Journal of Image and Signal Processing 图像与信号处理, 2021, 10(2), 88-98
Published Online April 2021 in Hans. http://www.hanspub.org/journal/jisp
https://doi.org/10.12677/jisp.2021.102010

Hans汉斯

基于混沌和位平面交换的彩色图像加密算法

梁杰涛，苏杰彬，王俊刚，叶瑞松*

汕头大学数学系，广东 汕头
Email: *rsye@stu.edu.cn

收稿日期：2021年4月3日；录用日期：2021年4月22日；发布日期：2021年4月29日

摘 要

为了提高图像加密算法的加密性能和安全性，本文设计了一种新的基于混沌和位平面交换彩色图像加密算法。将彩色明文图像三颜色分量的高比特平面进行重构，并通过斜帐篷映射产生的伪随机序列，结合广义Arnold映射来进行位平面的置乱，将三颜色分量的高位平面的信息均匀分散到低位平面，有效降低高位平面之间的相关性。为了进一步提高加密算法的安全性和加密性能，算法使用实参数的广义Arnold映射生成混沌序列，对置乱图像进行扩散操作。实验和安全分析表明，该加密算法具有较高的安全性和较好的加密性能。

关键词

混沌系统，图像加密，斜帐篷映射，Arnold映射

Color Image Encryption Algorithm Based on Chaos and Bit Plane Exchange

Jietao Liang, Jiebin Su, Jungang Wang, Ruisong Ye*

Department of Mathematics, Shantou University, Shantou Guangdong
Email: *rsye@stu.edu.cn

Received: Apr. 3rd, 2021; accepted: Apr. 22nd, 2021; published: Apr. 29th, 2021

Abstract

To improve the encryption performance and security of image encryption algorithm, a novel color image encryption algorithm based on chaos and bit plane exchange operation is designed. The high bit planes of three color components for color plain image are reconstructed. The pseudo-random sequence generated by skew tent mapping is combined with generalized Arnold map to scramble the bit plane. The information of the high bit planes of the three color components is

*通讯作者。

文章引用: 梁杰涛, 苏杰彬, 王俊刚, 叶瑞松. 基于混沌和位平面交换的彩色图像加密算法[J]. 图像与信号处理, 2021, 10(2): 88-98. DOI: 10.12677/jisp.2021.102010

evenly distributed to the low bit planes, which effectively reduces the correlation between the high bit planes. The proposed algorithm uses the generalized Arnold map of real parameters to generate chaotic sequences to diffuse the scrambled image to further enhance the security and performance of the proposed image encryption algorithm. Experiments and security analysis show that the proposed image encryption algorithm has high security and better encryption performance to resist various attacks.

Keywords

Chaotic System, Image Encryption, Skew Tent Map, Arnold Map

1. 引言

随着网络技术的快速发展，数字图像数据成为日常生活中交流信息的主要载体，经由网络在人群中传播共享。在公众重视信息安全和个人隐私的背景下，数字图像的保密需求也日益突出，减少图像数据受到非法复制、传播等有害行为的影响，保证图像在传输过程中的安全性和保密性具有重要的意义。图像数据本身具有信息量巨大、数据冗余度高、相邻像素高度相关性等固有特性，图像数据在通信中需要很强的实时性，因此需要速度快、安全性高的加密方法。这些特点使得针对文本数据设计的传统加密系统 DES、AES 已经不适用于图像加密[1]。因此有必要为图像的加密设计更有针对性的加密方法。许多学者对此作了诸多的研究，提出了许多有效算法，其中基于混沌理论的图像加密算法是被最广泛采用的方法之一。混沌现象是在非线性动力系统中出现的确定、伪随机的现象。混沌系统具有极强的初值和参数敏感性，生成的序列具有很强的伪随机性、遍历性和可重复生成等优良性质，这些属性与密码学的混淆与扩散等性质有着天然的高度相似性，因此混沌系统具有设计性能良好的图像加密系统的巨大潜力[2] [3]。

基于混沌理论的图像加密系统一般由置换与扩散两个过程构成。置乱过程通过混沌系统的遍历性与随机性将图像的像素灰度值重新排列，破坏图像灰度值对位置的高度相关性，有效地从视觉上破坏图像像素原本的位置信息。扩散过程利用混沌系统对初始值与系统参数高度敏感等特点，设计具有优良扩散效应的扩散函数，使得任何一个像素的亮度值的改变，可以对这个像素后面的像素产生骨牌多米诺效应的效果。基于混沌系统的图像加密算法的像素置乱可以采用各种各样的变换实现，如 Arnold 变换，Standard 变换等[3] [4]。这些经典的变换置乱形式相对简单，单一的应用会被轻易通过选择明文、已知明文等密码分析后破解[5] [6] [7]。为了提高加密算法抵御被黑客破解的能力，本文通过将经典的成熟混沌系统斜帐篷映射、Arnold 映射组成混合的系统，设计一种新的彩色图像加密算法。混沌系统的混合应用，可以扩大密码空间的大小，增强加密系统抵御蛮力攻击的性能。另一方面，通过使用明文图像信息相关的敏感特征量来修正 Arnold 映射和斜帐篷映射的参数和初值，使得加密算法对明文图像的信息具有更好的敏感性，实现一次一密的加密效果。研究表明简单仅仅通过像素位置的置乱算法是脆弱的，很容易被黑客破解[7] [8]。

