

基于像素置乱和比特替换的混沌图像加密算法

谢国波,王 添

(广东工业大学 计算机学院,广东 广州 510003)

摘 要: 分析了当前一类基于混沌系统的图像加密算法,指出普遍存在安全性方面的不足. 基于此,提出了一种全新的基于像素置乱和比特替换的混沌图像加密算法. 该算法采用了 Kent 映射和 Logistic 映射,并且使加密过程与明文图像的大小及像素值总和等特性密切相关. 首先,使用 Kent 映射产生混沌序列使得明文图像位置的全局置乱;然后,使用 Logistic 映射产生两组混沌序列,将位置置乱后的图像序列巧妙地融合到两组混沌序列中产生两个中间密文,使得明文图像信息得到很好的隐藏. 通过实验仿真表明,该算法不仅能较好地抵抗差分攻击、统计特性分析,还能有效地抵抗选择明文(密文)攻击,而且密钥空间大、加密效果好.

关键词: 混沌系统;图像加密;置乱;Kent 映射;Logistic 映射

中图分类号: TP309.7

文献标识码: A

文章编号: 1000-7180(2016)03-0080-06

A Chaotic Image Encryption Algorithm Based on Pixel Scrambling and Bit Substitution

XIE Guo-bo ,WANG Tian

(Faculty of Computer, Guangdong University of Technology, Guangzhou 510006, China)

Abstract: By analyzing the current image encryption algorithm based on a class of chaotic systems, we point that they had security flaws widely. Therefore, we propose a new chaotic image encryption algorithm based on bit substitution and scrambling. The algorithm uses Kent map and Logistic map, and makes the encryption process be related closely with the plaintext image's size and the sum of pixel values. First, A chaotic sequence generated by Kent map is used to make image position global scrambling; Then, use Logistic map to generate two chaotic sequence, and embed scrambling image sequence into the two sequence skillfully. The simulation results show that the algorithm can better resist differential attack, statistical characterization, and can effectively resist chosen plaintext (ciphertext) attacks, and have big key space, good encryption effect.

Key words: chaotic systems; image encryption; Kent map; Logistic map

1 引言

现代生活中,随着互联网信息技术的快速发展,使用多媒体表达信息已经变得十分普遍. 数字图像由于直观性强、信息量大,已被广泛应用于各个行业,因而图像的安全性问题就变得尤为重要. 怎样对图像进行安全性高的加密成为学者们致力研究的一

项课题. 近年来,混沌系统以其具备对初值敏感性高、无周期性和伪随机性等特点,在图像加密中的应用越发广泛^[1],学者们陆续提出了许多基于混沌系统的图像加密算法^[2-5]. 而目前基于混沌图像加密算法大部分采用像素位置置乱和像素值替代的思想,很好地体现出了置乱和扩散这两个密码设计的基本原则.

收稿日期: 2015-03-10; 修回日期: 2015-05-22

基金项目: 广东省重大科技专项(2012A080103010); 广东省重点实验室建设专项(2011A091000046); 粤港关键领域重点突破项目(2012A080107007); 广东省科技计划项目(2012B060500071); 广东省自然科学基金(2014A030313512)

文献[6-8]中提出的这类比较典型的混沌加密算法,存在明显的密文分布不均匀的问题,以致于不能有效抵抗统计特性方法攻击;而针对该问题,文献[9-11]提出一类典型“置乱~替代”结构的混沌加密算法,通过混沌系统产生中间密钥来对像素值进行替代,尽管该类算法具有形式简单、运算速度快等优点,但是它们均不能抵御选择明文(密文)攻击.而类似于文献[12-13]中提出的选择一组特殊明文(密文)攻击方法可以破解这类算法.

针对以上基于混沌的一系列图像加密算法所存在的安全性问题,本文提出了一种全新的基于像素置乱和比特替换的加密算法.首先,在利用混沌序列对明文图像进行位置置乱时,使得混沌序列的产生与明文图像自身的特性紧密相连.这样对于不同的明文图像就会产生完全不同的混沌序列,即可产生不同的密钥序列,以至选择明文(密文)攻击方法无效.其次,该算法有别于其他加密算法的是,它不是进行直接异或运算(这种运算很容易被选择一组特定明文或密文破解),而是将先置乱后的明文序列中的每个序列值进行二值化,再分别将其二进制数分开交叉嵌入到另外由 Logistic 混沌序列产生的两组混沌序列中,这样将会产生两组中间密文.对于这种情况,攻击者必须同时得到这两组中间密文才有可能破解,所以该设计过程在选择明文(密文)攻击方面提高了算法的安全性.实验仿真表明,本文加密算法同时具有较好的抗差分攻击能力和抗统计特性分析能力,还具有较大的密钥空间和对初始条件敏感性等密码学特征.

