对一种基于比特置乱的超混沌图像加密算法的选择明文攻击

朱淑芹[1] 王文宏[1] 孙忠贵[2]
(聊城大学计算机学院 聊城 252059)[1] (聊城大学数学与系统科学学院 聊城 252059)[2]

摘 要 最近,一种基于比特置乱的超混沌图像加密算法被提出,其核心思想为:首先,用混沌序列对明文图像进行像素置乱操作;然后,根据一个随机序列中相邻两个元素的大小关系对像素进行不同的比特位置乱;最后,把经过比特置乱后的序列与另一个混沌序列进行扩散、混淆运算得到最终的密文图像,从而使明文图像达到更好的加密效果。对该加密算法进行了安全性分析,发现该算法的安全性完全依赖于3个混沌序列,通过选择明文攻击依次破解出原算法中的3个混沌随机序列,恢复出了明文图像。理论分析和实验结果验证了所选择明文攻击策略的可行性,同时对该算法进行了改进,在改进算法中混沌系统的初始值与明文图像的SHA-256哈希值有关,从而使得密钥流与明文图像相关,因此算法可以抵抗选择明文的攻击。

关键词 超混沌图像加密,密码分析,比特位置乱,选择明文攻击,SHA-256哈希值
中图法分类号 TP391 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.11.041

Chosen Plaintext Attack on Image Encryption Algorithm Based on Bit Scrambling and Hyperchaos

ZHU Shu-qin[1] WANG Wen-hong[1] SUN Zhong-gui[2]
(School of Computer Science, Liaocheng University, Liaocheng 252059, China)[1]
(School of Mathematics and System Science, Liaocheng University, Liaocheng 252059, China)[2]

Abstract Recently, an image encryption algorithm based on bit scrambling and hyperchaos was proposed, whose main idea is as follows. First, a chaotic sequence is used to scramble pixel values of plaintext image. Then, according to the size of two adjacent elements in a random sequence, internal bit of each pixel is scrambled. In the end, the final ciphertext image is obtained by the diffusion and confusion of the scrambling sequence, and chaotic sequence, and plain image information can be well hidden. In this paper, the security of the above encryption algorithm were analyzed. It is found that the security of the algorithm depends entirely on three chaotic sequences by choosing plaintext attack. The three chaotic random sequences in the original algorithm were obtained, thus the plaintext image was restored. Theoretical analysis and experimental results verify the feasibility of the chosen plaintext attack strategy. At the same time, the improved method was given. In the improved algorithm, the initial value of the chaotic system is related to the SHA-256 hash value of the plaintext image, so that the key stream is related to the plaintext image. Then the algorithm is resistant to the attack of chosen plaintext.

Keywords Hyperchaotic image encryption, Cryptanalysis, Bit scrambling, Chosen plaintext attack, SHA-256 hash value

1 引言

图像加密是图像在空间域或变换域的一种变换。采用足够安全的算法得到的密文应充分且完全地随机,不能包含关于明文的任何信息。与文本数据不同的是,图像数据具有数据量大、冗余度高的特点,传统的加密算法不再适用于图像加密。而混沌对初始条件和系统参数的敏感性、遍历性和随机性等特性完美地与密码学的扩散和混淆两条基本原则相吻合,因此混沌被广泛地应用于图像加密领域。近年来,专家们提出了许多基于混沌的数字图像加密算法[1-10],其中大部分混沌图像加密算法都是基于置乱-扩散结构的[1-6],也有一些算法结合了传统密码和智能计算的思想来提高安全性[7-10]。

相应地,一些关于混沌图像加密算法安全性分析的工作同步开展[11-15]。Sharma等[11]对一种基于混沌的像素置乱和S盒变换的图像加密算法进行了安全性分析,在不知道密钥的前提下,利用选择明文攻击的方法恢复出待解密的明文图像。Zhu等[12]通过选择明文攻击结合选择密文攻击的方式破解了用于图像混淆和图像置乱的两个随机序列。朱淑芹等[13]详细分析了文献[16]的加密算法,发现该算法存在安全漏洞,通过选择明文攻击的方式恢复出了待解密的明文图像;

到稿日期:2017-04-16 返修日期:2017-06-29 本文受山东省自然科学基金(ZR2014FM032,ZR2017MEM019),聊城大学自然科学基金(318011606)资助。

朱淑芹(1979-),女,硕士,讲师,主要研究方向为混沌理论、信息安全、图像处理,E-mail:shuqinzhu2008@163.com;王文宏(1973-),男,博士,副教授,主要研究方向为图像处理、模式识别、机器视觉;孙忠贵(1971-),男,博士,副教授,主要研究方向为图像处理、模式识别。

