替代和置乱相结合的图像分块加密算法

Image Block Encryption Algorithm Based on Substitution and Scrambling

李　娟

（内蒙古化工职业学院计算机与信息工程系，内蒙古 呼和浩特　010070）

摘　要：为增强数字图像的安全性，提出了一种基于替代和置乱的图像分块加密算法。首先将原图像分块，并对每个图像块内像素点执行按位替代操作；然后利用均匀分块置乱算法，将各个图像块内像素完全扩散到其他图像块中；接着利用 Fibonacci 算法对每个图像块进行像素值置乱；最后采用 Fibonacci 算法对整幅图像做像素位置置乱，以消除图像的空间相关性。试验结果表明，该算法可以有效地对图像进行加密解密，可有效抵抗不同程度的剪切和噪声攻击，且实时性较好。

关键词：图像安全　图像加密　置乱　Fibonacci 变换　均匀分块

中图分类号：TP311　　**文献标志码**：A

Abstract: To strengthen the security of digital images, the image block encryption algorithm based on substitution and scrambling is proposed. Firstly, the original image is divided into sub-blocks, and bitwise substitute operation is executed for each pixel in image block; then by adopting uniform sub-block scrambling algorithm, each pixel in image block is fully diffused to other image blocks, and pixel value is scrambled for each image block by using Fibonacci algorithm; finally, pixel position scrambling is conducted for the whole image using Fibonacci algorithm to eliminate spatial correlation of the image. The experimental results indicate that this algorithm can effectively doing encryption and decryption for images, it is able to effectively resist attacks of shears and noises, and offers better real time performance.

Keywords: Image security　Image encryption　Scrambling　Fibonacci transform　Uniform sub-block

0　引言

当图像在网络上传输时，对图像内容的有效加密和保护非常重要，保证信息的安全传输成为近年来学者研究的热点[1]。图像加密领域以图像置乱为主，可分成三类：像素位置变换方法[2-3]、像素值变换方法[4-5]以及两种方法相结合[6-11]的方法。

近年来，国内外学者提出众多加密方案。Fridich 等人[12]提出一种基于二维标准 baker 映射的对称块加密技术；丁玮等人[13]提出按空间填充曲线、Arnold 变换、幻方的图像置乱（置换）变换；文献[14]提出基于骑士巡游变换的图像置乱方法，实现了图像细节的隐藏；南艳红等人[15]探讨 Fibonacci 变换的置乱效果及其在数字图像水印中的应用[16]，给出了一种描述数字图像置乱程度的定义，并比较 Arnold 变换和 Fibonacci 变换的置乱效果；邹建成等人[17]研究了 Fibonacci 变换在图像加密中的应用，取得了较好的加密效果；N. K. Pareek 等人[18]结合两个 Logistic 混沌映射实现图像加密；Mazloom 等人[19]基于非线性耦合混沌映射（CNCM）实现图像加密，通过对密钥做代数变换，有效地增强了加密系统的安全性；Sesha[10] 和 Vinod[20] 将三维矩阵转换成为二维矩阵，顺序执行行列置换、行列替代、行列置换完成彩色图像加密；Pareek[21] 利用像素替换和像素置换的方法，采用反馈机制增强系统鲁棒性。

本文基于二维 Fibonacci 变换和均匀分块的思想，提出了一种新的替代和置乱相结合的数字图像分块加密算法。该算法具有一定的抗剪切、抗噪声攻击的能力，而且实时性较好，可有效地对图像进行加密与解密。

1　图像置乱效果评价

图像置乱可以达到图像加密的目的，其目的是降低图像相邻像素相关性，使图像像素由确定性变为不确定性的过程，也就是使图像信息量增加的过程。用熵值来衡量置乱的效果，下面首先给出图像位置熵的定义：

$$H(R)=\sum_{k=1}^{B}H_k(P) \tag{1}$$

式中：B 为图像分块区域个数；$H_k(P)$ 为第 k 个分块区域的信息熵。

$$H_k(P)=\sum_{ij}P(i,j)\lg\frac{1}{P(i,j)} \tag{2}$$

式中：$P(i,j)$ 为原始图像坐标为 (i,j) 的像素出现在置

内蒙古化工职业学院基金资助项目（编号：ZJY0708C、KY200903）。

修改稿收到日期：2013-05-22。

作者李娟（1980-），女，2010 年毕业于内蒙古工业大学计算机技术专业，获硕士学位，讲师；主要从事网络技术、信息安全、图像加解密等方向的研究。

乱后图像的第 k 个图像块的概率。当 $P(i,j)$ 等概率时,熵函数 $H_k(P)$ 和位置熵 $H(R)$ 最大。最佳的置乱状态是置乱后的图像中任意块内的像素点来自原始图像各个位置的概率相同,此时置乱后图像信源的平均信息量最大,熵值越接近于 8,置乱效果越好。

