对一种基于混沌映射的对称图像加密算法的改进*)

张 伟[1,2] 廖晓峰[1] 杨华千[1,2] 韦鹏程[1,2] 黄 松[1,2]

(重庆大学计算机科学与工程学院 重庆 400044)[1] (重庆教育学院计算机与现代教育技术系 重庆 400067)[2]

摘 要 文[1]提出了一种基于3D Cat映射的对称图像加密算法,文[2]对其安全性进行了分析,指出该算法在抗选择明文攻击能力方面性能比较差。本文在文[1]的基础上,提出了一种改进的对称图像加密算法。在本算法中,通过复合离散混沌系统隐藏混沌序列产生时所经历的迭代次数,来避免文[2]的基于符号动力学的密码分析。理论分析和仿真实验表明,本文提出的改进算法在保持了原来算法的各种抗攻击能力性能的同时,进一步提高了原算法的抗选择明文攻击能力。

关键词 混沌图像加密算法,3D Cat映射,复合离散混沌系统,密码分析,选择明文攻击

A Modified Symmetric Image Encryption Scheme Based on Chaotic Map

ZHANG Wei[1,2] LIAO Xiao-Feng[1] YANG Hua-Qian[1,2] WEI Peng-Cheng[1,2] HUANG Song[1,2]

(Department of Computer Science and Engineering, Chongqing University, Chongqing 400044)[1]

(Department of Computer and Modern Education Technology, Chongqing Education College, Chongqing 400067)[2]

Abstract In ref. [1], a symmetric image encryption scheme is proposed, which is based on 3D chaotic cat maps. In ref. [2], a security analysis has been carried out for the scheme, and pointed that the performance is poor in resistance of chosen plain image attack. Hence, in this letter, a modified symmetric image encryption scheme is presented. In the proposed scheme, when the chaos sequence is generated, the iteration times are hidden to avoid cryptanalysis based on symbolic dynamic. Theoretical analyses and simulated experiment show that, the modified scheme enhances the resistance of chosen plain image attack. At the same time, which also preserves the good performance against others attacks.

Keywords Chaos image encryption scheme, 3D Cat map, Composite discrete chaotic system, Cryptanalysis, Chosen plain-image attack

1 引言

基于混沌的图像加密技术把待加密的图像信息看成是按照某种方式编码的二进制的数据流,利用混沌信号来对图像数据流进行加密。混沌之所以适合图像加密,这与它自身的动力学特性密切相关。混沌密码系统,正如其它密码系统一样,需提供三种重要特性来防止密码分析[13],即

(1) 对密钥敏感:对同一明文,密钥的微小变化将产生完全不同的密文。

(2) 对明文敏感:对同一密钥,明文的微小变化将产生完全不同的密文。

(3) 明文到密文的映射是随机的:一个好的密码系统,密文中不应该存在任何固定模式。

混沌系统的三个特征:(1)参数敏感性;(2)初值敏感性;(3)以同一分布遍历各态性。它们很好地对应了密码系统的这三个特性。

然而混沌在本质上是确定的,有关文献已经证明这些算法的抗选择明文或已知明文攻击的能力较差[2,9~12]。这主要是因为,计算机的有限精度和混沌序列的离散化导致了混沌动力系统的性能退化。

文[1]提出的基于3D Cat映射的对称图像加密算法,使用3D Cat映射来置乱图像像素的位置,使用Logistic映射来置混密文图像和明文图像的关系。理论分析和仿真实验表明,该算法对诸如统计分析攻击、差分攻击有很好的抗攻击能力。但是,文[2]的分析表明,文[1]的加密算法对选择明文攻击的抗攻击能力较差,详细分析见文[2]。本文在分析了文[1]和文[2]的基础上,提出了一种改进的基于3D Cat映射的对称图像加密算法。

本文第2节描述了文[1]的基于3D Cat映射的对称图像加密算法。第3节描述了文[2]对文[1]的算法安全性分析方法。第4节提出了本文的改进的基于3D Cat映射的对称图像加密算法。第5节对改进的算法从理论和仿真实验两个方面进行了安全性分析。最后总结了本文。

2 基于3D Cat映射的对称图像加密方案

在文[1]中,Chen, Mao等人提出了基于3D Cat映射的对称图像加密方案。该方案的核心思想是使用3D Cat映射来置乱被加密图像的像,在第6节素位置,然后使用另一个混沌映射产生的混沌序列,通过"异或"操作来修改图像的像素值。其加密/解密过程如下:

