引用格式：GUO Yuan, ZHOU Yan-yan, JING Shi-wei. Multiple-image Encryption Based on Image Recombination and Bit Scrambling[J]. *Acta Photonica Sinica*, 2020, **49**(4):0410002
郭媛,周艳艳,敬世伟.基于图像重组和比特置乱的多图像加密[J].光子学报,2020,**49**(4):0410002

基于图像重组和比特置乱的多图像加密

郭媛,周艳艳,敬世伟
(齐齐哈尔大学 计算机与控制工程学院,黑龙江 齐齐哈尔 161006)

摘　要:针对现有多图像加密算法只能同时加密多张同类型同大小的图像,适用范围不广、实用性差等问题,提出一种基于图像重组和比特置乱的多图像加密算法.该算法通过将任意数量、不同大小和不同类型的图像重新组合成新多灰度图,一次完成同时加密,极大提高了加密效率和适用范围.首先,依次提取所有待加密图像像素值重新组合出 N 张 $m\times n$ 新灰度图,并将其转化成 $m\times n\times 8N$ 二进制矩阵.然后,采用 3D 比特置乱方式,对高位页进行行列比特置乱,低位页进行整页比特置乱.最后,进行异或扩散操作,得到密文图像.高低位分开置乱提高了算法的抗噪声能力,最终密文信息熵达到 7.999 以上,很好地掩盖了明文的统计特性.构造一种新型 Logistic 与广义三阶 Fibonacci 级联的混沌系统产生随机序列,增加了初值和控制参数范围,扩大了密钥空间,使其达到 8×10^{84} 以上,极大地提高了抗穷举攻击能力.既提高了序列随机性,又同时保留了低维混沌系统的快速性.结合明文哈希值(SHA-256)产生密钥,明文像素值发生微小改变后密文像素值变化率达到 0.996 以上,极大地提高了的明文敏感性和算法抗选择明文攻击的能力.实验分析表明,提出的多图像加密算法安全性高、实用性强.

关键词:图像加密;多图像加密;图像重组;比特置乱;Logistic-Fibonacci 级联混沌;明文 SHA-256
中图分类号:TP309; TN918　　**文献标识码**:A　　**doi**:10.3788/gzxb20204904.0410002

Multiple-image Encryption Based on Image Recombination and Bit Scrambling

GUO Yuan, ZHOU Yan-yan, JING Shi-wei
(*School of Computer and Control Engineering, Qiqihar University, Qiqihar, Heilongjiang* 161006)

Abstract: Aiming at the problems that the existing multiple-image encryption algorithms can only encrypt multiple images of the same type and the same size at the same time, which limits the scope of its application and practicality, a multiple-image encryption algorithm based on image recombination and bit scrambling was proposed. By recombining the images of any number, any type and any size into the new multiple-gray scale images, the algorithm can complete simultaneous encryption at one time, which greatly improved the encryption efficiency and application range. Firstly, the pixel values of all images were extracted to be encrypted in turn and were recombined into N new gray-scale images of $m\times n$ size, which were converted into $m\times n\times 8N$ binary matrix next. Then, 3D bit scrambling is adopted to scramble rows and columns for high binary pages and the entire pages for low binary pages. Finally, the ciphertext image was obtained by XOR diffusion operation. The high-low separate scrambling improves the anti-noise ability of the algorithm. The information entropy of the final ciphertext was above 7.999, which well covered up the statistical characteristics of the plaintext. A new type of Logistic-Fibonacci cascade chaos was constructed to generate random sequences, which increased the range of initial values

基金项目:国家自然科学基金(No. 61872204),黑龙江省自然科学基金(No. F2017029),黑龙江省省属高等学校基本科研业务费科研项目(No. 135109236)
第一作者:郭媛(1974—),女,教授,博士,主要研究方向为光学检测及信息处理. Email:guoyuan171@126.com
通讯作者:周艳艳(1991—),女,硕士研究生,主要研究方向为图像处理. Email:15949810563@163.com
收稿日期:2020-01-08;**录用日期**:2020-03-18

and control parameters, expanded the key space to over 8×10^{84}, and greatly improve the ability to resist exhaustive attacks. The randomness of the sequence was improved, while the rapidity of the low-dimensional chaotic system was preserved. Combining with the plaintext hash value (SHA-256) to generate the key, the change rate of the ciphertext pixel value reached more than 0.996 after the plaintext pixel value was slightly changed, which greatly improved the sensitivity of the plaintext and the ability of resisting the selective plaintext attack. Experimental analysis show that the proposed multiple-image encryption algorithm has high security and strong practicability.

Key words: Image encryption; Multiple-image encryption; Image reorganization; Bit scrambling; Logistic-Fibonacci cascade chaos; Plaintext SHA-256

OCIS Codes: 100.4998;100.3020;000.5360;100.2000;100.2960

0 引言

图像加密是一种有效的图像保护技术,它将有意义图像转换成混乱状态,使攻击者无法观察到任何原始信息,实现图像保护.为保证图像的安全传输,人们提出了许多单图像加密算法[1-11].如 YANG Bo 等[1-2]提出基于矩阵变换的图像加密算法,ZHOU Guo-min 等[4-5]提出基于混沌系统的图像加密算法,LIU Zheng-jun [5-6]提出基于离散余弦变换域的彩色图像加密算法和 ZHANG Qiang 等[7-8]提出的基于 DNA 编码的图像加密算法等.以上方法均只能对单张图像进行多次单独加密,加密效率低,无法对多张图像同时加密.因此,高安全性和高效性的多图像加密成为新的需求.

目前,多图像加密方法按密文数量可分为两类.第一类方法是将多张图像加密成一张密文图像,如 DAS S 等[12]提出基于遗传算法的多图像加密方法,利用遗传算法对原始图像进行扩散,采用逐位异或运算,消除邻域像素的相似性,以获得加密图像.TANG Zhen-jun 等 [13]提出基于位平面分解和混沌映射的多灰度图加密方法,利用混沌映射产生的序列对分解的位平面进行随机交换位块和异或处理,获得一个 PNG 密文图像.该类算法无法通过密文数量得到明文数量,因而更加有效地掩盖了明文信息,但一次加密数量较少,加密效率低.第二类方法是将多张图像加密成多张密文图像,如 LIU Lei [14]等提出的利用稀疏化和空间复用的多图像加密方法以及 HUANG Zhi-jing 等 [15]提出的基于混沌系统和二维线性正则变换的非线性光学多图像加密方法.ZHANG Xiao-qiang 等 [16-17]提出一种基于脱氧核糖核酸编码和混沌系统的多张图像加密算法,与传统的图像加密算法不同,新算法的排列和扩散是在三维的脱氧核糖核酸矩阵上进行的.XIONG Y 等[18]提出一种新的基于像素交换操作和傅里叶域基本矢量分解的多图像加密方法,利用像素位置矩阵和相位密钥作为额外的私钥来增强基于 4-f 系统的密码系统的安全性.该类算法提高了加密图像数量,尤其文献[16-17]可同时加密任意数量图像,但密文图像数量与明文图像数量一致,安全性低.且都局限于一次加密同类型、同大小的多张图像,整体加密效率低,无法完成一次加密任意数量、不同类型和不同大小图像的现实需求.

针对以上问题,本文提出了一种基于图像重组和比特置乱的多图像加密算法,该算法通过将任意数量、不同大小和类型的多张图像像素依次提取出来,重新组合成设定大小新多图像的方式.使多图像加密不在局限于同大小、同类型的情况,为多图像加密提供新思路,增加了算法的实用性.采用高低位分开进行比特置乱的方式,减少了加密时间,极大地提高了加密效率和系统抗噪声攻击能力.采用一种新型 Logistic 与广义三阶 Fibonacci 级联的混沌系统(Logistic-Fibonacci,L-F)产生随机序列,序列分布均匀、随机性高、生成时间短,处于满映射区间宽,参数和初值个数多.利用密钥关联明文哈希值,使得加密系统达到"一次一密"的效果,提高明文敏感性和抗选择明密文攻击能力.

