一种基于时空混沌系统的彩色图像自适应位级加密算法

柴秀丽[1] 甘志华[2,3]
(河南大学图像处理与模式识别研究所 开封 475004)[1] (北京理工大学计算机学院 北京 100081)[2]
(河南大学软件学院 开封 475004)[3]

摘 要 基于时空混沌系统,提出了一种新的自适应的在位级进行操作的彩色图像加密策略。首先将原始明文图像转化为R、G、B 3个分量,接着采用自适应方法进行加密,即先用B加密R得到R',用R'加密G得到G',用G'加密B得到B',用B'加密R'得到R'',如此循环一轮即得到加密后的密文图像。加密操作包括置乱和扩散,使用时空混沌系统CML对原始图像在位级进行置乱,然后采用Logistic系统对置乱后的二值图像进行扩散。混沌系统的初始值受明文信息的影响,使得算法对明文敏感。对密钥空间、图像直方图、密钥敏感性、相关性、信息熵、明文敏感性、密码攻击进行的测试和分析,证明了算法的安全性和高效性,其在图像保密通信领域具有巨大的应用潜力。

关键词 保密通信,彩色图像加密,时空混沌系统,自适应,位级
中图法分类号 TP391 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.7.045

Self-adaptive Bit-level Colour Image Encryption Algorithm Based on Spatiotemporal Chaotic System

CHAI Xiu-li[1] GAN Zhi-hua[2,3]
(Institute of Image Processing and Pattern Recognition, Henan University, Kaifeng 475004, China)[1]
(School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China)[2]
(Software College, Henan University, Kaifeng 475004, China)[3]

Abstract A new self-adaptive colour image encryption scheme based on spatiotemporal chaotic system was introduced, and it operates at the bit level. Firstly, plain image is converted to R, G, B three vectors, and then a self-adaptive method is employed to encrypt the image. The method is as follows: B vector image is used to encrypt R vector image, and R' is given; R' is used to encrypt G vector image, and G' is given; G' is used to encrypt B vector image, and B' is gotten; B' is used to encrypt R', and R'' is attained, then cipher image appears after one turn. Encryption schemes are composed of confusion process and diffusion process. Spatiotemporal chaotic system——coupled map lattices(CML) is used to permute the positions of the image pixels at the bit level, and logistic chaotic system is adopted to diffuse the shuffled bit image. The initial values of chaotic systems are influenced by the plain image, and the method is sensitive to the plain image. Tests and analyses of key space, image histogram, key sensitivity, correlation, information entropy, plain image sensitivity and steganogram attack were carried out and the results demonstrate the superior security and high efficiency of the proposed scheme. Moreover, the encryption scheme has huge application potential in image secure communication field.

Keywords Secure communication, Colour image encryption, Spatiotemporal chaotic system, Self-adaptive, Bit level

1 引言

随着互联网和数字多媒体技术的飞速发展,多媒体通信尤其是图像通信变得越来越重要。数字技术在带给我们便利的同时,也给非法使用者和入侵者带来了方便,因此图像加密技术受到人们的广泛关注。数字图像具有数据量大、相关性强、冗余度高等特点,传统的加密算法如国际数据加密算法(international data encryption algorithm, IDEA)、高级加密标准(advanced encryption standard, AES)针对一维数据流而设计,不适于加密数字图像[1]。混沌系统对初始条件的敏感性和系统变化的不可预测性等类随机特性,使得混沌信息加密技术在图像加密场合具有广阔的应用前景。

自从Matthews[2]提出一维的混沌映射可以用于信息加密后,许多混沌图像加密算法被提出,包括用于灰度图像和彩色图像的算法[3-5]。彩色图像可以提供更丰富的信息,因此备受关注。但是,以往研究的混沌加密技术大多基于低维离散混沌映射[6-9],鉴于有限计算精度的限制,低维混沌系统存在周期短和周期轨道少的不足,而时空混沌系统可以完美地解决这些问题。此外,时空混沌系统具有较大的参数空间、更多的正的Lyapunov指数、更高的随机性和更多的混沌序列,产

到稿日期:2014-04-09 返修日期:2014-07-09 本文受国家自然科学基金资助项目(61004006,61203094),河南省基础与前沿技术研究项目(132300410475),河南省教育厅科技攻关项目(14A413015)资助。
柴秀丽(1980—),女,博士,副教授,主要研究方向为混沌保密通信,E-mail:chaixiuli@henu.edu.cn;甘志华(1979—),男,博士生,讲师,主要研究方向为信息处理,E-mail:800521@bit.edu.cn(通信作者)。

生的混沌序列也更加难以估计，因此时空混沌系统更适用于图像加密[10-12]。文献[10]提出了一种基于时空混沌系统和自适应的图像加密算法，其针对的是灰度图像。此外，之前的一些彩色图像加密算法使用同样的方法加密 R、G、B 分量，这就意味着独立地加密图像 3 次，忽视了 R、G、B 分量之间的相关性，较易受到攻击[13-15]。

