基于超混沌系统的位级自适应彩色图像加密新算法

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 提出一种采用超混沌系统的自适应彩色图像加密算法,在位级进行加密。首先利用陈氏超混沌系统产生的混沌序列对原始彩色图像的R、G、B分量图像进行置乱和扩散,采用自适应加密方法,用高四位的二值图像信息去加密低四位,再用加密后的低四位信息去加密高四位;接着将加密后的三基色分量图像横向排列组合联合加密,降低了三基色分量之间的相关性。加密算法使得密文与明文、密钥之间的关系复杂化,部分密钥依赖于明文,使得算法对明文敏感。对密钥空间、密钥敏感性、直方图、相关性、信息熵、明文敏感性进行测试和分析,结果证明了加密算法安全有效,在图像保密通信中具有较大的应用潜力。

关键词 保密通信,超混沌系统,自适应,位级,联合加密

中图法分类号 TP391 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.4.027

New Bit-level Self-adaptive Color Image Encryption Algorithm Based on Hyperchaotic 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]

(School of Software, Henan University, Kaifeng 475004, China)[3]

Abstract In the paper, a self-adaptive color image encryption algorithm using the hyperchaotic system was introduced, and we operated it at the bit level. Firstly, chaotic sequences produced by Chen hyperchaotic system are used to confused and diffused R, G, B components of the plain image. Moreover, self-adaptive encryption algorithm is adopted, namely, the higher four bit images are used to encrypt the lower four bit images, and the encrypted lower four bit images are used to encrypt the higher four bit images conversely. Then, the encrypted three base color components are combined horizontally and encrypted simultaneously, and this reduces the correlations of the three base color components. The encryption algorithm makes the relationship between the ciphered image and the plain image, keys more complex, some keys depend on the plain image, and the algorithm is more sensitive to the plain image. Tests and analyses of key space, key sensitivity, image histogram, correlation, information entropy and plain image sensitivity were carried out. The results demonstrate the superior security and high efficiency of the proposed scheme, and the encryption scheme has huge application in image secure communication field.

Keywords Secure communication, Hyperchaotic system, Self-adaptive, Bit level, Combined encryption

1 引言

随着计算机网络技术的快速发展,大量信息通过网络进行传输,信息安全引起了人们的广泛重视[1-3]。网络传输的信息中有1/3是图像信息,因此,图像信息的安全传输和存储备受关注,通常采用对图像进行加密的方式。图像加密技术主要包括两个过程:置乱和扩散[4,5]。置乱过程指的是在不改变图像像素值的情况下,改变像素的位置,从而使图像变得杂乱无章。扩散过程中,像素值被修改,明文图像像素值的一个微小变化就会扩散到密文图像的许多像素。这两个过程一般同时使用,从而实现对图像信息的高安全加密。

图像具有数据量大、相关性强、冗余度高等特点,使得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)加密效率降低,不能满足实时性需要,不适于加密数字图像[6]。混沌系统的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,使得混沌加密技术在图像加密场合具有广阔的应用前景。最近,一些灰度图像和彩色图像的混沌加密算法不断被提出。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[7-9],鉴于有限计算精度的限制,低维混沌系统存在周期小和周期轨道少的不足,导致密码系统安全性不高。而对于高维混沌系统尤其是

到稿日期:2015-03-20 返修日期:2015-06-20 本文受国家自然科学基金资助项目(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,主要研究方向为多媒体信息安全,E-mail:chaixiuli@henu.edu.cn;甘志华(1979-),男,博士生,讲师,主要研究方向为多媒体信息安全,E-mail:gzh@henu.edu.cn(通信作者)。

超混沌系统，其密钥空间大，具有两个以上的 Lyapunov 指数，非线性行为更加复杂和难以预测，在图像加密领域中具有巨大的应用潜力，引起了学者们浓厚的研究兴趣。

彩色图像包含 R、G、B 三基色分量，可以提供更丰富的信息。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，使之较易受到攻击[10-12]。文献[13]提出了一种新的彩色图像加密策略，采用联合置乱和联合扩散操作同时对 R、G、B 分量进行加密，降低了 R、G、B 分量之间的相关性，增强了加密效果；David 等[14]对该文章的安全性进行测试，指出采用一维 Logistic 映射作为加密系统的核心进行置乱和扩散操作，不符合理想加密系统设计的相关准则[15]，同时置乱过程中采用的密钥流与明文无关，这些都使得该算法置乱操作抗攻击性差，给整个密码系统带来了安全隐患。Ye 等[16]提出一种基于超混沌系统的图像加密算法，考虑了传输时滞的影响，针对的是灰度图像。文献[13,16]在像素级进行加密，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，这无疑降低了工作效率[17]。最近，位级操作的加密算法引起了人们的广泛关注，在位级进行置乱操作不仅能改变像素的位置，而且可以改变像素数值，使得图像加密的安全性更高[17-21]。Zhu 等[20]提出了一种基于置乱-扩散模式的灰度图像的加密算法，其工作在位级，利用 Arnold 映射进行置乱操作，采用 Logistic 映射对置乱后的图像进行扩散。Liu 等[21]提出了一种采用 PWLCM 混沌映射和三维陈氏混沌系统的位级彩色图像加密算法。高维超混沌系统的采用，必然会在增加密钥空间的同时提高算法的安全性。