均匀置乱是最好的置乱方法,它首先假设原始图像被分割成 $n\times n$ 块,每块含有 $n\times n$ 个点,且这些点分别出现在置乱后图像的 $n\times n$ 个图像块中。

2　本文加密算法

先将图像做分块处理,正方块在图像加密的研究中具有代表意义。假设图像的尺寸为 $M\times N$,以 $f(i,j)$ $(1\leqslant i\leqslant M,1\leqslant j\leqslant N)$ 为中心的 $m\times n(0\leqslant m\leqslant M,0\leqslant n\leqslant N)$ 个相邻像素组成的邻域,称为图像块,且约束条件如下:①图像行列数为 2 的指数;②每个图像块的行列数相等。对 16×16 的图像均匀分块,将该图像分成 8×8 块,每块含有 2×2 个像素点,其示意图如图 1 所示。

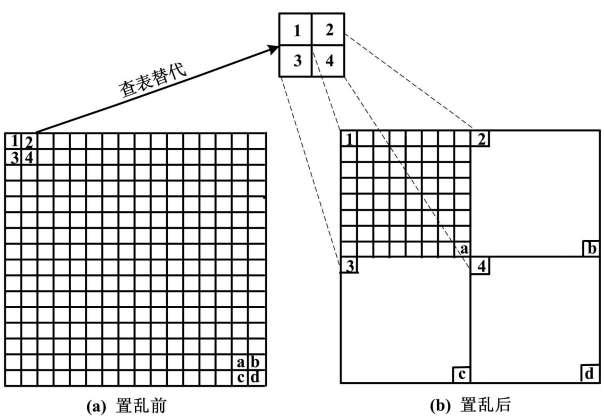

图 1　图像块内像素值替代和均匀分块示意图

Fig. 1　Pixel substitution in image block and uniform block dividing

加密算法具体步骤如下。

① 将图像分成 8×8 块(记作 $P_1,P_2,\cdots,P_{64}$),每块含有 2×2 个像素点(记作 p_1,p_2,p_3,p_4),假设图像灰度级是 256,即 8 位($b_1b_2\cdots b_8$)二进制构成每个像素点,根据前一像素点 p_{i-1} 的三个最重要位($b_1b_2b_3$)的值和如表 1 所示的该位值的操作,修改 p_i 的像素值。例如,首先取出 P_1 块,p_1 和 p_2 的像素值分别是 201(11001001)和 185(10111001)。像素点 p_1 相应的位值 6(110)进行查表,对 p_2 的像素值循环左移一位后取反,由新像素值 141(10001101)替代 185(10111001)。根据 p_2 新像素值修改 p_3 的像素值,同理修改 p_4 的像素值,并根据该值修改 p_1 的像素值。按照以上规律,依次完成块 $P_1,P_2,\cdots,P_{64}$ 的替代操作。

表 1　位值和相应的操作

Tab. 1　Bit value and appropriate operation

位值	加密像素点采用的运算
0	循环左移一位,即 $p_i=p_i<<1$
1	循环右移一位,即 $p_i=p_i>>1$
2	对所有位取反,即 $p_i=\mathrm{Not}(p_i)$
3	奇数位取反
4	偶数为取反
5	$p_i=p_i\oplus p_{i-1}$
6	p_i 循环左移一位后取反
7	p_i 循环右移一位后取反

② 对步骤①得到的图像块进行如下操作:根据前一像素点 p_{i-1} 的两个最重要位(b_1b_2)的值和表 1 对应该位值的操作,修改 p_i 的像素值。例如,p_3 和 p_4 的像素值分别是 140(10001100)和 186(10111010),则对 p_4 应用 p_3 相应的位值 2(10)进行运算,采用新值 69(01000101)替代 p_4 的原像素值。按照以上规律,依次实现块 $P_1,P_2,\cdots,P_{64}$ 的替代操作。

③ 对步骤②得到的图像块进行如下操作:根据前一像素点 p_{i-1} 的最重要位(b_1)的值和表 1 对应该位值的操作,修改 p_i 的像素值。例如,p_2 和 p_3 的像素值分别是 235(11101011)和 153(10011001),则 p_3 的像素值应用 p_2 相应的位值 1(1)进行运算后变成 76(01001100)。按照以上规律,依次对块 $P_1,P_2,\cdots,P_{64}$ 完成替代操作。