1 原理介绍

1.1 构建 L-F 级联混沌

为克服 logistic 产生的随机序列的稳定窗与空白区问题,构建一种 Logistic 与广义三阶 Fibonacci 级联的混沌系统,使得在参数 μ 处于混沌区间时能达到满映射且分布更加均匀.Logistic 与广义三阶 Fibonacci 函数[19]分别为

$$x_{n+1}=\mu x_n(1-x_n) \tag{1}$$

$$F_n=(AF_{N-1}+BF_{n-2}+CF_{n-3})\bmod M \tag{2}$$

式中,式(1)生成的序列 x_n 作为式(2)中的 A,B,C,每生成一个 F 换一组 A,B,C 值.为使 F 初值具有很好的敏感性,三个初值取同一值即 $F_1=F_2=F_3=\mathrm{int}F$,并将生成的序列对 1 取余,即

$$F_n=(x_{n-1}F_{n-1}+x_{n-2}F_{n-2}+x_{n-3}F_{n-3})\mathrm{mod}M \tag{3}$$

$$B_n=F_n\mathrm{mod}1 \tag{4}$$

为对比该级联混沌的可行性,令 $\mu=3.9$、$x_0=0.5$、$\mathrm{int}F=0.9$ 和 $M=191$.分叉图和序列分布图如图 1.

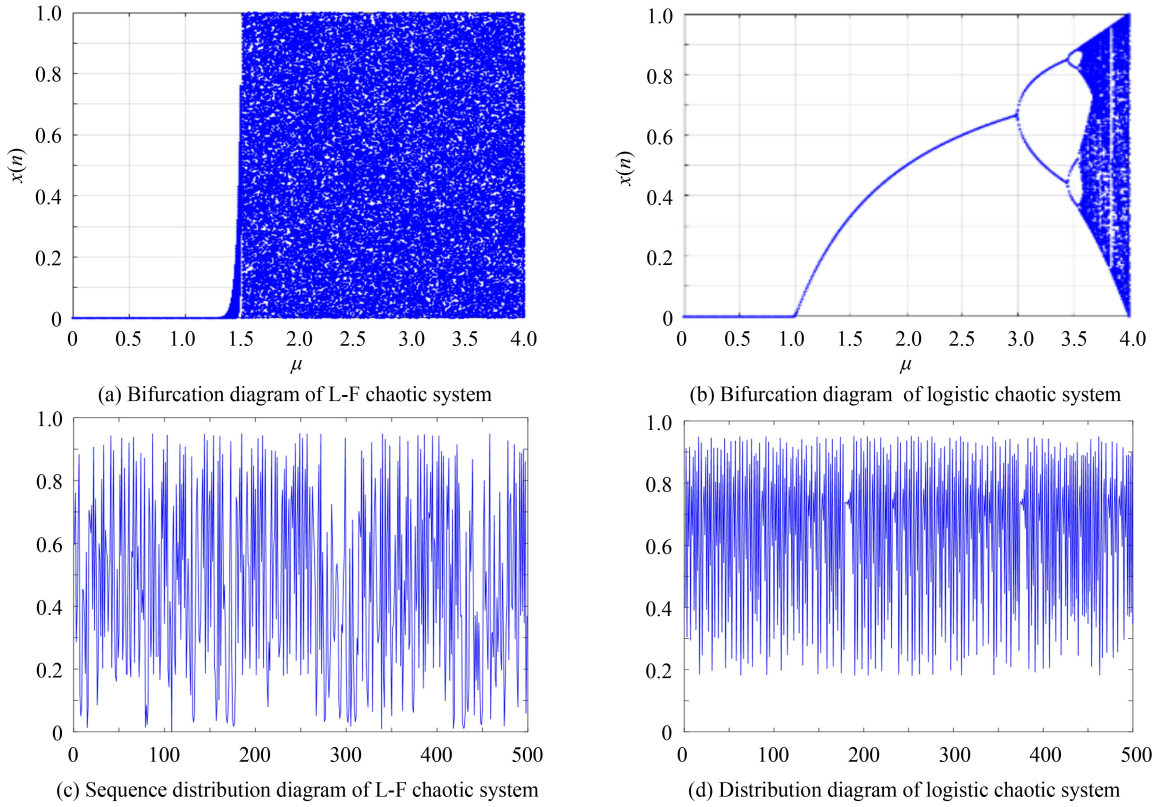


图 1 Logistic 和 L-F 的分叉图和序列分布图

Fig.1 Bifurcation diagram and sequence distribution diagram of Logistic chaotic system and L-F chaotic system

由图 1 可知 L-F 级联混沌系统的参数 μ 范围比 Logistic 更宽,且在处于混沌区间内不存在空白窗,分布更加均匀,同时增加了初值和控制参数个数.因此 L-F 用于图像加密安全性更高,能更好地抵御统计分析和蛮力攻击.

1.2 多图像重组与比特置乱

1.2.1 多图像重组

为达到可同时加密不同类型与大小图像的目的,采用多图像重组的方式.首先,依次读取 M 张原图像;其次,按先行后列再页的顺序依次提取所有像素值,并放入预先设定大小为 $m\times n\times N$ 的矩阵中.其中矩阵页数 N 由式(5)得出,若第 N 张有空余位置则由十进制数 170(10101010)填充.本文以设定新多图像尺寸大小为 512×512,对 4 张 256×256 灰度图、2 张 280×180 彩色图和 3 张 520×460 二值图同时加密为例,重组过程如图 2.

$$N=\left\lfloor\frac{\sum_{i=1}^{M}a_i\times b_i\times c_i}{m\times n}\right\rfloor\quad i=1,2,\cdots,M \tag{5}$$

式中,$\lfloor\rfloor$为向上取整,$m\times n$ 表示预先设定的矩阵大小,M 表示原图像个数,a,b,c 分别表示矩阵的行数、列数和页数,当明文为彩色图时 c_i 为 1,当明文为彩色图时 c_i 为 3.

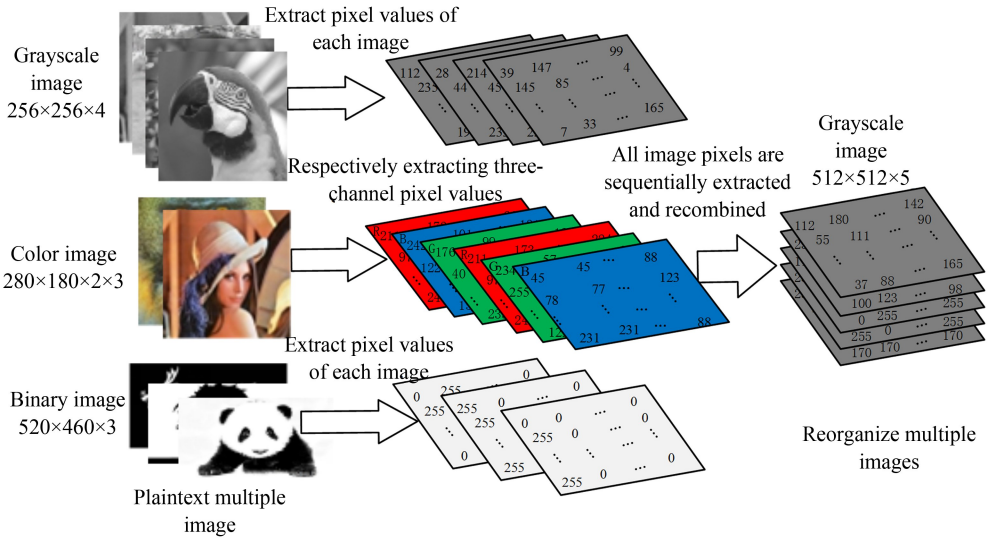


图 2 多图像重组过程

Fig.2 Multiple-image recombination process

1.2.2 比特置乱

将每个图像分解成 8 个位平面，由于每个位平面的权重不同，因此每个位平面所蕴含的图像信息也各不相同.各位平面所蕴含图像的信息量百分比计算表达式为

$$I^i=\frac{2^{i-1}}{255}\quad i=1,2,3,4,5,6,7,8 \tag{6}$$

可以看出 b_1 位到 b_8 位，图像信息逐渐增多，而 b_1 位到 b_4 位含信息不足整体的 6%.为了提高加密速度和抗噪声能力，采用将高位和低位分别进行比特置乱，高位先在每一页上分别按给出的随机序列进行行列循环移位置乱，所有页完成之后，再对页与页之间进行跨页行列循环移位操作，低位按随机数列进行整页的置乱即可.将高位页页数设为 4 的情况下高低位平面分解与置乱过程如图 3、图 4 和图 5 所示.