为了得到更加安全的图像加密方案，本文提出一种新的基于超混沌系统的彩色图像自适应加密算法，在位级进行置乱-扩散操作。首先给出采用的陈氏超混沌系统，然后具体介绍加密、解密算法，最后对该算法进行仿真实验和安全性分析。

2 陈氏超混沌系统

本算法采用陈氏超混沌系统，它是 1999 年由陈关荣首先提出的，系统结构简单，便于硬件实现。动力学方程如式(1)所示。

$$\begin{cases}\dot{x}_1=a(x_2-x_1)\\ \dot{x}_2=-x_1x_3+dx_1+cx_2\\ \dot{x}_3=x_1x_2-bx_3\\ \dot{x}_4=x_2x_3+ex_4\end{cases} \tag{1}$$

在 $a=35$，$b=3$，$c=12$，$d=7$ 的条件下，e 处于区间[0，0.085]、(0.085，0.798]、(0.798，0.900]时，系统分别表现为混沌运动、超混沌运动和周期运动。超混沌系统吸引子特性曲线如图 1 所示。

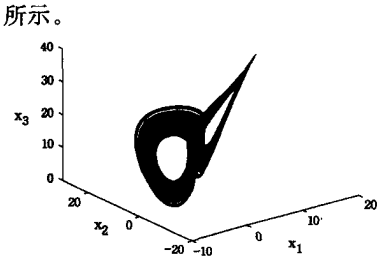


图 1 超混沌系统吸引子曲线($e=0.58$)

3 图像加密方法

采用自适应位级加密策略，即把图像平分为两个二值图像：高四位的二值图像部分 pic5－pic8 和低四位的二值图像部分 pic1－pic4。先用高四位的二值图像信息去加密低四位，再用加密后的低四位信息去加密高四位。

原始明文彩色图像记为 P，将 P 转化为 R、G、B 3 个分量，灰度图像像素值转化为 8 位二进制数值，图像(x,y)位置的像素值记作 $g(x,y)$，则 $g(x,y)=p(8)p(7)p(6)p(5)p(4)p(3)p(2)p(1)$。下面以 R 图像的加密过程为例来说明具体步骤。

(1)先用 R 图像高四位的二值图像部分去加密低四位部分，具体过程如下：

步骤 1 变换 R 为它的二值图像 $Rpic_n(n=1,2,\cdots,8)$，每一个图像的大小为 $M\times N$(M、N 都是整数)。把 $Rpic_n$ 转化为 8 个向量 $Rp_i(i=1,2,\cdots,8)$，每个向量长度为 $M\times N$。

步骤 2 设置混沌系统的参数 a、b、c、d、e 及系统状态初值 $x_0(1)$、$x_0(2)$、$x_0(3)$、$x_0(4)$，迭代混沌系统 $m+M\times N$ 次，舍弃前 m 个数值，以消除暂态过程带来的有害影响，得到 4 个长度为 $M\times N$ 的混沌序列，按升序排列 $x_i(n)=[x_{m+1}(n),x_{m+2}(n),\cdots,x_{m+MN}(n)](n=1,2,3,4)$ 的每个数值，得到 $x_i'(n)=[x'_{m+1}(n),x'_{m+2}(n),\cdots,x'_{m+MN}(n)](n=1,2,3,4)$，找出每个序列中 $x_i'(n)$ 在 $x_i(n)$ 中的位置，并记下相应的转换位置矩阵 $TN_{1n}=[t_1(n),t_2(n),\cdots,t_{MN}(n)]$。

步骤 3 根据 TN_{1n} 重新排列每一个低位向量 $Rp_i(i=1,2,3,4)$ 的元素，也就是移动向量 Rp_i 中的 $t_1(n)$ 元素到第一个元素位置，移动 $t_2(n)$ 到第二个元素位置等等，直到每个向量中的元素都被置乱，得到 Rp_i'。