王兴元等[16]提出了一种基于混沌的新的彩色图像加密方法，即使用一维 Logistic 映射对彩色图像的 R、G、B 分量进行加密，使得 3 个分量相互影响，该算法采用的联合置乱和联合扩散操作有效降低了 R、G、B 分量之间的相关性，增强了加密效果，在像素级进行置乱和扩散操作。所有像素级的图像加密算法存在一个共同问题：置乱操作仅改变像素的位置，对像素值没有影响，像素值的改变仅取决于扩散操作，和置乱操作相比，扩散操作需要更多的执行时间，会降低工作效率，同时置乱操作抗统计攻击和已知明文攻击的能力较差[17]。最近，位级操作的加密算法激发了人们的研究热情[10,17,18]。文献[19]采用 PWLCM 混沌映射和三维陈氏混沌系统加密彩色图像，工作在位级，研究结果表明，采用混沌特性比较复杂的三维陈氏混沌系统加密效果优于采用 PWLCM 混沌映射的。高维超混沌系统尤其是特性更加复杂的时空混沌系统的采用，在增加密钥空间的同时，必然会提高算法的安全性。

为了得到高安全的图像加密方案，本文提出一种新的基于时空混沌系统的彩色图像加密算法，在位级进行置乱和扩散操作，彩色图像的 R、G、B 分量相互影响进行加密以达到自适应的效果。安全性分析表明该算法可以有效抵抗各种典型攻击。

2 时空混沌系统——耦合映像格子(CML)

耦合映像格子(CML)是时空混沌系统的一种典型代表，是一个具有离散时间、离散时空和连续状态的动力系统。它在每个格子上都有一个非线性系统，称作局部混沌映射，根据一定的耦合规则同其他的局部映射耦合。CML 模型最初由 Kaneko 等提出[20]，其模型如下：

$$x_{n+1}(i)=(1-\varepsilon)f(x_n(i))+\frac{\varepsilon}{2}\times(f(x_n(i-1))+f(x_n(i+1))) \quad (1)$$

其中，n 是离散时间坐标，$i(i=1,2,\cdots,L)$是格点坐标，L 为格点数，$\varepsilon\in(0,1)$是格点间的耦合强度因子，$x_n(i)$代表第 i 个格点在 n 时间的状态，设定周期边界条件为 $x_n(0)=x_n(L)$。

为了缩短图像的加密时间，提高图像的加密效率，局部混沌映射 $f(x)$选用一维 Logistic 映射：

$$x_{n+1}=ax_n(1-x_n),x_n\in(0,1) \quad (2)$$

当参数 $a\in(3.5699456,4]$ 时，系统是混沌的。CML 系统的动力学行为如图 1 所示。

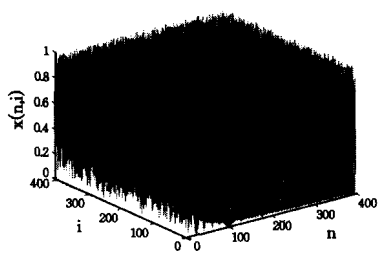


图 1 CML 的混沌吸引子($a=4$、$\varepsilon=0.1$)

3 图像加密策略

彩色图像中每个像素都可以分为 R、G、B 3 个基色分量，每一个基色的分量直接决定基色的强度。用 3 个矩阵来表示彩色数字图像，每一个矩阵对应其中一个基色。本文采用自适应的方法进行加密，先用 B 矩阵的信息加密 R 得到 R'；用 R'矩阵的信息加密 G 得到 G'；用 G'矩阵的信息加密 B 得到 B'；再用 B'的信息加密 R'得 R''。将 R''、G'、B'矩阵合为一个彩色图像，即为加密后的密文图像。

设彩色明文图像 P 的大小为 $M\times N$，将 P 转化为 R、G、B 3 个分量。每个分量矩阵的大小为 $M\times N$，像素值在 0 到 255 之间变化。矩阵中(x,y)位置的像素值记作 $f(x,y)$，将每一个像素值转化为 8 位二进制数值，$f(x,y)=p(8)p(7)p(6)p(5)p(4)p(3)p(2)p(1)$。先用 B 矩阵信息加密 R 矩阵，以该部分为例介绍加密的具体步骤。

(1)首先使用 CML 系统对原始图像在位级进行置乱，具体操作如下：

Step1 变换矩阵 R 为它的二值图像 $Rpic(n)$，$n=1,2,\cdots,8$，每一个图像的大小为 $M\times N$。把 $Rpic(n)$分别转化为对应的向量组 $Rp(n)$，每个向量长度为 $M\times N$。