按照图 3、图 4、图 5 所示的位平面分解和高、低位分别置乱的方式操作之后，将置乱后的高位矩阵 $\boldsymbol{H}''$ 和置乱后的低位矩阵 $\boldsymbol{L}'$ 组合起来，按图 3 逆过程得到十进制下的中间密文 $\boldsymbol{TC}$.

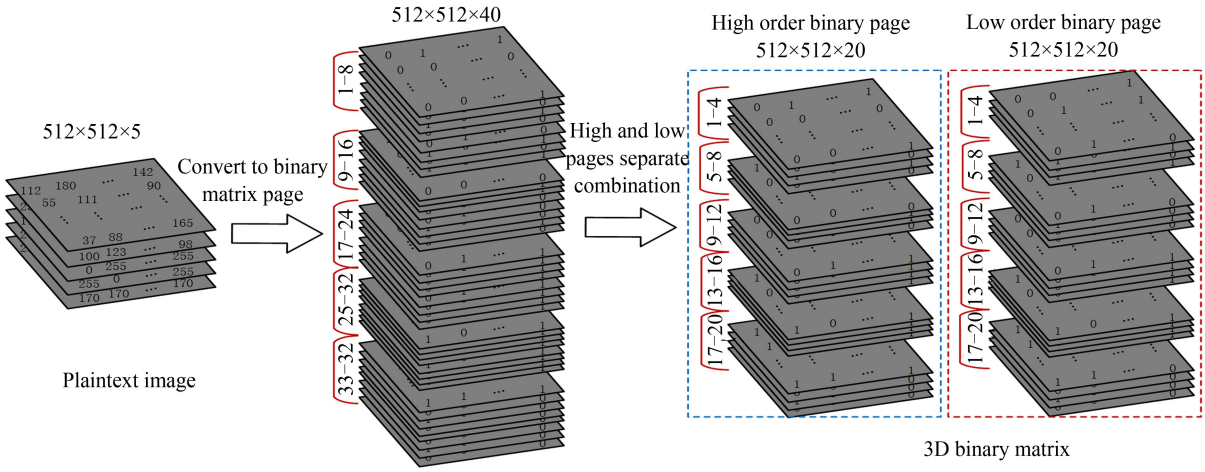


图 3 3D 二进制矩阵

Fig.3 3D binary matrix

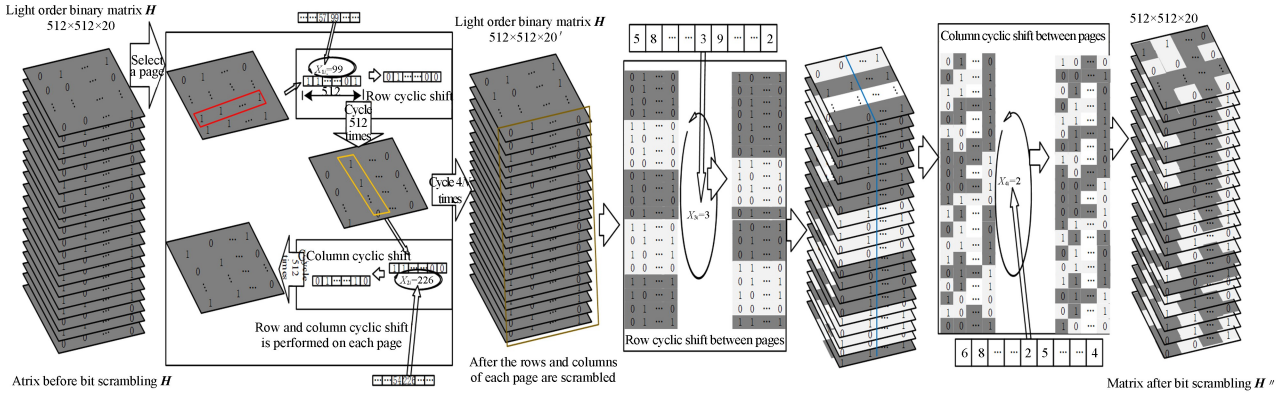


图 4　高平面比特置乱

Fig.4　High plane bit scrambling

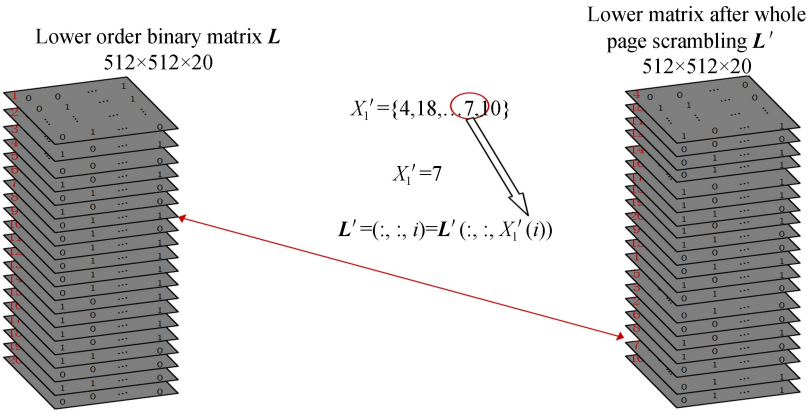


图 5　低平面比特置乱

Fig.5　Low plane bit scrambling

2　加解密过程

该算法加密主要分为三大部分:1)密钥及混沌序列的产生;2)3D比特置乱;3)扩散运算.加密过程如图6.

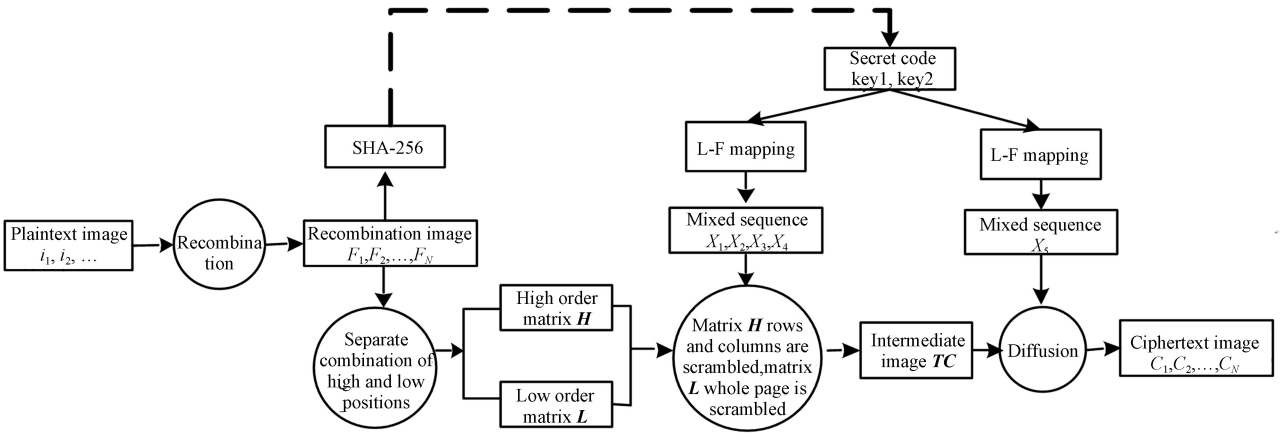


图 6　加密过程

Fig.6　Encryption process

2.1　密钥及混沌序列的产生

针对现有图像加密系统的抗选择明密文攻击能力弱,以及扩散效果不明显的问题.本文将混沌密钥与明文 SHA-256 关联产生随明文自适应变化的动态密钥,提高抗选择明(密)文攻击的能力.

