引用格式：GUO Yuan, JING Shi-wei. Lossless Compression Optical Image Encryption Based on L-L Cascade Chaos and Vector Decomposition[J]. *Acta Photonica Sinica*, 2020, **49**(7):0710002
郭媛,敬世伟.基于L-L级联混沌与矢量分解的无损压缩光学图像加密[J].光子学报,2020,**49**(7):0710002

基于L-L级联混沌与矢量分解的无损压缩光学图像加密

郭媛,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:为克服双随机相位编码的光学图像加密中,密钥、密文体积大、抗选择明密文能力弱的问题,提出了一种Logistic-Logistic级联混沌与矢量分解的无损压缩光学图像加密方法.先隔空取样置乱将明文分成两块,再用干涉合成一块,最后放入双随机相位编码系统得到密文.置乱能够克服干涉后看到明文信息的缺点,增加了加密系统的安全性.干涉使得密文体积变为原来的一半,便于密文传输.单位等模矢量分解的解密方式避免了现有压缩方式存在的解密图像分辨率降低的问题.Logistic-Logistic级联混沌极大缩小了双随机相位编码的密钥体积,同时还解决了Logistic序列分布不均匀问题,提高了序列随机性,保留了Logistic混沌的快速性.将明文的HASH值SHA256与密钥进行强关联,使整个系统达到一图一密的加密效果,提高了明密文间的雪崩效应,增强了算法抗选择明密文攻击的能力.

关键词:光学图像加密;隔空取样置乱;矢量分解;干涉;Logistic-Logistic级联混沌
中图分类号:TP309;TN918　　**文献标识码**:A　　**doi**:10.3788/gzxb20204907.0710002

Lossless Compression Optical Image Encryption Based on L-L Cascade Chaos and Vector Decomposition

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

Abstract: In order to avoid the characters of current double-random phase-encoded optical image encryption, whose key and ciphertext are large in size, and has weak ability to resist the attack of selecting plaintext and ciphertext, a lossless compression optical image encryption method was proposed based on Logistic-Logistic cascade chaos and vector decomposition. Firstly, the plaintext is divided into two images by space sampling and scrambling. Then the images are synthesized together by the interference. At last, the ciphertext can be gotten by putting the image into a double random phase encoding system. The scrambling improves the security of the encryption system, because it can avoid plaintext information to be seen after interference. The interference reduces the volume of the ciphertext to about the half in size, which is convenient for ciphertext transmission. The decryption method based on unit-mode vector decomposition could avoid the problem of low resolution of the decrypted image caused by the existing compression method. Logistic-Logistic cascade chaos can reduce the volume of double random phase encoding, improve the randomness of the sequence and keep the fastness of the Logistic chaos. It can also solve the problems of uneven distribution of the Logistic sequence. The HASH value SHA256 of plaintext is associated with the secret key strongly, which makes the whole system achieve the encryption effect of

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),研究生研究项目(No.YJSCX2019042)
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:敬世伟(1995—),男,硕士研究生,主要研究方向为图像处理. Email: 2641235293@qq.com
收稿日期:2020-03-10;**录用日期**:2020-05-18

one image with one key. This also improves the avalanche effect between plaintext and ciphertext, and enhances the capability of resisting the attack of selecting plaintext and selecting ciphertext.

Key words: Optical image encryption; Space sampling scramble; Vector decomposition; Interference; Logistic-Logistic cascade chaos

OCIS Codes: 100.2000; 100.2960; 070.4560; 070.3185

0 引言

图像信息具有直观生动形象的特性,在数字化时代被广泛运用,但易遭受黑客的各种攻击,如文献[1-2]提出的一系列图片检测、拷贝和伪造方案,所以图像安全成了一个急需解决的问题.由于光学具有多密钥维度、高速并行等特点,被广泛用到图像加密中[3-5], REFREGIER和JAVIDI提出的双随机相位编码(Double Random Phase Encoding, DRPE)[6],开启了光学图像加密先河.随后DRPE系统中傅里叶变换推广到了分数傅里叶、菲涅耳变换、gyrator变换[7-9],增加了密钥维度,使其安全性更高.但以上算法只进行线性运算,并且明文和密钥没有关联或关联不强,使得加密系统明密文间的雪崩效应不强,而使其被选择明文、已知明文和唯密文攻击[10-12]攻破.同时随机相位模板体积大,运用混沌系统产生中间密钥流,可以减小密钥体积,便于密钥的传输与分发,还提高了密钥敏感性[4],因此大量混沌被用于图像加密中.现有从一维Logistic到五维超混沌的多种混沌[13-17],一维的混沌Logistic简单、生成时间短,但存在空白窗分布不均匀的特点[18],高维的混沌动力学特性更强,但是耗时更长.

以上加密系统明密文大小一样,密文体积过大,不便于密文的传输与分发,为此一些压缩加密被提出.如用小波变换进行压缩再加密[19],这类算法将图像压缩到原图1/4,但是由于丢弃了细节信息而不能还原,解密图像也只能保持为原图的1/4.另外有研究者用压缩感知理论进行压缩和重构[20-22],或者引入深度学习[23]的压缩方式,使得解密图像与明文一样大小,但是图像有一定的失真现象,故这类算法在图片还原程度上还需要提高.

本文构造一种新的Logistic-Logistic(L-L)级联混沌,用于产生随机相位模板,解决Logistic序列分布不均匀,扩宽混沌区间,增加密钥空间,增强序列随机性.将明文的HASH值SHA256作为密钥的一部分,使得密钥与明文具有很强的关联性,增强明密文间的雪崩效应和抗选择明密文攻击能力,同时进一步扩大密钥空间,使得整个系统抗蛮力攻击能力更强.用干涉和单位等模矢量分解使得密文压缩接近一半,并能无损地解密出来,便于密文的传输与分发.用隔空取样置乱将明文分成两块的同时也起到了置乱作用,使得整个系统安全性更高.