(1) 把$W\times H$的二维图像折叠成一系列立方体图像T_1

*)中国博士后科学基金一等资助项目(No. 20060390175)、重庆市科委自然科学基金资助项目(No. CSTC, 2005BB2286, 2006BB2254)、重庆市教委资助项目(No. kj051501, No. kj061501)。张 伟 教授,博士后,主要研究方向为信息安全,计算智能与数据挖掘;廖晓峰 教授,博士生导师,主要研究方向为神经网络、混沌理论;杨华千 博士研究生,主要研究方向为信息安全、混沌数字水印;韦鹏程 博士研究生,主要研究方向为信息安全、混沌理论;黄 松 博士研究生,主要研究方向为图像处理、数字水印。

$\times T_1\times T_1, T_2\times T_2\times T_2, \cdots, T_i\times T_i\times T_i$。并且满足如下条件：

$$W\times H=\sum_{j=1}^{i}T_j^3+R$$

其中 $T_j\in\{2,3,\cdots,N\}$是每个立方体的边长，N 是最大边长。$R\in\{0,1,\cdots,7\}$是折叠后的余数。

$$A=\begin{bmatrix} 1+a_xa_zb_y & a_z & a_y+a_xa_z+a_xa_ya_zb_y \\ b_z+a_xb_y+a_xa_zb_yb_z & a_zb_z+1 & a_ya_z+a_xa_ya_zb_yb_z+a_xa_zb_z+a_xa_yb_y+a_x \\ a_xb_zb_y+b_y & b_x & a_xa_yb_xb_y+a_xb_x+a_yb_y+1 \end{bmatrix}$$

矩阵 A 中的 $a_x, a_y, a_z, b_x, b_y, b_z$ 是由 Chen 混沌系统产生的 3D Cat 映射控制参数，(x_n, y_n, z_n)和(x'_n, y'_n, z'_n)分别是像素在立方体中的置乱前的位置和置乱后的位置，N 是该立方体的边长。

(3) 对新的置乱的立方体按下述方式进行加密。

$$C(k)=\phi(k)\oplus\{[I(k)+\phi(k)]\bmod N\}\oplus C(k-1) \quad (2)$$

$$\phi(k)=\lfloor N(x(k)-x_{\min})/(x_{\max}-x_{\min})\bmod N\rfloor \quad (3)$$

其中，$x(k)$由 Logistic 映射

$$x(k+1)=4x(k)[1-x(k)] \quad (4)$$

产生，$(x_{\min}, x_{\max})$的典型取值区间是(0.2,0.8)，N 是图像的颜色深度(对于 256 级的灰度图像，$N=256$)，$I(k)$是当前操作的像素值，$C(k-1)$是前一位明文像素产生的密文像素，初始值 $I(0)=C(0)=S$，S 是任意的 0 到 255 的正整数，$C(k)$是当前明文像素产生的密文像素。(2)的逆变换如下：

$$I(k)=\{\phi(k)\oplus C(k)\oplus C(k-1)+N-\phi(k)\}\bmod N \quad (5)$$

(4) 把经过置乱与置混的三维立方体，按 (1) 中折叠的顺序还原成二维形式。

在该方案中，采用了 128bit 的二进制序列作为加密密钥。首先把 128bit 的二进制序列分成 8 个组，$k_{a_x}, k_{a_y}, k_{a_z}, k_{b_x}, k_{b_y}, k_{b_z}, k_l, k_s$ 每组 16 位。然后用 $k_{a_x}, k_{a_y}, k_{a_z}, k_{b_x}, k_{b_y}, k_{b_z}$来产生 Chen 混沌系统的六个控制参数，用 k_l, k_s 来产生 Logistic 映射的初始值 L_i 和(2)中模运算的初始值 S，并作为 $I(0)$。

3 基于 3D Cat 映射的对称图像加密方案的安全性问题

文[1]提出的方案在抵抗诸如统计攻击，差分攻击等方面的密码分析有较好的抗攻击性。但文[2]认为文[1]中的方案主要存在以下两个问题：

(1) 对于置混过程。由于混沌系统的离散化及其计算机的有限精度，使得文[1]中使用的混沌系统已经失去了连续混沌系统的某些良好的特性(如长周期性)。因此，借助 Gray 编码思想和符号动力学，通过逐渐逼近的方法，经过不太大的运算量就能得到了该混沌系统的初始值，详细过程见文[2]。但是，文[2]并没有给出一个更好的算法来解决这个问题。