1)密钥产生

先将所有的图像按图 2 所示重组形成一个三维矩阵 $\boldsymbol{F}$，求出其 SHA-256 并将 256 位哈希值每八位分为一组，可以表示为 $H=h_1,h_2,\cdots,h_{32}$；其中 h_i 为 $h_i=[h_{i,0},h_{i,1},\cdots,h_{i,7}]$.设定密钥为 key1($x_{0,1}$,$\mu_1$,int$F_{0,1}$,$k$)、key2($x_{0,2}$,$\mu_2$,int$F_{0,2}$)，分别作为 3D 比特置乱和扩散的混沌初值和参数，由式(7)～(9)求取

$$x_{0,1}=\mathrm{mod}\{\{x'_{0,1}+\mathrm{mod}[(h_1\oplus h_2\oplus h_3\oplus h_4\oplus h_5\oplus h_6\oplus h_7\oplus h_8),256]/256\},1\} \tag{7}$$

$$\mathrm{int}F_{0,1}=\mathrm{mod}\{\{\mathrm{int}F'_{0,1}+\mathrm{mod}[(h_9\oplus h_{10}\oplus h_{11}\oplus h_{12}\oplus h_{13}\oplus h_{14}\oplus h_{15}\oplus h_{16}),256]\},1\} \tag{8}$$

$$x_{0,2}=\mathrm{mod}\{\{x'_{0,2}+\mathrm{mod}[(h_{17}\oplus h_{18}\oplus h_{19}\oplus h_{20}\oplus h_{21}\oplus h_{22}\oplus h_{24}\oplus h_{25}),256]/256\},1\} \tag{9}$$

$$\mathrm{int}F_{0,2}=\mathrm{mod}\{\{\mathrm{int}F'_{0,2}+\mathrm{mod}[(h_{25}\oplus h_{26}\oplus h_{27}\oplus h_{28}\oplus h_{29}\oplus h_{30}\oplus h_{31}\oplus h_{32}),256]\},1\} \tag{10}$$

式中，mod 为取余运算，$\oplus$ 为异或运算，$x'_{0,1}$、$x'_{0,2}\in[0,1]$，int$F'_{0,1}$、int$F'_{0,2}\in[0,1]$.再利用产生的 $x_{0,1}$、int$F_{0,1}$、$x_{0,2}$、int$F_{0,2}$计算控制参数 μ_1、μ_2.

$$\mu_1=\mathrm{mod}(\mu'_1/4+x_{0,1}+\mathrm{int}F_{0,1},1)\times(4-1.5)+1.5 \tag{11}$$

$$\mu_2=\mathrm{mod}(\mu'_2/4+x_{0,2}+\mathrm{int}F_{0,2},1)\times(4-1.5)+1.5 \tag{12}$$

式中，μ'_1、$\mu'_2\in[1.5,4]$，$x'_{0,1}$、$x'_{0,2}$、int$F_{0,1}{}'$、int$F_{0,2}{}'$、μ'_1、μ'_2、k 根据需要设定，其中，高位页页数 k 为了直接控制，不与哈希值相关联.

2)混沌序列产生

随机序列由混沌序列 L-F 级联混沌生成，为了消除暂态效应预先迭代 $N_{0,1}$、$N_{0,2}$次，$N_{0,1}$、$N_{0,2}$均与初值与参数有关，其表达式为

$$N_{0,1}=200+\lfloor\mathrm{mod}[(x_{0,1}+\mathrm{int}F_{0,1}+\mu_1)\times1012,200]\rfloor \tag{13}$$

$$N_{0,2}=200+\lfloor\mathrm{mod}[(x_{0,2}+\mathrm{int}F_{0,2}+\mu_2)\times1012,200]\rfloor \tag{14}$$

式中，$\lfloor\ \rfloor$为向上取整.迭代 $N_{0,1}$次后继续迭代$(kN+1)\times(m+n)$次，得到混沌序列 T.再利用式(15)～(19)将 T 转化为可直接运用的序列，其中，$X_1\sim X_4$ 和 X'_1 的范围分别为$\{0\leqslant X_1\leqslant n\mid X_1\in N^*\}$、$\{0\leqslant X_2\leqslant m\mid X_2\in N^*\}$、$\{0\leqslant X_3\leqslant kN+1\mid X_3\in N^*\}$、$\{0\leqslant X_4\leqslant kN+1\mid X_4\in N^*\}$和$\{0\leqslant X'_1\leqslant(8-k)N\mid X'_1\in N^*\}$.再次设定初值和参数先迭代 $N_{0,2}$次后再迭代 $N\times m\times n$ 次得到序列 T'并由式(20)转换为 0 至 255 的整数序列 X_5，作为扩散序列.

$$X_{1i}=\lfloor\mathrm{mod}(T_i\times1012,n+1)\rfloor\quad i=1,2,\cdots,kN\times m \tag{15}$$

$$X_{2i}=\lfloor\mathrm{mod}(T_{kN\times m+i}\times1012,m+1)\rfloor\quad i=1,2,\cdots,kN\times n \tag{16}$$

$$X_{3i}=\lfloor\mathrm{mod}(T_{kN\times(m+n)+i}\times1012,kN+1)\rfloor\quad i=1,2,\cdots,m \tag{17}$$

$$X_{4i}=\lfloor\mathrm{mod}(T_{kN\times(m+n)+i}\times1012,kN+1)\rfloor\quad i=1,2,\cdots,n \tag{18}$$

$$X'_1=s_{\mathrm{ort}}(T_{i=1,2,\cdots,(8-k)N}) \tag{19}$$

$$X_{5i}=\lfloor\mathrm{mod}(T'_i\times1012,256)\rfloor\quad i=1,2,\cdots\cdots \tag{20}$$

式中，s_{ort}表示将序列 X_{1i}按从小到大顺序的排列，取得对应点位置的索引用序列 X'_1 表示.

2.2 3D 比特置乱加密

1) 将重组图像 $f_1\sim f_N$ 按图 3 方式转换为 512×512×kN 的高平面矩阵 $\boldsymbol{H}$ 和 512×512×$(8-k)N$ 的低平面矩阵 $\boldsymbol{L}$；

2)按图 4 方式运用序列 X_1、X_2、X_3、X_4 对矩阵 $\boldsymbol{H}$ 进行比特置乱，采用先行后列的顺序，先对每一页进行行列循环，再在页与页之间进行行列循环，得到矩阵 $\boldsymbol{H}''$；

3) 运用序列 X'_1 对矩阵 $\boldsymbol{L}$ 进行整页排序，得到矩阵 $\boldsymbol{L}'$；

4) 将置乱后矩阵 $\boldsymbol{H}''$和排序后矩阵 $\boldsymbol{L}'$利用 1.2.2 节的 3D 转换方式反向操作，得到十进制下的 512×512×N中间密文 $\boldsymbol{TC}$.

2.3 扩散操作

3D 比特置乱虽然改变了图像 0、1 比特的位置，但并未改变总体的比重.因此，为更好地掩盖图像的统计特性，增加明密文的雪崩效应，本文利用随机序列 X_5 对置乱排序后的中间密文图像 $\boldsymbol{TC}$ 进行异或扩散，首先将 $\boldsymbol{TC}$ 按先行后列再页的顺序转换成一维矩阵 $\boldsymbol{TC}'$，再对其进行异或扩散过程.

$$\begin{cases} C'_1 = \mathrm{mod}(X_{51} + TC'_1, 256) \oplus C_0 & i = 1 \\ C'_i = \mathrm{mod}(X'_{5i} + TC'_i, 256) \oplus C'_{i-1} & i \neq 1 \end{cases} \tag{21}$$

式中，C_0 为异或扩散初始值，取 0～255 之间的整数，本文取 150.

最后，将 C' 按先行后列再页的顺序转换成三维矩阵 $\boldsymbol{C}$，即密文图像 $\boldsymbol{C}$.

2.4 解密算法

解密过程为加密过程的逆过程，运用式(22)进行扩散的解密，得到一维矩阵 $\boldsymbol{TC}'$，按先行后列再页转换成三维矩阵 $\boldsymbol{TC}$，即中间密文.

$$\begin{cases} TC'_1 = \mathrm{mod}(C_0 \oplus C'_n + 256 - X_{51}, 256) & i = 1 \\ TC'_i = \mathrm{mod}(C'_{i-1} \oplus C'_i + 256 - X_{5i}, 256) & i \neq 1 \end{cases} \tag{22}$$

将中间密文转化为 3D 二进制状态，运用 X_4、X_3、X_2、X_1 和 X'_1 进行比特置乱的反向置乱，再将反向置乱后的高低位页组合起来，转化成十进制矩阵，最后根据明文图像的大小进行重组的逆过程得到解密图像.