④ 完成上述步骤后,采用均匀分块算法将每个图像块内的所有像素充分扩散到其他图像块中。如图 1 所示,实现原始图像各块中像素点间的距离由“最近”到“最远”,保证该块中所有像素点被分到置乱后图像的不同块中,满足条件 $S\geqslant P$;实现原始图像各块中像素点间的距离由“最远”到“最近”,按照规定的次序,在原始图像所有块中各取一点,同时分到置乱后图像的同一块中,满足条件 $S\geqslant p$。因为 $s\geqslant P$、$S\geqslant p$,则 $sS\geqslant PS\geqslant pP$,已知 $sS=pP$,那么 $s=P$、$p=S$。置乱后图像分成 2×2($S\times S$)块,每块含有 8×8($s\times s$)个点。

⑤ 分别对置乱后的每个图像块做 Fibonacci 像素值置乱,h 表示任意像素值横纵坐标的十六进制,分别取出每个像素高 4 位和低 4 位作为 Fibonacci 变换的输入,Fibonacci 像素值置乱表示形式如下:

$$\begin{bmatrix}\boldsymbol{h}'_1\\ \boldsymbol{h}'_2\end{bmatrix}=\boldsymbol{F}^n\boldsymbol{h}=\begin{bmatrix}1&1\\1&0\end{bmatrix}^n\times\begin{bmatrix}\boldsymbol{h}_1\\ \boldsymbol{h}_2\end{bmatrix}(\mathrm{mod}16)\qquad(3)$$

式中:$\boldsymbol{h}=[h_1,h_2]^{\mathrm{H}}$;$\boldsymbol{h}_i,\boldsymbol{h}'_i\in\{1,2,\cdots,15\}$,$i=1$、$2$,$\boldsymbol{h}'=(h'_1,h'_2)^{\mathrm{H}}$ 是对每个像素值 h 置乱 n 次后对应的像素值。

⑥ 对整幅图像做位置变换,将置乱后的整幅图像

作为 Fibonacci 位置变换的输入,利用以下公式进行变换。图像像素的位置矩阵表示为 $\boldsymbol{p}=[x,y]^H$,则对图像做 n 次 Fibonacci 位置变换表达式为:

$$\begin{bmatrix}x'\\y'\end{bmatrix}=\boldsymbol{F}^n\boldsymbol{p}=\begin{bmatrix}1&1\\1&0\end{bmatrix}^n\times\begin{bmatrix}x\\y\end{bmatrix}(\mathrm{mod}N) \tag{4}$$

式中:$x,y,x',y'\in\{0,1,\cdots,N-1\}$;整数 $N\geqslant 2$ 为数字图像矩阵的阶数;(x,y) 和 (x',y') 分别为原图像和变换后图像像素的行位置和列位置坐标。

图像加密流程如图 2 所示。

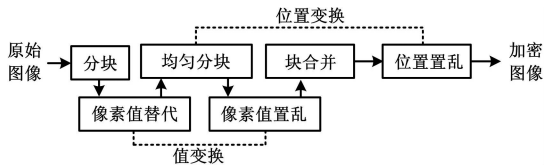

图 2　图像加密流程图

Fig. 2　Image encryption process

3　试验效果与分析

3.1　置乱效果比较

从美国南加州大学 USI-SIPI image database 和美国麻省 media 实验室图像库中选择实验图像。通过对大量图像进行试验分析,均得到了一致的结果。本试验选择典型的 Lena 图像,文献[22]和本文算法的分块示意图如图 3 所示。

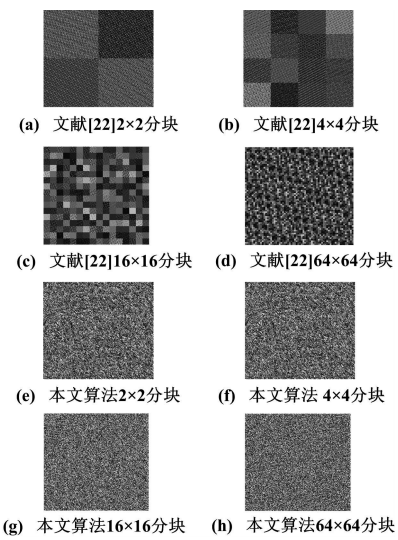

图 3　图像分块示意图

Fig. 3　Diagram of image sub-block

图 3(a) ~ 图 3(d)所示为采用文献[22]提出的高效率分块图像置乱算法得到的分块示意图,该算法分两步进行:首先对图像分块;然后对图像块进行 Arnold 变换。图 3(e) ~ 图 3(h)为采用本文算法由不同分块数目获得的加密效果。加密图像所对应的灰度直方图如图 4 所示。直观上看本文算法置乱效果更均匀,既改变了图像的纹理信息又改变了统计信息,达到了混乱和扩散的效果,加密图像的直方图的均匀分布也说明了这一点。