1 原理分析

1.1 单位等模矢量分解

干涉和矢量分解过程互为逆过程,在明文分为同等大小两块的情况下,用干涉进行图像压缩.解密过程中用单位等模矢量分解无损地还原图像.干涉与单位等模矢量分解原理如图1所示.

图1中圆为单位圆.干涉过程为

$$\boldsymbol{C}=\boldsymbol{E}_1+\boldsymbol{E}_2 \tag{1}$$

分解过程由余弦定理可知

$$\cos\theta_k=\frac{A_k^2+1-1}{2A_k1}=\frac{A_k}{2} \tag{2}$$

则θ_k为

$$\theta_k=\arccos\left(\frac{A_k}{2}\right) \tag{3}$$

又因为向量角范围在$[-\pi,\pi]$,则两个单位向量的相位角$\phi_{1,k}$、$\phi_{2,k}$为

$$\begin{cases}\phi_{1,k}=\begin{cases}2\pi+\psi_k+\arccos\left(\dfrac{A_k}{2}\right), -\pi\geqslant\psi_k+\arccos\left(\dfrac{A_k}{2}\right)\\ \psi_k+\arccos\left(\dfrac{A_k}{2}\right), -\pi<\psi_k+\arccos\left(\dfrac{A_k}{2}\right)<\pi\\ 2\pi-\psi_k+\arccos\left(\dfrac{A_k}{2}\right), \psi_k+\arccos\left(\dfrac{A_k}{2}\right)\geqslant\pi\end{cases}\\ \phi_{2,k}=\begin{cases}2\pi+\psi_k-\arccos\left(\dfrac{A_k}{2}\right), -\pi\geqslant\psi_k-\arccos\left(\dfrac{A_k}{2}\right)\\ \psi_k-\arccos\left(\dfrac{A_k}{2}\right), -\pi<\psi_k-\arccos\left(\dfrac{A_k}{2}\right)<\pi\\ 2\pi-\psi_k-\arccos\left(\dfrac{A_k}{2}\right), \psi_k-\arccos\left(\dfrac{A_k}{2}\right)\geqslant\pi\end{cases}\end{cases} \tag{4}$$

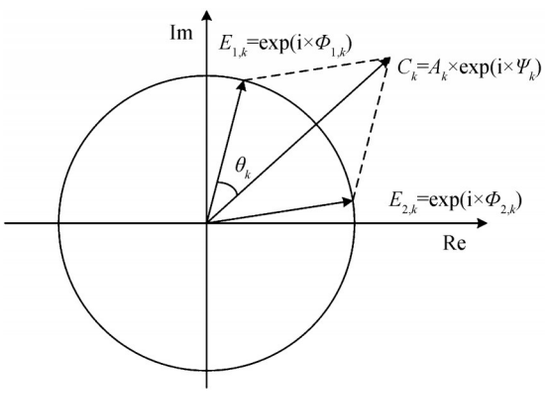


图1　干涉与单位等模矢量分解原理

Fig. 1　Principle diagram of interference and unit equal mode vector decomposition

1.2　隔空抽取置乱

为克服干涉还能看到明文轮廓的问题，用隔空抽取置乱的方式，在将明文分为两块的同时起到置乱的效果。为了在反向置乱过程中能完全恢复，置乱过程中用0和1在一个16行的矩阵中记录对应取出来两个

像素值大小，最后将每16位转化为十进制数放在置乱得到的两块含有明文信息的图像后面，即

$$a_j=\frac{1}{65535}\sum_{i=1}^{16}t_3(i,j)\times 2^{16-i} \tag{5}$$

式中，a_j为对应每行的二进制转换为十进制的数，$t_3(i,j)$为对应行列的二进制数。隔空抽取置乱主要过程为按照起始位隔空抽取两个像素值，并按照大小分别放入两个矩阵中，再用一个矩阵记录其大小关系。起始位置为6、空格数为4的一个6×6的二值图像隔空抽取置乱过程如图2所示，整个置乱过程表示为

$$\boldsymbol{t}_1,\boldsymbol{t}_2=\mathrm{SSS}(\boldsymbol{f},s_1,s_2) \tag{6}$$

式中，SSS表示整个隔空抽取过程，$\boldsymbol{f}$为明文图像，s_1为空格数，s_2为起始位置，$\boldsymbol{t}_1$、$\boldsymbol{t}_2$分别为置乱后的两图像。针对Lean(256×256)的灰度图，设置起始位置为200、空格数为200，进行隔空抽取置乱排列得到两图像如图3所示。

由图3可见置乱后的图像已经完全看不出原始图像信息，系统安全性进一步提高。还可以看出置乱后的图像只有原图的0.53倍(原图越大，压缩率越接近0.5)，更便于密文的传输与分发。