灰度图像的亮度值的高比特位占据图像的主要信息，彩色图像三颜色通道的分量值的高比特位也是颜色的主要贡献部分[9] [10]。图像相邻像素间，三颜色 R、G、B 分量之间均具有很强的相关性，所以设计加密算法的时候，应该考虑通过像素层次和比特层次间的置乱，达到破坏这种彩色图像的像素间和颜色分量间的强相关性。因此本文首先通过将三颜色分量的高 2 位比特值重组成 6 比特值，其他低比特值

保留不变，从而可以将 8 比特的彩色图像重构成 4 个 6 比特的灰度图像。然后通过使用计算明文图像的信息不变量，修改斜帐篷映射的参数和初始值，使得斜帐篷映射生成的密钥流与明文高度相关。通过量化斜帐篷映射迭代生成的序列值，得到广义的离散 Arnold 变换的参数，并用离散 Arnold 变换对比特重构后的 4 个矩阵进行像素置乱。为了提高效率，置乱在高比特位矩阵与 3 个低比特位矩阵之间进行，通过斜帐篷映射的混沌序列具有均匀分布的特性，生成一个均匀分布的三值序列，来操控高比特矩阵与 3 个低比特矩阵之间的像素交换。通过上述比特重构和像素置乱后，达到了破坏像素值和像素位置的目的。为了进一步提高加密算法的性能和安全性，算法中还安排了一个像素层次的扩散过程，通过引入广义实数参数的 Arnold 变换用于生成扩散过程的密钥流。加密算法采用按位比特异或和加法模运算相结合的模式，既保证了扩散过程的可逆性也使得安全性能更好。结果表明，本文所设计的加密算法具有很好的安全性和加密性能，可以抵御蛮力攻击、统计分析攻击，差分分析攻击、选择明文和已知明文攻击等。

2. 相关知识

2.1. 斜帐篷混沌映射

斜帐篷混沌映射为分段的线性映射，广泛应用于混沌加密系统中，具体定义如(1)所示：

$$t_{n+1}=T\left(t_n\right)=\begin{cases}t_n/\mu, t_n\in[0,\mu]\\(1-t_n)/(1-\mu), t_n\in(\mu,1]\end{cases} \tag{1}$$

其中 $t_n\in[0,1]$，$\mu\in(0,1)$ 是控制参数，控制着斜帐篷混沌映射的动力学特性。对于任意一个 $\mu\in(0,1)$，系统(1)的 Lyapunov 特征指数为 $-\mu\ln(\mu)-(1-\mu)\ln(1-\mu)>0$，说明该映射为混沌映射，该映射具有良好的动力学特性，生成的序列具有很好的伪随机性，分布均匀，高度依赖于初值和参数，可以用来生成加密算法的密钥流，t_0,μ 作为密钥。

2.2. 广义 Arnold 混沌映射

广义 Arnold 映射可以被用于置乱大小为 $N\times N$ 的图像的像素位置，其矩阵表示形式如(2)：

$$\begin{pmatrix}x_{n+1}\\y_{n+1}\end{pmatrix}=\begin{pmatrix}1 & a\\ b & ab+1\end{pmatrix}\begin{pmatrix}x_n\\y_n\end{pmatrix} mod\ N \tag{2}$$

其中 (x_n,y_n) 是原始像素的位置，(x_{n+1},y_{n+1}) 是置乱之后像素的位置，a 和 b 是整数，在 $\{1,2,\cdots,N-1\}$ 中取值。对于映射(2)，容易计算得其最大 Lyapunov 特征指数为 $\lambda=1+\dfrac{ab+\sqrt{a^2b^2+4ab}}{2}>1$，说明该映射是混沌的[3]。

本文将使用参数是整数和实数两种类型的广义 Arnold 映射。扩展(2)的整数 a,b 为实数，映射修改为公式(3)，其中的状态变量取值在 $[0,1)\times[0,1)$ 中。这样的实参数广义 Arnold 映射将可以产生具有优良混沌特性的序列，其中的初值和系统参数的选择范围大大扩大，从而密钥空间也得到扩大。系统所生成的两组混沌序列，将用于扩散过程的加密。

$$\begin{pmatrix}x_{n+1}\\y_{n+1}\end{pmatrix}=\begin{pmatrix}1 & a\\ b & ab+1\end{pmatrix}\begin{pmatrix}x_n\\y_n\end{pmatrix} mod\ 1 \tag{3}$$

