文章编号:1001 - 9081(2007)08 - 1888 - 03

一种基于高维混沌系统的彩色图像加密新算法

韩凤英[1,2],朱从旭[1],胡玉平[1,3]
(1. 中南大学 信息科学与工程学院,长沙 410083; 2. 长沙航空职业技术学院,长沙 410124;
3. 湖南人文科技学院 计算机系,湖南 娄底 417000)
(hanxiangok@163.com)

摘 要:根据高维混沌系统具有更高安全性的特点,提出一种基于统一混沌系统和广义猫映射的彩色图像加密新算法。该算法先利用广义猫映射分别实现空域彩色图像三基色置乱变换,然后由统一混沌系统输出的三维混沌序列分别实现空域彩色图像三基色逐像素替代变换。研究结果表明,该算法具有良好的像素值混淆、扩散性能和较大的抵抗强力攻击的密钥空间,加密图像像素值具有类随机均匀分布特性,且相邻像素的值具有零相关特性,证明了所提出方案具有较高的安全性。

关键词:彩色图像加密;统一混沌系统;广义猫映射;三基色置乱
中图分类号: TP309.7 **文献标志码**:A

New colour image encryption algorithm based on high-dimension chaotic system

HAN Feng-ying[1,2], ZHU Cong-xu[1], HU Yu-ping[1,3]
(1. *School of Information Science and Engineering, Central South University, Changsha Hunan* 410083, *China*;
2. *Changsha Aeronautical Vocational and Technical College, Changsha Hunan* 410124, *China*;
3. *Department of Computer, Hunan Institute of the Humanities, Science and Technology, Loudi Hunan* 417000, *China*)

Abstract: According to the characteristic of higher secrecy of high-dimension chaotic system, a new colour image encryption algorithm based on unified chaotic system and general cat maps was proposed. Firstly, tricolor scrambling transformation was realized respectively in space domain by using the general cat maps. Then the three chaotic sequences of unified chaotic system were adopted to realize the tricolor Substitution transformation pixel by pixel. The results demonstrate that the algorithm has good properties of confusion and diffusion. The key space is large enough to resist the brute-force attack. For the encrypted image the distribution of pixel-values has a random-like behavior and the values of adjacent pixels satisfy zero correlation, showing that the proposed scheme is of high security.

Key words: colour image encryption; unified chaotic system; general cat map; tricolor scrambling

0 引言

随着网络技术的飞速发展和多媒体数字产品的广泛应用,确保多媒体信息在传播和使用过程中的安全是迫切需要解决的问题。由于数字图像具有数据量大、数据相关度高等特点,用传统的加密方式对图像加密时存在效率低的缺点。近年来兴起的新型混沌加密方式为图像加密提供了一种新的有效途径,已成为近年的研究热点[1-3]。

混沌系统具有许多重要特性,例如对初始条件和系统参数的极端敏感性;拓扑传递性即相空间中任一点的邻域在混沌系统作用下将“撒遍”整个度量空间;周期点的稠密性即系统具有很强的确定性和规律性,绝非一片混乱。混沌又是一种貌似无规则的运动,是在确定性非线性系统中不需附加任何随机因素也可出现的一种内在随机性,因此其伪随机行为能够准确再生。这些特性与密码学要求的扩散、混合和随机特性相吻合[4]。但是,目前许多图像加密方案采用了一维混沌系统,因此其安全性不高。原因之一是密钥空间不够,不能抵御穷举攻击;而且容易利用相空间重构方法进行混沌系统识别[5],只要截获足够长的明文/密文对,就能够破解种子密钥,从而不能抵御已知明文攻击。此外,现有图像加密算法很少涉及对彩色图像加密的研究。

为此,本文作者采用广义猫映射与统一混沌系统模型结合,提出一种基于高维非线性混沌系统的彩色图像加密新算法。

1 二维广义猫映射与图像置乱

将猫映射进行推广,得到下列广义猫映射公式:

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^n \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \bmod N \tag{1}$$

由式(1)知,该映射存在一个不动点(0,0),即点(0,0)经过 n 次迭代映射后不变,为避免产生不动点,对坐标点的取值改用 $\{1,2,\cdots,N\} \times \{1,2,\cdots,N\}$ 表示,并将映射方程改造为含两个独立参数的形式:

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix}^n \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \bmod N + 1 \tag{2}$$