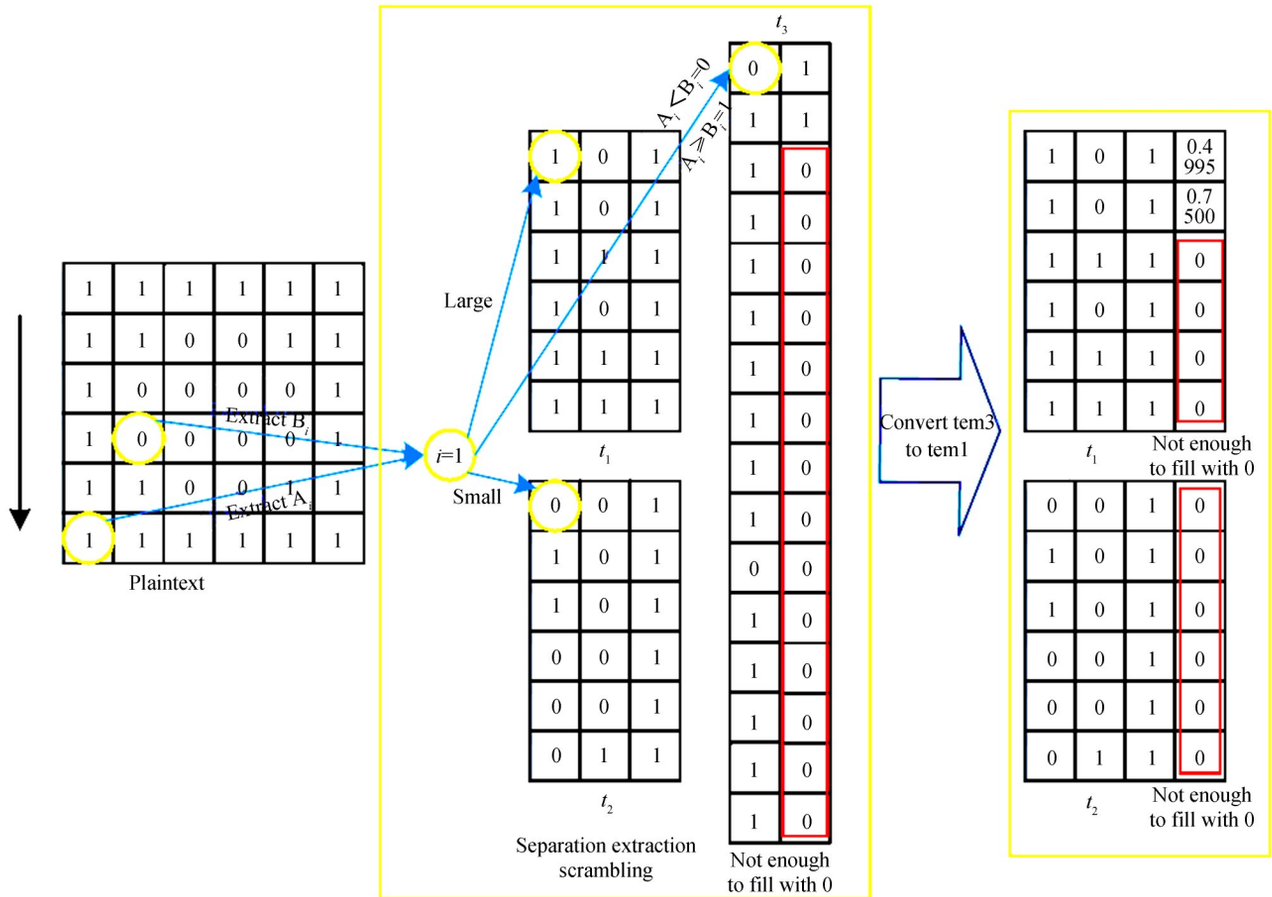


图 2 隔空抽取置乱原理图

Fig. 2 Schematic diagram of space separation extraction scrambling

图 3 隔空抽取置乱效果

Fig. 3 Scrambling effect of space separation extraction

1.3 L-L 级联混沌

Logistic 混沌映射简单，随机性良好，被广泛应用于混沌保密通信的各个领域．其定义为[13,18]

$$x_{n+1}=\mu_1 x_n(1-x_n) \tag{7}$$

$$y_{n+1}=1-\mu_2 y_n^2 \tag{8}$$

其中，当参数 $\mu_1\in(3.75,4]$，$\mu_2\in(1.4,2]$ 内时该混沌映射处于混沌状态，序列 $x\in(0,1)$，$y\in(-1,1)$．为克服 Logistic 产生的随机序列分布不均匀、存在空白窗问题，将两个 Logistic 进行级联形成一个二维混沌．

$$\begin{cases} x_{n+1}=[\mu_1 y_n(1-x_n)]\bmod 1 \\ y_{n+1}=\left|1-\mu_2 x_n y_n\right|\bmod 1 \end{cases} \tag{9}$$