另外，她还成功破解了对一种结合超混沌序列和移位密码的数字图像加密算法，并对原算法进行了改进，使改进算法可以抵抗选择明文的攻击[14]。文献[15]通过选择明文攻击的方法破解了 Fridrich[17] 的多轮置换-扩散结构算法，但是随着轮数的增加，破解难度也增大。以上加密算法被破解的主要原因在于加密过程中密钥流与待加密的图像无关，即加密不同的图像所用的混沌随机序列完全相同。事实上，密码分析和密码设计相互促进，是一对矛盾的统一体。密码分析可以促进加密算法设计水平不断提高。

最近，谢国波等[18]提出了一种基于比特置乱的超混沌图像加密算法。该算法的核心思想是：首先，利用随机序列对明文图像的像素进行位置置乱；然后，将置乱后的明文序列中的每个元素值转化为 8 位二进制形式，根据一个随机序列中相邻两个元素的大小关系对像素进行不同的比特位置乱；最后，将经过比特置乱后的 8 位二进制形式转换成十进制数，再将其与混沌序列进行扩散、混淆运算从而得到最终的密文图像。该算法具有设计新颖、算法复杂度小、抗统计分析、对初始条件敏感、抗噪声污染、抗剪切攻击的优点，但是无法抵御选择明文的攻击，本文将在第 2 节作详细的阐述。

2 原加密算法的描述

原算法在加密过程中采用的两个混沌系统分别为 Kent 映射和 Hyperhenon 映射。Kent 映射的映射关系为：

$$w_{n+1}=F(w_n)=\begin{cases}w_n/a, & w_n\in(0,a]\\(1-w_n)/(1-a), & w_n\in(a,1]\end{cases} \tag{1}$$

其中，a 为混沌系统的控制参数，当 $w_n\in(0,1)$，$a\in(0,1)$ 时，Kent 映射将处于混沌状态。

Hyperhenon 映射的映射关系为：

$$\begin{cases}x_{n+1}=c-y_{n+1}^2-d*z_{n+1}\\y_{n+1}=x_n\\z_{n+1}=y_n\end{cases} \tag{2}$$

当 $c=1.76$，$d=0.1$，且初始值 $x_0,y_0\in(0,1)$ 时，系统将进入混沌状态。

加密系统所用到的密钥集 $keys=\{x_0,y_0,w_0,c_0$，Kent 映射的参数 $a\}$，其中 x_0 和 y_0 是 Hyperhenon 映射的初始值，w_0 是 Kent 映射的初始值，c_0 是混淆阶段设定的一个值，$c_0\in[0,255]$。

2.1 图像像素位置的置乱

(1)设待加密的图像为 A，大小为 $m\times n$，将明文图像 A 转换成长度为 $m\times n$ 的一维序列 $L=\{l_1,l_2,l_3,\cdots,l_{m*n}\}$。设置 Kent 映射的初始值 w_0 和参数 $a=\mathrm{mod}(100*s,m*n)/(m*n)$，$t=m+n+\mathrm{mod}(avg\times10^8,m+n)$，其中，$s=sum(L)$ 表示图像 A 的所有像素值总和，$avg=s/(m*n)$ 表示明文图像的像素平均值。利用设定的初值 w_0 和参数 a 迭代 Kent 映射，舍去前 t 个数值以消除暂态效应带来的不良影响，从而生成一个长度为 $m\times n$ 的一维混沌序列 $K=\{k_1,k_2,k_3,\cdots,k_{m*n}\}$，因此生成的混沌序列 K 与 s 和 t 相关。

(2)对混沌序列 K 按从小到大的顺序进行排序，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 $T=\{t_1,t_2,t_3,\cdots,t_{m*n}\}$，用它对明文序列 L 进行位置置乱，得到置乱后的图像序列为 $L'=\{l_1',l_2',l_3',\cdots,l_{m*n}'\}$。

2.2 图像像素的比特置乱和扩散

(1)设置 Hyperhenon 映射的两个初值 x_0,y_0，迭代 Hyperhenon 映射得到长度为 $m\times n$ 的混沌序列 $P=\{p_1,p_2\ p_3,\cdots,p_{m*n}\}$，然后通过式(3)得到混沌图像序列 $Q=\{q_1,q_2,q_3,\cdots,q_{m*n}\}$。

$$q_i=\mathrm{mod}(p_i\times10^8,256),i=1,2,3,\cdots,m*n \tag{3}$$

(2)把置乱后的图像序列 L' 中的每个元素转化为 8 位二进制的形式，通过比较 P 中相邻两数的大小来对像素进行比特位置乱：若 $p_i>p_{i+1}$，则 l_i' 的 8 位二进制的 1,2,3,4 位依次与其 5,6,7,8 位对换；若 $p_i<p_i+1$，则 l_i' 的 8 位二进制的 1,3,5,7 位依次与其 2,4,6,8 位对换。当 $i=m*n$ 时，比较 p_{mn} 和 p_1 的大小。例如，$l_i'=10110110$，若 $p_1>p_2$，则对换后 $l_i'=10110110$；若 $p_1<p_2$，则对换后 $l_i'=01111001$。