式(2)表示由初值点 (x_0, y_0) 先经过 n 次模 N 的迭代运算后,再将结果加 1 作为变换后的坐标 (x_n, y_n)。可以证明式(2)具有混沌映射的某些特性,而且是一一映射。因此利用式(2)来

收稿日期:2007 - 02 - 08;**修回日期**:2007 - 04 - 16。
基金项目:湖南省自然科学基金资助项目(06JJ5098);湖南省教育厅科研基金资助项目(06A031)。
作者简介:韩凤英(1975 -),女,湖南宁乡人,硕士研究生,讲师,主要研究方向:混沌密码学; 朱从旭(1963 -),男,湖南武冈人,副教授,博士,主要研究方向:信息保密、信息隐藏; 胡玉平(1969 -),男,湖南娄底人,教授,博士,主要研究方向:数字水印与网络信息安全。

置乱图像像素点的位置:将原始明文图像的各像素坐标(i,j)作为初值(x_0,y_0),用给定系数矩阵(由独立参数p,q决定)和迭代次数n作密钥,生成的迭代结果(x_n,y_n)作为原图像点(i,j)处像素置换后的新位置(i',j')。由于映射的混沌特性,当迭代次数足够大时,任意两个相邻的像素点,它们的新位置将会产生极大的分离;又由于该映射是一一映射,不同位置的明文像素置乱到密文图像空间的位置不会重叠。这样,原始图像的全部像素将被随机而均匀地置乱到密文图像的整个像素空间。

由于RGB彩色图像可以分解成三个基色图像,每一基色分量图像可以看成是亮度图像。在本文的置乱算法中,分别用广义猫映射置乱每个基色图像;而且置乱每个基色图像时使用不同的密钥参数(p_i,q_i,n_i),$i=1$、2或3,分别对应R、G、B三基色图像。设原始彩色图像用矩阵$\boldsymbol{A}$表示,分解成三个基色图像分别用矩阵$\boldsymbol{RA}$、$\boldsymbol{GA}$和$\boldsymbol{BA}$表示,然后用不同参数的猫映射分别对矩阵$\boldsymbol{RA}$、$\boldsymbol{GA}$和$\boldsymbol{BA}$进行置乱变换,将置乱后的3个基色图像再合成为彩色图像矩阵$\boldsymbol{A}1$,$\boldsymbol{A}1$就是置乱后的彩色图像。这种分别置乱每个基色图像的算法可以使最终的合成彩色图像每点的颜色成分发生变化,能混淆彩色图像每一像素的R、G、B三元素,使加密图像在视觉上发生了色彩变化。因此,比将同一点的三基色值统一置乱到一个相同新位置的安全性更高。

2　三维统一混沌系统与图像替代

置乱是重新排列图像像素位置,仅改变每个基色图像相邻像素之间的相关性,但不能改变每个基色图像的直方图。替代是对每个基色图像的像素值进行变换,可以改变整个基色图像的直方图分布特性。因此,在置乱的基础上再进行像素值的替代变换,将获得更好的加密安全性。

文献[6]提出了一个新的三维混沌系统,该系统将Lorenz系统和Chen系统连接起来,而Liu系统仅为其一个特例,故称其为统一混沌系统,其数学模型为:

$$\begin{cases}\dfrac{\mathrm{d}x}{\mathrm{d}t}=(25\alpha+10)(y-x)\\[2ex]\dfrac{\mathrm{d}y}{\mathrm{d}t}=(28-35\alpha)x-xz+(29\alpha-1)y\\[2ex]\dfrac{\mathrm{d}z}{\mathrm{d}t}=xy-(8+\alpha)z/3\end{cases}\tag{3}$$