式中，mod 为取余运算．两类 Logistic 混沌和 L-L 级联混沌的分叉图如图 4 所示．

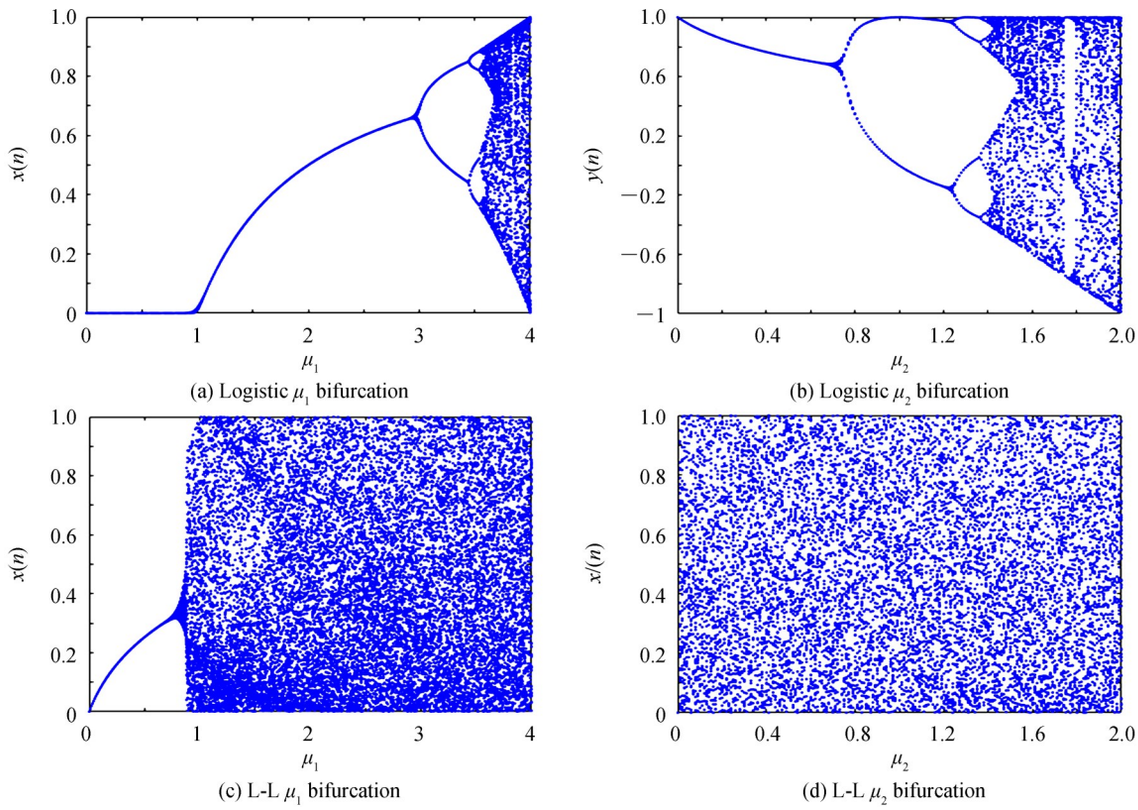


图4　Logistic和L-L的分叉图

Fig. 4　Bifurcation of Logistic and L-L

图4可见L-L级联混沌参数μ处于混沌区间的范围比Logistic更宽，且在处于混沌区间内不存在空白窗，分布也更为均匀，随机性更强，能更好抵御统计特性分析．为测试不同混沌的生成时间，表1给出了在Intel(R) core(TM) i5-8500 CPU @ 3.00Hz，内存8GB，Win10 64位操作系统电脑上，用MATLAB 2016a生成10^6个序列值的平均时间．可见L-L级联混沌的时间明显比其他混沌时间更短，说明其保留了Logistic简单、生成序列时间短的特点．

表1　不同混沌间时间对比

Table 1　Time comparison between different chaos

Chaos	Logistic Eq.(8)	Logistic Eq.(9)	L-L	Coupled tent chaos[14]	Chen chaos[15]	Four-dimensional hyperchaos[16]	Five-dimensional hyperchaos[17]
Time/s	0.077 343	0.072 966	0.041 443	0.719 836	2.624 962	2.862 689	1.461 286

2　加解密过程

算法加密过程如图5所示．首先求出明文的HASH值SHA256并与安全密钥进行级联得到动态密钥，根据动态密钥将明文进行隔空抽取置乱后得到两图像，再变为相位信息后进行干涉，最后放入双随机相位编码系统中得到密文．

2.1　加密过程

Step1 动态密钥生成，将明文的256位哈希值，每8位分为一组，表示为$\boldsymbol{H}=[\boldsymbol{h}_1,\boldsymbol{h}_2,\cdots,\boldsymbol{h}_{32}]$；其中$\boldsymbol{h}_i$为$\boldsymbol{h}_i=[h_{i,0},h_{i,1},\cdots,h_{i,7}]$．再根据式(10)～(14)生产动态密钥．

$$x_0=\mathrm{mod}\left(x_0'+\boldsymbol{h}_1\oplus\boldsymbol{h}_2\oplus\boldsymbol{h}_3\oplus\boldsymbol{h}_4\oplus\boldsymbol{h}_5\oplus\boldsymbol{h}_6/256,1\right) \tag{10}$$

$$\mu_1=\mathrm{mod}\left(\mu_1'+\boldsymbol{h}_7\oplus\boldsymbol{h}_8\oplus\boldsymbol{h}_9\oplus\boldsymbol{h}_{10}\oplus\boldsymbol{h}_{11}\oplus\boldsymbol{h}_{12}\oplus\boldsymbol{h}_{13}/64,0.25\right)+3.75 \tag{11}$$

$$y_0=\mathrm{mod}\left(y_0'+\boldsymbol{h}_{14}\oplus\boldsymbol{h}_{15}\oplus\boldsymbol{h}_{16}\oplus\boldsymbol{h}_{17}\oplus\boldsymbol{h}_{18}\oplus\boldsymbol{h}_{19}/256,1\right) \tag{12}$$

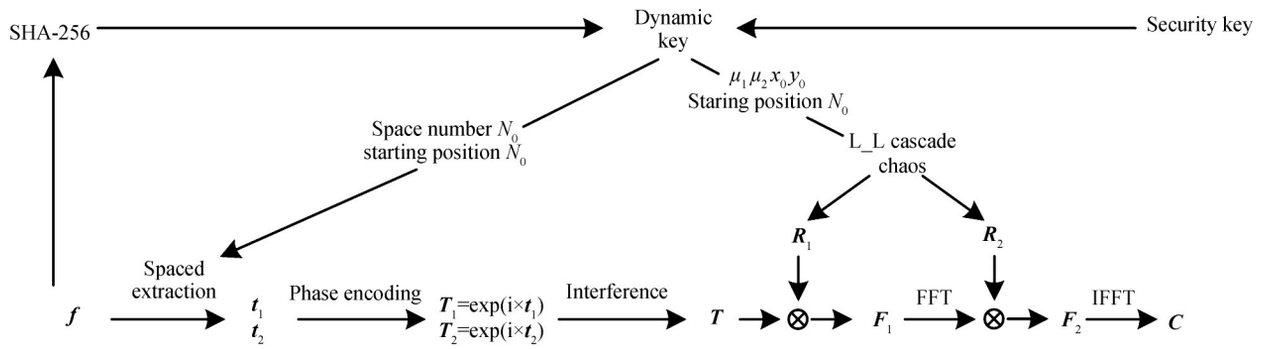


图5 加密过程

Fig.5 Encryption process

$$\mu_2 = \mathrm{mod}(\mu_2' + \boldsymbol{h}_{20} \oplus \boldsymbol{h}_{21} \oplus \boldsymbol{h}_{22} \oplus \boldsymbol{h}_{23} \oplus \boldsymbol{h}_{24} \oplus \boldsymbol{h}_{25} \oplus \boldsymbol{h}_{26}/128, 0.6) + 1.4 \tag{13}$$

$$N_0 = \mathrm{mod}(N_0' + \boldsymbol{h}_{27} \oplus \boldsymbol{h}_{28} \oplus \boldsymbol{h}_{29} \oplus \boldsymbol{h}_{30} \oplus \boldsymbol{h}_{31} \oplus \boldsymbol{h}_{32}, 200) + 100 \tag{14}$$