(3)将比特置乱后的所有 l_i' 转成十进制数，得到序列 $C'=\{c_1',c_2',c_3',\cdots,c_{m*n}'\}$。利用序列 C' 和序列 Q 做如式(4)所示的混淆、扩散操作，得到密文序列 $C=\{c_1,c_2,\cdots,c_{mn}\}$，将其转化为矩阵即得密文图像。

$$c_i=\mathrm{mod}(q_i+c_i',256)\oplus c_{i-1},i=1,2,3,\cdots,m*n \tag{4}$$

其中，c_0 为[0,255]中的任意数，可作为一个密钥。

2.3 解密算法

解密过程是加密过程的逆过程，首先按式(5)解密出 c_i'。

$$c_i'=\mathrm{mod}(c_i\oplus c_{i-1}+256-q_i,256) \tag{5}$$

然后把 c_i' 转化为 8 位二进制形式，进行比特位的反置乱得到 l_i'，最后将 L' 进行像素反置乱即可得到明文序列 L。

3 原算法的安全性分析

从原算法的加密过程可以看出，整个加密算法的等效密钥就是 3 个混沌序列 T,P,Q。其中，混沌序列 T 用于图像像素空间位置的置乱；混沌序列 P 用于像素比特位的置乱；混沌序列 Q 用于像素值的扩散。序列 T 的生成与明文图像中所有像素的总和 s 有关，而 P 和 Q 的生成与明文图像或其对应的密文图像没有任何关系，即加密不同的明文图像所用的序列 P 和 Q 是不变的，这是破解原算法的关键。一般来说，如果一个加密系统加密不同的明文所用密钥不变，而且加密算法设计简单，没有密文扩散机制，那么可以采用选择明文攻击的方法来破解密钥序列。所谓选择明文攻击就是攻击者暂时获得加密系统的使用权，其能加密任意的明文，并获得相对应的密文，以此破译出全部或部分明文和密钥。因此，可以采用选择明文攻击的方法先破解 P 和 Q，从而恢复出明文图像置乱后的序列 L'。而序列 L' 的所有元素之和即为明文图像中所有像素的总和 s。再选择多幅像素值总和为 s 的明文图像进行选择明文攻击即可破解出序列 T。例如，用原算法选择加密一幅像素值全为 0 的图像，因为像素置乱和像素比特位的置乱对该幅图像都不起作用，在原算法的像素值扩散阶段式(4)转换成式(6)：

$$c_i=q_i\oplus c_{i-1},i=1,2,3,\cdots,m*n \tag{6}$$

从式(5)中很容易求解出混沌序列 Q；再用原算法加密一幅像素值全为 240 的图像，利用求解出的混沌序列 Q 即可恢

复出该图像扩散前的像素值,由于像素位置置乱对该幅图像无影响,因此这些像素值都取 240 或 15。根据像素取值是 240 或 15,可以破解出比特位置乱序列 P 的等效序列 S。利用求解出的混沌序列 Q 和 S 可以恢复待破解明文图像置乱后的序列 $L'=\{l_1',l_2',l_3',\cdots,l_{m*n}'\}$,由于置乱不改变像素值,从序列 L' 中可以计算出待破解明文图像的所有像素值之和 s,再用原算法加密多幅像素值之和为 s 的特殊图像,根据相应的密文分析出置乱序列 T。3 个混沌序列 T,P,Q 具体的攻击步骤将在第 4 节给出。

4　混沌序列的选择明文攻击

由第 3 节的分析可知,只要破解出 3 个混沌序列 T,P,Q 就能恢复出原明文图像,原加密算法即被攻破。

4.1　混沌序列 Q 的选择明文攻击

(1)采用原加密算法加密一幅与待解密图像同样大小的像素值全为 0 的图像 B,设得到的密文图像序列为 $BC=\{bc_1,bc_2,\cdots,bc_{mn}\}$。由于像素置乱和比特位置乱对图像 B 无影响,因此 B 经过像素置乱和比特位置乱后得到 $BC'=\{bc_1',bc_2',bc_3',\cdots,bc_{m*n}'\}=\{0,0,\cdots,0\}$。由扩散操作式(4)可得式(7):

$$\begin{aligned}bc_i&=\mathrm{mod}(q_i+bc_i',256)\oplus bc_{i-1}\\&=\mathrm{mod}(q_i+0,256)\oplus bc_{i-1}\\&=q_i\oplus bc_{i-1}\end{aligned}\tag{7}$$