3. 加密方案

本节提出了一种新的图像加密算法，并对其在信息安全中的应用进行了验证。加密算法中所使用的 7 个参数 $\{t_0,\mu,x_0,y_0,a,b,D\}$ 作为密钥。加密算法的主要框架如图 1 所示。

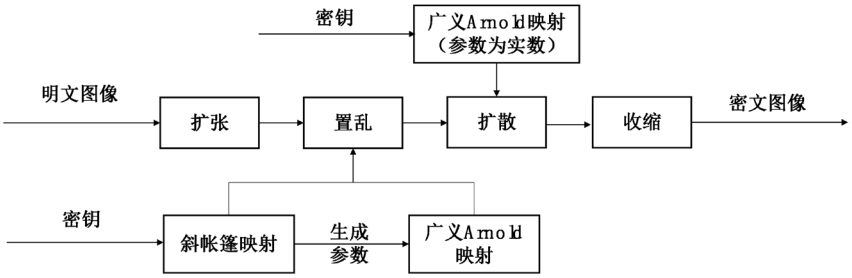

Figure 1. The main frame of encryption algorithm
图 1. 加密方案的主要框架

3.1. 置换操作

3.1.1. 扩张－收缩策略

文献[9]通过使用比特级置换代替传统的像素级置换，混淆效果得到了改善。但是该方法并没有在不同位平面之间置换，因此不能平滑不同位平面的波动分布，而是保持每个位平面的统计信息不变。文献[10]揭示了数字图像中比特分布的内在特征。像素的高位代表图像信息的高权重，高位平面之间有很强的相关性。统计表明，第 8 位平面和第 7 位平面的值趋于相反[10]。在安全的密码系统中，这些特性不应被忽视。针对上述问题，文献提出一种扩张－收缩的策略，用一种新型的置换方式巧妙地同时进行位平面内和位平面间的置换，从而解决了上述的问题，有利于实现三个目标：1) 比特在彩色图像的三维矩阵中的整体分布应均匀；2)每个位平面内的比特分布应均匀；3) 相邻位平面之间的相关性应尽可能低。

为了描述方便，考虑一个大小为 $N\times N$ 的彩色图像，将原图像看作一个大小为 $N\times N\times 3$ 的三维矩阵 P，P 的元素值记录了原始明文图像的颜色分量值，即原图像位于像素 (i,j) 的 R、G、B 分量值 $P(i,j,k),k=1,2,3$。读取彩色图像后，即可以得到图像的 R、G、B 分量所对应的二维矩阵。

在扩张策略中，R、G、B 通道中每个像素的最高两个比特被分离出来组成一个新的 6 比特数值，其中最高的两位来自 B 通道，其次两位来自 G 通道，最低的两位来自 R 通道。各颜色通道中每个像素余下的 6 位比特保持不变，那么将会得到 4 个 $N\times N$ 的 6 比特像素平面。将这 4 个平面按顺时针次序依次放置在 $2N\times 2N$ 矩阵的四个分块中，得到扩张矩阵 M。扩张收缩策略如图 2 所示。随后对扩张矩阵 M 进行置乱与扩散，加密完成后按扩张的逆过程进行收缩得到原图像。