式中，x_0、μ_1、y_0、μ_2为L-L级联混沌的初值、参数；N_0为混沌的预迭代次数以及隔空抽取置乱过程的起始位置和空格数；x_0'、μ_1'、y_0'、μ_2'、N_0'为方便人为控制的安全密钥$\left\{1 \leqslant N_0' \leqslant 200 \middle| N_0' \in N^*\right\}$.

Step2 隔空抽样置乱，用明文$\boldsymbol{f}$、N_0求得置乱后的图像，即

$$\boldsymbol{t}_1, \boldsymbol{t}_2 = \mathrm{SSS}(\boldsymbol{f}, N_0, N_0) \tag{15}$$

Step3 对置乱后得到的两图像进行相位编码和干涉，即

$$\boldsymbol{T} = \exp(\mathrm{i} \times \boldsymbol{t}_1) + \exp(\mathrm{i} \times \boldsymbol{t}_2) \tag{16}$$

Step4 将x_0、μ_1、y_0、μ_2代入式(10)先迭代N_0次以消除暂态效应，再迭代$m \times \left(\left\lfloor \frac{\lfloor m \times n/32 \rfloor}{m} \right\rfloor + \lfloor n/2 \rfloor\right)$次，将$x$序列和$y$序列分别转化为$m \times \left(\left\lfloor \frac{\lfloor m \times n/32 \rfloor}{m} \right\rfloor + \lfloor n/2 \rfloor\right)$的矩阵$\boldsymbol{r}_1$和$\boldsymbol{r}_2$，其中$m$、$n$为原图$\boldsymbol{f}$的长宽.再将其转化为相位模板$\boldsymbol{R}_1$和$\boldsymbol{R}_2$，即

$$\begin{cases} \boldsymbol{R}_1 = \exp(\mathrm{i} \times 2\pi \times \boldsymbol{r}_1) \\ \boldsymbol{R}_2 = \exp(\mathrm{i} \times 2\pi \times \boldsymbol{r}_2) \end{cases} \tag{17}$$

Step5 将$\boldsymbol{T}$与相位模版进行基于傅里叶变换的双随机相位编码，得到密文$\boldsymbol{c}$即

$$\boldsymbol{c} = \mathrm{IFFT}[\mathrm{FFT}(\boldsymbol{T} \cdot \boldsymbol{R}_1) \cdot \boldsymbol{R}_2] \tag{18}$$

式中，FFT为傅里叶变换，IFFT为傅里叶逆变换.

2.2 解密步骤

解密过程为加密过程的逆过程，除了动态密钥和随机相位模板的生成外主要过程为：

Step1 用相位模版的共轭复数和密文$\boldsymbol{c}$得到干涉后的图像$\boldsymbol{T}$为

$$\boldsymbol{T} = \mathrm{IFFT}[\mathrm{FFT}(\boldsymbol{c}) \cdot \mathrm{conj}(\boldsymbol{R}_2)] \cdot \mathrm{conj}(\boldsymbol{R}_1) \tag{19}$$

式中，conj为取复数的共轭运算.

Step2 将$\boldsymbol{T}$代入式(4)得到变为相位信息的$\boldsymbol{T}_1$和$\boldsymbol{T}_2$.再取其相位角得到$\boldsymbol{t}_1$和$\boldsymbol{t}_2$，即

$$\begin{cases} \boldsymbol{t}_1 = \mathrm{angle}(\boldsymbol{T}_1) \\ \boldsymbol{t}_2 = \mathrm{angle}(\boldsymbol{T}_2) \end{cases} \tag{20}$$

式中，angle为复数取复角运算.

Step 3 在$\boldsymbol{t}_1$中取出$m \times \lfloor n/2 \rfloor$列后的数，再乘以65535后转化为二进制数得到$\boldsymbol{t}_3$.

Step 4 最后用$\boldsymbol{t}_1$、$\boldsymbol{t}_2$和$\boldsymbol{t}_3$的前$m \times n$项进行空格数为N_0、起始位置为N_0的反向置乱过程，得到明文$\boldsymbol{f}$.