由式(7)可得式(8):

$$q_1=bc_1\oplus c_0,q_i=bc_i\oplus bc_{i-1},i=2,3,\cdots,m*n\tag{8}$$

从而解密出混沌序列 Q。但是 c_0 未知,q_1 待定。

(2)采用原加密算法加密一幅与待解密图像同样大小的像素值全为 255 的图像 C,得到的密文图像序列为 $CC=\{cc_1,cc_2,\cdots,cc_{mn}\}$。同样,像素置乱和比特位置乱对图像 C 无影响,则 C 经过像素置乱和比特位置乱可得到 $CC'=\{cc_1',cc_2',\cdots,cc_{m*n}'\}=\{255,255,\cdots,255\}$,由扩散操作式(4)可得式(9):

$$\begin{aligned}cc_i&=\mathrm{mod}(q_i+cc_i',256)\oplus bc_{i-1}\\&=\mathrm{mod}(q_i+255,256)\oplus cc_{i-1}\end{aligned}\tag{9}$$

由式(8)和式(9)可得式(10):

$$cc_1=\mathrm{mod}(bc_1\oplus c_0+255,256)\oplus c_0\tag{10}$$

式(9)中,cc_1 和 bc_1 都是已知的,从而解出 c_0,继而得到 q_1。这样通过两幅选择明文图像攻击可以破解出混沌序列 Q 和 c_0。

为了更直观地说明密码分析方法的可行性和准确性,下面用一组简单的数值实验进行演示。

假设像素值全为 0 的明文图像序列为 $L=\{0,0,0,0,0,0,0,0,0,0\}$,经像素位置置乱和比特置乱后得到的 $L'=L$。像素值全为 255 的明文图像序列为 $LL=\{255,255,255,255,255,255,255,255,255,255\}$,经像素位置置乱和比特置乱后得到的 $LL'=LL$。

设原算法中选择的 $c_0=232$,混沌序列 $Q=\{112,23,45,98,124,235,245,21,156\}$,则加密 L 和 LL 后得到的密文分别为 C 和 CC。$C=\{152,143,162,192,188,87,162,183,43\}$,$CC=\{135,145,189,220,167,77,185,173,54\}$。

根据步骤(1)的分析,对序列 C 中相邻的两个元素分别作异或运算,得到一个长度为 8 的序列 $qq=\{23,45,98,124,235,245,21,156\}$,$qq$ 序列恰好是序列 Q 的后 8 个元素。此时,Q 中的第一个元素和 c_0 还未解出,但是可知 $Q(1)=bitxor(C(1),c_0)=bitxor(152,c_0)$。再由步骤(1)中的式(10)可得:

$$cc(1)=\mathrm{mod}(c(1)\oplus c_0+255,256)\oplus c_0$$

即 $135=\mathrm{mod}(152\oplus c_0+255,256)\oplus c_0$,可解出 $c_0=232$,从而得到 Q 中的第一个序列 $Q(1)=112$。至此,Q 序列被完全破解。

4.2　比特置乱序列 P 的选择明文攻击

原算法通过比较 P 中相邻两数的大小来对像素进行比特位置乱,因此对于序列 P,我们更关心 P 中相邻两数的大小关系。若 $p_i>p_{i+1}$,则 $s_i=1$;若 $p_i<p_{i+1}$,则 $s_i=0$;若 $p_{mn}>p_1$,则 $s_{mn}=1$;若 $p_{mn}<p_1$,则 $s_{mn}=0$。可得到序列 $S=\{s_1,s_2,\cdots,s_{mn}\}$。因此在比特置乱阶段的等效密钥由序列 P 转化为序列 S。比特置乱有改变像素值的作用,但是,如果比特置乱一些特殊的图像,置乱结果就有一定的规律:比如按原算法比特置乱一幅像素值全为 240 的图像,240 转化为二进制为 11110000,因此,置乱后像素值为 240 或者 15;如果按原算法比特置乱一幅像素值全为 170 的图像,170 转化为二进制为 10101010,因此置乱后像素值为 170 或者 85。根据置乱后的像素值的变化来破解序列 S。破解序列 S 的具体步骤如下。

(1)采用原加密算法加密一幅与待解密图像同样大小的像素值全为 240 的图像 D,设得到的密文图像序列 $DC=\{dc_1,dc_2,\cdots,dc_{mn}\}$。

(2)利用 4.1 节破解出的混沌序列 Q 和 c_0,根据式(5)可以恢复出图像 D 比特位置乱后的序列 $DC'=\{dc_1',dc_2',\cdots,dc_{m*n}'\}$。由于像素置乱过程对图像 D 无影响,$d_i=11110000$,经过比特置乱后 d_i 变为 dc_i',$dc_i'=11110000$ 或 $dc_i'=00001111$。即比特位置乱得到的序列 DC' 中的元素要么是 240,要么是 15。

(3)根据原算法比特位置乱规则,若 $dc_i'=15$,则 $p_i>p_{i+1}$,令 $s_i=1$;若 $dc_i'=240$,则 $p_i<p_{i+1}$,令 $s_i=0$,从而破解出序列 S。