2 算法原理

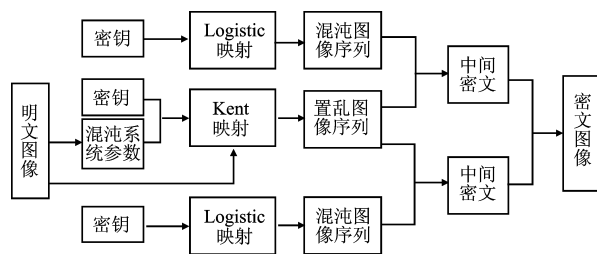
本文提出的加密算法在加密过程中与明文特性紧密相关,不同的密钥将产生不同的密钥.该算法先是通过混沌系统对明文图像像素点位置进行全局置乱,然后通过比特替换和异或操作来进行像素值的改变来达到图像的加密.本文算法的加密、解密过程如图1所示.

2.1 Kent 与 Logistic 混沌系统

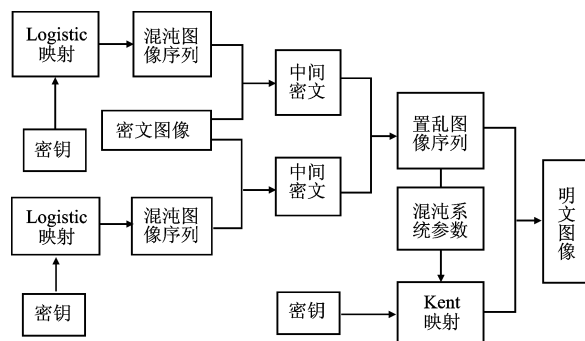
Kent 映射是一个性能很好的混沌系统,所以本文选取它来产生混沌序列,其映射关系为

$$F(x) = \begin{cases} x/S, & x \in (0, S] \\ (1-x)/(1-S), & x \in (S, 1] \end{cases} \quad (1)$$

式中, S 为混沌系统的控制参数,当 $x \in (0, 1)$, $S \in (0, 1)$ 时,式(1)具有一个正的 Lyapunov 指数, Kent



(a) 加密过程



(b) 解密过程

图1 图像加密与解密过程

映射将处于混沌状态,因此由初始条件 x_0 在 Kent 映射中产生的序列是非周期且不收敛的伪随机序列. Kent 映射对初始条件非常敏感,当初始值发生微小变化时,将产生完全不同的两个伪随机序列.

Logistic 映射是一种最为常见的混沌模型,它是一个非线性混沌方程,而且经常被应用于混沌图像加密算法中.尽管运算简单,但却很好地反映了混沌的各种特性.其定义如下:

$$x_{n+1} = \lambda x_n (1 - x_n) \quad (2)$$

式中, λ 为系统非线性强度控制参数, x_n 表示状态量第 n 次迭代后的值,且 $0 < x_n < 1$. 通过研究表明,当 $3.569\ 945\ 6 < \lambda < 4$ 时, Logistic 映射将处于混沌状态. 同样,对于初始条件 x_0 , 在 Logistic 映射作用下产生的序列是非周期、不收敛和对初始条件敏感的.

2.2 加密和解密原理

2.2.1 图像像素位置的置乱

设 A 表示大小为 $m \times n$ 的灰度图像, t 为混沌系统迭代次数, sum 为像素值总和, avg 为像素平均值,加密算法步骤如下所示.

Step 1: 将明文图像 A 按照行优先的顺序转换为长度为 $m \times n$ 的一维序列 $L = \{l_1, l_2, l_3, \dots, l_{m \times n}\}$, 其取值范围为 $[0, 255]$.