3 实验分析

为验证本文算法的有效性和可行性，采用MATLAB R2016a作为仿真平台，同时选取灰度图、二值图作

为明文．设置x_0'、μ_1'、y_0'、μ_2'、N_0'分别为0.55、3.9、0.55、1.9、100，加解密结果如图6所示．

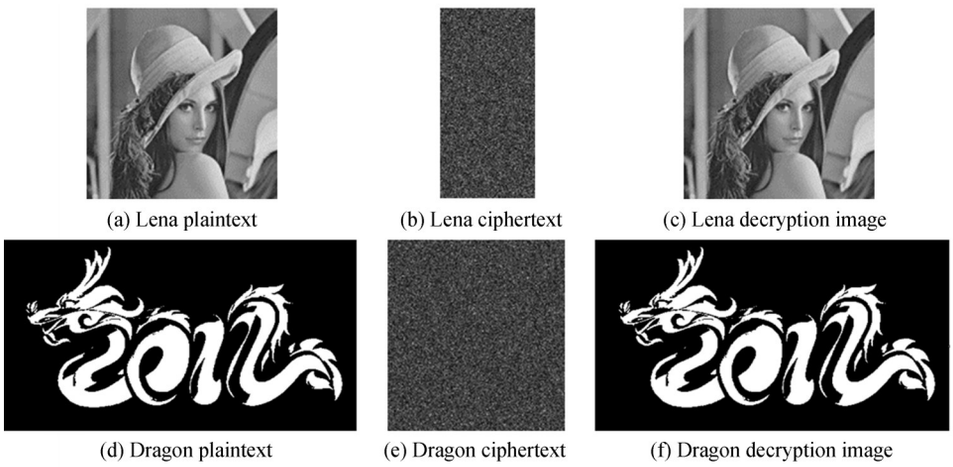


图6　加解密效果

Fig.6　Encryption and decryption effect

图6可见灰度和二值图像的密文均为类噪声图像，且正确密钥下的解密图像与明文完全一样，表明本算法加解密效果良好．

3.1　明文敏感性分析

本文采用像素值变化率（Number of Pixels Change Rate，NPCR）和归一化平均变化强度（Unified Average Changing Intensity，UACI）来定量描述明文敏感性．将明文图像任意一点加1或将不同像素值的两点交换后进行加密，计算明文变化前后密文间的NPCR和UACI值如表2所示．

表2　明文敏感性分析

Table 2　Plaintext sensitivity analysis

Comparison item	Lena		Dragon	
	NPCR	UACI	NPCR	UACI
Pixel at any position plus 1	0.991 8	24.333 9	0.991 6	22.787 3
Swap two different pixels	0.992 5	23.992 3	0.991 9	23.657 3

表2可见明文稍作改变时，密文的所有像素基本都得到了改变，同时变换强度都能达到22以上，可见本算法对明文变化极其敏感．

3.2　密钥敏感性分析

用图6(b)密文在密钥发生微小变化时解密，解密效果如图7所示．

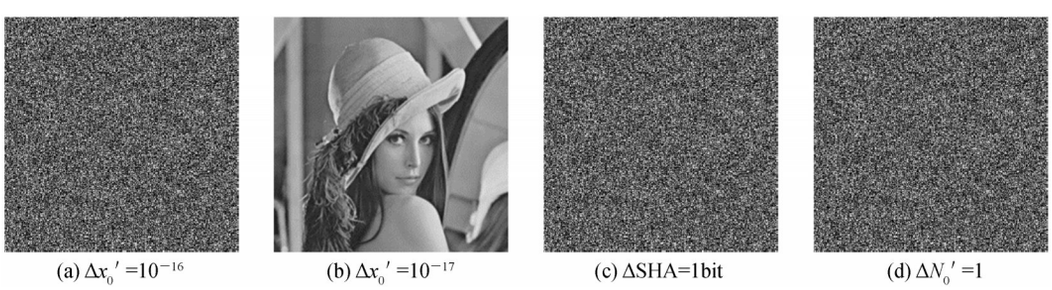


图7　密钥敏感性分析

Fig.7　Key sensitivity analysis

由图7可知当混沌密钥x_0'变化10^{-16}时解密图像仍是一个类噪声图像，而x_0'变化10^{-17}时就可以看到明文信息，说明x_0'的敏感度为10^{-16}．同理其他混沌密钥μ_1'、y_0'、μ_2'的敏感度为10^{-14}、10^{-16}、10^{-14}．在图7中还可以看出明文的HASH值SHA256改变1位比特，空格数、起始位置和混沌的预迭代次数改变1得到的解密图像

都无法用肉眼看到明文信息，说明加密系统对这些密钥也非常敏感.

3.3 密钥空间分析

本文的密钥包括混沌密钥x_0'、μ_1'、y_0'、μ_2'、明文的HASH值SHA256，以及空格数、起始位置和混沌的预迭代次数这一共同密钥N_0'.混沌密钥为双精度小数，由密钥分析可以得出最小敏感度为10^{-14}，故保留小数点后14位有效数字.本文的密钥空间至少为$200^2\times(10^{14})^4\times 2^{256}\approx 2.3\times 10^{135}$.从安全的角度，密钥空间$\geqslant 2^{100}\approx 10^{30}$就能满足较高的安全级别[3]，所以本算法能很好地抵御穷举攻击.

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[4].将图6(a)任意位置的像素值加1的图像作为攻击图像，得到对应的密钥流.并用其对图6(b)密文解密，结果如图8所示.


(a) Attack image　　(b) Crack image

图8 选择明文攻击

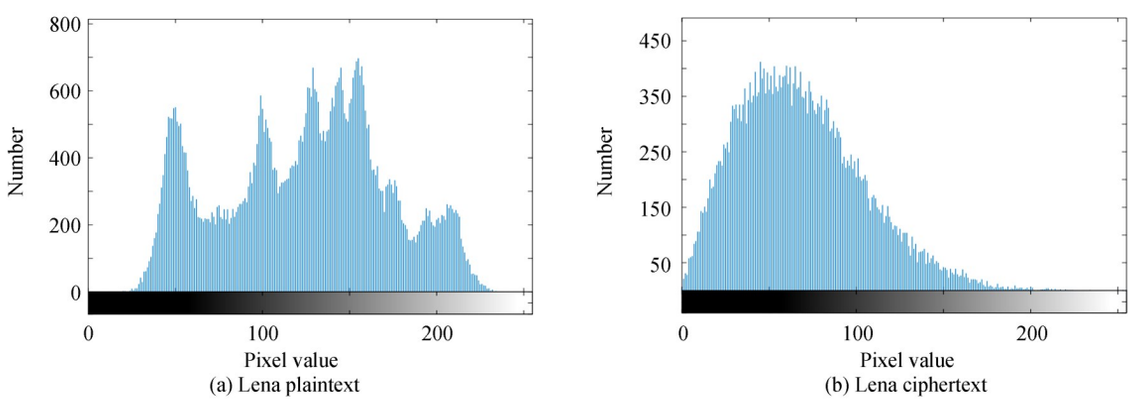
Fig.8 Selecting a plaintext attack

从图8可见当攻击图像与待破解得到的明文仅仅只有一个像素值差1，在肉眼无法分辨的情况下，无法攻击成功，足以表明该算法的安全性.这主要是由于密钥与明文的HASH值SHA256进行了联系，使得每一个明密文对都有不同的密钥，从而产生不同的密钥流，达到一图一密的效果，使得用其他明密文对的密钥流去解密不同的密文失去效果.