下面用一组简单的数值实验演示序列 S 的破解。

假设像素值全为 240 的明文序列为 $D=\{240,240,240,240,240,240,240,240,240,240\}$,加密所用混沌序列 Q 与 4.1 节算例中所用的 Q 相同,混沌序列 $P=\{0.23456,0.54378,0.13455,0.94236,0.45782,0.75431,0.66432,0.35687,0.13568\}$,得到的密文序列为 $DC=\{136,174,179,194,174,84,80,116,248\}$,利用 4.1 节破解出的沌序列 Q 和 c_0,由式(5)可以恢复出图像 D 比特位置乱后的序列 $DC'=\{240,15,240,15,240,15,15,15,240\}$,从而得到序列 $S=\{0,1,0,1,0,1,1,1,0\}$,确定了混沌序列 P 中相邻元素的大小关系。

4.3　像素置乱序列 T 的破解

由 4.1 节、4.2 节破解出的混沌序列 Q 和 c_0 以及序列 S,可以恢复出待破解的明文图像的置乱后的图像序列 $L'=\{l_1',l_2',l_3',\cdots,l_{m*n}'\}$。由于置乱不改变像素值,序列 L' 的所有元素的和即为原明文图像的所有像素之和,因此在生成序

列 T 阶段所用到的参数 a 和 t 也因此确定，选择明文攻击时所选择的明文图像的所有像素值之和都等于恢复出来的待求明文图像置乱后的序列 L' 的所有元素的总和 s，这样置乱不同的图像时所用的置乱序列 T 不变。因此可以采用选择明文攻击的方法破解出置乱待求明文图像时所用的置乱序列 T。如何选择一幅像素值总和为定值 s 的图像是破解置乱序列 T 的关键。

可以按如下方法选择明文图像：设图像大小为 $m\times n$，连续的 253 个像素的像素值分别为 1,2,3,…,253，则其余的所有像素之和为 $s-253*254/2$，设 $\mathrm{mod}((s-253*254/2),254)=h$，连续的 h 个像素值取值 255，连续的 $(s-253*254/2-h*255)/254$ 个像素取为 254，其余的像素值全取为 0。这样即可保证所有的像素值之和等于已被破解出的 s 值。

举例来说，假设破解出的像素总和 $s=7780728$，图像大小为 $256*256=65536$，连续的 253 个像素的像素值分别取为 1,2,3,…,253，则其余的所有像素之和为 $7780728-253*254/2=7748597$，因为 $\mathrm{mod}(7748597,254)=73$，因此 $7748597-73$ 能被 254 整除，从而 $7748597-73*255=7748597-73-73*254$ 能被 254 整除，即 $7748597=30433*254+73*255$，因此在余下的 $65536-253=65283$ 个像素中，连续的 30433 个取值 254，连续的 73 个取值 255，剩下的像素全取为 0，这样每次可以破译出置乱序列 T 中的 253 个值。

具体思路为：若向量 L' 的像素数目 $z=mn$ 小于或等于 253，则只需选择一幅明文序列 $P=\{1,2,\cdots,mn\}$，并得到相应的置乱后的密文序列，借助明文-密文对破译出像素位置置乱序列 T。若向量 L' 的元素数目 mn 大于 253，则依次选择像素总数为 mn 的 $KL=\lceil mn/253\rceil$ 幅明文图像（这里 $\lceil x\rceil$ 表示取大于或等于 x 的最小整数），每次选择的明文图像序列的像素取值形式如图 1 所示。明文图像的选取方法为：将长度为 mn 的图像序列以 253 个连续像素为一组进行子块划分，最后一个子块可能不足 253 个像素；每一幅选择明文图像中仅有一个子块的像素取值为[1,253]范围内互不相同的整数，其余子块的像素均为 254,255 或 0，这样即可得到 $KL=\lceil mn/253\rceil$ 幅明文图像。

The first chosen plaintext

i=1	2	…	253	254	…	…	…	z-1	z
1	2	…	253	0	…	255	…	254	254

The second chosen plaintext

i=1	…	254	255	…	506	507	…	z-1	z
254	…	1	2	…	253	0	…	255	255

…

The KL chosen plaintext(namely the last one)

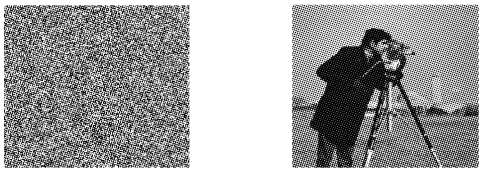
i=1	…	$z-k$-1	…	z
0 … 254 … 255 … 1 2 … k				

图 1 破解置乱的等效密钥流 T 所选择的多幅明文图像序列

由图 1 可以看出，利用每一幅选择的明文图像和得到的对应置乱后的密文图像，每次可以破译出置乱序列 T 中的 253 个值。利用 T 把恢复出来的序列 L' 还原为序列 L，即得明文图像。