Step 2: 将所有的图像像素值相加得到总和为 sum , 再用 sum 除以像素点个数即 $m \times n$, 从而获得到

整个图像的平均像素值 avg , 由式(3)、(4) 分别得出 Kent 混沌系统的控制参数 a 和迭代次数 t .

$$a = \frac{\text{mod}(\text{sum} \times 100, m \times n)}{m \times n} \quad (3)$$

$$t = m + n + \text{mod}(\text{avg} \times 10^8, m + n) \quad (4)$$

Step 3: 设置一个初始值为 x_1 , 将 x_1 和上一步计算出的 a 代入式(1), 迭代 Kent 映射 t 次以消除暂态效应带来的不良影响, 以此为起点继续迭代式(1) $m \times n$ 次, 产生一个长度为 $m \times n$ 的混沌序列 $K = \{k_1, k_2, \dots, k_{m \times n}\}$. 再对混沌序列 K 进行从小到大的排序, 从而产生一个用于记录排序后的序列中各元素在原序列 K 中所在位置的位置序列 $K' = \{k'_1, k'_2, \dots, k'_{m \times n}\}$, 用它来对明文序列 L 进行位置置乱, 得到置乱图像序列 $L' = \{l'_1, l'_2, \dots, l'_{m \times n}\}$.

2.2.2 图像像素值的比特位置乱

此阶段将使用 Logistic 映射产生两个大小同为 $m \times n$ 的混沌序列, 且将其所有的序列值转化为二进制形式, 再将位置置乱后的图像序列 L' 中的像素值进行二值化后交叉嵌入到这两个混沌序列中, 即完成像素比特替换过程, 最后将各自包含一半明文像素值信息的两个混沌序列进行异或操作得到加密密文.

Step 1: 设置两个初始值 x_2, x_3 , 设定一个 Logistic 混沌系统的系统参数 λ . 将 x_2, x_3 分别代入 Logistic 映射进行迭代舍去前 500 次, 继续迭代 $m \times n$ 次, 构成两个长度为 $m \times n$ 的混沌序列 $P' = \{p'_1, p'_2, \dots, p'_{m \times n}\}$ 和 $Q' = \{q'_1, q'_2, \dots, q'_{m \times n}\}$.

Step 2: 将混沌序列 P' 和 Q' 中的各序列值依次代入式(5)、(6) 中进行转化, 使其取值范围为 $[0, 255]$, 得到混沌图像序列 $P = \{p_1, p_2, \dots, p_{m \times n}\}$ 和 $Q = \{q_1, q_2, \dots, q_{m \times n}\}$.

$$P = \text{mod}(p'_i \times 10^8, 256), \quad 1 \leq i \leq m \times n \quad (5)$$

$$Q = \text{mod}(q'_i \times 10^8, 256), \quad 1 \leq i \leq m \times n \quad (6)$$

Step 3: 将以上所得的置乱图像序列 L' 和混沌图像序列 P, Q 中所有的值按照式(7) 转化成八位二进制形式来表示, 用 L' 中各序列值的二进制形式的第 1、3、5、7 位来替换 P 中该序列值二进制形式的第 1、3、5、7 位, 再用 L' 中像素点的二进制形式的第 2、4、6、8 位来替换 Q 中该序列值的二进制形式的第 2、4、6、8 位. 例如, 假设 L' 的第一个像素值二进制形式为 $l'_1 = 01110111$, 而 P 和 Q 中的第一个像素点二进制形式分别为 $p_1 = 01100110, q_1 = 11110000$, 替换后

p_1, q_1 将变为 $w_1 = 00100111, v_1 = 11110101$. 对图像序列 L' 中所有的序列值进行该操作得到中间密文 $W = \{w_1, w_2, w_3, \dots, w_{m \times n}\}$ 和 $V = \{v_1, v_2, v_3, \dots, v_{m \times n}\}$.

Step 4: 在上一步骤中, 通过比特值交叉替换操作把原图像的信息嵌入到了两个构造的混沌图像序列中, 让每个混沌图像序列都包含有一半的原图像信息, 这样就很好地隐藏了原图像的像素点信息. 再将 W 和 V 中所有序列值又按照公式转化为十进制数, 且按照行优先的顺序转化为两个大小为 $m \times n$ 的二维矩阵 W' 和 V' , 最后将 W' 和 V' 进行异或操作得到最终密文图像 C .