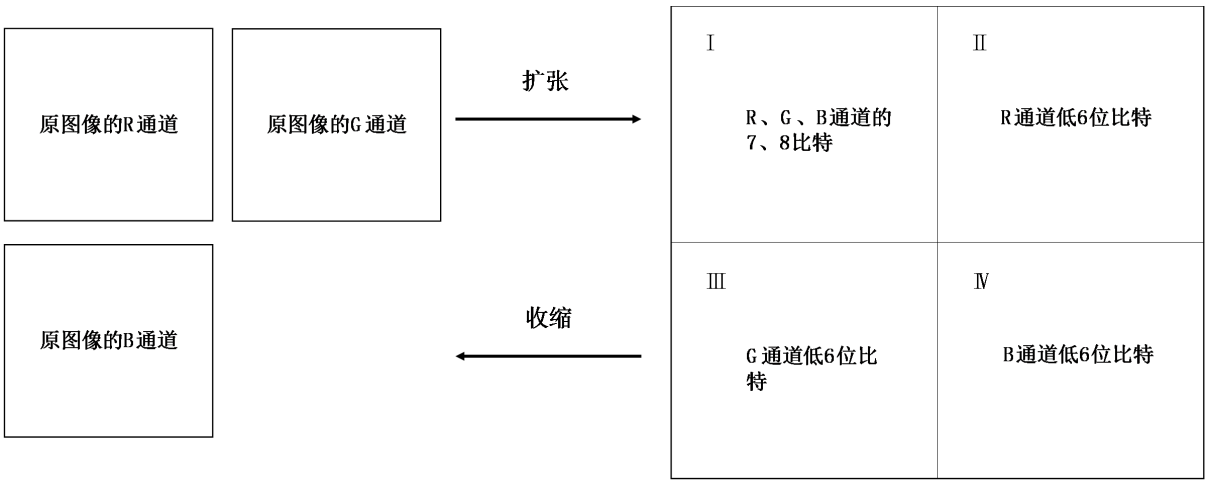

Figure 2. Expansion-shrinkage strategy
图 2. 扩张－收缩策略

3.1.2. 置乱过程

在这一阶段，通过斜帐篷映射产生混沌序列，将该序列的值量化之后作为 Arnold 映射的参数，通过改变扩张后的矩阵 M 中的像素位置来对图像进行置乱处理。

首先，利用斜帐篷映射(1)生成混沌序列 $\{t_k\}$，舍去前面的 s 个值，s 为矩阵 M 中元素的总和：$s=\sum_{i=1}^{2N}\sum_{j=1}^{2N}M(i,j)$，从而使得混沌序列 $\{t_k,:k=s,s+1,\cdots,s+N^2\}$ 与明文图像 P 相关，可以很好的抵御差分攻击。

然后，利用 $\{t_k\}$ 对区域 I 中的像素进行置乱，将其像素信息均匀分布至低位比特所组成的像素平面(II, III, IV)中。为此，利用 $\{t_k,:k=s,s+1,\cdots,s+N^2\}$ 量化生成随机整数序列 $\{T_k:k=1,\cdots,N^2\}$，使得 $T_k\in\{1,2,3\}$。T_k 的定义如式(4)所示：

$$T_k=floor(3\times t_k)+1,k=1,\cdots,N^2 \tag{4}$$

将 T_k 重塑为 $N\times N$ 的矩阵 S，根据 $S(i,j)$ 的取值判断区域 I 中对应位置的像素与 II, III, IV 中的哪个区域的像素进行交换。交换的位置由广义 Arnold 混沌映射(5)生成：

$$\begin{pmatrix}x'_n\\y'_{n+1}\end{pmatrix}=\begin{pmatrix}1&q\\p&pq+1\end{pmatrix}\begin{pmatrix}x_n\\y_n\end{pmatrix} \tag{5}$$

其中参数 p,q 由斜帐篷映射的值决定：

$$p=mod\left(floor\left(t_{s+1}\times10^8\right),N-1\right)+1;$$
$$q=mod\left(floor\left(t_{s+2}\times10^8\right),N-1\right)+1.$$

用三维坐标 (x,y,z) 表示像素在矩阵 M 中的位置，其中 $z\in\{1,2,3,4\}$ 表示像素所处的区域，$(x,y):x,y\in1,2,\cdots,N$ 表示像素在所处区域的位置，则上述置乱过程可表示为交换关系(6)：

$$(x_i,y_j,1)\leftrightarrow(x'_i,y'_j,S(i,j)+1) \tag{6}$$

经过一轮的置乱操作，高位比特所处的平面(第 I 区域)的像素被均匀分布到区域 II, III, IV 中去，使得相邻比特平面之间的相关性尽可能低。

3.2. 扩散操作

3.2.1. 一次扩散

Step 1. 将置乱后的扩张矩阵 M 按照左右均分为两个大小为 $2N\times N$ 的矩阵 A,B，然后将这两个矩阵组合得到一个大小与 A,B 矩阵一致的 12 比特矩阵 C，其中矩阵 C 中数据的奇数比特位与对应位置的矩阵 A 的比特保持一致，偶数比特位与对应位置的矩阵 B 的比特保持一致。

Step 2. 用 2.2 节的广义 Arnold 映射式(3)进行迭代得到两个长度为 $2N\times N+50$ 的混沌序列，其中 x_0,y_0,a,b 作为密钥。然后去掉该序列的前 50 位消除暂态影响，得到序列 $\{x_n\}$，$\{y_n\}$，对这两个序列作如式(7)的处理，得到 12 比特序列 $\{X_n\}$，$\{Y_n\}$。

$$\begin{cases}X_n=mod\left(floor\left(x_n\times10^{12}\right),4096\right)\\Y_n=mod\left(floor\left(y_n\times10^{12}\right),4096\right)\end{cases} \tag{7}$$

Step 3. 提取 $\{X_n\}$ 的奇数比特位与 $\{Y_n\}$ 的偶数比特位组成一个新的 12 比特序列 $\{Z_n\}$，其中序列 $\{Z_n\}$ 中数字的奇数比特位与 $\{X_n\}$ 的奇数比特位一致，$\{Z_n\}$ 中数字的偶数比特位与 $\{Y_n\}$ 的偶数比特位一致，之后将序列 $\{Z_n\}$ 重塑为一个 $2N\times N$ 的矩阵 T。