3.5 统计特性分析

3.5.1 直方图

为形象地观察出明密文的像素变换情况，画出图6中明文和密文对应的直方图如图9所示.由图9可见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，很好地隐藏了明文信息.



(a) Lena plaintext　　(b) Lena ciphertext

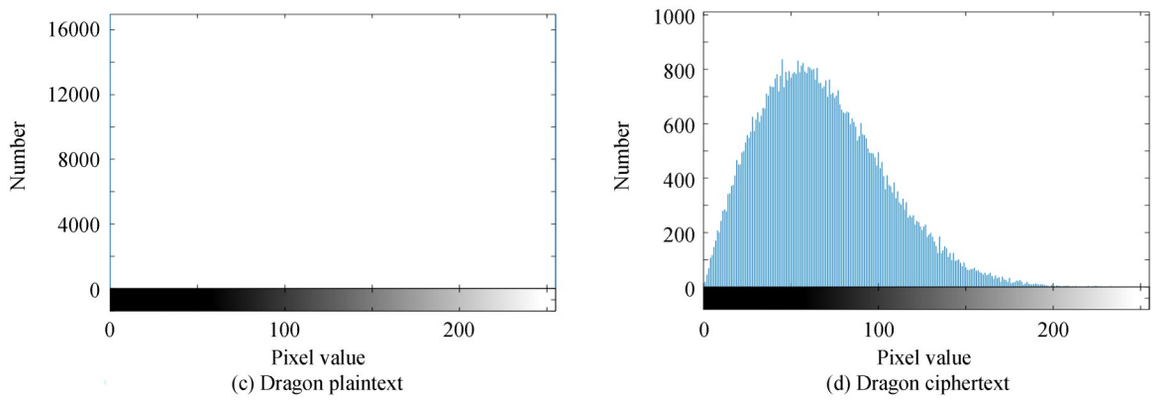


图9　明密文直方图

Fig.9　Histogram of plaintext and ciphertext

3.5.2　相邻像素相关性分析

为精确对比明密文相邻像素的相关性，计算出水平、垂直和对角三个方向的相邻像素的相关系数（Correlation Coefficient，CC），如表3所示.

表3　相邻像素相关性

Table 3　Correlation of adjacent pixels

	Horizontal	Vertical	Diagonal
Lena plaintext	0.935 7	0.968 2	0.908 5
Lean ciphertext	−0.003 9	−0.005 0	−0.004 9
Dragon plaintext	0.917 3	0.916 8	0.870 0
Dragon ciphertext	−0.003 8	0.005 5	−0.006 9

由表3可见，明文相关系数接近1而密文接近0，说明明文相邻像素几乎相同而密文相邻像素相差巨大，故本算法很好地破坏了明文相邻像素相关性.

3.6　对比分析

为验证本算法的先进性，将不同的加密和压缩算法与本算法进行对比，加密主要对比明密文敏感性、抗选择明密文攻击能力，压缩主要比较压缩比以及在压缩后的恢复图像与原图的峰值信噪比（Peak Signal to Noise Ratio，PSNR）.以Lena（256×256）作为实验对象其结果如表4所示.

表4　不同算法的对比分析

Table 4　comparative analysis between different algorithms

Algorithm	NPCR	UACI	Resistant to selected plaintext and ciphertext attacks	Key space	Compression ratio	PSNR
DRPE	0.979 6	10.186 4	Broken	-	-	-
Ref.[3]	0.995 2	16.557 4	Weak	10^{135}	-	-
Ref.[5]	0.978 5	5.865 9	Weak	-	-	-
Ref.[14]	0.991 9	7.472 1	Weak	10^{144}	-	-
Ref.[21]	-	-	Weak	4.08×10^{137}	0.25	33.45
Ref.[22]	-	-	Weak	10^{136}	0.610 4	30.408 9
Ref.[20]	0.996 1	33.36	Strong	10^{105}	0.562 5	34.937 0
The algorithm	0.991 8	24.333 9	Strong	4.6×10^{137}	0.47	INF

由表4可见本算法的明文敏感性比光学图像加密的DRPE和文献[3]、[5]、[14]更强，主要是本算法加密密钥与明文的HASH值SHA256有关，使得明文与密文和密钥有强烈的雪崩效应.而DRPE和文献[5]、

[14]的密钥与明文无关,文献[3]关联性不强,所以明文对密钥和密文敏感度不高,抗差分攻击和选择明文攻击能力弱.同时DRPE和文献[5]的密钥为整个随机模板,导致密钥体积过大不利于传输与分发.文献[20]的变换率和变换强度优于本文,它采用数字图像的置乱和扩散原理来加密,密文分布更加均匀,所以更加接近理想值,但是没有光学的高速并行的特性.同时可以看出只有本算法在压缩的同时还能无损地恢复.由以上分析可知本算法具有一定的先进性和可行性.