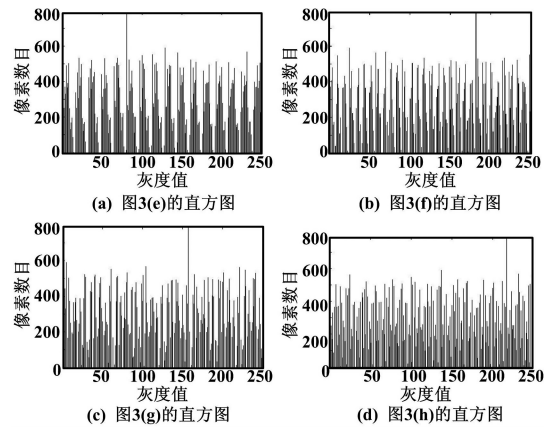

图 4　加密图像灰度直方图

Fig. 4　Contrast of scrambling effects

从直观上比较两种算法的置乱效果欠缺说服力,本文引入置乱度(SM)来衡量图像的置乱性能,它能较好地反映图像的置乱程度[23]。SM 的计算式为:

$$SM(X,\tilde{X})=\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(x_{ij}-\tilde{x}_{ij})^2}{\sum_{i=1}^{m}\sum_{j=1}^{n}(x_{ij}-r_{ij})^2} \tag{5}$$

式中:$X=\{x_{ij}\}_{m\times n}$为原始图像;$\tilde{X}=\{\tilde{x}_{ij}\}_{m\times n}$为加密图像。

为了衡量图像分块数对本算法的影响,分别采用不同的分块数对原始图像进行加密,试验结果如表 2 所示。

表 2　分块数对置乱度的影响

Tab. 2　The number of sub-blocks versus scrambling degree

分块数目	置乱度	
	文献[22]	本文方法
2×2	0.608 2	0.826 0
4×4	0.689 3	0.839 9
16×16	0.862 8	0.926 0
64×64	0.880 3	0.974 4

从表 2 可以看出,两种算法的置乱度随分块数的增加呈非线性递增趋势,而本文方法置乱度增加缓慢,说明该算法的置乱程度受分块数影响较小,算法有效。

3.2　相邻像素相关性分析

图像的本质特征决定了图像中相邻像素间具有较强的相关性。基于这一性质,利用统计攻击方法来分析图像加密算法具有较高的可行性,因此用相关系数

来衡量加密算法破坏相邻像素相关性的能力。

$$E(x)=\frac{1}{N}\sum_{1}^{N}x_j \tag{6}$$

$$D(x)=\frac{1}{N}\sum_{1}^{N}[x_j-E(x)]^2 \tag{7}$$

$$Cov(x,y)=\frac{1}{N}\sum_{1}^{N}[x_j-E(x)][y_j-E(y)] \tag{8}$$

$$r=\frac{Cov(x,y)}{\sqrt{D(x)}\times\sqrt{D(y)}} \tag{9}$$

式中：x 和 y 分别为相邻两个像素的像素值；$E(\cdot)$、$D(\cdot)$和 $Cov(\cdot,\cdot)$分别为期望、方差和协方差；r 为相邻两像素的相关系数，r 的值接近 1 的程度越高，则图像相邻像素的相关性越强。

分别采用 Arnold-Fibonacci 变换(即 A-F 变换)、文献[22]算法和本文算法对 Lena 图像进行加密，从图像中随机选取 1 000 对相邻像素点(水平、垂直和对角)，然后利用以上公式分别计算图像在三个方向的相邻像素相关系数，其结果如表 3 所示。由表 3 可知，原始图像的相邻像素高度相关，本文算法去相关性能力较强，加密图像的像素相关性接近于 0，且熵值更接近 8，可见本文加密算法优于其他算法。