2.2.3 解密算法

解密过程其实就是加密过程的逆过程. 首先, 将加密密文 C 按照行优先顺序转化为一个一维图像序列且把所有序列值转化为八位二进制形式, 可得序列 C' , 再将 C' 分别与混沌图像序列 P, Q 进行异或操作可得到序列 K_1 和 K_2 , 值得注意的是, 该算法与其他算法中的异或操作进行解密不同, 所得的 K_1, K_2 并不和加密过程中的中间密钥 W, V 对等, 但是 K_1, K_2 各自分别携带明文图像一半的像素值信息. 然后, 将 K_1 中各序列值的第 2、4、6、8 位和 K_2 中各序列值的第 1、3、5、7 位提取出来进行整合即可得到图像序列 L' . 最后, 将 L' 进行反置乱即可得到明文序列 L , 再将一维明文序列 L 转化为二维矩阵即明文图像 A .

3 实验仿真及性能分析

3.1 算法仿真

本文仿真过程中选择的是经典的大小为 256×256 的 Lena 灰度图像作为明文, 实验过程中, 加密系统的初始密钥有 Kent 混沌系统中的 $x_1 = 0.314\ 159\ 265\ 0$ 和 Logistic 混沌系统中的 $x_2 = 0.454\ 647\ 4849, x_3 = 0.242\ 526\ 272\ 8$, 其中 Kent 混沌系统的控制参数 S 由图像本身决定, Logistic 混沌系统的控制参数设置为 $\mu = 3.954\ 567\ 432\ 1$, 实验可得如图 2 所示加密效果.

3.2 算法统计特性分析

本文算法统计特性分析主要从两个方面进行, 首先, 从加密前后的灰度直方图来观察. 如图 3 所示, 加密前明文图像的灰度直方图是不均匀, 可很好展示出图像像素值的分布特点, 而加密后密文图像的灰度直方图是均匀分布的, 这样就很好地隐藏了明文图像信息.

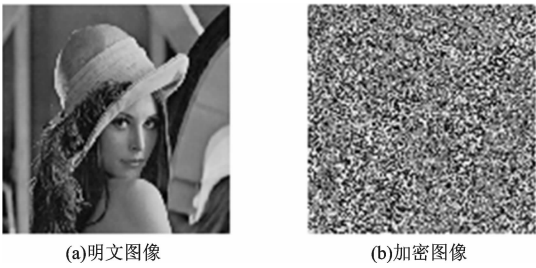
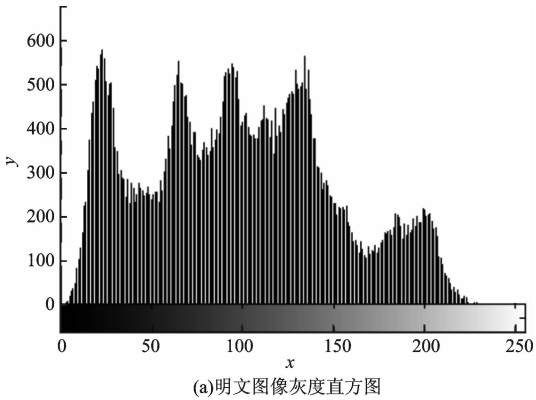
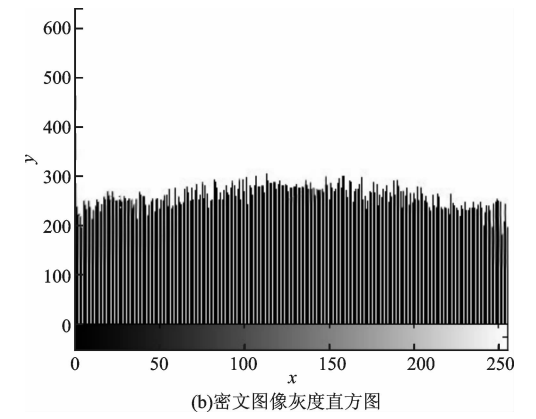


图 2 加密解密图



(a)明文图像灰度直方图



(b)密文图像灰度直方图

图 3 灰度直方图

然后,从加密前和加密后图像的相邻像素相关性来观察.在明文图像中任意选取一组相邻像素(水平、垂直或者对角的),通过以下公式来定量计算出它们的相关性:

$$\bar{x} = \frac{1}{N} \sum_{i=1}^N x_i \tag{7}$$

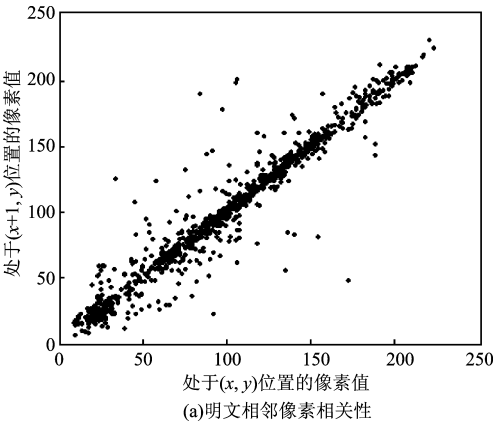
$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - \bar{x}) \tag{8}$$

