色图像。

(3)最后,将以上两幅加密后的图像进行比较。

其实验结果如图 4 所示。

由图 4 可见,即使混沌系统初始值有微小的变化也会得到完全不同的加密图像,图 4(d)、(f)、(h)为密钥有微小差别的两幅加密图像的差。

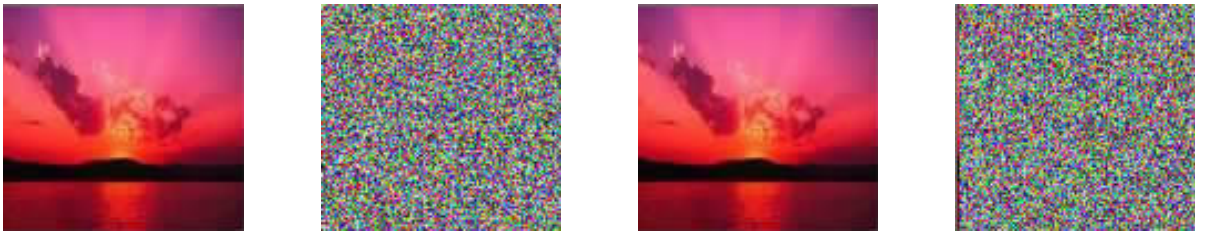
3.2.3 直方图

从一幅 24 位真彩色图像及其加密图像中,分别提取出 R、G 和 B 分量,然后计算它们的直方图(图 5)。从图 5 可以看出,密文的 R、G 和 B 分量的直方图很均匀，且在很大程度上不同于原始图像的 R、G 和 B 分量的直方图。

3.2.4 UACI 和 NPCR 定量测试

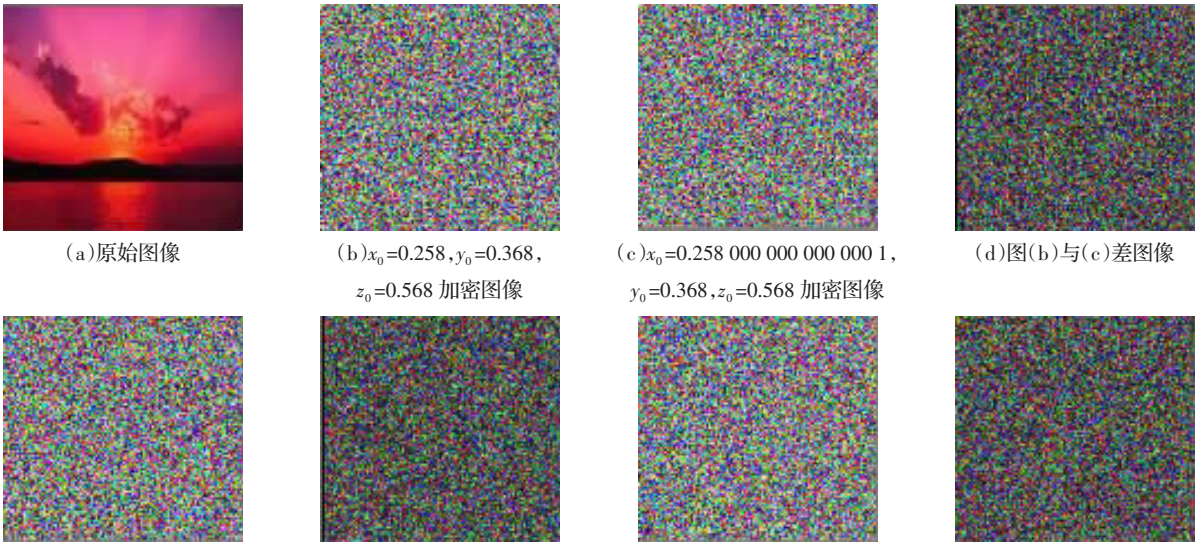
通过前一节的分析,知道通过对 UACI 和 NPCR 进行定量测试,可以判断本算法抵抗唯密文攻击的能力。对彩色图像,分别对 R、G 和 B 进行测试,测试结果如表 1 所示。