步骤 4 将高四位二值图像 $Rpic_n(n=5,6,7,8)$ 的所有像素值相加，和记作 sum_1，计算 $h_1=sum_1 \bmod 4$ 的值，选择 $x_i(n)$ 中第 h_1 个混沌序列记为 Z_1。按照下式对 Z_1 进行变换得到序列 Z_1'。

$$Z_1'=floor(|Z_1|-floor(|Z_1|))\times 10^{14}) \bmod 256 \tag{2}$$

步骤 5 转换 Z_1' 为二值序列 Z_1''，选择 Z_1'' 的低四位，形成 4 个向量 $Z_i(i=1,2,3,4)$，每个向量长度为 $M\times N$。

步骤 6 根据式(3)对低四位进行扩散操作。

$$C_i=(Rp_i'+Rp_{i+4}+Z_i) \bmod 2(i=1,2,3,4) \tag{3}$$

转换 C_i 为 4 个二值图像，即得到加密后低四位的二值图像 $Rpic_i'(i=1,2,3,4)$。

(2)再用加密后的低四位的图像信息去加密高四位部分，具体操作如下：

步骤 1 用与上面不同的系统初值 $y_0(1)$、$y_0(2)$、$y_0(3)$、$y_0(4)$ 迭代混沌系统 $m_1+M\times N$ 次，舍弃前 m_1 个数值，得到 4 个长度为 $M\times N$ 的混沌序列。按升序排列 $y_i(n)=[y_{m_1+1}(n),y_{m_1+2}(n),\cdots,y_{m_1+MN}(n)](n=5,6,7,8)$ 的每个数值，得到 $y_i'(n)=[y'_{m_1+1}(n),y'_{m_1+2}(n),\cdots,y'_{m_1+MN}(n)](n=5,6,7,8)$，找出 $y_i'(n)$ 在 $y_i(n)$ 中的位置，并记下转换位置矩阵 $TN_{2n}=[t_1(n),t_2(n),\cdots,t_{MN}(n)]$。

步骤 2 根据 TN_{2n} 重新排列 R 图像矩阵每一个高四位向量 $Rp_i(i=5,6,7,8)$ 的元素，也就是移动向量 Rp_i 中的第 $t_1(n)$ 个元素到第 1 个元素位置，移动 $t_2(n)$ 个元素到第 2 个元素位置等等，直到每个向量中的元素都被置乱，得到置乱后

的向量 Rp_i'。

步骤 3　将已加密的低四位二值图像 $Rpic_n'$ 的所有二值图像像素值相加得到和 sum_2，计算 $h_2=sum_2 \bmod 4$。选择 $x_i(n)$ 中第 h_2 个混沌序列，记为 Z_2，按照下式对 Z_2 进行变换。

$$Z_2'=floor(|Z_2|-floor(|Z_2|)\times 10^{14}) \bmod 256 \quad (4)$$

步骤 4　转换 Z_2' 为二值序列 Z_2''，选择 Z_2'' 的高四位，形成了 4 个向量 $Z_i(i=5,6,7,8)$，每个向量长度为 $M\times N$。

步骤 5　根据式(5)进行像素值扩散操作。

$$C_i=(Rp_i'+C'_{i-4}+Z_i) \bmod 2(i=5,6,7,8) \quad (5)$$

转换 C_i 为 4 个二值图像，即得到加密后高四位的二值图像 $Rpic_i'(i=5,6,7,8)$。

(3)经过操作(1)和(2)得到的 $Rpic_i'(i=1,2,3,4,5,6,7,8)$ 是加密后的二值图像，将其合并即可得到加密后的图像 R_1。

接着以同样的方法依次加密 G、B 图像，得到加密后的图像 G_1、B_1。然后将图像矩阵 R_1、G_1、B_1 横向排列组合为图像 P_1，按照同样的方法加密 P_1，得到加密后的密文图像 P_2。联合加密降低了图像三基色分量之间的相关性，可有效增强加密效果。R 图像矩阵的具体加密步骤如图 2 所示。

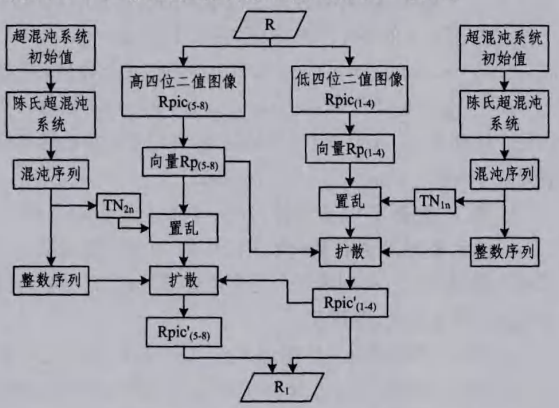


图 2　R 矩阵加密流程

4　图像解密方法

解密步骤与加密步骤相似，但顺序相反。

首先对需要解密的密文图像进行 R、G、B 三基色分离，对密文图像 P_2 解密后得到 P_1，分解 P_1 得到 R_1、G_1、B_1，再对 R_1、G_1、B_1 分别解密得到 R、G、B，三基色分量组合得到解密后的图像 P。