3 实验分析

为验证本文算法的有效性和可行性，本文选取一张 lena(256×256)和 gril(260×280)的灰度图、一张彩色图 lena(200×200×3)和 monkey(512×512×3)的彩色图像和一张 dragon(500×269)二值图作为明文图像.并设置 $x'_{0,1}$、$x'_{0,2}$、$\mathrm{int}F'_{0,1}$、$\mathrm{int}F'_{0,2}$、μ'_1、μ'_2 和 k 分别为 0.9、0.95、0.9、0.95、1.6、1.65 和 3，再根据图像的 SHA-256 生成动态密钥.采用 MATLAB R2016a 作为仿真平台，加解密结果如图 7.

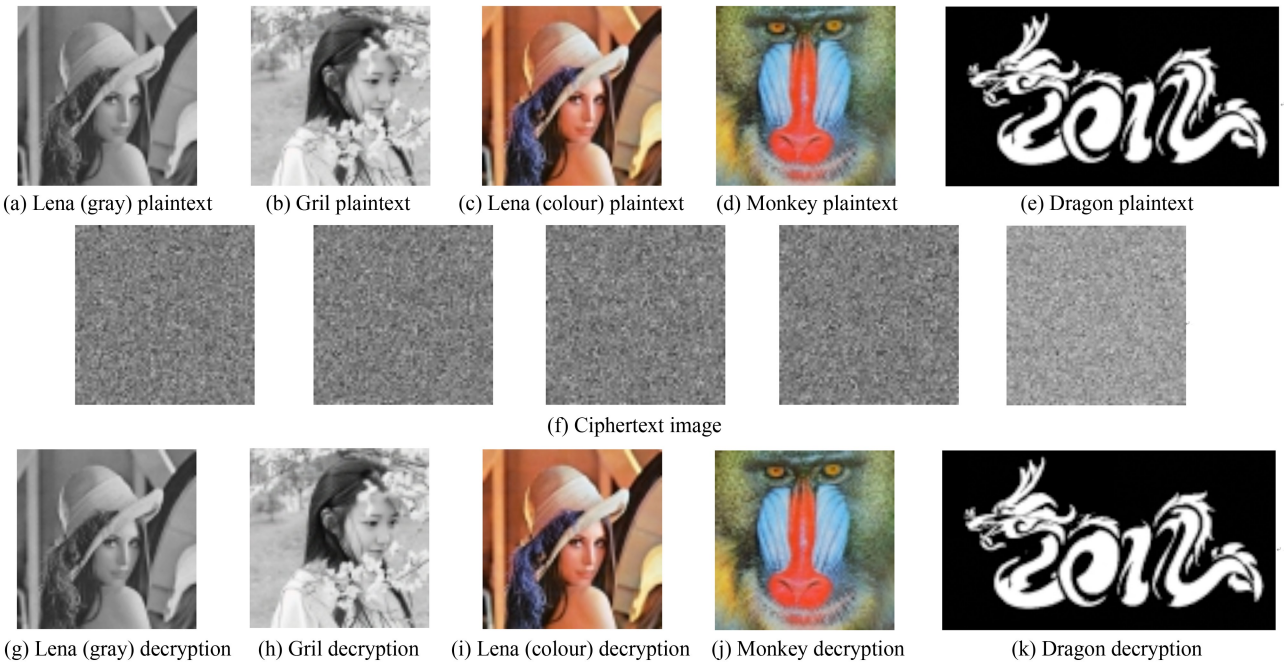


图 7 加解密效果

Fig.7 Effect of encryption and decryption

本算法将五张不同大小和类型的图像一次性进行了加密，得到的密文为类噪声图像，完全看不出明文特征，很好地掩盖了明文信息，而解密后得到的图像也与明文图像完全一样，证明本算法加解密效果良好，实用性强.

3.1 明文敏感性分析

明文敏感性指当明文发生微小的变化时，密文将会完全不同.为测试该算法的明文敏感性，将明文图像任意一点加 1，交换两个像素值不同两点位置后进行加密，利用式(23)、(24)计算明文变化后与未变化的密文间的像素值变化率(The Number of Pixels Change Rate，NPCR)和归一化平均变化强度(The Unified Average Changing Intensity，UACI)的值，结果如表 1.

$$\mathrm{NPCR}=\frac{\sum_{i}\sum_{j}p(i,j)}{M\times N} \tag{23}$$

$$\mathrm{UACI}=\frac{1}{M\times N}\left[\sum_{i}\sum_{j}\left|C_1(i,j)-C_2(i,j)\right|\right]\times 100\% \tag{24}$$

式中，当 $C_1(i,j)=C_2(i,j)$ 时 $p(i,j)=0$，否则 $p(i,j)=1$.

表 1 明文敏感性分析

Table 1 Analysis of clear text sensitivity

Any position pixel plus 1		Swap positions of two different pixel values	
NPCR	UACI	NPCR	UACI
0.996 1	0.334 8	0.996 0	0.335 1

从表 1 可以看出当明文的像素值作微小的改变时，密文的所有像素基本都得到了改变，而且改变强度能达到 33%以上，说明该算法具有很好的明文敏感性.

3.2 密钥敏感性分析

密钥敏感性指当密钥发生微小变化时，得到的加密图像将完全不同，同样密钥发生的改变不同解密的结果也将不同.为测试算法的密钥敏感性，将加密过程的密钥值作不同的微小改变，并利用式(25)求出两密文相关系数(Correlation Coefficient, CC)，如表 2 所示.解密过程中改变密钥后的解密效果如图 8.

表 2 加密过程中密钥发生变化时前后密文的相关系数

Table 2 Correlation coefficient of ciphertext before and after key changes in encryption process

$\Delta x'_{0,1}=10^{-14}$	$\Delta \mathrm{int}F'_{0,1}=10^{-14}$	$\Delta u'_1=10^{-14}$	$\Delta k=1$	$\Delta x'_{0,2}=10^{-14}$	$\Delta \mathrm{int}F'_{0,2}=10^{-14}$	$\Delta u'_2=10^{-14}$
0.007 8	0.005 9	0.008 9	0.006 3	−0.002 0	−0.001 0	0.000 1

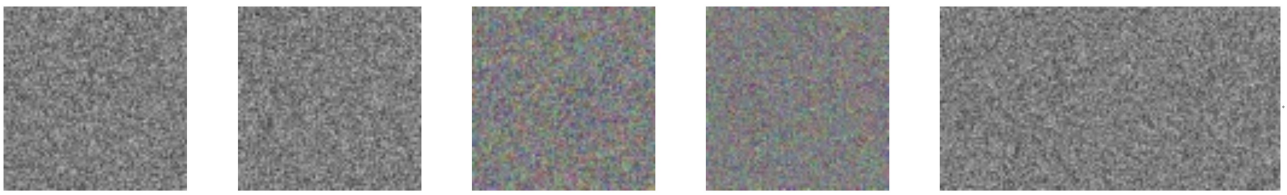


图 8 解密过程中改变密钥后的解密图像

Fig.8 The decrypted image after changing the key during decryption

$$\mathrm{CC}=\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\left[f(x,y)-\bar{f}\right]\left[F(x,y)-\bar{F}\right]}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}\left[f(x,y)-\bar{f}\right]^2}\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}\left[F(x,y)-\bar{F}\right]^2}} \tag{25}$$

式中，$\bar{f}$ 和 $\bar{F}$ 为对应图像像素值的均值.

如表 2 所示，加密过程中密钥发生微小变化前后得到的密文图像相关系数均接近于 0，两密文之间几乎没有关系.图 8 为解密过程中 $\Delta x'_{0,1}=10^{-14}$ 时的解密图像，解密失败，同时其他密钥变换量为表 2 中一样时解密图像也是如图 8 所示的类噪声图像.因此，说明加密和解密过程都对密钥非常敏感，即本文算法具有良好的密钥敏感性 .