Step 4. 对矩阵 C 和矩阵 T 进行异或运算(8)，得到一次扩散矩阵 $cipher_1$：

$$cipher_1(i,j)=C(i,j)\oplus T(i,j) \tag{8}$$

3.2.2. 二次扩散

Step 1. 对 $cipher_1$ 进行进一步的扩散。首先将 $cipher_1$ 按行拉直为 $1\times 2N^2$ 的向量 V_1，将 V_1 按式(9)进行扩散操作得到二次扩散密文向量 V_2。

$$\begin{aligned} V_2(k)&=mod\left(V_1(k)+Z(k),4096\right)\oplus V_2(k-1)\\ V_2(0)&=D \end{aligned} \tag{9}$$

Step 2. 将 V_2 重塑为 $2N\times N$ 大小的密文矩阵 $cipher_2$。

Step 3. 对 $cipher_2$ 的比特进行拆分。再次将 $cipher_2$ 分为两个 6 比特矩阵 A',B'，比特矩阵 A' 由 $cipher_2$ 的前 6 比特位组成，比特矩阵 B' 由 $cipher_2$ 的后 6 比特位组成，最后将 A',B' 按收缩策略重新合并为最终的加密矩阵 $cipher_3$，得到最后的彩色密文图像。

4. 仿真结果和安全性分析

为了说明所提出的加密方案的安全性，给出了实验结果和安全性分析。所有模拟均在 2.80GHz CPU，8GB 内存的计算机上运行，编译平台为 MATLAB R2017a。

4.1. 初值选取

读取大小 $N\times N$ 为彩色明文图像 I，并求出 I 的颜色分量值总和 k，对 k 进行如式(10)的变换得到 s_1。

$$s_1=mod\left(100k,97\right)+50 \tag{10}$$

构造一个初值 $t_0=0.32$，控制系数 $\mu=0.6$ 的斜帐篷映射，生成长度为 $7+s_1$ 的序列，然后丢掉前 s_1 项，得到一个长度为 7 的序列 $series$，对这个序列内的各个数字作如下处理得到加密所需要的各个密钥值。

$$t_0=mod\left(series(1)\times 10^8,1\right),\quad \mu=mod\left(series(2)\times 10^8,1\right),$$

$$x_0=series(3),\quad y_0=series(4),\quad a=series(5)\times 27,\quad b=series(6)\times 111,$$

$$D=mod\left(floor\left(series(7)\times 10^8\right),4096\right).$$

各个密钥的具体说明如表 1 所示。相较于直接对密钥进行赋值，该做法将明文与混沌序列相关联，组合成密钥，可以增强明文敏感性，同时明文与密钥生成相关，可以实现一图一密的效果。在实际加密中，所有这些参数，即 $Key=\{t_0,\mu,x_0,y_0,a,b,D\}$，均可以作为密钥使用。

Table 1. Cipher keys
表 1. 密钥说明

图像置乱	
斜帐篷映射初值	t_0
斜帐篷映射控制系数	μ
图像扩散	
Arnold 映射初值	x_0
	y_0
Arnold 映射控制系数	a
	b
像素扩散初值	D

4.2. 仿真结果

在本节中，我们选择大小为256×256的Lenna彩色图像作为测试图像进行加密和解密实验。产生的实验的视觉效果如图3所示。结果表明，加密图像是类噪声图像，算法还可以有效地应用于各种形式的图像，如灰度图像、彩色图像和二值图像。

(a) 原图像　　(b) 加密图像

Figure 3. The encryption results
图3. Lena图像的加密结果

4.3. 密钥空间分析

密钥空间是所有可行密钥构成的集合。所提出的加密算法的密钥是双精度数字。为了更好的安全性能，加密算法应该对其安全密钥的任何变化都非常敏感，并拥有大于 2^{100} 的空间，足以承受强力的穷举攻击。本文构建的加密方案有7个密钥：$Key=\{t_0,\mu,x_0,y_0,a,b,D\}$。如果实数计算精度为 10^{-14}，我们可以计算得到总的密钥空间为 $10^{14\times6}\times4096$，根据[11]中的建议，密钥空间至少为 2^{100}，故此加密算法有足够大的密钥空间，可有效的抵御穷举攻击与暴力破解。

4.4. 密钥敏感性分析

一个好的加密系统应该对密钥和明文图像的细微变化非常敏感。灵敏度可通过NPCR (像素数变化率)和UACI(统一平均变化强度)进行定量评价，NPCR和UACI的值越接近其数学期望值NPCR = 99.6094%，UACI = 33.4635%，加密性能越好，说明密文对密钥的变化越敏感[12]。NPCR和UACI的计算式如(11)~(12)所示。

$$\mathrm{NPCR}=\frac{\sum_{i,j}Dif\left(I_1,I_2\right)}{M\times N}\times100\% \tag{11}$$

$$\mathrm{UACI}=\frac{1}{M\times N}\left[\sum_{i,j}\frac{\left|I_1(i,j)-I_2(i,j)\right|}{255}\right]\times100\% \tag{12}$$