以解密 P_1 为例：

步骤 1　选取与加密过程中相同的初始参数和初值，以同样的方法得到 TN_{1n}、TN_{2n}、$x_i(n)$、$y_i(n)$。

步骤 2　图像 P_1 转化为对应的二进制灰度图像 $Rpic_i'(i=1,2,3,4,5,6,7,8)$，由低四位二值图像 $Rpic_n'$ 得出 h_2 的值，确定扩散所用的混沌序列 Z_i，计算选择方法与加密时相同。

用式(6)进行高四位反向扩散操作，得到逆扩散矩阵向量 $Rp_i'(i=5,6,7,8)$。

$$Rp_i'=(C_i-C'_{i-4}-Z_i) \bmod 2(i=5,6,7,8) \quad (6)$$

步骤 3　由 TN_{2n} 反向置乱高四位图像向量 Rp_i'，得到解密后的高四位图像矩阵 $Rpic_n(n=5,6,7,8)$。

步骤 4　由高四位二值图像 $Rpic_n$ 计算 h_1，确定扩散用混沌序列 Z_i，计算选择方法与加密时的相同。

用式(7)进行低四位反向扩散操作，得到逆扩散矩阵向量 $Rp_i'(i=1,2,3,4)$。

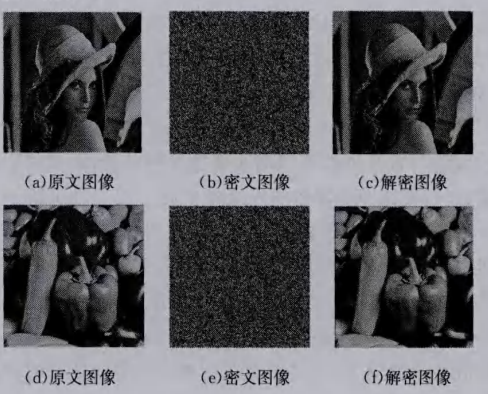
$$Rp_i'=(C_i-Rp_{i+4}-Z_i) \bmod 2(i=1,2,3,4) \quad (7)$$

步骤 5　由 TN_{1n} 反向置乱低四位矩阵向量 Rp_i'，得到解密后的低四位图像矩阵 $Rpic_n(n=1,2,3,4)$。

最后，将 8 个 $Rpic_n(n=1,2,\cdots,8)$ 二值图像矩阵合并转化为十进制图像，即可得到解密后的图像 P。

5　实验仿真及安全性分析

实验中选用 256×256 的 Lena 和 Pepper 图像作为被加密图像，在 Matlab7.1 下进行仿真。Chen 超混沌系统的参数取 $a=35$，$b=3$，$c=12$，$d=7$，$e=0.58$，这样，系统是超混沌的。混沌系统状态的初始值分别为 $(x_0(1),x_0(2),x_0(3),x_0(4))=(-4,-3,5,-6)$，$(y_0(1),y_0(2),y_0(3),y_0(4))=(-6,-4,4,-3)$。选择 $m=1000$，$m_1=1200$。图像加密、解密的结果如图 3 所示。



(a)原文图像　(b)密文图像　(c)解密图像

(d)原文图像　(e)密文图像　(f)解密图像

图 3　2 种测试图像加密、解密仿真结果

一个好的算法应该可以抵抗所有的已知攻击类型，例如穷举攻击、统计攻击和选择明文攻击。下面对本文所提算法的安全性进行分析。

5.1　密文图像的随机性测试

本文使用 NIST SP 800-22a 测试组来验证密文图像(图 3(b)和图 3(e))的随机性，测试结果取决于接受水平 P。如果 $P=1$，表明测试序列完全随机；如果 $P=0$，则测试序列完全不随机。每次测试时，显著性水平 α 被选择。如果 $P\geqslant\alpha$，则测试序列是随机的。为了便于进行随机性测试，从密文图像中随机选择 1256000 位的二进制序列，选择 $\alpha=0.01$，测试结果如表 1 所列。