(2) 对于置乱过程。文[1]中采用 3D Cat 映射，并按(1)式来置乱像素的位置。根据文[2]的分析，我们只需构造一个与 A 模等的矩阵 A'，即使得 A'满足：$A'\equiv A(\bmod N)$，$|\det(A')|=1$。则有

$$\begin{bmatrix}x'_n\\y'_n\\z'_n\end{bmatrix}=A\begin{bmatrix}x_n\\y_n\\z_n\end{bmatrix}\bmod N=A'\begin{bmatrix}x_n\\y_n\\z_n\end{bmatrix}\bmod N \quad (6)$$

$$\begin{bmatrix}x_n\\y_n\\z_n\end{bmatrix}=(A')^{-1}\begin{bmatrix}x'_n\\y'_n\\z'_n\end{bmatrix}\bmod N \quad (7)$$

(2) 对每一个立方体图像执行如下的 3D Cat 映射变换，产生新的被置乱的立方体。

$$\begin{bmatrix}x'_n\\y'_n\\z'_n\end{bmatrix}=A\begin{bmatrix}x_n\\y_n\\z_n\end{bmatrix}\bmod N \quad (1)$$

因此，根据式(7)，明文图像很容易从被置乱的图像中恢复过来。矩阵 A'的构造过程见文[2]。

4 改进的基于 3D Cat 映射的对称图像加密方案

从上面的分析看，文[1]的加密方法，在抗选择明文攻击方面，无论是其置乱过程还是置混过程都是比较脆弱的。因此，本文将通过改进文[1]中混沌序列产生的方法，对其置混过程进行改进，增强其抗选择明文攻击性能。

4.1 复合离散混沌系统的定义

定义 设两个离散混沌系统 $f(\cdot), g(\cdot): x_{n+1}=f(x_n, p_f), y_{n+1}=g(y_n, p_g)$，则定义一个新的离散混沌系统 $\Phi(\cdot)$ 如下：

$$x_{n+1}=\Phi^{(M)}(x_n)=f^{(M)}(x_n, p_f) \quad (8)$$

其中，

$$M=\lceil Q(y_{n+1}-x_{\min})/(x_{\max}-x_{\min})\bmod Q\rceil+\Delta \quad (9)$$

Q 是大于 0 的自然数，$(x_{\min}, x_{\max})$的典型取值区间是(0.2,0.8)。y_{n+1}是由 $g(\cdot)$产生的混沌序列，其值通常也要求在(0.2,0.8)之间；Δ 是 $f(\cdot)$的迭代次数修正量，其取值情况如下：如果 $f^{\lceil Q(y_{n+1}-x_{\min})/(x_{\max}-x_{\min})\bmod Q\rceil}(x_n)\in(x_{\min}, x_{\max})$，则 $\Delta=0$。否则，继续迭代 $f^{\lceil Q(y_{n+1}-x_{\min})/(x_{\max}-x_{\min})\bmod Q\rceil}(x_n)$，直到其值位于区间$(x_{\min}, x_{\max})$内，则 Δ 就等于继续迭代的次数。

4.2 图像的置乱过程

由于文[1]中的 3D Cat 映射有很好的抗统计攻击、差分攻击效果。因此，本文仍然使用文[1]中的 3D Cat 映射来置乱图像像素的位置。算法的具体过程见文[1]和本文的第 2 节。

4.3 图像的置混过程

根据 4.1 的描述，本文选择 Logistic 映射作为 $\Phi(\cdot)$中的 $f(\cdot)$，Tent 映射作为 $\Phi(\cdot)$中的 $g(\cdot)$，构成改进的离散混沌系统 $\Phi(\cdot)$。Logistic 映射和 Tent 映射分别定义如下：

$$\text{Logistic Map: } x_{k+1}=4x_k(1-x_k) \quad (10)$$

$$\text{Tent Map: } y_{k+1}=\left(1-2\left|y_k-\frac{1}{2}\right|\right) \quad (11)$$

则图像的置混过程如下：

(1) 选定两个初始参数 i_l, i_t，分别作为 Logistic 映射和 Tent 映射的初始值。

(2) 利用(11)式和 i_t 产生混沌序列 $y_1, y_2, \cdots, y_n$。

(3) 利用 (8) 和 (9) 式得到 $\Phi(\cdot)$的混沌序列 $x_1, x_2, \cdots, x_k, \cdots, x_n$。

(4) 利用 (3) 式将该序列离散化得到密钥流 $\phi(1), \phi(2), \cdots, \phi(k), \cdots, \phi(n)$。

(5) 首先对 (2) 式做一个修正，得到

$$C(k)=\{\phi(k)\oplus\{[I(k)+\phi(k)]\bmod N\}\oplus C(k-1)\}\bmod 256 \quad (2')$$