其中 I_1 和 I_2 是对应于两个微小差别的密钥所对应的加密图像。在实验中面对图像在加密过程中做微小调整，对密钥中的各个值进行微小的变化 $\Delta=10^{-14}$，对进行检验的密钥分别采取 $+\Delta$ 和 $-\Delta$ 的变化，分别计算两次变化的NPCR与UACI值，求得两次变化的平均值如表2所示。从表2可以看出，所提出的图像加密算法对密钥均非常敏感。

Table 2. The results of key sensitivity (%)
表 2. 密钥敏感性的结果(%)

$\Delta\mu = 10^{-14}$	NPCR	UACI
t_0	99.62	33.45
μ	99.62	33.46
x_0	99.36	33.52
y_0	99.33	33.40
a	99.36	33.57
b	99.33	33.46

4.5. 统计分析

为了证明所提出的加密方案的安全性，我们进行了以下统计测试。

直方图分析。图像直方图可以较为直观的看出图像的灰度值分布情况，如果密文的灰度值频率直方图分布越均匀，表明加密效果越好，从加密图像中推断原图像信息越是困难。在经过置乱与扩散后，图像的R、G、B 三个分量的灰度值发生了变化，对原图像和加密图像的灰度值进行直方图统计，结果如图 4 所示。由图 4 可知密文图像的 R、G、B 分量值的直方图发生了显著变化，直方图变得平坦，表明 256 个灰度级所对应的像素点个数相对平均，从直方图分析角度来看，加密效果好。

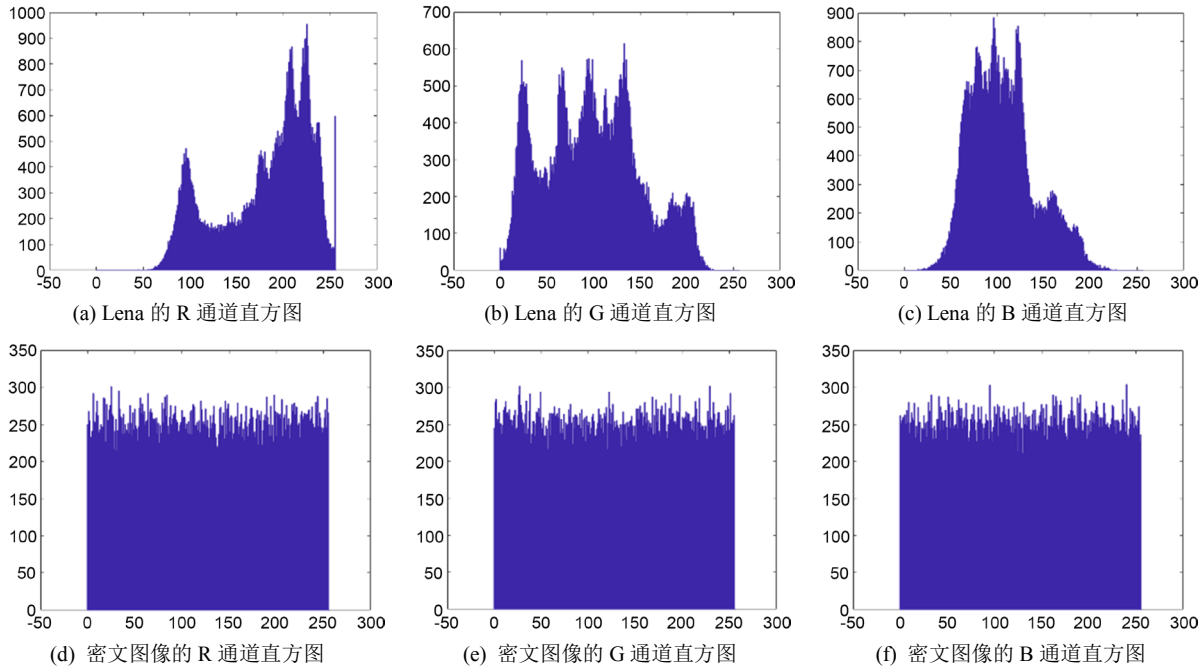

Figure 4. The histograms of R, G, B components for plain image and cipher image
图 4. 明文图像和密文图像三颜色分量的直方图

相关性分析。相邻像素相关性反映图像相邻位置像素值的相关程度。良好的图像加密算法能有效降低相邻像素的相关性。在实验中，我们从原始图像和加密图像中随机选取 6000 对相邻像素，并在水平、垂直和对角线方向上分析相关性。相关系数由式(13)计算。

$$r_{xy}=\frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{13}$$

式中，x_i 和 y_i 表示某对相邻像素的像素值。协方差与方差的计算公式如下：

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

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)^2,\quad E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i。$$