表 1　密文图像的随机性测试

NIST SP 800-22a	图 3(b)		图 3(e)	
测试项目	接受水平 P	测试结果	接受水平 P	测试结果
频率	0.9833	通过	0.7604	通过
块式频率	0.9001	通过	0.8104	通过
动向	0.3568	通过	0.2102	通过
块内最长游程	0.1296	通过	0.4561	通过
矩阵的秩	0.2834	通过	0.6519	通过
频谱	0.6147	通过	0.5468	通过
非重叠字匹配	0.5096	通过	0.3109	通过
重叠字匹配	0.5689	通过	0.4672	通过
Maurer 通用统计	0.4879	通过	0.3451	通过
线性复杂度	0.7568	通过	0.9811	通过
系列	0.8865	通过	0.7655	通过
近似熵	0.9995	通过	0.9992	通过
正向累积和	0.9036	通过	0.8766	通过
反向累积和	0.7890	通过	0.9102	通过

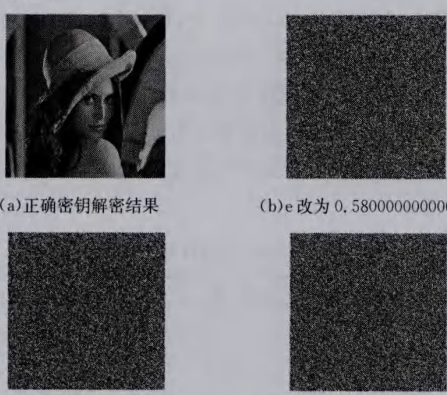
由表 1 可知，每项测试得到的 $P>0.01$，本文算法成功通过 NIST SP 800-22a 测试，这表明利用本文算法加密得到的密文随机分布，算法具有足够的安全性。

5.2 密钥空间分析

根据 Kerckhoff 准则，加密系统的安全性仅仅取决于它的密钥，无论加密算法设计得多么强大，如果密钥选择不好或者密钥空间太小，那么这个系统也很容易被攻破[15]。本文算法中，陈氏超混沌系统的参数 a、b、c、d、e，4 个状态变量的初始条件($x_0(1)$，$x_0(2)$，$x_0(3)$，$x_0(4)$，$y_0(1)$，$y_0(2)$，$y_0(3)$，$y_0(4)$)和混沌运算迭代参数 m、m_1 作为原始密钥，每个数据用 14 位十进制数字的实数表示。密钥空间为 $10^{210}\approx 2^{699}$，相当于二进制的 699bit 密钥长度，密钥空间巨大。DES 算法密钥长度为 56bit，3-DES 为 112bit，IDEA 为 128bit，AES 最大为 256bit。文献[20]设计的加密系统中只有 3 个密钥，如果每个数据精度为 10^{14}，密钥空间为 $10^{42}\approx 2^{126}$，相当于二进制的 126bit 密钥长度。本文算法中若将参数 h_1 和 h_2 也作为加密密钥，则密钥空间更大，这么大的密钥空间足以抵抗任何穷举攻击。

5.3 密钥敏感性分析

一个好的密码算法对密钥必须非常敏感，这意味着密钥的 1bit 的变化都应该导致完全不同的加密和解密结果。针对 Lena 图像，将密钥分别进行改变，对密文进行解密，结果如图 4 所示。使用正确的密钥解密结果如图 4(a)所示，得到的解密图像与原始图像相同；图 4(b)是将 e 改为 0.58000000000001后所得的解密图像；图 4(c)和图 4(d)是分别将($x_0(1)$，$x_0(2)$，$x_0(3)$，$x_0(4)$)改为(−4.00000000000001，−3，5，−6)和将($y_0(1)$，$y_0(2)$，$y_0(3)$，$y_0(4)$)改为(−6，−4.00000000000001，4，−3)后所得到的解密图像，解密图像与原始图像截然不同。密钥的微小变化就可以得到一个完全不同的解密结果，即该算法对密钥非常敏感。



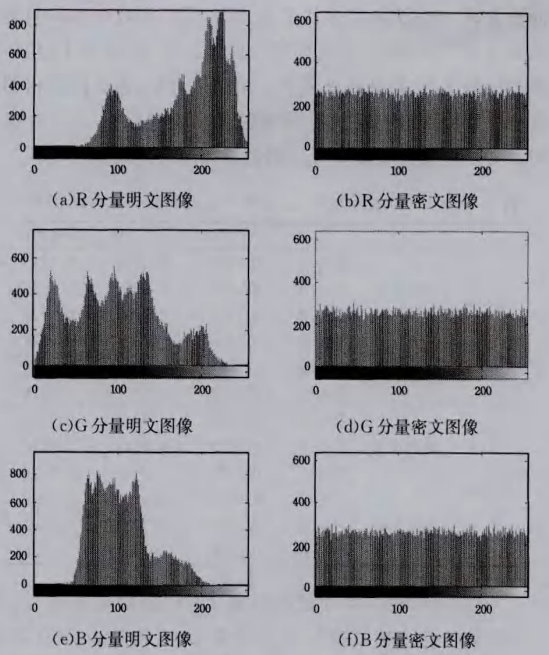
(a)正确密钥解密结果　(b)e 改为 0.58000000000001

(c)$x_0(1)$改为−4.00000000000001　(d)$y_0(2)$改为−4.00000000000001

图 4　密钥敏感性测试

5.4 图像直方图分析

直方图反映了图像的灰度级与其出现频率之间关系的统计特性。图 5 分别为 Lena 图像明文和密文 R、G、B 分量图像的直方图，可见密文图像的直方图比明文图像的直方图更为均匀，表明加密算法能有效地隐藏明文图像的统计信息，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　明文和密文图像 R、G、B 分量直方图