利用 (2′) 式对图像的明文像素流进行加密，得到图像的密文像素流：$C(1), C(2), \cdots, C(k), \cdots, C(n)$。注意，在计算过

程中设定 $C(0)$为任意的 0 到 255 之间的一个正整数。

4.4 图像的加密和解密过程

本文的加密算法框图如图 1。

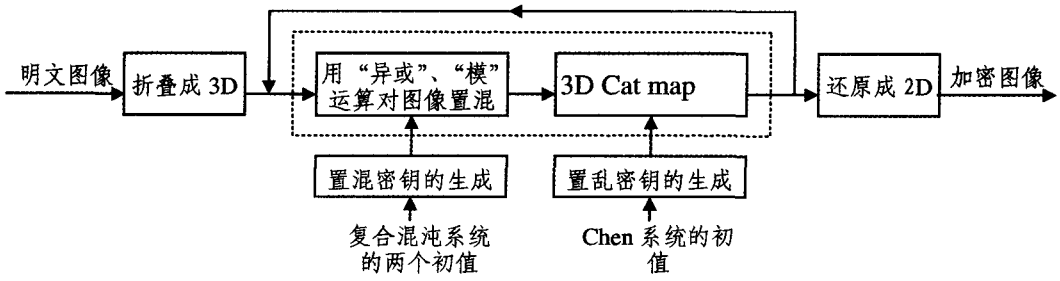


图 1 图像加密框图

加密步骤如下：

(1) 将明文图像折叠成一系列 3D 图像，方法见第 2 节。

(2) 选定复合混沌系统的两个初始值(i_t, i_l)，按 4.3 节的方法对立方体图像进行置混。

(3) 按第 2 节的方法对置混后的图像进行置乱。

(4) 把经过置混与置乱后的立方体图像还原成 2D 加密图像。

出于安全性的需要，可以重复(2)、(3)两步多次。由于本文的重点在于改进文[1]中算法的抗选择明文攻击能力，所以下面的实验中，我们没有直接采用 Chen 系统来计算步骤(3)所需要的 3D Cat 映射矩阵 A，而使用了文[2]中的与 A 模等的矩阵 $A^{(2)}$，见公式(15)。其解密过程与加密过程类似，只是还原置乱过程采用矩阵 $(A^{(2)})^{-1}$，对于还原置混过程，采用如下的修正公式(5′)。

$$I(k)=\{\{\phi(k)\oplus C(k)\oplus C(k-1)+N-\phi(k)\}\bmod N\}\bmod 256 \tag{5'}$$

5 新算法的安全性分析

一个好的加密算法应该能够抵抗各种密码分析攻击。针对本文提出的加密方案进行的各种安全性做如下分析。

5.1 密钥空间分析

与文[1]的加密方案比较，本文只是改变了文[1]的混沌密钥流的产生方法，并且需要两个初始条件来决定混沌密钥流的产生。假设计算机的计算精度为 16 位，那么仅在混沌密钥流的产生过程中的密钥空间就为 10^{32}。如果计算上 3D Cat 映射变换的密钥空间，这将远远大于文[1]中的密钥空间 2^{128}。

5.2 密钥敏感性测试

对于一个好的图像加密方案，其加密和解密过程都应该对密钥非常敏感。这有两层含义：

(I)加密密钥的细微改变，应该得到两个几乎完全不同的加密图像；

(II)解密密钥的细微改变，其解密过程将失败。

为此，采用密文像素变化率(Cipher-text Pixel Change Rate，CPCR)来衡量密钥的敏感性：

$$CPCR=\frac{\sum_{i=1}^{W}\sum_{j=1}^{H}Difp(I(i,j),I'(i,j))}{W\times H} \tag{12}$$

其中

$$Difp(I(i,j),I'(i,j))=\begin{cases}1, & I(i,j)\neq I'(i,j)\\ 0, & I(i,j)=I'(i,j)\end{cases} \tag{13}$$