由表 1 可见,加密后图像、错误解密后图像与原图像相比变化很大,而解密后恢复图像与原图像相比则毫无变化。且 R、G、B 三色系的变化率都已经达到了 99%以上,所以可以有效地抵抗唯密文攻击。



(a)原始图像　(b)x_0=0.258,y_0=0.368,z_0=0.568 加密图像　(c)正确解密图像　(d)x_0=0.258 000 000 000 000 1,y_0=0.368,z_0=0.568 错误解密图像

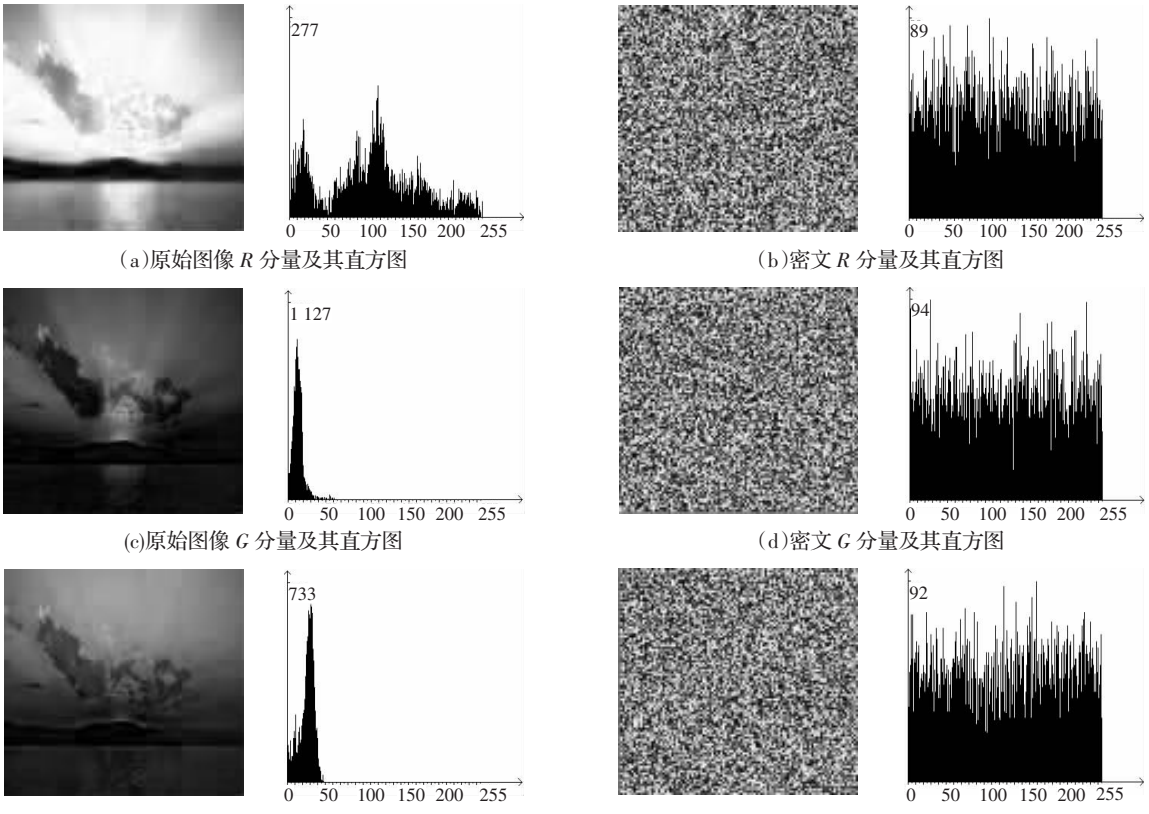
图 3　图像加密解密结果



(a)原始图像　(b)x_0=0.258,y_0=0.368,z_0=0.568 加密图像　(c)x_0=0.258 000 000 000 000 1,y_0=0.368,z_0=0.568 加密图像　(d)图(b)与(c)差图像