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

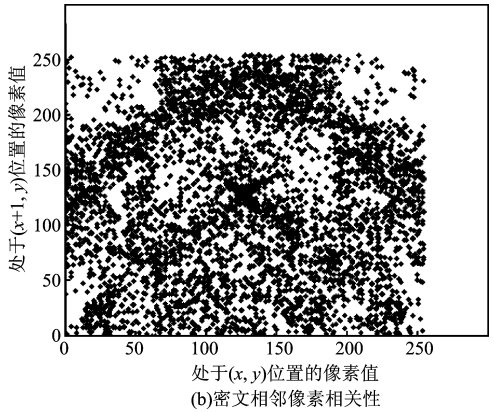
$$\gamma_{xy} = \frac{\text{Conv}(x,y)}{\sqrt{D(x)} \sqrt{D(y)}} \tag{10}$$

式中, x 和 y 分别表示的是图像中两个相邻像素的灰

度值, γ_{xy} 为两个相邻像素的相关系数.从明文图像和密文图像中随机抽取水平方向 500 组相邻点用来作出像素值关系图,图 4 中的两个图分别表明了明文图像水平相邻点的像素值关系和密文图像水平相邻点的像素值的关系,显然,加密后相邻点的像素值几乎没有任何关系了.



(a)明文相邻像素相关性



(b)密文相邻像素相关性

图 4 相邻像素相关性图

分别对图像的水平、垂直、和对角线方向选取所有点来计算它们各自的相关系数,并且与文献[14-16]所得到的结果进行对比,由表 1 可得,明文图像的相关系数接近 1,说明明文图像的相邻像素高度相关.而加密图像的相邻像素相关系数接近 0,说明密文图像的相邻元素基本没有关系了,即已达到很好的加密效果,使得密文具有良好的抗统计分析攻击能力.

表 1 密文图像像素相关系数

方向	原始图像	加密图像	文献[14]	文献[15]	文献[16]
水平	0.945 07	0.002 53	0.017 21	-0.032 41	0.254 61
垂直	0.962 71	-0.000 46	-0.031 76	0.007 75	-0.057 32
对角	0.937 24	0.017 53	-0.005 72	0.008 65	-0.002 45

3.3 抗差分攻击性能分析

对抗差分攻击性能的分析上,主要进行两个方面的分析:第一,对密钥敏感性分析;第二,对明文敏感性分析.

3.3.1 密钥敏感性分析

密钥敏感性指的是即使密钥发生微小的变化也会导致图像显著性变化.在对明文图像进行解密时,即使其中一个解密密钥发生微小的变化,最终都会得不到明文图像.在实验仿真中,正确解密时所得解密图像为图5(a),将 $x_1=0.314\ 159\ 265\ 0$ 改为 $x_1=0.314\ 159\ 265\ 1$,而其他都不变由可得如图6(b)所示的解密图像,将 x_2, x_3 也依次做该操作分别可得如图5(c)和图5(d)所示的解密图像.由此可见,即使是 10^{-10} 的微小改变也无法成功解密图像,所以该算法具有较好的密钥敏感性.