式中:系统参数$\alpha\in[0,1]$,在此范围内统一系统具有全域性混沌特性。当$\alpha\in[0,0.8)$时,系统属于广义Lorenz系统;当$\alpha=0.8$时,系统属于广义Liu系统;当$\alpha\in(0.8,1]$时,系统属于广义Chen's系统。本文用统一混沌系统式(3)产生的混沌序列来构造图像像素替代变换的密钥。这里,使用统一混沌系统的x、y和z序列分别对三基色图像像素进行逐点替代加密。对每个像素点,用一个混沌实数序列值中小数点后某3位数字构造密钥(这里取小数点后5、6和7这3位数字构造密钥)。设图像大小为$N\times N$,则从生成的3个混沌序列中各取长度为$N\times N$的子序列用于构造密钥。对置乱后的一个基色图像的任一点(i,j)(像素值表示为$A_1(i,j,k)$,其中$k=1$、2、3分别对应红、绿、蓝基色),根据k的值分别从x、y或z序列中选择实数序列值来构造整数加密密钥。设从混沌序列中选择的当前实值混沌序列值为r,则由r的小数点后5,6和7这3位数字组成正整数Intkey,将该正整数对256取模运算后将得到1字节的无符号整数,然后将此1字节的无符号整数作为该像素点的加密密钥;加密采用密钥与像素值进行二进制位异或运算的方式。算法类Matlab关键伪代码如下:

1)对第(i,j)点进行加密。

```
n = (i-1)*N+j;                          % 计算点(i,j)的顺序号n
for k =1:3
  If k ==1
    r = x(n);                           %从x序列中选择一个实数
  Else if k ==2
    r = y(n);                           % 从y序列中选择一个实数
  Else
    r = z(n);                           % 从z序列中选择一个实数
  End
Intkey = fix((r*10^4 - fix(r*10^4))*10^3);
Intkey = mod(Intkey,256);
A2(i,j,k) = bitxor(A1(i,j,k), Intkey);
```

其中,fix(x)表示对x向0方向的取整,mod(x,y)取x整除以y之后的余数;$A_2(i,j,k)$为第k个基色平面的第(i,j)点替代后的密文值。

2)对每个基色图像另一坐标点(i,j)处像素,重复步骤1),直到每点均完成像素值的替代变换。最后得到置乱和替代变换后的最终加密彩色图像$A2$。

从上述算法看,对图像的每一个像素点都采用了不同的加密密钥,因此,符合一次一密加密原则。

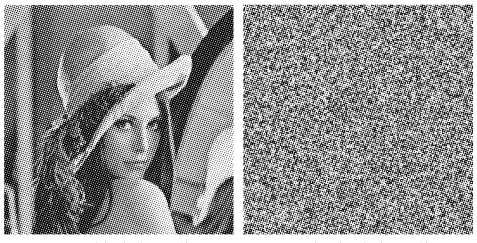
图像解密是加密的逆过程,只要利用相同的混沌系统生成相同的密钥序列,先对密文图像每个基色平面的像素值进行反替代;然后再对反替代后每个基色图像的像素进行位置反置乱;最后将反置乱后的三个基色平面合成,即得到解密彩色图像。

3　实验结果及分析

利用Matlab 7.0平台,取256×256 Lena彩色图像进行实验($N=256$)。在图像置乱变换中,广义猫映射式(2)的参数依次取$p=3$、4、5,$q=5$、6、7,$n=20$、21、22分别用于R、G、B三基色平面的像素置乱。统一混沌系统的系统参数和初值分别为:$a=0.9$;$x(0)=0.1$,$y(0)=1.0$,$z(0)=0.0$;系统演化时间区间为[0,850];采用变步长的四阶五级Runge-Kutta-Felhberg算法解微分方程(3),生成3个长度大于256×256的序列,删除每个序列前面的部分元素,得到三个长度等于256×256的序列$x(i)$、$y(i)$、$z(i)$($i=1,2,\cdots,256\times256$),用于图像像素的替代加密。

3.1　可视效果

图1所示为最终加密结果和原始图像的对比。可知,加密图像已经变得杂乱无章,不可辨认。图2是加密前后三基色图像的直方图分布特性对比。原图像的三基色平面的直方图表明,不同像素值的像素数目分布是不均等的;而加密后的直方图表明,密文像素值在整个取值空间的取值概率趋于均等,呈现良好的均匀分布特性。当密钥完全正确时,解密图像完全与图1(a)相同,即可以完全正确解密。