Step2 选取 B 矩阵的第一个像素值 $I_1=B(1,1)$，令 $h=I_1 \bmod 8$，计算出 h 的值作为密钥。对 R 矩阵的每个像素值的 8 位二进制数位循环右移 h 位，得到新的向量组 $Rp'(n)$。

Step3 变换 B 为它的二值图像 $Bpic(n)$，$n=1,2,\cdots,8$，将其分别转化为向量组 $Bp(n)$，每个向量长度为 $M\times N$。将 $Bpic(n)$中的所有二值数值相加，计算得出 8 个值 $sum(n)$，$n=1,2,\cdots,8$。设 $g(i,j)$为图像矩阵第 i 行、第 j 列的二值数值，由图像 $Bpic(n)$得到 $sum(n)$，表示为 $sum(n)=\sum_{(i,j)\in Bpic(n)}g(i,j)$。

Step4 将 CML 系统格子的格点数 L 设为 8，用参数 a、ε 和数值 $x_0(n)=1/((sum(n)+1)\times n)(n=1,2,\cdots,8)$对系统进行初始化，迭代混沌系统 $m+MN$ 次，舍弃前 m 个数值以避免有害的影响。每一个晶格生成 MN 个数值 $x_i(n)(i=(m+1),(m+2),\cdots,(m+MN);n=1,2,\cdots,8)$，所以该混沌系统总共生成 $8MN$ 个数值。按升序排列每个 $x_i(n)$值$[x_{m+1}(n),x_{m+2}(n),\cdots,x_{m+MN}(n)]$，得到 $x_i'(n)=[x'_{m+1}(n),x'_{m+2}(n),\cdots,x'_{m+MN}(n)]$，找出 $x_i'(n)$在 $x_i(n)$中的位置，并记下转换位置得到转换位置矩阵 $TN_n=[t_1(n),t_2(n),\cdots,t_{MN}(n)]$，$n=1,2,\cdots,8$。

Step5 根据 TN_n 重新排列每一个向量$Rp'(n)(n=1,2,\cdots,8)$的元素，即移动向量 $Rp'(n)$中的第 $t_1(n)$个元素到第 1 个元素位置，第 $t_2(n)$个元素到第 2 个元素位置，以此类推，直到每个向量中的元素都被置乱，置乱后的向量组记为 $Rp''(n)$。

(2)利用 Logistic 系统对经过置乱后的二值图像进行扩散，具体操作如下：

Step1 设定 Logistic 混沌系统的参数为 a_1，初值为 x_0，迭代 Logistic 系统 m_1+MN 次，舍弃前 m_1 个数值得到一个混沌序列 $Z(j),j=1,2,\cdots,MN$。

Step2 将 $Z(j)$按式(3)转化为整数序列 $Z_1(j)$。

$$Z_1(j)=floor(Z(j)\times 10^{14}) \bmod 256 \quad (3)$$

式中，$j=1,2,\cdots MN$，$floor(i)$是取小于 i 的最大整数，$Z_1(j)$中的元素从 0 到 255 变化。转换 $Z_1(j)$为二值序列 $Z_1'(j)$，形成 8 个二值向量 $Z_1'(n)(n=1,2,\cdots,8)$，每个向量长度为 MN。

Step3 根据式(4)对 R 部分进行扩散操作：

$$C_i(n)=(Rp_i''(n)+Bp_i'(n)+Z_{1i}'(n)) \bmod 2 \quad (4)$$

其中，$n=1,2,\cdots,8$，$Rp_i''(n)$为置乱后的向量组$Rp''(n)$中的第i个元素，$Bp_i'(n)$为向量组$Bp'(n)$中的第i个元素，$Z_{1i}'(n)$为向量组$Z_1'(n)$中的第i个元素，$C_i(n)$为经过处理后的8个二值图像，从而得到加密后的R'矩阵分量。

(3) 以同样的方法，用R'矩阵的信息加密G，得到G'；用G'矩阵的信息加密B得到B'；再用B'的信息加密R'得到R''。将R''、G'、B'矩阵合为一个彩色图像P'，即为加密后的密文图像。