(e)y_0=0.368 000 000 000 000 1,x_0=0.258,z_0=0.568 加密图像　(f)图(b)与(e)差图像　(g)z_0=0.568 000 000 000 000 1,x_0=0.258,y_0=0.368 加密图像　(h)图(b)与(g)差图像

图 4　密钥敏感性测试



(a)原始图像 R 分量及其直方图　(b)密文 R 分量及其直方图

(c)原始图像 G 分量及其直方图　(d)密文 G 分量及其直方图

(e)原始图像 B 分量及其直方图　(f)密文 B 分量及其直方图

图 5　原始图像、密文的 R、G、B 分量及其直方图

表 1　彩色图像 UACI 和 NPCR 定量测试结果(与原图像之差)

	加密图像			正确解密图像			错误加密图像		
	R	G	B	R	G	B	R	G	B
NPCR/%	99.413 3	99.581 9	99.611 3	0	0	0	99.185 9	99.163 9	99.229 0
UACI	0.3246 5	0.4515 4	0.4136 8	0	0	0	0.3195 6	0.4478 8	0.408 1

4　结论

本文提出的基于三维混沌的图像加密新方法,是在传统混沌加密算法的基础上,将密文当中的像素值嵌入到密钥发生器中,并在加密算法中应用了密文反馈算法,从而使得运用本算法来加密图像可以达到良好的加密效果。综合上述实验结果,可以归纳出本文提出的加密算法的特点:

(1)本文所采用的三维混沌映射对初始值 x_0、y_0 和 z_0 具有很强的敏感依赖性,三者只要其中一个有微小的变化就无法得到正确的解密结果。因此,采用本算法进行图像加密是非常安全的,其密钥空间大,可达到 10^{54}。

(2)从实验结果可以看出,应用本算法对图像进行加密处理后,原始图像已失去了它本来的面目,变得杂乱无章,无法辨认,因此本文提出的算法有很好的加密效果。

(3)由于本文采用的算法仅在空域对图像数据进行整数运算处理,处理操作(异或及加法运算)比较简单,所以加密效率很高。

(4)从图 5 和表 1 可以看出,密文的 R、G 和 B 分量的直方图与原始图像相比很均匀,且加密和错误解密后的 R、G、B 三色系的变化率都已经达到了 99%以上,因此可以有效地抵抗统计攻击和唯密文攻击。

(5)本文算法是分别对图像的 R、G 和 B 分量进行加密的,数据量没有发生数据膨胀,它能克服基于秘密共享加密算法的缺陷。

参考文献:

[1] 李昌刚,韩正之,张浩然.图像加密技术综述[J].计算机研究与发展,2002,39(10).

[2] Zou Jian-cheng,Zhong Wen-qi,Ward R K.A novel digital image encryption method based on DES[C]//IASTED International Conference on Communication Systems and Applications,2005.

[3] Lukac Rastislav,Plataniotis Konstantinos N.Bit-level based secret sharing for image encryption[J].Pattern Recognition,2005,38(5):767-772.

[4] Zhang Lin-hua,Liao Xiao-feng,Wang Xue-bing.An image encryption approach based on chaotic maps [J].Solitons and Fractals,2005,24:759-765.

[5] Gao Hao-jiang,Zhang Yi-sheng,Liang Shu-yun,et al.A new chaotic algorithm for image encryption [J].Chaos,Solitons and Fractals,2006,29(2).

[6] 张可,王典洪.基于 Logistic 混沌序列的图像空域复合加密研究[J].计算机与现代化,2005(1):66-69.

[7] 黄润生.混沌及其应用[M].武汉:武汉大学出版社,2000-01.

[8] Fei Peng,Qiu Shui-sheng,Min Long.An image encryption algorithm based on mixed Chaotic Dynamic Systems and External Keys[C]//2005 International Conference on Communications,Circuits and Systems-Proceedings,2005:1135-1139.