(a) 原始彩色图像　　(b) 加密彩色图像

图1　图像加密效果

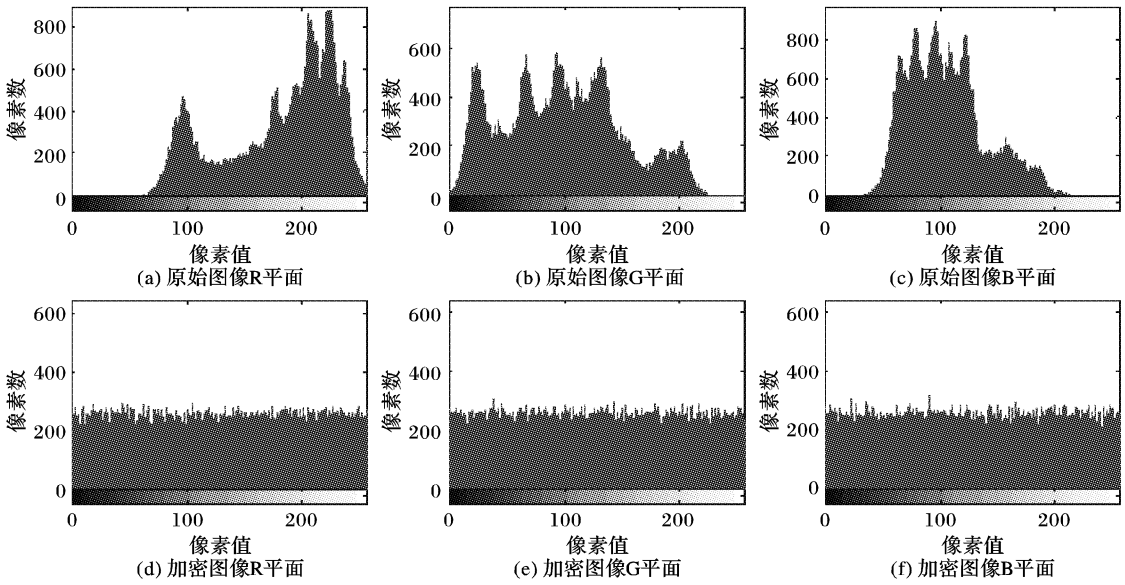


图2 原始图像和加密图像直方图

3.2 相邻像素的相关性

为了检验明文图像和密文图像相邻像素的相关性,从图像中随机选取全部水平方向相邻像素对,全部垂直方向相邻像素对和部分对角方向相邻像素对,用如下公式定量计算相邻像素的相关系数[7]:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{4}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x)]^2 \tag{5}$$

$$Conv(x,y) = \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x)][y_i - E(y)] \tag{6}$$

$$g_{xy} = \frac{Conv(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{7}$$

其中,x 和 y 分别表示单基色图像中相邻 2 个像素的像素值,γ_{xy} 即为单基色图像相邻 2 像素的相关系数。

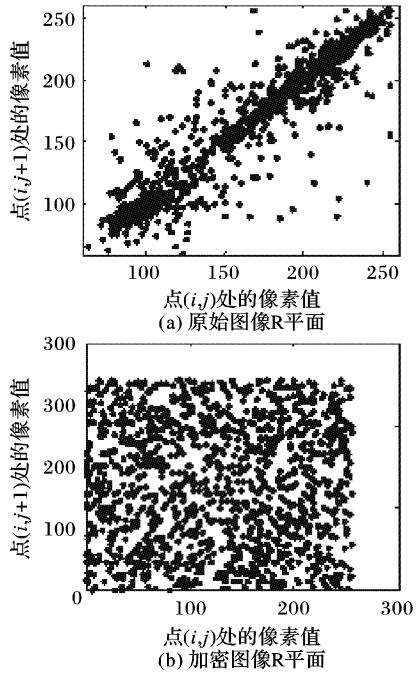


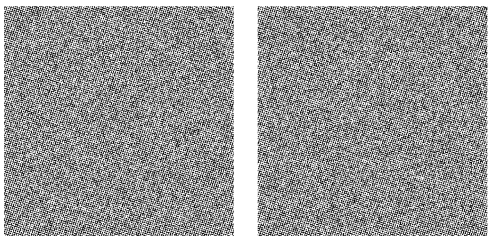
图3 水平方向 R 平面分量相邻像素的相关性

图3 所示为 G 分量图像水平方向明文和密文相邻像素的相关性。表1 则列出了按水平、垂直及对角 3 种方向计算所得的三种基色图像的相关系数结果。可知,原始明文图像各基色平面的相邻像素高度相关,相关系数接近 1;而加密图像各基色图的相邻像素相关系数接近 0,表明相邻像素已基本不相关,说明明文图像的统计特征已被扩散到随机的密文中。