整个加密流程如图2所示，图2中置乱、扩散的具体流程如图3所示，这里以用B矩阵的信息对R进行置乱、扩散的过程为例进行说明。

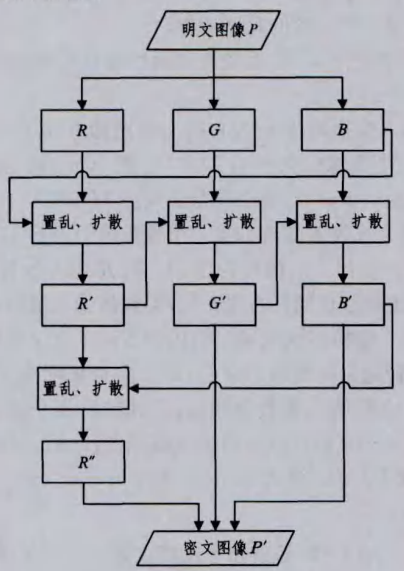


图2 加密流程

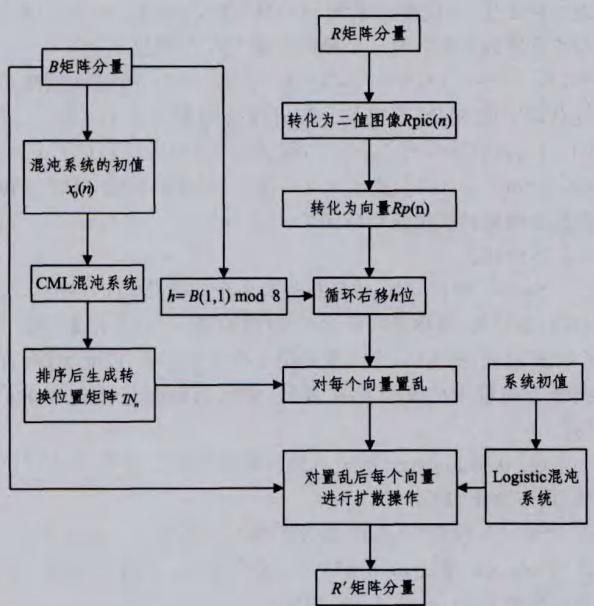


图3 置乱、扩散的具体流程

4 图像解密策略

解密步骤与加密步骤相似，但顺序相反。

(1)将需要解密的密文图像P'转化为R''、G'、B' 3个分量。

(2)先用矩阵B'的信息解密R''。选取同加密过程中相同的参数，耦合映像格子CML和Logistic混沌系统产生的序列与加密时相同。

像素值反向扩散公式如下：

$$Rp_i''(n)=(C_i(n)-Bp_i'(n)-Z_{1i}'(n)) \bmod 2$$
$$n=1,2,\cdots,8 \tag{5}$$

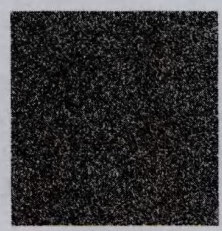
由TN_n反向变换$Rp_i''(n)$得到$Rp'(n)(n=1,2,\cdots,8)$，根据h的值反向移位，即循环左移h位得到向量$Rp(n)$，将向量$Rp(n)$转换为矩阵R'。

(3)依次用R'的信息解密G'得到G，用G'的信息解密B'得到B，用B的信息解密R'得到R。最后将R、G、B分量组合即得原文图像P。

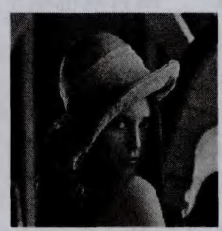
5 安全性分析

用Matlab实现本文的加解密算法，对256×256的"Lena"彩色图像加密再解密，以验证本文所提算法的安全性。令参数$m=m_1=500$，时空混沌系统CML的参数$a=4$、$\varepsilon=0.1$，Logistic映射的参数和初始值为$a_1=3.99$和$x_0=0.12345678912345$。图像加密、解密的结果见图4。

(a)明文图像



(b)密文图像



(c)解密图像

图4 图像加密、解密的实验结果

一个好的加密算法应该可以抵抗所有的已知攻击，下面对本文提出的算法的安全性进行具体分析。

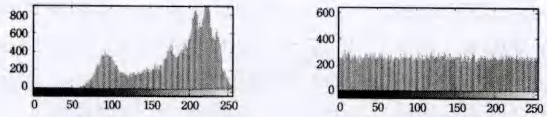
5.1 密钥空间分析

一个安全的加密算法密钥空间应该足够大，使得强力攻击无效。在本算法中，初始条件和参数a、ε、a_1、x_0、$x_0(n)$、h，混沌以及系统的初始迭代参数m、m_1都被作为密钥。如果选取的运算精度为10^{-14}，密钥空间大小可达到10^{210}。DES算法密钥长度为56bit，3-DES为112bit或168bit，IDEA为128bit，AES最大为256bit。本文的密钥长度相当于二进制的690bit，如此大的密钥空间足以抵抗任何强力攻击。

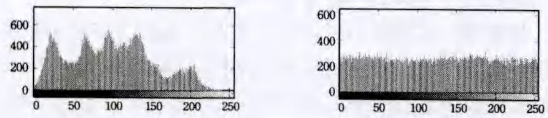
5.2 图像直方图分析

直方图描述了数字图像中所有灰度级的像素出现的频率。一个好的图像加密算法加密得到的密文图像的灰度直方图应该平滑且均匀，避免信息的泄露。

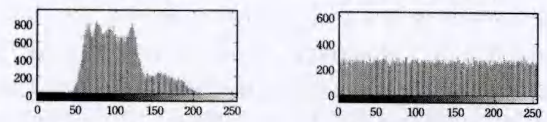
图5分别为明文图像和密文图像R、G、B分量的直方图。由图可见，明文图像的像素分布很不均匀，密文图像的像素是均匀分布的，这使得攻击者难以通过统计的方法来攻击密文，从而提高了密文的安全性。