3.3 密钥空间分析

本文的密钥 key1($x_{0,1}$，u_1，$\mathrm{int}F_{0,1}$，k)、key2($x_{0,2}$，u_2，$\mathrm{int}F_{0,2}$)分别为用于 3D 比特置乱的初值和参数以及用于扩散操作的初值与参数.其中$\{0\leqslant k\leqslant 8\,|\,k\in N\}$，由密钥分析可得，$x_{0,1}$、$x_{0,2}$、$u_1$、$u_2$、$\mathrm{int}F_{0,1}$、$\mathrm{int}F_{0,2}$ 变化量为 10^{-14} 时密钥已极为敏感，因此将其保留到小数点后 14 位，得到密钥空间至少为 $8\times(10^{14})^6=8\times 10^{84}$.本文加密算法还可将混沌的另一参数 M、混沌序列预迭代次数、明文的 SHA-256 值和扩散初值 C_0 作为密钥，从而使得密钥空间进一步扩大.从安全的角度分析，密钥空间$\geqslant 2^{100}\approx 10^{30}$，就能满足较高的安全级别[20]，所以本算法的密钥空间对穷举攻击是安全的.

3.4 抗选择明密文攻击分析

由于选择明密文攻击对加密系统最有威胁，如果加密系统能够抵抗选择明密文攻击，则可以抵抗针对加密系统的其他攻击.因此，用选择明文攻击来进一步测试系统的安全性.选择明文攻击，即攻击者已经知道加密和解密算法，并且可以任意选择明文，放入加密系统获取相应的密文，进而分析出密钥的过程.将图 7 中明文任意位置的像素值加 1 的图像作为攻击图像得到密钥流，并对其对应的密文解密，结果如图 9.

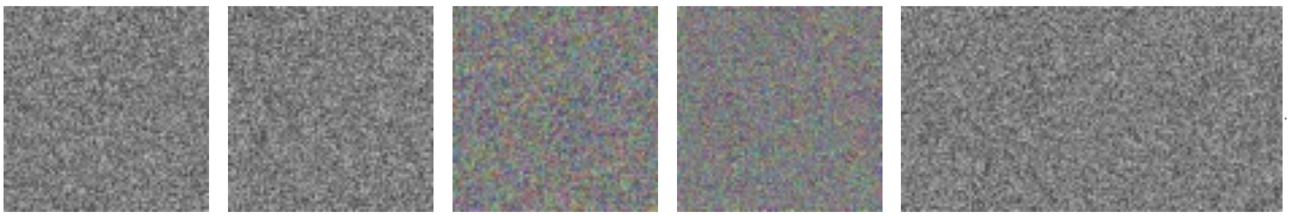


图 9 任意像素值加 1 后的解密图像

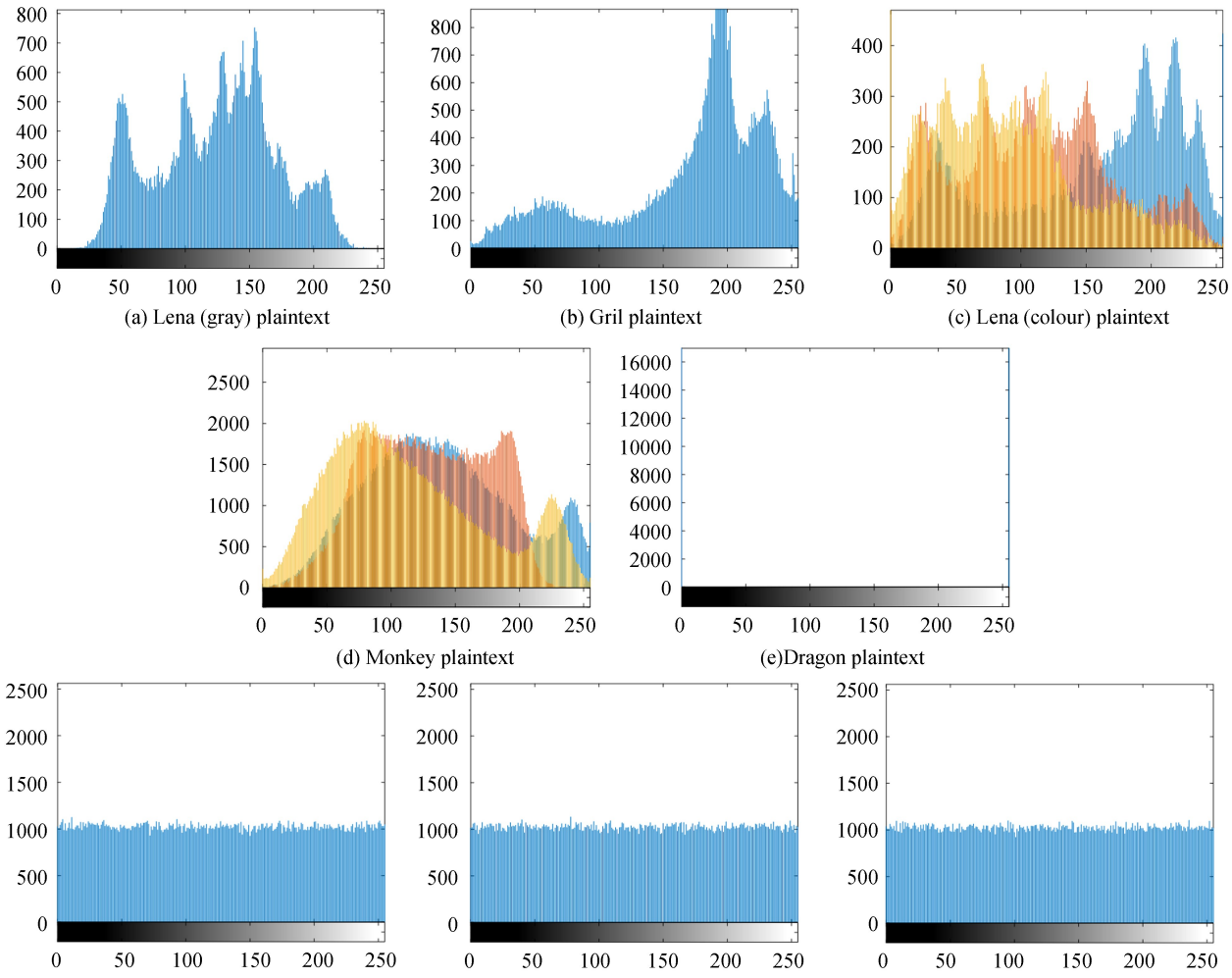
Fig.9 Decrypted image with arbitrary pixel value plus 1

从图 9 可知即便当攻击图像与明文仅仅只有一个像素值差，也无法攻击成功，说明本算法具有很强的抗攻击能力.主要原因在于采用了密钥与明文的哈希值 SHA-256 进行了联系，实现“一次一密”的效果.

3.5 统计特性分析

3.5.1 直方图

直方图表示数字图像中每个灰度级和其出现的概率的对应关系，是反映图像像素值分布的重要图形化指标，明文和密文直方图如图 10.



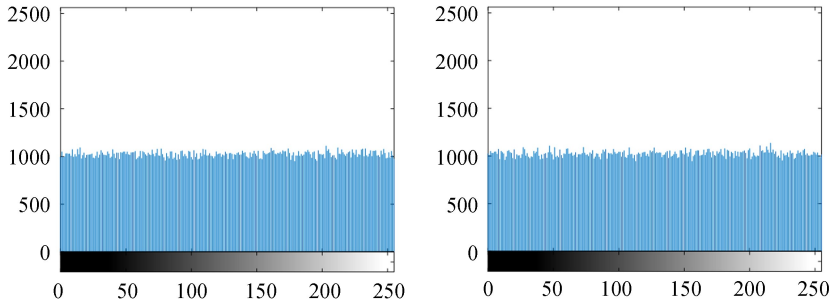


图 10 明文和密文直方图

Fig.10 Histogram of plaintext and ciphertext

由图 10 可知密文的直方图与明文的相差巨大，说明明文的像素值得到了很大的变化，能很好地隐藏明文信息.

3.5.2 信息熵

信息熵指图像整体随机性，在 uint8 类型的数据下信息熵理想值为 8.如果密文图像的信息熵越接近于 8，抗攻击性越强.本文算法的信息熵如表 3 所示，其中彩色明文的信息熵为 RGB 三通道的均值.