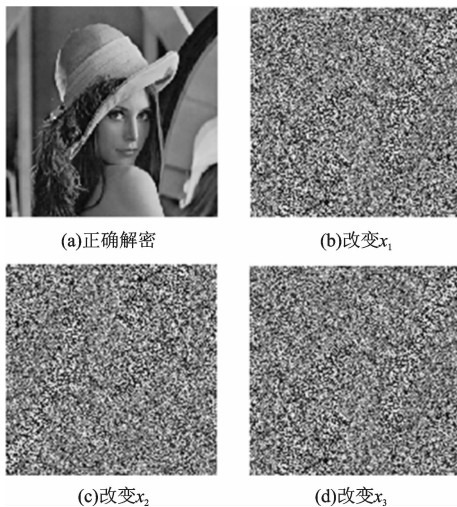


图5 正确解密和错误解密图

3.3.2 明文敏感性分析

明文敏感性指的是即使明文图像发生微小的变化也会导致密文图像发生显著改变,例如,任意把明文图像的某个像素点的像素值加1或者减1,都会造成最终截然不同的两个密文图像.而密文对明文的敏感性越强则说明该加密算法具有越好的抗差分攻击,因为攻击者就是通过对明文的微小改变来观测密文的变化特征从而推导出加密过程,从而破解算法.本文充分考虑到这一点,所以在加密过程中融合了明文像素值总和sum和行列数 m, n 等,使得加密过程与明文特性密切相关,而且在计算过程(式(3))对像素值总和有一个放大100倍的操作,即哪怕像素值仅改变1也会被放大到100,因此只要明文发生微小变化都会导致整个加密过程发生很大程

度的变化.一般采用像素值变化率(NPCR)和归一化平均变化强度(UACI)这两个参数来对密钥与明文雪崩效应进行描述.令两幅加密图像分别为 Q_1 和 Q_2 ,其中 Q_1 是明文图像加密后的密文,而 Q_2 为明文图像中某个像素点的像素值发生微小变化加密后的密文,位置 (i, j) 的像素值依次为 $Q_1(i, j)$ 和 $Q_2(i, j)$.定义二维矩阵 P 和 Q_1 大小相同,当 $Q_1(i, j) = Q_2(i, j)$ 时,令 $P(i, j) = 0$,否则 $P(i, j) = 1$,.则 Y_{NPCR} 和 Y_{UACI} 可定义如下:

$$Y_{NPCR} = \frac{\sum_i \sum_j P(i, j)}{M \times N} \times 100\% \quad (11)$$

$$Y_{UACI} = \frac{1}{M \times N} \left[\sum_i \sum_j \frac{|Q_1(i, j) - Q_2(i, j)|}{256} \right] \times 100\% \quad (12)$$

现从实验中所用到的明文图像中任取一点作相应微小改变,如位置为 $(3, 99)$ 的像素点,将其像素值由103改为104,然后根据式(8)、(9)可计算出 $Y_{NPCR} = 99.78\%$, $Y_{UACI} = 33.95\%$.由此可见,明文图像的微小变化会使得密文图像发生显著变化,所以该加密算法能够有效地抵抗差分攻击.

3.4 抗选择明文(密文)攻击分析

选择明文(密文)攻击是指攻击者可以选择一组特定的明文(密文),通过该加密系统来获取对应的密文(密文),然后通过该密文的特点来推导出中间密钥,最后可破解出明文图像.近年来,一些学者已通过选择明文和选择密文破解了基于“置乱-替代”这类结构的混沌图像加密算法^[6],他们通常采用的方法是选择一个与密文图像同样大小的且像素值全部为0的图像来破解出中间密钥,然后选取一个唯一表示像素点位置的图像来进行对该像素点的追踪,以而破解出该像素点在原图像中的位置,进而成功破解出明文图像.

而类似的破解方法在本文的加密算法中是不可行的.首先,因为本文一开始对明文图像进行全局置乱时,采用的混沌系统参数 S 和迭代次数 K 与明文图像的sum和avg紧密相连,而当明文像素值全为0时使得 $S = 0$,根本无法产生混沌序列,即不可能获得中间密文;其次,即使攻击者采用的非全为0的特殊明文攻击,由于本文加密算法的特殊性,它在进行像素比特值替换时同时使用了两个初始密钥 x_2 和 x_3 来产生两个混沌序列,之后又将明文图像的比特值交叉嵌入到这两个混沌序列中产生了两个中间密

文 C_1 和 C_2 , 以致于只要攻击者得不到精确的 x_2 和 x_3 , 几乎不可能得到中间密文 C_1 和 C_2 . 同理, 对于选择密文攻击也是同样的道理. 综上, 本文设计的图像加密算法能够很好地抵抗选择明文(密文)攻击.

3.5 密钥空间分析

一个好的加密算法必须有足够大的密钥空间, 本文所使用的初始密钥为 x_1 和 x_2, x_3 , 它们均在 $(0, 1)$ 范围内取值, 若是每个密钥均采用双精度型数据, 即可保留 15 或 16 位有效数字, 那么密钥空间至少为 10^{45} . 而本文算法中还有由明文特性决定的 Kent 混沌系统控制参数 S 和混沌序列初始迭代次数 K , 以及 Logistic 混沌系统中所用到的系统参数 λ 和其他迭代次数等, 如果将这些都算作密钥, 那么密钥空间会变得更大. 而如此大的密钥空间足够用来抵抗穷举攻击了, 也更好地保证加密算法的安全性.