表1 明文和密文相邻像素的相关系数

方向	R 平面	G 平面	B 平面
水平明文	0.9460	0.9465	0.9046
水平密文	-3.5×10^{-5}	0.0040	-9.4×10^{-5}
垂直明文	0.9720	0.9729	0.9465
垂直密文	−0.0053	0.0030	−0.0014
对角明文	0.9215	0.9240	0.8682
对角密文	−0.0028	−0.0053	−0.0029

3.3 对密钥的敏感性和密钥空间



(a) $x(0)$误差10^{-12}时 (b) a误差10^{-8}时

图4 错误密钥的解密图像

将解密时所用的混沌系统初始值分别取为:$x'(0) = x(0) + 10^{-12}$, $y'(0) = y(0)$ 和 $z'(0) = z(0)$;仅 $x'(0)$ 与加密时采用的值 $x(0)$ 相差 10^{-12},得到解密结果如图4(a) 所示。而解密时系统初值相同,仅将系统参数 a 与加密时采用的值相差 10^{-8},得到解密结果如图4(b) 所示。可见,密钥的细微差别导致完全不能解密。对 $y(0)$ 和 $z(0)$ 的敏感性实验结果同样表明,当 $y(0)$ 和 $z(0)$ 分别改变 10^{-12} 时,也完全不能解密。以上结果表明算法对密钥具有高度的敏感性。若以统一混沌系统参数、系统初值为最初密钥,采用精确到小数点后 15 位的双精度实数表示,则密钥空间为 $10^{15}\times10^{15}\times10^{15}\times10^{15} = 10^{60} \approx 2^{199}$,相当于 199 bit 长的密钥空间(远远大于 128 bit 密钥长度),为一维混沌系统密钥的 10^{30} 倍。所以,密码系统足以抵抗现有硬件条件下的强力攻击。

(下转第 1894 页)

3)能够有效抵御像素相关统计分析攻击。为了说明加密后图像的相关特征被完全破坏,采用文献[11]提供的相关分析方法。随机取一些点,以该点为中心,计算其相邻各个点颜色值数学期望值、自相关和互相关以及协方差。每种颜色的自相关值为:

$$E_x(i,j) = \frac{1}{49}\sum_{p=i-3}^{i+3}\sum_{q=j-3}^{j+3} x_{pq}$$

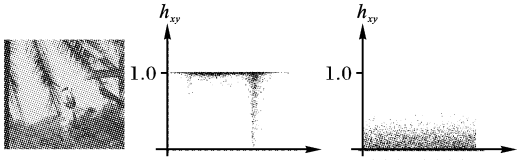
$$R_x(i,j) = \frac{1}{49}\sum_{p=i-3}^{i+3}\sum_{q=j-3}^{j+3} (x_{pq} - E(x_{ij}))^2$$

颜色之间的互相关值为:

$$R_x(i,j) = \frac{1}{49}\sum_{p=i-3}^{i+3}\sum_{q=j-3}^{j+3} (x_{pq} - E(x_{ij}))(y_{pq} - E(y_{ij}))$$

$$\eta_{xy}(i,j) = \frac{R_{xy}(i,j)}{\sqrt{R_x(i,j)R_y(i,j)}}$$

应用上述计算公式,分别取像素(i,j)为中心的7×7点阵进行分析,分析结果如图5所示。图中给出彩色图像加密前后随机选取的6000个像素邻域相关分析结果。可以看出,原图像的大部分像素的邻域相关性在1.0附近,而加密后的图像各个像素的颜色值相关性非常小,因此,该加密方法可以有效地抵御采用像素相关分析的攻击。



(a) 原始图像 (b) 原图相关分析 (c) 加密后相关分析

图5 彩色图像邻域相关分析

5 结语

提出一个把扩散、Arnold映射、Logistic系统和Chen系统有机结合的多混沌系统图像置乱加密算法。从信息论出发,算法首先对图像进行扩散和在位平面进行多次Arnold映射,实现对图像的置乱操作,然后用Chen系统产生的超混沌序列对不同基色进行多次加密,可以实现对各种图像进行加密和解密。该算法简单、易用硬件实现;该加密算法的安全性仅取决于密钥,且有足够大的密钥空间,在完全公开算法的情况下,能够有效抵御各种攻击。相应的算法已经在某公司技术图纸的加密/解密上得到应用。

参考文献:

[1] 朱从军,李力,陈志刚.基于多维混沌系统组合的图像加密新方法[J].计算机工程,2007,33(2):142.