表 3 图像信息熵

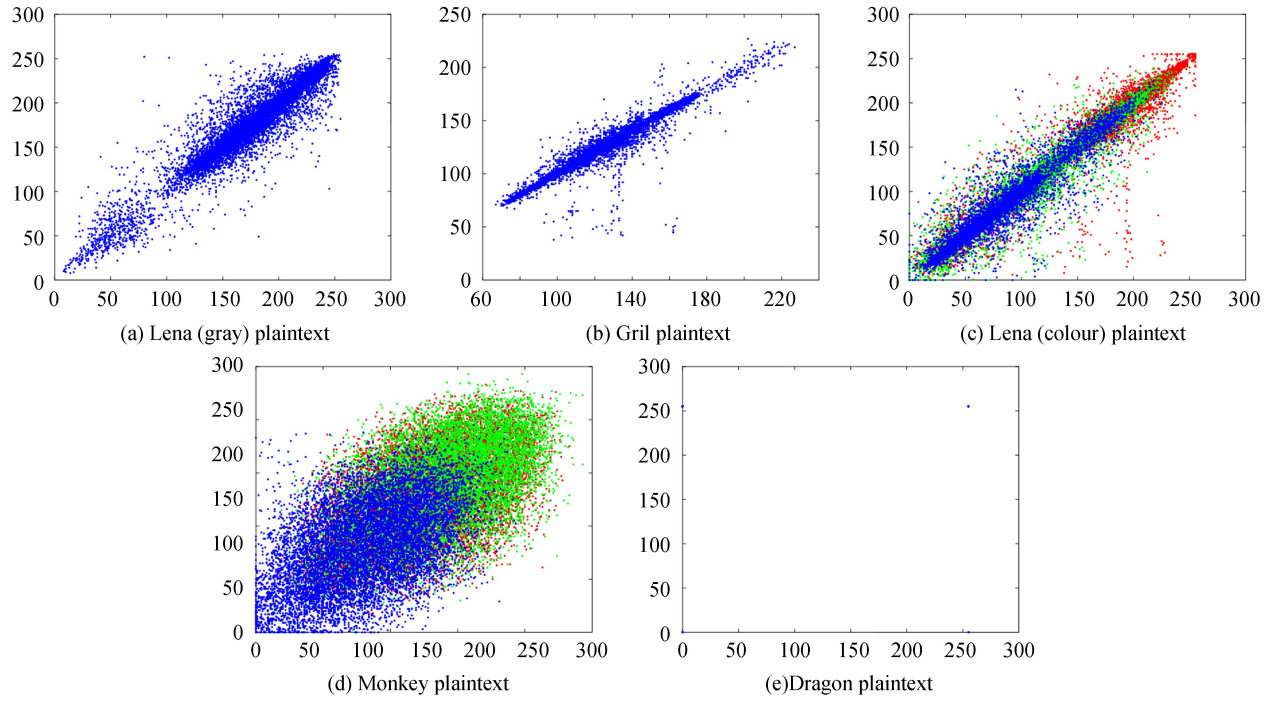
Table 3 Image information entropy

Lena	Gril	Lena	Monkey	Dragon	Ciphertext1	Ciphertext 2	Ciphertext 3	Ciphertext 4	Ciphertext 5
7.460 3	7.524 3	7.724 2	7.659 2	0.768 2	7.999 2	7.999 3	7.999 3	7.999 3	7.999 3

由表 3 可知本文算法密文图像信息熵达到 7.999 以上，接近理想值 8，说明该算法有很强的密文抗攻击能力.

3.5.3 相邻像素相关性分析

明文图像相邻像素在水平垂直和对角三个方向上具有很高的相关性，攻击者可以通过分析相关信息来恢复平面图像.因此，有效的加密算法应该去除这些像素相关性，生成低相关性的密文.为了更加直观地看出像素间的相关性，给出本加密算法明文和密文左上角 10 000 个水平方向的相邻像素点关系图，如图 11，并用式(24)计算相邻像素的相关系数，如表 4.



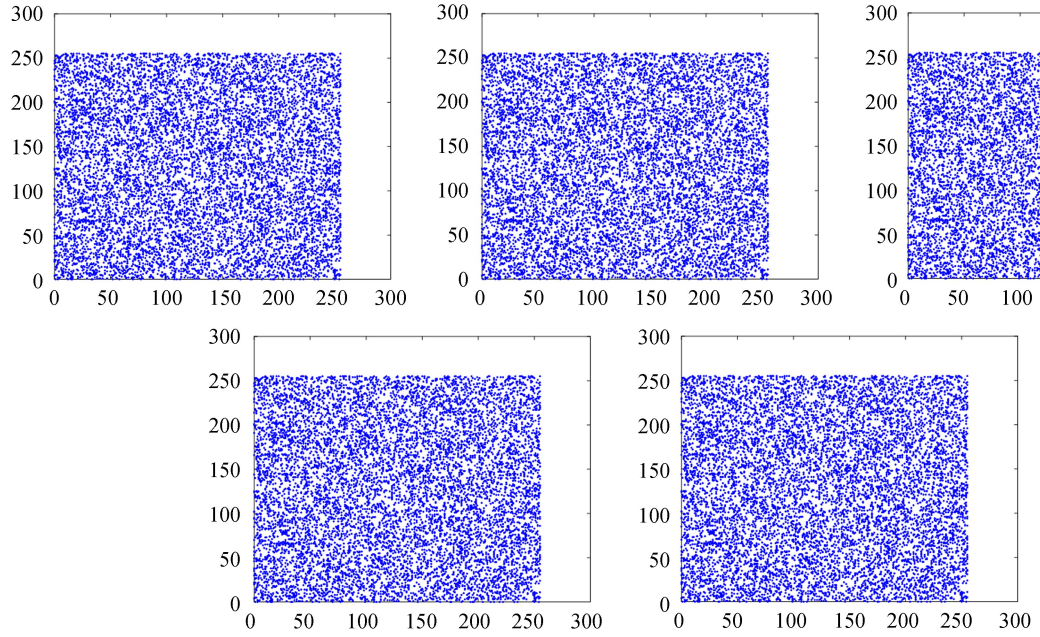


图 11　水平方向相邻像素相关性图

Fig.11　Correlation diagram of adjacent horizontal pixels

表 4　相邻像素相关性

Table 4　Correlation of adjacent pixels

	Lena	Gril	Lena	Monkey	Dragon	Cipher-text1	Cipher-text 2	Cipher-text 3	Cipher-text 4	Cipher-text 5
Level	0.968 4	0.916 8	0.960 3	0.876 9	0.936 0	0.001 7	0.001 6	0.001 9	−0.002 2	0.000 3
Vertical	0.935 2	0.917 3	0.919 6	0.916 9	0.922 4	0.002 3	0.000 1	−0.000 6	−0.000 1	−0.001 2
Diagonal	0.908 3	0.870 0	0.891 2	0.845 9	0.894 9	−0.002 5	0.000 1	0.000 3	−0.000 2	−0.003 3

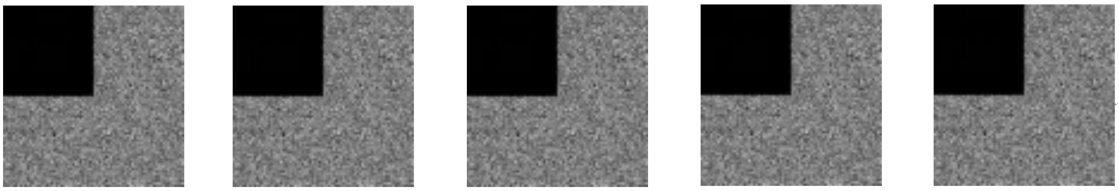
由图 11 得出,Lena(灰)、Gril(灰)、Lena(彩)和 Monkey 明文主要分布在对角线上,说明其相邻像素基本相同,而 Dragon 明文只有四个点,可知这是个二值图像,而所有明文图像对应的密文分布比较均匀,说明本算法很好地破坏了明文相邻像素相关性.由表 4 中密文相关系数几乎接近于 0 可知,本算法密文相关性已经非常低.