表 3　相邻像素的相关系数对比

Tab. 3　Correlation coefficients of adjacent pixels

方向	相关系数			
	原始图像	A-F 算法	文献[22]算法	本文算法
水平	0.967 81	0.053 45	0.004 09	0.000 55
垂直	0.901 22	0.061 15	0.007 98	0.003 95
对角线	0.930 13	0.080 89	0.020 12	0.006 01
熵	7.442 10	7.643 31	7.856 31	7.999 51

3.3　抗剪切性能

数字图像经常发生剪切攻击，如果图像受到不同程度上的剪切，算法仍然能够在一定程度上恢复原始信息，则说明该加密解密算法对剪切具有鲁棒性。首先利用本文算法对 Lena 图像进行加密，然后进行一定程度的剪切，最后对剪切图像进行解密，如图 5 所示。

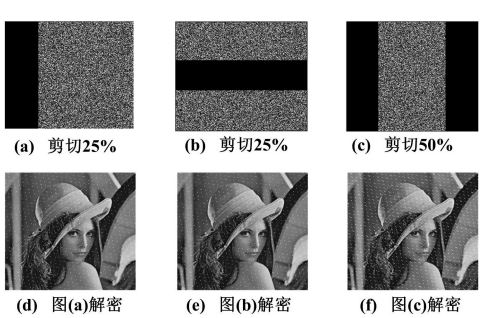

图 5　抗剪切试验结果图

Fig. 5　Anti-shear experiments results

由图 5 可以看出，即使图像受到 50% 的剪切，解密算法仍然能够恢复出原始图像，说明本算法是有效的，可抗剪切攻击。本文加密算法具有均匀置乱步骤，保证了被剪切掉的部分具有最大的不相关性，同时加密后的图像具有最大的不相关性，从而可以很容易地恢复原始图像。

3.4　抗噪声试验

为了验证本文算法的抗噪声性能，在加密后的图像中加入均值为 0、方差为 σ 的高斯白噪声。在图 3(h)中加入不同方差的高斯噪声然后采用本文算法进行加密与解密，抗噪声试验结果如图 6 所示。

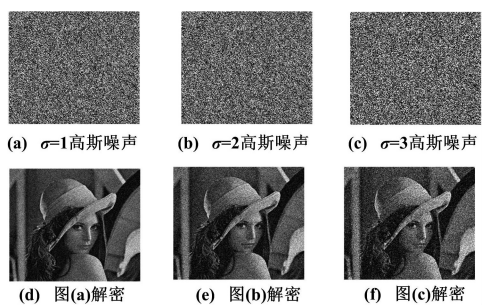

图 6　抗噪声试验结果图

Fig. 6　Anti-noise experiments results

通过上述噪声攻击试验可以看出，当加密图像受到不同程度的高斯白噪声影响时，本文的解密算法也能基本恢复原始图像，而且基本不会影响图像整体视觉效果，表明本算法可以抵抗不同程度的高斯白噪声攻击。

3.5　执行速度分析

试验运行平台为 Pentium(R)、双 CPU、2.10 GHz、内存 2 GB 的计算机，操作系统为 Windows XP 企业版，利用 VC++6.0 编写相应的加密、解密算法，并记录执行时间，对文献[22]、文献[24]、文献[25]算法进行了对比，得到的执行时间如表 4 所示。由表 4 可知，本文算法远优于文献[24]，文献[24]与文献[22]的执行时间相差不到 1 s。

表 4　不同算法的执行时间

Tab. 4　Run time of different algorithms

加密算法	最短时间/s	最长时间/s	平均时间/s
文献[22]算法	13.596	13.962	13.779
文献[24]算法	16.750	16.896	16.823
文献[25]算法	17.672	17.716	17.694
本文算法	14.384	14.796	14.590

4　结束语

本文基于二维 Fibonacci 变换和均匀分块的思想，

提出了一种新的图像分块加密算法[25-27]。首先对原图像分块,对块内像素点执行按位替代操作,然后利用均匀分块算法置乱,再对置乱后的每个图像块进行Fibonacci像素值置乱,最后对块置乱后的图像进行Fibonacci位置置乱。试验表明,本文算法加密、解密效果较好,可以抵抗不同程度的剪切、噪声等常规攻击,而且算法具有一定的实时性,满足实际应用。

参考文献

[1] 齐东旭,邹建成,韩效宥. 一类新的置乱变换及其在图像信息隐蔽中的应用[J]. 中国科学(E辑),2000,43(3):304-312.