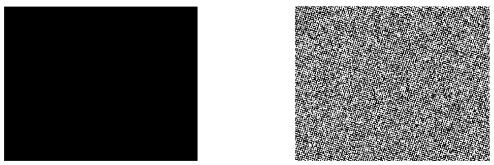
4.4 密文破译仿真实验

仿真实验采用 Matlab2014a 平台，选用大小为 256×256 的 256 级灰度图像 cameraman，取 Kent 映射的初始值 $w_0=0.4234678$，取 Hyperhenon 映射的两个初始值 $x_0=0.457893581$，$y_0=0.784598771$，得到对应的密文图像如图 2(a)所示。各参数不变，采用原算法分别加密大小为 256×256 的像素值全为 0 的、像素值全为 255 的以及像素值全为 240 的 3 幅图像，得到对应的密文图像分别如图 3(b)、图 4(b)、图 5(b)所示。利用图 3(b)、图 4(b)可以在不知道密钥 w_0,x_0,y_0 的情况下恢复出扩散阶段所用序列 Q 及 c_0，利用恢复出来的序列 Q 及 c_0 对图 5(b)进行反扩散操作即可得图 6，再利用图 6 即可恢复出用于比特置乱的序列 S，用 Q,c_0 及 S 可以恢复出待解密的明文图像，根据序列 T 置乱后的图像，将其按行优先的顺序转化为一维序列可得到序列 L'，计算 L' 的所有像素的总和得到 s 的值，从而得到 avg 的值。最后通过多幅选择明文图像攻击的方法恢复出置乱序列 T，在不知道密钥 w_0,x_0,y_0 的情况下恢复出明文图像，如图 2(b)所示。



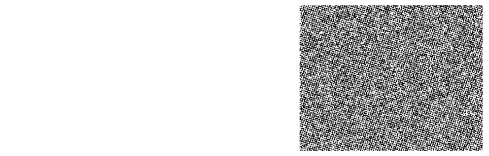
(a)密文图像 (b)解密后的明文图像

图 2



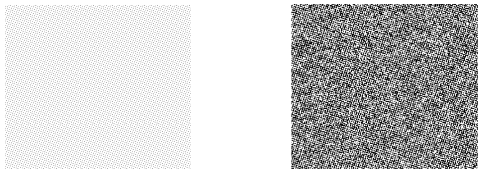
(a)像素值为 0 的全黑图像 (b)全黑图像的密文图像

图 3



(a)像素值为 255 的全白图像 (b)全白图像的密文图像

图 4



(a)像素值为 240 的图像 (b)图(a)的密文图像

图 5

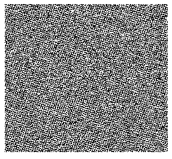


图 6 恢复出来的图 5(a)比特位置乱后的图像

5 改进算法及其安全性分析

5.1 改进算法

哈希算法可以认为是一种压缩算法，它将任意长度的二

进制值映射为固定长度的较小二进制值，称这个小的二进制值为哈希值。一段明文即使只更改该段落的一个字母，随后的哈希算法都将产生不同的哈希值。要找到散列为同一个值的两个不同的输入，在计算方面而言基本上是不可能的，因此哈希值可以作为图像的一种唯一性判别。SHA-256 就是一种哈希算法，哈希值大小为 256 位。

原算法被破解的主要原因在于在加密过程中用到的混沌序列与明文图像无关。在改进算法中使混沌系统的初始值与图像的 SHA-256 哈希值相关，这样混沌系统产生的混沌序列与明文相关。改进算法的具体步骤如下。

(1)混沌系统初始值的生成。

将明文图像的 SHA-256 哈希值 H 以 8 位为一组分成 32 组，因此 H 可以表示为 $H=h_1,h_2,h_3,\cdots,h_{32}$（$h_i$ 为由 0 和 1 组成的 8 位二进制位），则在图像像素位置置乱阶段所用到的 Kent 映射的初值如式(11)所示：

$$w_0=\mathrm{mod}(w_0'+\frac{h_1\oplus h_2\oplus h_3\oplus h_4\oplus h_5\oplus h_6\oplus h_7\oplus h_8}{256},1) \tag{11}$$

Hyperhenon 映射的初始值 x_0 和 y_0 分别如式(12)、式(13)所示：

$$x_0=\mathrm{mod}(x_0'+\frac{h_9\oplus h_{10}\oplus h_{11}\oplus h_{12}\oplus h_{13}\oplus h_{14}\oplus h_{15}\oplus h_{16}}{256},1) \tag{12}$$

$$y_0=\mathrm{mod}(y_0'+\frac{h_{17}\oplus h_{18}\oplus h_{19}\oplus h_{20}\oplus h_{21}\oplus h_{22}\oplus h_{23}\oplus h_{24}}{256},1) \tag{13}$$

混淆阶段设定的一个值 c_0（$c_0\in[0,255]$）如式(14)所示：

$$c_0=h_{25}\oplus h_{26}\oplus h_{27}\oplus h_{28}\oplus h_{29}\oplus h_{30}\oplus h_{31}\oplus h_{32} \tag{14}$$