(a)R 分量明文图像　(b)R 分量密文图像



(c)G 分量明文图像　(d)G 分量密文图像



(e)B 分量明文图像　(f)B 分量密文图像

图 5　明文图像与密文图像的灰度直方图

5.3　密钥敏感性测试

将密钥分别进行改变后，对加密的图像进行解密，结果如图 6 所示。

(a)正确密钥解密图像　(b)a 改为 3.99999999999999　(c)ε 改为 0.10000000000001

(d)a_1 改为 3.990000000001　(e)x_0 改为0.123456789123451

图 6　密钥敏感性测试

图 6(a)是使用正确的密钥解密得到的图像，与原始明文图像相同；图 6(b)和(c)是分别将 a 改为 3.99999999999999 以及将 ε 改为 0.10000000000001 后得到的解密图像；(d)和(e)是分别将 a_1 改为 3.990000000001 和将 x_0 改为 0.123456789123451后得到的解密图像。由结果可知，密钥的一个微小的改变就可以造成一个完全不同的解密结果，不能得到正确的明文图像，这表明本文算法对密钥是非常敏感的。

5.4　相邻像素相关性分析

图像相邻像素的相关性很大，很容易泄漏信息。为了有效抵抗统计攻击，加密算法应该把相邻像素之间的相关性降到最低。随机地在明文、密文图像中选择 2000 对像素点，测试它们在水平、垂直和对角方向的相邻像素之间的相关性。计算公式如下：

$$R_{x,y}=\frac{cov(xy)}{\sqrt{D(x)D(y)}} \tag{6}$$

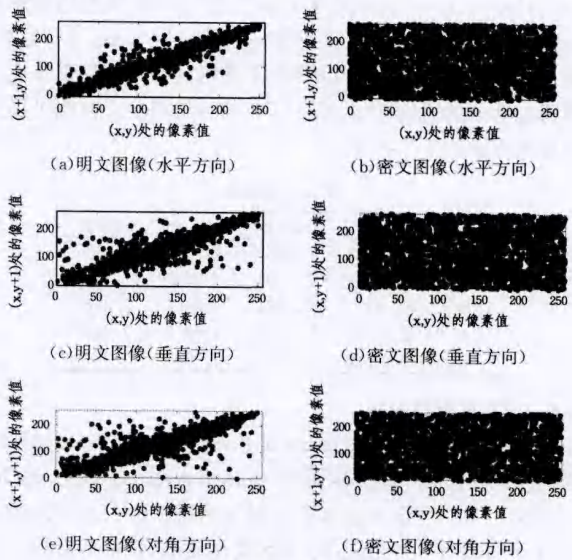
$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{7}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \tag{8}$$

$$cov(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \tag{9}$$

式中，x、y 表示图像中相邻的两个像素值，$D(x)$ 表示均方差，$E(x)$ 表示平均值，$cov(x,y)$ 表示相关函数，$R_{x,y}$ 表示相邻像素相关性。

实验结果如图 7 及表 1－表 3 所示。由结果可知，原始明文图像的相邻像素相关性很大，而利用本文算法得到的密文图像的像素随机均匀分布，相邻像素之间的相关性远远小于明文图像的。



(a)明文图像(水平方向)　(b)密文图像(水平方向)

(c)明文图像(垂直方向)　(d)密文图像(垂直方向)

(e)明文图像(对角方向)　(f)密文图像(对角方向)

图 7　相邻像素相关性

表 1　R、G、B 分量中水平方向相邻像素相关性

	R 分量	G 分量	B 分量
明文图像	0.9536	0.9504	0.9159
密文图像	−0.0224	−0.0107	−0.0031

表 2　R、G、B 分量中垂直方向相邻像素相关性

	R 分量	G 分量	B 分量
明文图像	0.9317	0.9029	0.8582
密文图像	0.0092	−0.0456	0.0362

表 3　R、G、B 分量中对角方向相邻像素相关性

	R 分量	G 分量	B 分量
明文图像	0.9124	0.8821	0.8528
密文图像	0.0221	0.0297	0.0426

彩色图像 R、G、B 分量间的相关性也很大，好的加密算法也应当使 R、G、B 分量间的相关性大大降低。测试明文图像和密文图像的 R、G、B 分量之间相同位置像素的相关性，结果见表 4。由表 4 可知，与明文图像相比，密文图像 R、G、B 分量间相同位置像素的相关性计算结果接近 0，远远小于明文图像的。把本文的测试结果与 Wang[16]、Rhouma[21]、Sahar[22]和 Liu[23]的结果进行比较，可知，本文算法抵抗统计攻击的能力均优于上述文献的。