W, H 分别表示图像 I 和 I' 的宽和高。在本文的加密方案中，图像的置乱与置混是两个分离的过程。所以，在下面的密钥敏感性测试实验中，没有采用 Chen 系统来计算文[1](见本文第 2 节)中的 A, L_i, S，而直接使用了文[2]中的矩阵 $A^{(2)}$(其 $\det(A^{(2)})=1$)

$$A^{(2)}=\begin{bmatrix}2080 & 11 & 21097\\ 14749 & 78 & 149596\\ 3787 & 20 & 38411\end{bmatrix} \tag{14}$$

对于 S，实验中直接取值 93。

(1) 加密密钥敏感性测试

实验结果表明，当密钥仅仅只有 2^{-16} 的微小变化时，加密后图像的像素灰度变化率都大于 99%，而解密几乎失败。因此，本文的改进算法保留了文[1]的密钥敏感性。

(a). Original Image

(b). Encrypted Image
it=0.726727294921875
il=0.926727294921857

(c). Encrypted Image
it=0.726727294921875
il=0.926727294921858

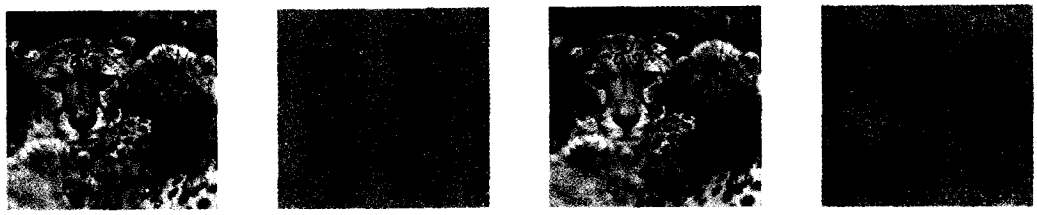
(d). Difference Image
(b) and (c)

图 2 加密密钥敏感性测试

(2) 解密密钥敏感性测试(见图 3)

5.3 抗选择明文图像攻击

对于文[1]提出的方案，在进行选择明文图像密码分析的过程中，可以根据观察到的 $C(k)$，$C(k-1)$ 和 $I(k)$ 估算出 $\phi(k)$ 的取值区间，然后借助符号动力学和混沌迭代函数的逆映射，在计算机的有限精度下，可以得到混沌动力系统的初始值，即加密密钥，其详细过程见文[2]。从式(4)可以知道，文[1]在密钥流产生过程中泄漏了如下两个重要信息：每一位密



(a). Original Image

(b). Encrypted Image
it=0.726727294921875
il=0.926727294921857

(c). Decrypted Image
it=0.726727294921875
il=0.926727294921857

(d). Decrypted Image
it=0.726727294921875
il=0.926727294921858

图 3　解密密钥敏感性测试

钥产生的混沌动力系统以及每一位密钥产生所经历的迭代次数。本文针对这一缺陷，对文[1]的密钥流产生方法进行了改进，详细描述见第 4 节。从式(8)和(9)可以看出，混沌序列依赖于两个混沌动力系统 $f(\cdot)$，$g(\cdot)$，并且在产生混沌序列时，$f(\cdot)$所经历的迭代次数也是未知的，所以在进行文[2]中的选择明文图像密码分析时，将很难用符号动力学和混沌迭代函数的逆映射来分析加密密钥。下面将仅仅从计算复杂性来进行分析。

在文[2]中，从估计得到的 $\varphi(K)=[x'_{\min}, x'_{\max}]$($K$ 表示图像的第 K 个像素)计算混沌系统的初值 x_0 的上下边界时，执行的逆映射次数约为

$$n_1=4\cdot\left(\frac{k\cdot(k-1)}{2}\right)=2k\cdot(k-1) \tag{15}$$

在本文的算法中，如果取(9)式的 $Q=128$，则从 $\varphi(K)$计算混沌系统的初值 x_0 的上下边界时，执行的逆映射次数约为

$$n_2=4\cdot 2^{8(k-1)} \tag{16}$$

在文[2]中，当 $K=42$ 时，得到了混沌系统的初值 x_0 所经历的逆映射次数 $n_1=3444$。如果按本文的算法加密，则得到混沌系统的初值 x_0 所经历的逆映射次数 $n_2=2^{248}$，并且这种逆映射次数将随着 K 的增大以指数形式增长，使得计算上不可能实现。

5.4　统计分析

一个好的图像加密算法应该具有好的抗统计分析攻击能力。下面的实验证明，本文在改善了文[1]中算法的抗选择明文攻击能力的同时，仍然保持了文[1]的抗统计分析攻击能力。