3.6　鲁棒性分析

由于密文在传输过程中极易发生噪声污染和数据丢失的情况,因此要求加密算法必须具备一定的抗剪切和噪声攻击的能力.将图 7 中所有密文剪切 1/4 的区域和用式(26)加入强度为 0.2 的高斯噪声,其相应的解密图像如图 12.

(a) Ciphertext image with 0.2 gaussian noise

(b) Decrypt image with 0.2 gaussian noise



(c) Cut 1/4 of the ciphertext image

(d) Decrypt image after 1/4 ciphertext cut

图 12 鲁棒性分析

Fig.12 Robustness analysis

$$r=r_1\times(1+sG) \tag{26}$$

式中，s 为噪声强度，G 为均值为 0，方差为 1 的高斯噪声，r_1 为原图，r 为加入噪声后的图像.

从图 12 可以看出，当数据丢失 1/4 和加入强度为 0.2 的高斯噪声时，解密后的图像仍然可以识别，这说明本加密算法对裁剪和噪声攻击具有较强的鲁棒性.

3.7 对比分析

为验证本算法的先进性，利用不同的多图像加密算法和本算法同样对 4 张 512×512 灰度图进行一次加密，通过明密文敏感性、抗选择明密文攻击能力、密文随机性及加密时间进行对比，结果如表 5.

表 5 对比分析

Table 5 Comparative analysis

	NPCR	UACI	Information entropy	Correlation coefficient (horizontal, vertical, diagonal)			Times
Ref.[16]	0	0	7.997 9	−0.078 1	0.066 5	0.060 7	9.656
Ref.[17]	0	0	7.614 8	−0.007 1	−0.001 4	−0.002 6	----
Ref.[18]	0.996 2	0.334 3	7.999 3	−0.002 2	−0.003 1	0.001 6	0.710 3
This paper	0.996 1	0.334 8	7.999 2	0.001 7	0.002 3	−0.002 5	0.502 3

由表 5 可知，当明文像素值作微小变化时，文献[16]、[17]的密文间像素值变化率 NPCR 和归一化平均变化强度 UACI 的值为 0.这是由于明文与密钥无关，及加密算法的扩散效果不明显或较弱导致的，而文献[16]的 NPCR 值和 UACI 值也没有本文算法高，主要是由于文献[18]明文与密钥关联性不强.本文算法的明文与密钥关联实现“一密一钥”，使得明文发生微小变化而密钥发生巨大变化，密钥也发生巨大变化，说明本文算法敏感性更好.由信息熵和相关系数对比可以看出，本文算法的密文随机性更好，相邻像素相关性最低，说明抗差分能力及抗攻击能力最强.本文算法的加密时间最短，效率更高.另外，文献[16]、[17]一次只能加密 4 张同大小的灰度图像，文献[18]一次只能加密同大小的灰度图像，而本文算法一次可对任意数量、不同大小和不同类型的图像同时加密，实用性更高.

4 结论

本文提出了一种图像重组和比特置乱的多图像加密方法，利用构建新多图像的方法实现一次加密任意数量、不同类型和大小图像的目的，极大地提高了图像加密的效率.采用 3D 比特置乱的方式，高位进行行列循环移位置乱，低位只进行整页简单排序的方法，减少了加密时间，提高了加密算法抗噪声攻击能力.采用 L-F 级联混沌解决了低维 logistic 混沌系统序列分布不均匀，存在空白窗等问题，同时还提高其序列的随机性，增加了控制参数和初值个数，更加有效地抵御蛮力攻击.将明文的 SHA256 作为密钥的一部分，有效地提高了明文敏感性和抗选择明密文攻击能力.实验表明，本算法的密文分布均匀，明文、密钥敏感性强，还能抵御

常见的多种攻击方式.在多图像加密中具有更高的实用性和安全性.

参考文献

[1] YANG Bo, ZHANG Wei-peng, RUNLING, *et al*. Micro-lens array based 3-D color image encryption using the combination of gravity model and Arnold transform[J]. *Optics Communications*, 2015,**355**(15): 419-426.

[2] ZHU He-hui, ZHAO Cheng. An image encryption scheme using generalized Arnold map and affine cipher[J]. *Optik*, 2014, **125**(22): 6672-6677.

[3] ZHOU Guo-min, ZHANG Da-xing, LIU Yan-jian, *et al*. A novel image encryption algorithm based on chaos and line map[J]. *Neurocomputing*, 2015, **169**: 150-157.

[4] CHEN Jun-xin, ZHU Zhi-liang, FU Chong, *et al*. A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism[J]. *Communications in Nonlinear Science and Numerical Simulation*, 2015, **20**(3): 846-860.

[5] LIU Zheng-jun, XU Lie, LIU Ting, *et al*. Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains[J]. *Optics Communications*, 2011, **284**(1): 123-128.

[6] KUMAR S A, MAYANK D. Multilevel encrypted text water marking on medical images using spread-spectrum in DWT domain[J]. *Wireless Personal Communications*, 2015, **83**(3): 2133-2150.

[7] ZHANG Qiang, LIU Li-li, WEI Xiao-peng. Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps[J]. *AEU-International Journal of Electronics and Communications*, 2014, **68**(3): 186-192.

[8] WANG Xing-yuan, ZHANG Ying-qian. A novel chaotic image encryption scheme using DNA sequence operations[J]. *Optics and Lasers in Engineering*, 2015, **73**: 53-61.

[9] TANG Zheng-jun, ZHANG Xian-quan, LAN Wei-wei. Efficient image encryption with block shuffling and chaotic map [J]. *Multimedia Tools & Applications*, 2015, **74**(15): 5429-5448.

[10] BECHIKH R, HERMASSI H, EI-LATIF A A A, *et al*. Breaking an image encryption scheme based on a spatiotemporal chaos system,signal processing[J]. *Image Communication*,2015,**39**(A): 151-158.

[11] NOROUZI B, MIRZAKUCHAKI S. Breaking an image encryption algorithm based on the new substitution stage with chaotic functions[J]. *International Journal for Light and Electron Optics*, 2016:**127**(14): 5695-701.

[12] DAS S, MANDAL S N, GHOSHAL N, *et al*. Multiple-image encryption using genetic algorithm [M]. Intelligent Computing and Applications. Springer India, 2015.

[13] TANG Zhen-jun, SONG Juan, ZHANG Xian-quan, *et al*. Multiple-image encryption with bit-plane decomposition and chaotic maps[J]. *Optics and Lasers in Engineering*, 2016, **80**: 1-11.

[14] LIU Lei, SHAN Ming-guang, ZHANG Zhi, *et al*. Multiple-image encryption and authentication based on optical interference by sparsification and space multiplexing[J]. *Optics and Laser Technology*, 2019, **122**:105858.

[15] HUANG Zhi-jing, CHENG Shan, GONG Li-hua, *et al*. Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform[J]. *Optics and Lasers in Engineering*, 2019, **124**: 105821.

[16] ZHANG Xiao-qiang, WANG Xue-song. Multiple-image encryption algorithm based on mixed image element and permutation[J]. *Optics and Lasers in Engineering*, 2017, **92**: 6-16.

[17] ZHANG Xiao-qiang, WANG Xue-song. Multiple-image encryption algorithm based on DNA encoding and chaotic system[J].*Multimedia Tools and Applications*, 2019,**78**(3): 7841-7869.

[18] XIONG Y, QUAN C, TAY C J. Multiple image encryption scheme based on pixel exchange operation and vector decomposition[J]. *Optics and Lasers in Engineering*, 2018, **101**: 113-121.

[19] HSU W J. Fibonacci cubes-a new interconnection topology[J]. *IEEE Transactions on Parallel & Distributed Systems*, 1993, **4**(1): 3-12.

[20] GUO Yuan, XU Xin, JING Shi-wei. A hybrid chaotic virtual optical image encryption method[J]. *Acta Photonica Sinica*, 2019, **48**(7): 710002.
郭媛，许鑫，敬世伟. 一种混合混沌虚拟光学图像加密方法[J]. 光子学报，2019，**48**(7)：710002.

Foundation item: The National Natural Science Foundation of China (No.61872204), Heilongjiang Provincial Natural Science Fund (No. F2017029), Basic Scientific Research Operating Expenses of Institutions of Higher Learning in Heilongjiang Province (No.135109236)