5.5 相关性分析

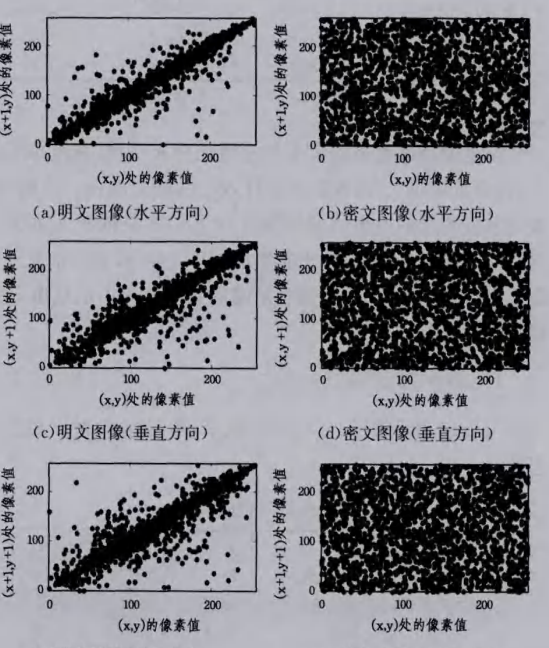
图像文件相邻像素具有很大的相关性，这为信息泄露提供了可能。为达到抵抗统计攻击的目的，加密算法应尽可能地降低相邻像素之间的相关性。相关性系数计算公式如下：

$$R_{x,y}=\frac{cov(xy)}{\sqrt{D(x)D(y)}} \tag{8}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \tag{9}$$

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{10}$$

$$cov(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \tag{11}$$



(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)　(b)密文图像(对角方向)

图 6　相邻像素的相关性

在 Lena 原文图像及加密后的图像中各随机选择 5000 对

的像素点，测试它们的水平方向、垂直方向和对角方向的相邻像素之间的相关性，结果如图 6 所示。对 Lena 和 Pepper 图像进行测试，结果如表 2 所列。由结果可知，原文图像相邻像素相关系数接近 1，密文图像相邻像素相关系数接近 0，这表明本文所提算法有效降低了图像相邻像素之间的相关性。

表 2　R、G、B 分量中水平、垂直和对角方向相邻像素的相关性

			水平方向	垂直方向	对角方向
Lena	原文图像	R 分量	0.9607	0.9261	0.9116
		G 分量	0.9489	0.9077	0.9051
		B 分量	0.9112	0.8799	0.8723
	密文图像	R 分量	0.0453	−0.0013	−0.0343
		G 分量	−0.0016	0.0127	0.0483
		B 分量	0.0906	0.0326	0.0518
Pepper	原文图像	R 分量	0.9626	0.9648	0.9393
		G 分量	0.9750	0.9641	0.9470
		B 分量	0.9590	0.9586	0.9226
	密文图像	R 分量	0.0391	0.0339	0.0137
		G 分量	0.0346	0.0236	0.0391
		B 分量	0.0236	−0.0017	−0.0284

彩色图像 R、G、B 分量之间也具有很强的相关性为了测试本文算法的去相关能力，接着计算 Lena 和 Pepper 原文、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 3。由表可知，密文图像 R、G、B 分量之间相同位置像素的相关性远小于原文图像。与文献[10,13,21,23]结果相比可知，利用本文算法得到的密文图像相邻像素的相关性更低，其可以更有效地抵抗统计攻击的影响。

表 3　R、G、B 分量之间相同位置像素的相关性

	R、G 分量之间相邻位置	R、B 分量之间相邻位置	G、B 分量之间相邻位置
Lena 原文图像	0.8793	0.6775	0.9104
Lena 密文图像	−0.0096	0.0031	0.0124
Pepper 原文图像	0.3040	0.3901	0.8601
Pepper 密文图像	0.0141	0.0534	−0.0148
文献[10]密文图像	0.2480	0.1390	0.1713
文献[13]密文图像	−0.0126	−0.0077	−0.0463
文献[21]密文图像	0.3053	0.2042	0.2525
文献[23]密文图像	0.2312	0.1254	0.1611