4 结束语

混沌理论近年来已广泛应用于通信安全方面, 也取得了很多研究成果. 然而针对于一些在安全性上存在漏洞的一些混沌图像加密算法, 本文提出了一种全新的基于比特替换和置乱的加密算法. 该算法主要有两个方面的特点: 第一, 在加密过程中使密钥序列与明文图像的特性密切相关, 随着明文图像的改变, 加密过程中所用到的密钥序列也随之改变; 第二, 该算法加密过程将产生两组中间密文, 而且解密过程得出的两组中间密文与加密过程的加密密文是不对等的, 这样就大大提高了差分攻击的难度. 除此以外, 该算法采用一次加密运算, 没有进行反复迭代等运算来增加加密过程的复杂性, 加密算法简单可行且加解密速度快. 通过实验仿真证明, 本文算法不仅具有较好的加密效果, 而且具有较高的安全性.

参考文献:

- [1] Pareek N K, Patidar V, Sud K K. Image encryption using chaotic Logistic map [J]. Image and Vision Computing, 2006, 24(9): 926-934.
- [2] Guan Z H, Huan W J. Chaos based image encryption algorithm [J]. Physics Letters A, 2005, 364 (1-3): 153-157.
- [3] Pisarchik A N, Zanin M. Image encryption with Chaotically coupled chaotic maps [J]. Physics Letters, 2008, 237(20): 2638-2648.
- [4] 曹建秋, 肖华荣, 蓝章礼. 像素位置与像素值双重置换的混沌加密算法 [J]. 计算机工程与应用, 2010, 46

(28): 192-195.

- [5] Lu Ping, Dong Husheng, Ma Xiaohu. Image scrambling optimization algorithm based on mixed chaos system and bit decomposition [J]. Comput Eng Appl, 2011, 47(21): 191-194.
- [6] 彭飞, 丘水生, 龙敏. 外部密钥控制系统参数的图像加密算法 [J]. 华南理工大学学报: 自然科学版, 2005, 33(7): 20-23.
- [7] Liao Xiao-feng, Li Xue-ming, Chen Guan-rong, et al. A digital secure image communication scheme based on the chaotic chebyshev map [J]. International Journal of Communication Systems, 2004, 17(5): 437-445.
- [8] 张孔涛. Arnold 反变换的一种新算法 [J]. 软件学报, 2004, 15(10): 1558-1564.
- [9] Chen G R, Mao Y B, Charles K. A system image encryption scheme based on 3D chaotic cat maps [J]. Chaos, Solitons & Fractals, 2004, 21(3): 749-761.
- [10] Zhu Z L, Zhang W, Kwok-wo W. A chaos-based symmetric image encryption scheme using a bit-level permutation [J]. Information Sciences, 2011, 181(6): 1171-1186.
- [11] Zhang G J, Liu Q. A novel image encryption method based on total shuffling scheme [J]. Optics Communication, 2011, 284(12): 2775-2780.
- [12] Xiao D, Liao X F, Wei P C. Analysis and improvement of a chaos-based image encryption algorithm [J]. Chaos, Solitons and Fractals, 2009, 40(5): 2191-2199.
- [13] Zhu C X, Liao C L, Deng X H. Breaking and improving an image encryption scheme based on total shuffling scheme [J]. Nonlinear Dynamics, 2013, 71(1-2): 25-34.
- [14] Teng L, Wang X Y. A bit-level image encryption algorithm based on water wave motion and water drop diffusion models [J]. Optics Communications, 2012, 285 (20): 4048-4054.
- [15] Liao X F, Lai S Y, Zhou Q. A novel image encryption algorithm based on self-adaptive wave transmission [J]. Signal Processing, 2010, 90(9): 2714-2722.
- [16] Kanso A, Ghebelen M. A novel image encryption algorithm based on a 3D chaotic map [J]. Communications in Nonlinear Science and Numerical Simulation, 2012, 17(4): 2943-2959.

作者简介:

谢国波 男, (1977-), 博士, 教授. 研究方向为嵌入式系统、混沌保密通讯. Email: guoboxie@163.com

王 添 男, (1990-), 硕士研究生. 研究方向为嵌入式系统、混沌保密通讯.