(1) 图像的灰度值统计直方图(图 4)；

(2) 两个相邻像素的相关性。

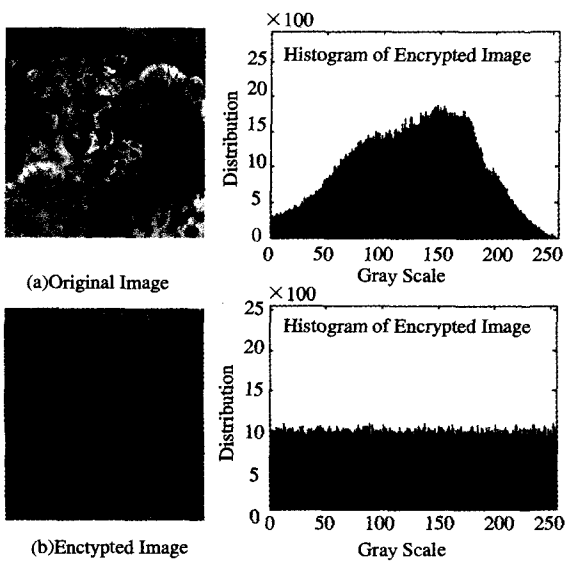


图 4　图像的灰度直方图

图像的本质特征决定了图像中相邻像素间存在较大的相关性，基于统计分析的攻击方法正是利用了图像的这一固有性质来进行密码分析。所以，一个好的图像加密算法应该破坏像素间的这种相关性，从而增强算法的抗统计分析能力。可以借助概率论的相关系数来衡量相邻像素的相关性。仿真实验演示了从明文图像和加密图像中随机选取的 1000 个水平相邻像素对的灰度值之比(图 4)。在图(a)中，大多数水平相邻像素的灰度值之比接近于 1，表明相邻像素的相关性比较高。而在图(b)中，大多数水平相邻像素的灰度值之比比较分散，表明图像经加密后相邻像素的相关性较低。

结论　本文提出了一种对文[1]的基于 3D Cat 映射的图像对称加密算法的改进方案。理论分析和仿真实验表明，本文的算法通过改进文[1]的混沌序列的生成方式，在保持了原来算法的密钥敏感性、抗统计攻击、差分攻击的同时，扩大了算法的密钥空间和提高了算法的抗选择明文攻击能力。不过，由于在加密的过程中，每个密钥的生成要经过多次迭代，所以本文的算法在加密的速度上较文[1]的算法有所降低。

参 考 文 献

1　Chen G R, Mao Y B, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons and Fractals, 2004,21:749～761

2　Wang K, Pei W J, Zou L H, et al. On the security of 3D Cat map based symmetric image encryption scheme. Physics Letters, 2005,A 343:432～439

3　Masuda N, Aihara K. Cryptosystems with discredited chaotic maps. IEEE Trans Circuits Syst-I: Fundamental Theory and Application, 2002,49 (1):28～40

4　Yen J C, Guo J I, Efficient hierarchical image encryption algorithm and its VLSI realization. IEEE Proc. Vis. Image Signal Process,2000,147 (2):430～437

5　Yen J C, Guo J I, A new chaotic key-based design for image encryption and decryption. In:ISCAS, IEEE International Symposium on Circuits and Systems, May, Geneva, Switzerland, vol IV. 2000. 49～52

6　Mao Y B, Chen G, Lian S G. A novel fast image encryption scheme based on the 3D chaotic baker map. Int J Bifurcation Chaos,2004,14 (10):3613～3624

7　Kocarev L, Jakimovski G. Chaos and cryptography: from chaotic maps to encryption algorithms. IEEE Trans Circ Syst-I,2001,48(2):163～9

8　Li S J, Zheng X. Cryptanalysis of a chaotic image encryption method. In: IEEE Int Symposium Circuits and Systems, Scottsdale, AZ, USA, 2002

9　Li S J, Mou X Q, Cai Y L, et al. On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision. Computer Physics Communications,2003, 153:52～58

10　Alvarez G,Montoya F, Romera M, et al. Cryptanalyzing an improved security modulated chaotic encryption scheme using ciphertext absolute value. Chaos, Solitons and Fractals,2005,23: 1749～1756

11　Alvarez A, Montoya F, Romera M, et al. Cryptanalysis of dynamic look-up table based chaotic cryptosystems. Physics Letters,2004, A 326:211～218

12　Alvarez G, Montoya F, Romera M, et al. Cryptanalysis of an ergodic chaotic cipher. Physics Letters,2003, A 311:172～179

13　Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurc Chaos,1998, 8(6):1259～1284