5.6　信息熵分析

信息熵用来度量图像中灰度值的分布情况，灰度分布越均匀，信息熵越大，图像抵抗统计攻击的能力越强。一幅 256 级的灰度图像的理想信息熵值应该为 8，如果低于 8，预示着有可能受到安全威胁；如果非常接近理论值 8，表示信息的遗漏是可以忽略的，加密系统有足够的安全性级。信息源 m 的信息熵计算公式如下：

$$H(m)=\sum_{i=0}^{2^n-1}p(m_i)\log\frac{1}{p(m_i)} \tag{12}$$

其中，$p(m_i)$表示符号 m_i 出现的概率，2^n 是信息源 m 的总状态数。

表 4　信息熵

	R 分量	G 分量	B 分量
本文算法 Lena 密文图像	7.9973	7.9973	7.9975
本文算法 Pepper 密文图像	7.9973	7.9971	7.9971
文献[21]Fig. 6(d)	7.9791	7.9802	7.9827
文献[21]Fig. 8(a)	7.9871	7.9881	7.9878
文献[13] Lena 密文图像	7.9973	7.9981	7.9978

对标准 Lena 和 Pepper 图像采用本文算法加密，密文图像 R、G、B 分量的信息熵结果见表 4。将本文结果与文献[21]采用 PWLCM 混沌序列位级加密的密文图像(图 6(d))、采用三维陈氏混沌系统位级加密的密文图像(图 8(a))以及文献[13] Lena 密文图像的信息熵结果相比较可知，利用本文算法得到的信息熵结果更接近理想值 8，这说明利用本算法加密后的密文图像更接近随机分布，可以更有效地抵抗统计攻击。

5.7　明文敏感性分析

根据密码学原理，好的加密算法应该对明文充分敏感，敏感性越强，抵抗差分攻击的能力也就越强[24]。加密算法对明文的敏感性可以用像素数改变率 NPCR(Number of Pixels Change Rate)和归一化像素值平均改变强度 UACI(Unified Average Changing Intensity)来度量。计算公式如下：

$$NPCR=\frac{\sum_{i,j}D(i,j)}{W\times H}\times 100\% \tag{13}$$

$$UACI=\frac{1}{W\times H}\left[\sum_{i,j}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right]\times 100\% \tag{14}$$

对于 8 位灰度图像，NPCR 和 UACI 的理想期望值可以用下面的公式计算：

$$NPCR_E=(1-2^{-n})\times 100\% \tag{15}$$

$$UACI_E=\frac{1}{2^{2n}}\frac{\sum_{i=1}^{2^n-1}i(i+1)}{2^n-1}\times 100\% \tag{16}$$

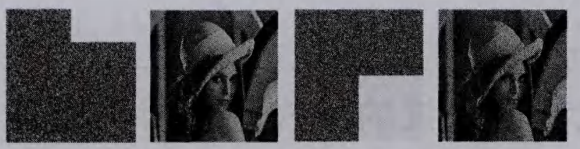
对于 8 位灰度图像，将 $n=8$ 代入上面公式进行计算，$NPCR_E=99.60\%$，$UACI_E=33.46\%$。Lena 明文图像第一个像素的数值由 226 改为 227 后得到一个新的图像，然后用同样的密钥对这两个图像加密形成相应的密文 C_1 和 C_2，利用式(13)和式(14)计算密文图像的 NPCR 和 UACI，结果见表 5。与文献[13]和文献[21]的结果相比，本文结果更接近理想值，这表明本文算法可以有效抵抗明文攻击。为便于和灰度图像的加密算法进行比较，本文定义 $NPCR_{average}=(NPCR_R+NPCR_G+NPCR_B)/3$，$UACI_{average}=(UACI_R+UACI_G+UACI_B)/3$，则 $NPCR_{average}=0.9961$，$UACI_{average}=0.33453$。与 Zhu 等[20]设计的加密系统循环三轮后的最好结果 0.99605 和 0.33399 相比较可知，利用本文算法得到的 UACI 值更接近理想值，这表明本文算法具有更强的抗明文攻击性能。

表 5　C_1 和 C_2 的 NPCR、UACI 值

相关性	R 分量	G 分量	B 分量
本文 NPCR	0.9962	0.9960	0.9961
文献[13]NPCR	0.9964	0.9960	0.9965
文献[21]NPCR	0.9963	0.9959	0.9956
本文 UACI	0.3344	0.3346	0.3346
文献[13]UACI	0.3342	0.3342	0.3347
文献[21]UACI	0.3349	0.3340	0.3322