[2] 马在光,丘水生.基于广义猫映射的一种图像加密系统[J].通信学报,2003,24(2):51-57.

[3] 刘英,孙丽莎.基于三维猫映射的图像加密算法[J].计算机工程与应用,2005,41(36):127-130.

[4] 郭建胜,金晨辉.对基于广义猫映射的一个图像加密系统的已知图像攻击[J].通信学报,2005,26(2):131-135.

[5] 李雄军,彭建华,徐宁,等.基于二维超混沌的图像加密算法[J].中国图象图形学报:A版,2003,8(10):1172-1177.

[6] 孔涛,张亶.Arnold反映射的一种新算法[J].软件学报,2004,15(10):1558-1564.

[7] CHEN G, DONG X. From chaos to order methodologies: perspectives and application[J]. Singapore: World Scientific, 1998, 24(16):760-767

[8] UETA T, CJHEN G R. Bifurcation analysis of Chen's equation[J]. International Journal Bifurcation and Chaos, 200, 10(8): 1917-1931.

[9] YASSEN M T. Chaos control of Chen chaotic dynamical system[J]. Chaos Solitons & Fractals, 2003, 15(2): 271-283.

[10] 张丽丽,雷友发.一个三维非线性系统的混沌动力学特征[J].动力学与控制学报,2006,4(1):5-7.

[11] CHEN G R, MAO Y B, CHARLES K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons and Fractals, 2004, 3(21): 749-761.

[12] 徐江峰,杨有,黄小粟.基于广义同步混沌的图像加密方案[J].计算机工程,2006,32(6):154-156.

[13] CHEN G, UETA T. Yet another chaotic attractor[J]. International Journal of Bifurcation and Chaos, 1999, 9(7):1465-1466.

(上接第1890页)

4 结语

利用统一混沌系统模型结合广义猫映射,提出了基于高维非线性混沌系统实现彩色图像像素置乱和替代加密的新算法。算法具有以下主要优点:

1)实现了对彩色图像三基色分量分别置乱,置乱算法不仅能打破相邻像素的相关性,而且能混淆彩色图像每一像素的R、G、B三元素,使加密图像在视觉上发生了色彩变化,图像保密性更高。

2)像素的位置置换和像素值的替代均基于复杂非线性高维混沌系统,克服了一维混沌系统不能抵御相空间重构攻击的缺点;且以三维统一混沌系统的系统参数和初值为密钥,大大拓展了密钥空间,使算法具有抵御穷举攻击的能力。

3)统一混沌系统具有复杂的非线性混沌行为,因此生成的密钥具有较高的复杂性;且每次随机产生的密钥不同,具有一次一密特性;密文具有在整个取值空间均匀分布的特性,相邻像素具有近似于零的相关性。

混沌加密和解密的速度是较快的,但求解高维混沌系统微分方程的时间开销较大。如果将其用于对网络通信的实时图像加密,可以离线生成混沌序列,然后进行在线加密。这样,算法既具有图像加密的实时性,又确保了加密效果的高安全性。

参考文献:

[1] GUAN Z H, HUANG F J, GUAN W J. Chaos-based image encryption algorithm[J]. Physics Letters A, 2005, 346(1-3): 153-157.

[2] GAO H J, ZHANG Y S, LIANG S Y, *et al.* A new chaotic algorithm for image encryption[J]. Chaos, Solitons and Fractals, 2006, 29(2):393-399.

[3] LONG M, PENG F, QIU S S, *et al.* Implementation of a new chaotic encryption system and synchronization[J]. Journal of Systems Engineering and Electronics, 2006, 17(1): 43-47.

[4] ZHANG L H, LIAO X F, WANG X B. An image encryption approach based on chaotic maps[J]. Chaos, Solitons and Fractals, 2005, 24(3): 759-765.

[5] WANG S H, KUANG J Y, LI J H, *et al.* Chaos-based communications in a large community[J]. Physical Review E-Statistical, Nonlinear, and Soft Matter Physics, 2002, 66(6): 1-4.

[6] Lü J H, CHEN G R, ZHANG S C. The compound structure of a new chaotic attractor[J]. Chaos, Solitons and Fractals, 2002, 14(5):669-672.

[7] CHEN G R, MAO Y B, CHARLES K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons and Fractals, 2004, 21(3):749-761.