Table 3. The correlation coefficients of adjacent pixels
表 3. 相邻像素之间的相关性系数

方向	明文	密文
垂直	0.9614	0.0109
水平	0.9796	−0.0024
对角线	0.9436	−0.0127

结果如表 3 所示，结果显示明文图像的相邻像素相关性极强，密文图像的相邻像素相关性极弱，加密算法可以很好地削弱相邻像素的相关性。为更加直观展示结果，每种方向的相关性分布如图 5 所示：

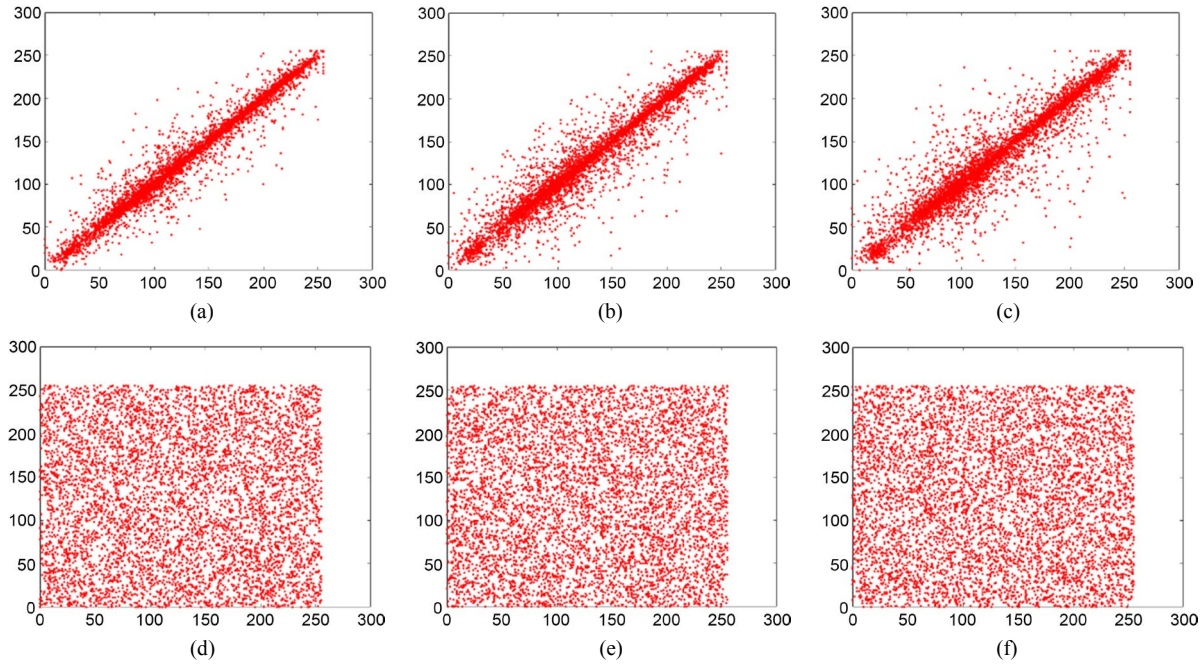

Figure 5. (a)~(c) and (d)~(f) are the correlation analysis of the pixels in the horizontal, vertical and diagonal directions of the three color channels of the plaintext and cipher-text
图 5. (a)~(c)和(d)~(f)分别是明文图像和密文图像的三颜色分量在水平、垂直和对角方向上的相关性分析

从图 5 中可以看出明文中垂直、水平、对角线三个方向的像素点都集中在对角线方向上，表明像素之间的相关性较强。而密文中三个方向的像素点较均匀地布满整个平面，表明密文的像素之间的相关性很弱，近乎随机。

4.6. 信息熵分析

图像的信息熵是一种度量随机特征的统计形式，能测试不确定性，能反映出图像中平均信息的多少。当图像中信息量越大时熵的值越大，图像越粗糙，当图像中信息量越小是熵的值越小，图像越平滑。由于灰度值的范围是[0, 255]，灰度级总数记为 $L=256$，所以熵的取值范围为[0, 8]。信息熵的计算公式如(14)。

$$H(X)=-\sum_{i=0}^{2^L-1}P(X_i)\log_2 P(X_i) \tag{14}$$

式中 $P(X_i)$ 表明信息 X_i 出现的频率。按式(14)计算，加密后的图像信息熵为 7.9973，很接近于最大值 8，表明图像中的信息不确定度很大，能被攻击的可能性很小，很难泄露信息。