4 结论

本文提出了一种级联混沌系统和一种无损压缩方法,L-L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,提高了其序列的随机性.用其产生随机相位模板,用初值和参数作为密钥极大地减小了密钥体积,便于密钥的传输.用单位等模矢量分解和干涉原理设计出一种无损的压缩方法,使得密文接近原来的一半,利于密文传输与分发.为了解决干涉图像能看到干涉前两图像轮廓的问题,在将图像分为两块的时候,用一种隔空抽取的置乱方式,既解决了干涉轮廓问题,还增加了系统安全性.将明文的HASH值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,同时增加了密钥空间,更加有效地抵御蛮力攻击.

参考文献

[1] HOSNY K M, HAMZA H M, LASHIN N A. Copy-for-duplication forgery detection in colour images using QPCETMs and sub-image approach[J]. *IET Image Processing*, 2019, **13**(9): 1437-1446.

[2] LI Y, ZHOU J. Fast and effective image copy-move forgery detection via hierarchical feature point matching[J]. *IEEE Transactions on Information Forensics and Security*, 2019, **14**(5): 1307-1322.

[3] GUO Yaun, XU Xin, JING Shi-wei, *et al*. Virtual optical image encryption method based on hybrid chaotic system[J]. *Acta Photonica Sinica*, 2019, **48**(7): 0710002.
郭媛,许鑫,敬世伟,等.一种混合混沌虚拟光学图像加密方法[J].光子学报,2019,**48**(7): 0710002.

[4] GUO Yuan, JING Shi-wei, XU Xin, *et al*. Asymmetric optical image encryption based on vector decomposition and phase-truncated[J]. *Infrared and Laser Engineering*, 2020, **49**(4): 0426001.
郭媛,敬世伟,许鑫,等.基于矢量分解和相位剪切的非对称光学图像加密[J].红外与激光工程, 2020, **49**(4): 0426001.

[5] AHOUZI E, ZAMRANI W, AZAMI N, *et al*. Optical triple random-phase encryption[J]. *Optical Engineering*, 2017, **56**(11): 113114.

[6] REFREGIER P, JAVIDI B. Optical image encryption using input plane and fourier plane random encoding[J]. *Optics Letters*, 1995, **20**(7):767-769.

[7] HENNELLY B, SHERIDAN J T. Optical image encryption by random shifting in fractional Fourier domains[J]. *Optics Letters*, 2003, **28**(4):269-271.

[8] HENNELLY B M, SHERIDAN J T. Random phase and jigsaw encryption in the Fresnel domain[J]. *Optical Engineering*, 2004, **43**(10):2239-2249.

[9] XU L, AHMAD M A, GUO Q, *et al*. Double image encryption by using iterative random binary encoding in gyrator domains[J]. *Optics Express*, 2010, **18**(11):12033-12043.

[10] CAMICER A, MONTES M, ARCOS S, *et al*. Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys[J]. *Optics Letters*, 2005, **30**(13):1644-1646.

[11] PENG X, ZHANG P, WEI H, *et al*. Known-plaintext attack on optical encryption based on double random phase keys[J]. *Optics Letters*, 2006, **31**(8):1044-1046.

[12] PENG Xiang, TANG Hong-qiao, TIAN Jin-dong. Ciphertext-only attack on double random phase encoding optical encryption system[J]. *Acta Physica Sinica*, 2007, **56**(5):2629-2636.
彭翔,汤红乔,田劲东.双随机相位编码光学加密系统的唯密文攻击[J].物理学报,2007, **56**(5):2629-2636.

[13] YANG B, LIAO X. A new color image encryption scheme based on logistic map over the finite field Z N[J]. *Multimedia Tools & Applications*, 2018, **77**(16):21803-21821.

[14] ZHU Wei, YANG Geng, CHEN Lei, *et al*. An improved image encryption algorithm based on double random phase encoding and chaos[J]. *Acta Optica Sinica*, 2014, **34**(6):66-76.
朱薇,杨庚,陈蕾,等.基于混沌的改进双随机相位编码图像加密算法[J].光学学报,2014,**34**(6):66-76.

[15] GAN Z H, CHAI X L, HAN D J, *et al*. A chaotic image encryption algorithm based on 3-D bit-plane permutation[J]. *Neural Computing & Applications*, 2019, **31**(11): 7111-7130.

[16] ZHANG H, CAI R. Image encryption algorithm based on bit-plane scrambling and multiple chaotic systems combination[C].International Conference on Intelligent Computing & Integrated Systems, 2010:113-117.

[17] SUN S. A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling[J]. *IEEE Photonics Journal*, 2018, **10**(2): 1-14.

[18] ZHANG Xue-feng, FAN Jiu-lun. A new piecewise nonlinear chaotic map and its performance[J]. *Acta Physica Sinica*, 2010, **59**(4):2298-2304.
张雪锋,范九伦.一种新的分段非线性混沌映射及其性能分析[J].物理学报,2010,**59**(4):2298-2304.

[19] CHUNLAI L, HONGMIN L, FUDONG L, *et al*. Multiple-image encryption by using robust chaotic map in wavelet transform domain[J]. *Optik*, 2018, **171**: 277-286.

[20] PONUA R, AMUTHA R. Compressive sensing and chaos-based image compression encryption[J]. *Advances in Soft Computing and Machine Learning in Image Processing*, 2018, **730**: 373-392.

[21] LIU Q, WANG Y, WANG J, *et al*. Optical image encryption using chaos-based compressed sensing and phase-shifting interference in fractional wavelet domain[J]. *Optical Review*, 2018, **25**: 46-55.

[22] ZHANG D, LIAO X, YANG B, *et al*. A fast and efficient approach to color-image encryption based on compressive sensing and fractional Fourier transform[J]. *Multimedia Tools and Applications*, 2018, **77**(2): 2191-2208.

[23] SHI W, JIANG F, LIU S, *et al*. Image compressed sensing using convolutional neural network[J]. *IEEE Transactions on Image Processing*, 2020, **29**: 375-388.

Foundation item: 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), Graduate Research Project (No. YJSCX2019042).