[2] Won Y, Hyoungshick K. An image encryption scheme with a pseudorandom permutation based on chaotic maps [J]. Communication in Nonlinear Science and Numerical Simulation, 2010,15(12):3998-4006.

[3] NayakC K, Acharya A K, Das S. Image encryption using an enhanced block based transformation algorithm [J]. International Journal of Research and Review in Computer Science,2011,2(2):275-279.

[4] Ismail I A, Amin M, Diab H. A digital image encryption algorithm based a composition of two chaotic logistic map [J]. International Journal of Network Security,2010,11(1):1-10.

[5] Chen Dongming, Chang Yunpeng. A novel image encryption algorithm based on logistic maps [J]. Advances in Information Science and Service Sciences,2011,3(7):364-372.

[6] Pareek N K, Patidar V, Sud K K. Image encryption using chaotic logistic map[J]. Image and Vision Computing,2006(24):926-934.

[7] Patidar V,Sud K K. Modified substitution-diffusion image cipher using chaotic standard and logistic maps [J]. Communication in Nonlinear Science and Numerical Simulation,2010(15):2755-2765.

[8] Jolfaei A,Mirghadri A. Image encryption using chaos and block cipher[J]. Computer and Information Science,2011,4(1):172-185.

[9] Sathishkumar G A, Bagan K B. A novel image encryption algorithm using pixel shuffling base 64 encoding based chaotic block cipher[J]. WSEAS Transactions on Computers,2011,10(6):169-178.

[10] Indrakanti S P, Avadhani P S. Permutation based image encryption technique [J]. International Journal of Computer Applications, 2011,28(8):45-47.

[11] Patidar V, Pareek N K, Purohit G. A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption [J]. Optics Communications, 2011 (284): 4331-4339.

[12] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps[J]. Internation Journal of Bifurcat Chaos,1988,8(6):1259-1284.

[13] 丁玮,齐东旭. 数字图像变换及信息隐藏与伪装技术[J]. 计算机学报,1998,21(9):839-843.

[14] 柏森,曹长修,曹龙汉. 基于骑士巡游变换的图像细节隐藏技术[J]. 中国图像图形学报,2001,6A(11):1096-1100.

[15] 南艳红,李南,邹建成. Fibonacci变换及其在数字图像水印中的应用[J]. 中山大学学报:自然科学版,2004,43(2):148-151.

[16] Zou J C, Qi D X, Rabab K. A novel watermarking method based on Fibonacci numbers [C]//Proceedings of ACM International Conference on Virtual Reality Continuum and its Applications, 2006:335-338.

[17] Zou J C, Rabab K W, Qi D X. A new digital image scrambling method based on fibonacci numbers [C]//Proceedings of the 2004 IEEE International Symposium on Circuits and Systems,2004:965-968.

[18] Pareek N K, Patidar V, Sud K K. Image encryption using chaotic logistic map[J]. Image and Vision Computing,2006(24):926-934.

[19] Mazloom S, Eftekhari A M. Color image encryption algorithm based on coupled nonlinear chaotic map[J]. Chaos, Solitons & Fractals, 2009,42(3):1745-1754.

[20] Patidar V, Purohit G, Sud K K. Image encryption through a novel permutation-substitution scheme based on chaotic standard map[C]// International Workshop on Chaos-Fractals Theories and Applications, 2010,5(8):164-169.

[21] Pareek N K. Design and analysis of a novel digital image encryption scheme [C]//International Journal of Network Security & its Applications,2012,4(2):95-108.

[22] 王圆妹,李涛. 基于Arnold变换的高效率分块图像置乱算法的研究[J]. 电视技术,2012,36(3):17-19.

[23] 侯启槟,杨小帆,王阳生等. 一种基于小波变换和骑士巡游的图像置乱算法[J]. 计算机研究与发展,2004,41(2):369-375.

[24] 王道顺,杨地莲,齐东旭. 数字图像的两类非线性变换及其周期性[J]. 计算机辅助设计与图形学报,2001,13(9):829-833.

[25] Zou J C, Rabab K W, Qi D X. The generalized fibonacci transformations and application to image scrambling [C]//Proceedings of the 2004 IEEE International Conference on Acoustic, Speech, and Signal Processing(ICASSP),2004:385-388.

[26] 李太勇,贾华丁,吴江. 基于三维混沌序列的数字图像加密算法[J]. 计算机应用,2006(7):52-56.

[27] 向德生,熊岳山. 基于约瑟夫遍历的数字图像置乱算法[J]. 计算机工程与应用,2005(10):23-24.