4.7. 明文敏感性分析

图像加密算法的差分攻击分析是研究在相同密钥下密文图像会在多大程度上受明文图像的影响，攻击者通常通过选择明文分析或选择密文分析来实现差分攻击。为了分析加密算法抵御差分攻击的能力，很有必要分析明文敏感性，分析中有两个特征量可以很好地刻画该项性能，即是公式(11)，(12)所计算的 NPCR 和 UACI，只不过这里改变量是明文，对明文实施最微小的变化，用同样的密钥加密，得到两幅密文图像并计算这两个值，如果很接近数学期望值 NPCR = 99.6094%，UACI = 33.4635%，则表明算法抵御差分攻击的能力越强。本文随机选取像素图像中的 100 个像素，在每一次改变中对其中一个像素的值增加 1，将变更后加密的图像与原加密图像进行对比，计算两副密文图像的 UACI 及 NPCR。经过 100 次的试验后得到 NPCR 和 UACI 的平均值分别为 99.62%和 33.50%。结果表明本文的图像加密算法对明文的微小差异非常敏感，可以有效抵御差分分析的攻击。

5. 总结

本文设计了一种新的基于混沌和位平面交换的彩色图像加密算法。将彩色明文图像三颜色分量中权重大的第 7~8 比特位平面进行重构，结合广义 Arnold 映射来进行重构后的位平面之间的交换置乱，将三颜色分量的高位平面的信息均匀分散到低位平面，有效削弱了相邻像素和颜色分量间的相关性。算法还应用实参数的广义 Arnold 映射生成混沌序列，对置乱图像进行一种高效率的扩散，进一步提升了算法的安全性和性能。实验和安全分析表明，该加密算法具有较高的安全性和较好的加密性能，满足图像加密的需求。

基金项目

论文研究资助项目为广东省大学生创新创业项目以及国家自然科学基金项目(No. 11771265)；广东省普通高校重点研究项目(No. 2019KZDXM034)；广东省基础与应用基础研究基金项目(No. 2020B1515310018)。

参考文献

[1] Schiener, B. (1996) Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley and Sons, New York.

[2] Fridrich, J. (1998) Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. *International Journal of Bifurcation and Chaos*, **8**, 1259-1284. https://doi.org/10.1142/S021812749800098X

[3] Ye, R. (2011) A Novel Chaos-Based Image Encryption Scheme with an Efficient Permutation-Diffusion Mechanism. *Optics Communications*, **284**, 5290-5298. https://doi.org/10.1016/j.optcom.2011.07.070

[4] Vinod, P., Pareek, N.K. and Sud, K.K. (2009) A New Substitution-Diffusion Based Image Cipher Using Chaotic Standard and Logistic Maps. *Communications in Nonlinear Science and Numerical Simulations*, **14**, 3056-3075. https://doi.org/10.1016/j.cnsns.2008.11.005

[5] 马俊明, 叶瑞松. 一种图像加密算法的密码学分析[J]. 网络新媒体, 2015, 4(6): 37-42+54.

[6] Zhao, X., Chen, G., Zhang, D., *et al.* (2004) Decryption of Pure-Position Permutation Algorithms. *Journal of Zhejiang University* (*Science Version*), **5**, 803-809. https://doi.org/10.1631/jzus.2004.0803

[7] Li, S., Li, C., Chen, G., Bourbakis, N.G. and Lo, K. (2009) A General Quantitative Cryptanalysis of Permutation-Only Multimedia Ciphers against Plaintext Attacks. *Signal Processing*: *Image Communication*, **23**, 212-223. https://doi.org/10.1016/j.image.2008.01.003

[8] Li, C., Lin, D. and Lu, J. (2017) Cryptanalyzing an Image-Scrambling Encryption Algorithm of Pixel Bits. *IEEE Multimedia*, **24**, 64-71. https://doi.org/10.1109/MMUL.2017.3051512

[9] Zhu, Z.-L., Zhang, W., Wong, K.-W. and Hai, Y. (2011) A Chaos-Based Symmetric Image Encryption Scheme Using a Bit-Level Permutation. *Information Science*, **181**, 1171-1186. https://doi.org/10.1016/j.ins.2010.11.009

[10] Zhang, W., Wong, K.-W., Yu, H. and Zhu, Z.-L. (2013) A Symmetric Color Image Encryption Algorithm Using the Intrinsic Features of bit Distributions. *Communications in Nonlinear Science and Numerical Simulation*, **18**, 584-600. https://doi.org/10.1016/j.cnsns.2012.08.010

[11] Alvarez, G. and Li, S.J. (2006) Some Basic Cryptographic Requirements for Chaos-Based Cryptosystem. *International Journal of Bifurcation and Chaos*, **16**, 2129-2151. https://doi.org/10.1142/S0218127406015970

[12] Hasheminejad, A. and Rostami, M.J. (2019) A Novel Bit Level Multiphase Algorithm for Image Encryption Based on PWLCM Chaotic Map. *Optik—International Journal for Light and Electron Optics*, **184**, 205-213. https://doi.org/10.1016/j.ijleo.2019.03.065