其中，x_0'，y_0'，w_0'是给定的初始值。这样加密系统的密钥集为 $keys=\{x_0',y_0',w_0'$，Kent 映射的参数 a，图像的 SHA-256 哈希值$\}$。

(2)设置好混沌系统的初值，按照原算法生成混沌序列，然后再对图像进行加密，具体加密过程与文献[18]的算法一致，这里不再赘述。

5.2　改进算法的安全性分析

文献[18]对原算法的安全性进行了全面的分析，原算法具有密文分布均匀，相邻像素相关性很小，密文对密钥和明文敏感，密钥空间大等优点。改进算法与原算法的区别在于：改进算法设置的混沌系统的初值与待加密的明文图像的 SHA-256 哈希值有关。加密算法与原算法完全一样，故改进算法也具有原算法的上述优点。与原算法相比，改进算法还具有以下优点。

(1)抵抗选择明文的攻击。

由于混沌系统的初值与待加密图像的哈希值有关，加密不同的图像所用的混沌序列不同，达到了“一次一密”的效果，攻击者不能利用特殊的明文图像的密文图像来获得加密原明文图像所需的混沌序列。因此，改进算法能抵抗选择明文的攻击。

(2)与原算法相比，改进算法对明文更敏感。

原算法对明文敏感的主要原因在于设置 Kent 映射的参数与待加密图像的所有像素值总和 s 有关，即 $a=\mathrm{mod}(100*s,m*n)/(m*n)$。这样明文像素值改变时，图像的所有像素值总和 s 改变，Kent 映射生成的置乱序列 T 就不同，而 Hyperhenon 映射生成的序列 P,Q 不变。如果改变多个像素的值，有可能使得图像的所有像素值总和 s 不变，这样置乱序列 T 就不变，原算法对明文的敏感性就会变差。但是，改进算法设置的两个混沌系统的初值与待加密图像的哈希值有关，若明文图像的一个像素值发生变化，则产生的哈希值与原来的差别将很大，因此生成的 3 个混沌序列 T,P,Q 也会发生很大变化，改进算法对明文也会更敏感。

下面比较当明文图像有两个像素值发生改变且图像的像素总和不变时，原算法与改进算法对明文敏感性的高低。

使用像素数改变率 *NPCR* 和归一化平均改变强度 *UACI* 来度量加密算法对明文的敏感程度。对于 8 位灰度图像而言，*NPCR* 与 *UACI* 的理想期望值分别为 99.6094% 和 33.4635%。*NPCR* 与 *UACI* 的计算公式[19]分别如式(15)和式(16)所示：

$$NPCR=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}D_{ij}}{M\times N}\times 100\% \tag{15}$$

$$UACI=\frac{(\sum_{i=1}^{M}\sum_{j=1}^{N}(\frac{c_1(i,j)-c_2(i,j)}{255}))}{M\times N}\times 100\% \tag{16}$$

当两个明文图像仅存在两个像素不同时，假设它们的密文图像中第(i,j)点的像素值分别为 $C_1(i,j)$和 $C_2(i,j)$，则定义 $D(i,j)$如式(17)所示：

$$D(i,j)=\begin{cases}0, & \text{if } C_1(i,j)=C_2(i,j)\\ 1, & \text{if } C_1(i,j)\neq C_2(i,j)\end{cases} \tag{17}$$

本文随机选取原图像中的 5 对像素点改变其像素值，计算的 *NPCR* 和 *UACI* 如表 1 所列。

表 1　改进算法与原算法明文图像微小改变但像素总和不变的 *NPCR* 和 *UACI* 测试比较结果/%

明文的两个像素微小改变，像素总和不变	本文算法		文献[18]算法	
	NPCR	*UACI*	*NPCR*	*UACI*
G(138,95)由 210 变为 211，G(98,195)由 219 变为 218	99.5497	33.6532	99.5318	33.2789
G(112,157)由 234 变为 235，G(12,17)由 156 变为 155	99.6858	33.4987	89.5856	31.8756
G(235,145)由 119 变为 120，G(35,245)由 229 变为 228	99.8933	33.5986	39.8965	33.7856
G(205,215)由 129 变为 130，G(96,77)由 229 变为 228	99.5876	33.4389	90.5891	23.3573
G(25,21)由 29 变为 30，G(196,47)由 229 变为 228	99.6876	33.2356	96.5658	33.2341

由表 1 可以看出，当明文图像有两个像素值发生改变且图像的像素总和不变时，改进算法比原算法对明文的变化更敏感。

5.3 改进算法的时间复杂度的理论分析

改进算法与原算法相比只是在设置混沌系统的初值时，将明文图像的哈希值分为 32 段并分别进行异或运算，其他加密过程与原算法相同。而异或运算是计算机最简单的一种运算，时间复杂度可以忽略。因此改进算法与原算法的时间复杂度一样，但改进算法的安全性大大提高。