5.8　抗剪切攻击分析

图像在传输过程中，可能出现数据信息丢失的情况。对密文图像分别进行 1/8、1/4 剪切攻击，测试算法在密文图像信息不完整情况下的解密效果，具体见图 7。由图可知，本算法有一定的抗剪切攻击能力，密文图像在丢失部分数据信息后，本文算法依然能解密出原图像的大部分信息；随着密文图像数据丢失量的增大，解密图像获得的有效信息逐渐减少。



(a)1/8 剪切图像　(b)解密图像　(c)1/4 剪切图像　(d)解密图像

图 7　抗剪切攻击实验

5.9　算法效率分析

本算法的测试软件是 Matlab7.1，PC 机硬件 CPU 为 3GHz，内存为 8GB。文献[25]中图像加密需要重复运行混沌系统 7 次，而本文算法只需要 1 次就能得到很好的加密效果，加解密速度相对更快。分别用本文加密算法和文献[25]的算法对同一图像进行加密，文献[25]的加密操作需要 10.54s，而本文加密算法需要 7.2s，因此，本文的加密算法具有较好的加密效率。

结束语　本文提出了一种在位级进行加密的彩色图像自适应加密算法，利用陈氏超混沌系统产生的混沌序列对图像进行置乱和扩散操作。自适应加密中用高四位的二值图像信息去加密低四位，再用加密后的低四位信息去加密高四位。将加密后的图像三基色分量矩阵横向排列组合联合加密，降低了图像三基色分量之间的相关性，可有效增强加密效果。加密算法使得密文与明文、密钥之间的关系复杂化，部分密钥依赖于明文，增加了算法对明文的敏感性。实验结果和安全性分析表明，该算法的密钥空间大，密文相邻像素的相关性远低于明文，密文分布均匀，明文敏感性高，可有效抵抗穷举攻击、差分攻击和选择明文攻击。因此，本文算法在彩色图像保密通信等领域具有更大的应用潜力。

参 考 文 献

[1] Wang Z, Huang X, Li Y X, et al. A new image encryption algorithm based on the fractional-order hyperchaotic Lorenz system [J]. Chinese Physics B, 2013, 22(1): 010504

[2] Armand Eyebe Fouda J S, Yves Effa J, Sabat Samrat L, et al. A fast chaotic block cipher for image encryption[J]. Communications in Nonlinear Science and Numerical Simulation, 2014, 19(3): 578-588

[3] Yuen C H, Wong K W. Chaos-based encryption for fractal image coding[J]. Chinese Physics B, 2012, 21(1): 010502

[4] Tong X J. Design of an image encryption scheme based on a multiple chaotic map[J]. Communication Nonlinear Science and Numerical Simulation, 2013, 18(7): 1725-1733

[5] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps[J]. International Journal of Bifurcation and Chaos, 1998, 8(6): 1259-1284

[6] Wen Chang-ci, Wang Qin, Huang Fu-min, et al. Self-adaptive encryption algorithm for image based on affine and composed chaos [J]. Journal on Communications, 2012, 33(11): 119-127 (in Chinese)
文昌辞，王沁，黄付敏，等. 基于仿射和复合混沌的图像自适应加密算法[J]. 通信学报，2012，33(11)：119-127

[7] 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

[8] Li S S, Zhao Y H, Qu B Y, et al. Image scrambling based on chaotic sequences and VeginSre cipher [J]. Multimedia Tools and Applications, 2013, 66(3): 573-588

[9] 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

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

[11] 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

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

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

[14] Arroyo D, Diaz J, Rodriguez F B. Cryptanalysis of a one round chaos-based substitution permutation network[J]. Signal Processing, 2013, 93: 1358-1364

[15] Alvarez G, Li S. Some basic cryptographic requirements for chaos based cryptosystems[J]. International Journal of Bifurcation and Chaos, 2006, 16(8): 2129-2151

[16] Ye G D, Wong K W. An image encryption scheme based on time-delay and hyperchaotic system[J]. Nonlinear Dynamics, 2013, 71(1/2): 259-267

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

[18] 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

[19] 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

[20] 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

[21] 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

[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] Zhu Cong-xu, Sun Ke-hui. Cryptanalysis and improvement of a class of hyperchaos based image encryption algorithms[J]. Acta Phys. Sin., 2012, 61(12): 120503(in Chinese)
朱从旭，孙克辉. 对一类超混沌图像加密算法的密码分析与改进[J]. 物理学报，2012，61(12)：120503

[25] Xu Bing, Sun Yong-wei, Li Yang, et al. Improved encryption algorithm based on high-dimension chaotic system[J]. Journal of Jilin University(Information Science Edition), 2012, 30(1): 12-17(in Chinese)
许冰，孙永维，李洋，等. 基于高维混沌系统的图像加密改进算法[J]. 吉林大学学报(信息科学版)，2012，30(1)：12-17