表 4　R、G、B 分量之间相同位置像素的相关性

	R、G 分量之间同位置像素相关性	R、B 分量之间同位置像素相关性	G、B 分量之间同位置像素相关性
本文算法明文图像	0.8871	0.6874	0.9115
本文算法密文图像	−0.0035	−0.0050	−0.0013
Wang[16]密文图像	−0.0038	−0.0509	0.0127
Rhouma[21]密文图像	0.2480	0.1390	0.1713
Sahar[22]密文图像	0.3053	0.2042	0.2525
Liu[23]密文图像	0.2312	0.1254	0.1611

5.5 信息熵分析

信息加密后，理想的熵值应该为 8。计算公式如下：

$$H(m)=\sum_{i=0}^{2^n-1}p(m_i)\log\frac{1}{p(m_i)} \tag{10}$$

式中，2^n 表示信息源 m 的总状态数，$p(m_i)$代表符号 m_i 出现的概率。

对标准"Lena"图像用本文算法进行加密，得到密文图像 R、G、B 分量的信息熵结果，如表 5 所列。与文献[19,24,25]的加密结果相比，利用本文算法加密得到的信息熵更接近理想值 8，分别为 7.9969、7.9961、7.9975，说明本文算法可以更加有效地抵抗统计攻击。

表 5 信息熵

	R 分量	G 分量	B 分量
本文算法密文图像	7.9969	7.9961	7.9975
文献[19]Fig. 6(d)	7.9791	7.9802	7.9827
文献[19]Fig. 8(a)	7.9871	7.9881	7.9878
文献[24]密文图像	7.9921	7.9879	7.9852
文献[25]密文图像	7.9910	7.9815	7.9826

5.6 明文敏感性分析

用像素数改变率(Number of Pixels Change Rate，NPCR)和归一化像素值平均改变强度(Unified Average Changing Intensity，UACI)度量加密算法对明文的敏感性。*NPCR* 越接近 100%，说明明文变化时加密系统越敏感，抵抗明文攻击的能力越强。*UACI* 越大，说明加密系统能越有效地抵抗各种攻击。计算公式如下：

$$NPCR=\frac{\sum_{i,j}D(i,j)}{M\times N}\times 100\% \tag{11}$$

$$UACI=\frac{1}{M\times N}\left[\sum_{i,j}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right]\times 100\% \tag{12}$$

$$D(i,j)=\begin{cases}0, & C_1(i,j)=C_2(i,j)\\ 1, & C_1(i,j)\neq C_2(i,j)\end{cases} \tag{13}$$

式中，M 和 N 表示图像的行数和列数，C_1 表示密文图像，C_2 表示明文改变后得到的新的密文图像，$C_1(x,y)$和 $C_2(x,y)$表示坐标(i,j)处的像素值。

将原始明文图像的第一个像素点的灰度值加 1 得到一个新的图像，然后将这两个图像用相同的密钥加密得到密文图像 C_1 和 C_2。根据式(11)－式(13)计算出它们的 *NPCR* 和 *UACI* 值，如表 6 所列。由表 6 可知，$NPCR_{R,G,B}$的值都大于 99%，$UACI_{R,G,B}$的值都大于 33%，即明文图像中 1 个像素的微小变化将引起密文图像中 99%以上的像素的变化，变化幅度在 33%以上，这说明本文算法密文敏感性强，可以有效抵抗差分攻击，且略优于文献[10,24,25]的算法。

表 6 密文图像的 *NPCR* 和 *UACI* 值

	R 分量	G 分量	B 分量
本文算法 NPCR	0.9960	0.9954	0.9957
本文算法 UACI	0.3357	0.3334	0.3350
文献[10] NPCR	0.9957	0.9948	0.9941
文献[10] UACI	0.3345	0.3321	0.3342
文献[24] NPCR	0.9951	0.9948	0.9945
文献[24] UACI	0.3343	0.3335	0.3332
文献[25] NPCR	0.9960	0.9946	0.9948
文献[25] UACI	0.3338	0.3331	0.3330

5.7 密码攻击分析

本文用自适应方法加密原始明文图像，即用明文的部分信息加密另一部分，所以不同的加密图像具有不同的加密信息，攻击者不可能用一个明文和其对应的密文来解密其它的已加密图像。同时 CML 系统的初始值受明文信息的影响，要攻击密文就必须知道明文图像信息，只有知道明文才能得到正确的混沌序列，从而实现正确解密。这表明该算法可以有效抵抗选择明文和选择密文攻击。