结束语 本文对一种基于比特置乱的超混沌图像加密算法进行了安全性分析，发现该算法存在安全漏洞，不能抵抗选择明文的攻击，通过选择明文攻击依次破解出原算法的等效密钥，即 3 个混沌序列 T,P,Q，并给出了简单的算例。仿真实验验证了攻击方法的有效性。针对原算法不能抵抗选择明文攻击的缺陷，对加密算法做了改进：设计混沌系统的初始值与明文图像的 SHA-256 哈希值有关，众所周知，明文的微小变化都会使其哈希值发生很大的变化，从而混沌系统产生的混沌序列完全不同，这样加密不同的明文所用的密钥流不同，达到了“一次一密”的效果，因此改进算法能抵抗选择明文的攻击，而且改进算法比原算法对明文更敏感。

参 考 文 献

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

[2] WU X,LI Y,KURTHS J. A new color image encryption scheme using CML and a fractional-order chaotic system[J]. Plos One, 2015,10(3):119660-119687.

[3] WANG X,LIU C,XU D,et al. Image encryption scheme using chaos and simulated annealing algorithm[J]. Nonlinear Dynamics,2016,84(3):1-13.

[4] WANG X,XU D. A novel image encryption scheme based on Brownian motion and PWLCM chaotic system[J]. Nonlinear Dynamics,2014,75(1-2):345-353.

[5] WEN C C,WANG Q,HUANG F M,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.

[6] LIU Q,LI P Y,ZHANG M C,et al. Image encryption algorithm based on chaos system having markov portion[J]. Journal of Electronics & Information Technology, 2014, 36(6): 1271-1277. (in Chinese)
刘泉，李佩玥，章明朝，等. 基于可 Markov 分割混沌系统的图像加密算法[J]. 电子与信息学报，2014,36(6):1271-1277.

[7] JAWAD A, SEONG O H. A secure image encryption scheme based on chaotic maps and affine transformation[J]. Multimedia Tools and Applications,2016,75(21):13951-13976.

[8] RITESH B,SHAILENDER G,GAURAV S. An innovative image encryption scheme based on chaotic map and Vigenère scheme[J]. Multimedia Tools and Applications, 2016, 76(15): 16529-16562.

[9] WANG X, LIU C, XU D, et al. Image encryption scheme using chaos and simulated annealing algorithm[J]. Nonlinear Dynamics,2016,84(3):1417-1429.

[10] WANG X, ZHANG H. A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems[J]. Nonlinear Dynamics,2016,83(1):333-346.

[11] SHARMA P K, AHMAD M, KHAN P M. Cryptanalysis of image encryption algorithm based on pixel shuffling and chaotic S-box transformation[M]//Security in Computing and Communications, Berlin: Springer, 2014: 173-181.

[12] ZHU C, LIAO C, DENG X. Breaking and improving an image encryption scheme based on total shuffling scheme[J]. Nonlinear Dynamics,2013,71(1/2):25-34.

[13] ZHU S Q, LI J Q, WANG W H. Security analysis of improved image encryption method based on DNA coding and chaotic map [J]. Computer Application Research, 2017, 34(10): 3090-3093. (in Chinese)
朱淑芹，李俊青，王文宏. 对改进的基于 DNA 编码和混沌的图像加密算法的安全性分析[J]. 计算机应用研究，2017,34(10):3090-3093.

[14] ZHU S Q, LI J Q. Chosen plain text attack and improvements of a chaos image encryption algorithm[OL]. http://www.cnki.net/kcms/detail/11.2127.TP.20161221.0841.016.html. (in Chinese)
朱淑芹，李俊青. 一种混沌图像加密算法的选择明文攻击和改进[OL]. http://www.cnki.net/kcms/detail/11.2127.TP.20161221.0841.016.html.

[15] SOLAK E, COKAL C, YILDIZ O, et al. Cryptanalysis of Fridrich's chaotic image encryption[J]. International Journal of Bifurcation and Chaos, 2010, 20(5): 1405-1413.

[16] WEI G Z, JIN X, ZHAO G, et al. Improved image encryption method based on DNA encoding and chaotic mapping[J]. Application Research of Computers, 2015, 10(32): 3049-3051. (in Chinese)
魏广政，金鑫，赵耿，等. 一种改进的基于 DNA 编码和混沌映射的图像加密方法[J]. 计算机应用研究，2015,10(32):3049-3051.

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

[18] XIE G B, WANG T. A novel hyperchaotic image encryption algorithm based on bit scrambling[J]. Microelectronics and Computer,2016,33(7):28-32,38. (in Chinese)
谢国波，王添. 一种基于比特置乱的超混沌图像加密算法[J]. 微电子学与计算机，2016,33(7):28-32,38.

[19] RHOUMA R, BELGHITH S. Cryptanalysis of a new image encryption algorithm based on hyper-chaos [J]. Physics Letters A,2008,372(38):5973-5978.