结束语 本文提出了一种基于时空混沌系统的彩色图像加密算法，在位级进行置乱-扩散操作，使彩色图像的 R、G、B 分量相互影响进行加密以达到自适应的效果，同时 CML 系统的初始值受明文信息的影响，使得算法对明文敏感。实验结果和分析表明，该算法具有如下特点：密钥空间大，足以抵抗强力攻击；密文图像的像素均匀分布，抗统计攻击能力强；密钥敏感性高；原始明文图像的相邻像素之间存在很大的相关性，密文图像的相邻像素之间的相关性要远远小于明文图像的，信息熵接近 8，抵抗统计分析的能力较强；$NPCR_{R,G,B}$的值都大于 99%，$UACI_{R,G,B}$的值都大于 33%，可以有效抵抗差分攻击。因此，本文提出的加密算法安全高效，在医学、军事等图像保密通信领域具有巨大的应用潜力。

参 考 文 献

[1] 朱从旭，胡玉平，孙克辉. 基于超混沌系统和密文交错扩散的图像加密新算法 [J]. 电子与信息学报，2012，34(7)：1735-1743
Zhu Cong-Xu, Hu Yu-ping, Sun Ke-hui. New image encryption algorithm based on hyperchaotic system and ciphertext diffusion in crisscross pattern[J]. Journal of Electronics & Information Technology, 2012, 34(7): 1735-1743

[2] Matthews R. On the derivation of a chaotic encryption algorithm [J]. Cryptologia, 1989, 13(1): 29-42

[3] Sahar M, Amir M E. Color image encryption based on coupled nonlinear chaotic map [J]. Chaos, Solitons & Fractals, 2009, 40(1): 309-318

[4] Ye Guo-dong, Kwok-Wo W. An image encryption scheme based on time-delay and hyperchaotic system [J]. Nonlinear Dynamics 2013, 71(1/2): 259-267

[5] Ziba E, Atieh B. An improvement over an image encryption method based on total shuffling [J]. Optics Communications, 2013, 286: 51-55

[6] Akhavan A, Samsudin A, Akhshani A. A symmetric image encryption scheme based on combination of nonlinear chaotic maps [J]. Journal of Franklin Institute, 2011, 348(8): 1797-1813

[7] Zhu Z L, Zhang W, Wong K W, et al. A chaos-based symmetric image encryption scheme using a bit-level permutation [J]. Information Sciences, 2011, 181(6): 1171-1186

[8] Akhshani A, Akhavan A, Lim S C, et al. An image encryption scheme based on quantum logistic map [J]. Communication Nonlinear Science and Numerical Simulation, 2012, 17(12): 4653-4661

[9] Wang Y, Wong K W, Liao X, et al. A new chaos-based fast image encryption algorithm [J]. Applied Soft Computing, 2011, 11(1): 514-522

[10] Teng L, Wang X Y. A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive [J]. Optics Communications, 2012, 285(20): 4048-4054

[11] Xiang T, Kwok-Wo W, Liao X F. Selective image encryption using a spatiotemporal chaotic system [J]. Chaos, 2007, 17(2):

023115

[12] Sun F Y, Liu S T, Li Z Q, et al. A novel image encryption scheme based on spatial chaos map [J]. Chaos, Solitons & Fractals, 2008, 38(3): 631-640

[13] Rhouma R, Soumaya M, Safya B. OCML-based colour image encryption [J]. Chaos, Solitons & Fractals, 2009, 40(1): 309-318

[14] Guo Q, Liu Z G, Liu S T. Colour image encryption by using Arnold and discrete fractional random transforms in HIS space [J]. Optics and Lasers in Engineering, 2010, 48(12): 1174-1181

[15] Sahar M, Amir M E. Colour image encryption based on coupled nonlinear chaotic map [J]. Chaos, Solitons and Fractals, 2009, 42(3): 1745-1754

[16] Wang X Y, Teng L, Qin X. A novel colour image encryption algorithm based on chaos [J]. Signal Processing, 2012, 92(4): 1101-1108

[17] Zhang W, Wong K W, Yu H, et al. A symmetric color image encryption algorithm using the intrinsic features of bit distributions [J]. Communications in Nonlinear Science and Numerical Simulation, 2013, 18(3): 584-600

[18] Fu C, Lin B, Miao Y, et al. A novel chaos-based bit-level permutation scheme for digital image encryption [J]. Optics Communication, 2011, 284(23): 5415-5423

[19] Liu H J, Wang X Y. Color image encryption using spatial bit-level permutation and high-dimension chaotic system [J]. Optics Communications, 2011, 284(16/17): 3895-3903

[20] Kaneko K. Spatiotemporal intermittency in Coupled Map Lattices[J]. Progress of Theoretical Physics, 1985, 74(5): 1033-1044

[21] Rhouma R, Soumaya M, Safya B. OCML-based colour image encryption [J]. Chaos, Solitons & Fractals, 2009, 40(1): 309-318

[22] Sahar M, Amir M E. Colour image encryption based on coupled nonlinear chaotic map [J]. Chaos, Solitons & Fractals, 2009, 42(3): 1745-1754

[23] Liu H J, Wang X Y. Colour image encryption based on one-time keys and robust chaotic maps [J]. Computers&Mathematics with Applications, 2010, 59(10): 3320-3327

[24] 罗松江，丘水生. 基于时空混沌和S盒的彩色图像加密算法[J]. 电路与系统学报，2010，15(3)：117-122
Luo S J, Qiu S S. Color image encryption algorithm based on spatiotemporal chaos and S-box [J]. Journal of Circuits and Systems, 2010, 15(3): 117-122

[25] He J, Li Z B, Qian H F. Cryptography based on spatiotemporal chaos system and multiple maps [J]. Journal of Software, 2010, 5(4): 421-428

(上接第 177 页)

量大小，横坐标表示6种不同文件类型，右纵坐标表示重复数据删除率的大小。对6种不同格式的文件采用本文算法和传统算法进行云存储系统重复数据删除，结果表明本文算法重复数据准确删除率较高，去重的效果更佳，有效避免了数据信息流的干扰特征造成的误删和漏删，重复数据删除准确性能较好，误删率降低了13.11%，云存储系统的CPU执行时间提高了17.8%，从而展示了算法的优越性能。

结束语 云存储系统中的重复数据是各类数据管理成本快速上升过程中留下的冗余数据产物，云存储系统中产生的数据量以几何级数增长。为了有效面对爆炸式增长的云存储系统运行数据管理的需求，减轻服务器开销，研究了一种有效的云存储系统重复数据删除算法，对消除数据冗余、降低系统能耗和提高存储性能具有重要意义[9]。本文提出一种改进的基于分数阶Fourier变换累积量检测的云存储系统重复数据删除算法，即采用4阶累积量切片实现对云存储系统重复数据信息流的能量聚集和噪声抑制，进行重复数据检测后置滤波处理，创建多个线程的信息流特征编码，实现对重复数据的删除。分析研究和实验结果表明，采用本文算法能有效避免数据信息流的干扰特征造成的误删和漏删，对云存储系统中重复数据的检测性能较好，重复数据删除准确性高，综合性能优于传统算法。

参 考 文 献

[1] 谢平. 存储系统重复数据删除技术研究综述[J]. 计算机科学，2014，41(1)：22-30
Xie Ping. Surey on data deduplication techniques for storage systems[J]. Computer Science, 2014, 41(1): 22-30

[2] Miorandi D, Sicari S, Pellegrini F D, et al. Internet of things: vision, applications and research challenges [J]. Ad Hoc Networks, 2012, 10(7): 1497-1516

[3] Wu T Y, Lee W T, Lin Y S, et al. Dynamic load balancing mechanism based on cloud storage[C]// Computing, Communications and Applications Conference (ComComAp), 2012. IEEE, 2012: 102-106

[4] 蒋海波，王晓京，范明钰，等. 基于水平纠删码的云存储数据布局方法[J]. 四川大学学报(工程科学版)，2013，45(2)：103-109
Jiang Hai-bo, Wang Xiao-jing, Fan Ming-yu. A Data Placement Based on Level Array Codes in Cloud Storage [J]. Journal of Sichuan University (Engineeging Science Edition), 2013, 45(2): 103-109

[5] 敖莉，舒继武，李明强. 重复数据删除技术[J]. 软件学报，2010，21(5)：916-929
Ao Li, Shu Ji-wu, Li Ming-qiang. Data Deduplication Techniques [J]. Journal of Software, 2010, 21(5): 916-929

[6] 付印金，肖侬，刘芳. 重复数据删除关键技术研究进展[J]. 计算机研究与发展，2012，49(1)：12-20
Fu Ying-jin, Xiao Nong, Liu Fang. Research and Development on Key Techniques of Data Deduplicaton[J]. Journal of Computer Research and Development, 2012, 49(1): 12-20

[7] 李渊. 智能PID控制区优化仿真研究[J]. 计算机仿真，2012，29(12)：180-182
Li Yuan. Parameters Optimization of PID Controller[J]. Computer Simulation, 2012, 29(12): 180-182

[8] 谭鹏许，陈越，兰巨龙，等. 用于云存储的安全容错编码[J]. 通信学报，2014，35(3)：109-114
Tan Peng-xu, Chen Yue, Lan Ju-long, et al. Secure fault-tolerant code for cloud storage[J]. Journal on Communications, 2014, 35(3): 109-114

[9] Tang Pei-he, Xu Yi-yi. Resource Scheduling Strategy Based on Credibility in the Enterprise Gloud Strorage[J]. Journal of Convergence Information Technology, 2012, 7(16): 393-400