一种基于复合离散混沌系统的对称图像加密算法*)

杨华千[1,2] 张 伟[1,2] 韦鹏程[1,2] 王 永[1,3] 杨德刚[1,4]

(重庆大学计算机学院 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]

(重庆邮电大学经济管理学院 重庆 400065)[3] (重庆师范大学数学与计算机科学学院 重庆 400047)[4]

摘 要 提出了一种基于复合离散混沌系统的对称图像加密算法。在该算法中,通过复合离散混沌系统隐藏了混沌序列产生时所经历的迭代次数,来避免常用的基于符号动力学的密码分析。理论分析和仿真实验表明,本文提出的算法具有较高的安全性能,特别是在统计攻击、差分攻击和选择明文攻击能力方面具有很好的抗攻击性能。

关键词 混沌图像加密算法,复合离散混沌系统,密码分析,选择明文攻击,符号动力学

A Symmetric Image Encryption Scheme Based on Composite Discrete Chaotic System

YANG Hua-Qian[1,2] ZHANG Wei[1,2] WEI Peng-Cheng[1,2] WANG Yong[1,3] YANG De-Gang[1,4]

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

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

(Economic and Management Institute, CQUPT, Chongqing 400065)[3]

(Math and Computer Science Institute, Chongqing Normal University, Chongqing 400047)[4]

Abstract In this paper, a symmetric image encryption scheme based on composite discrete chaotic system 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 analysis and simulated experiment show that, the scheme has excellent performances against attacks, in particular statistical attack, differential attack and chosen plain image attack.

Keywords Chaos image encryption scheme, Composite discrete chaotic system, Cryptanalysis, Chosen plain-image attack, Symbolic dynamic

1 引言

随着互联网和计算机的飞速发展,我们迫切需要新的快速而安全的图像加密算法。为了应对这种挑战,研究人员已经提出了大量的图像加密算法[1,3~11]。基于混沌的图像加密技术是目前的研究热点。正如其它密码系统一样,混沌密码系统需提供3种重要特性来防止密码分析[16],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3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3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[2,12~15]。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。

本文提出了一种新的基于复合离散混沌映射的对称图像加密算法。在该算法中,通过隐藏混沌序列产生时所经历的迭代次数,避免了常用的基于符号动力学的选择明文密码分析。因此,从计算安全性角度,提高了算法的抗明文攻击能力。

本文其余章节是按如下方式组织的:第2节描述了本文的基于复合离散混沌系统的对称图像加密算法;第3节对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 基于复合离散混沌系统的对称图像加密方案

2.1 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:

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

其中,

$$M=\lceil Q(y_{n+1}-x_{\min})/(x_{\max}-x_{\min})\bmod Q\rceil+\Delta \tag{2}$$

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 $f^{(\lceil N(y_{n+1}-x_{\min})/(x_{\max}-x_{\min})\bmod N\rceil)}(x_n)\in(x_{\min},x_{\max})$,则 $\Delta=0$。否则,继续迭代 $f^{(\lceil N(y_{n+1}-x_{\min})/(x_{\max}-x_{\min})\bmod N\rceil)}(x_n)$,直到其值介于区间$(x_{\min},x_{\max})$内,则 Δ 就等于继续迭代的次数。

2.2 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

*)重庆市教委资助项目(No. KJ061501,No. KJ051501)、重庆市科委资助项目(No. CSTC,2005BB2286)。杨华千 博士生,研究方向为计算机信息安全;张 伟 教授,博士,研究方向为计算智能;韦鹏程、王 永、杨德刚 博士生,主要研究方向为混沌密码学和信息安全。

图像像素的位置，简述如下(算法的具体过程见文[1])。

(1)把 $W\times H$ 的二维图像折叠成一系列立方体图像。

$T_1\times T_1\times T_1, T_2\times T_2\times T_2, \cdots, T_i\times T_i\times T_i$ 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。

(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。

$$\begin{bmatrix} x'_n \\ y'_n \\ z'_n \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} \bmod N \tag{3}$$

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

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。

2.3 图像的置混过程

根据 2.1 节的描述，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：

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

$$\text{Tent Map: } y_{k+1}=\left(1-2\left|y_k-\frac{1}{2}\right|\right) \tag{5}$$

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

(3)利用 (1)式得到 $\Phi(\cdot)$ 的混沌序列 $x_1, x_2, \cdots, x_k, \cdots, x_n$。

(4)利用 (6)式将该序列离散化得到密钥流 $\phi(1), \phi(2), \cdots, \phi(k), \cdots, \phi(n)$。

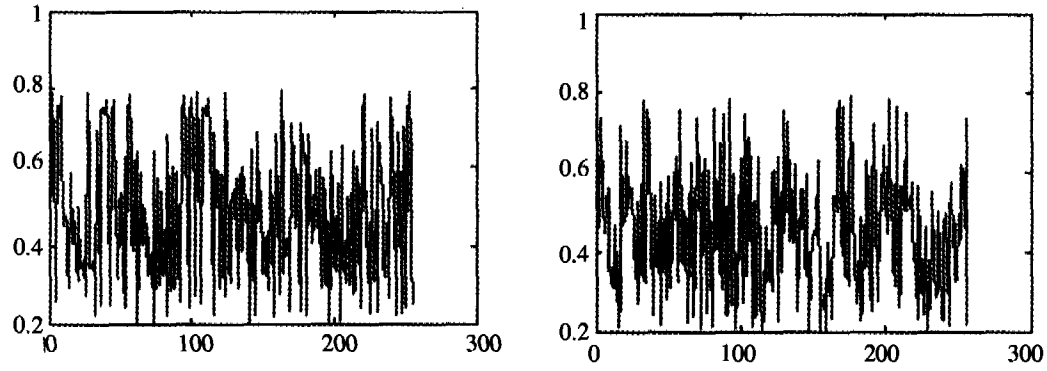
$$\phi(k)=\lfloor N(x_k-x_{\min})/(x_{\max}-x_{\min})\bmod N\rfloor \tag{6}$$

N 是图像的颜色深度(对于 256 级的灰度图像，$N=256$)，$(x_{\min}, x_{\max})$ 的典型取值区间是(0.2,0.8)。

(5)利用 (7)式对 2.2 节的置乱后的每个立方体图像像素流进行加密：

$$C(k)=\{\phi(k)\oplus\{[I(k)+\phi(k)]\bmod N\}\oplus C(k-1)\}\bmod 256 \tag{7}$$

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，$I(k)$ 是当前操作的像素值。Logistic 映射序列和复合映射序列如图 1 所示。



(a). Logistic map f (.)
(Initial value i_l: 0.926727294921857)

(b). Composite map Φ(.)
(Initial value i_l: 0.926727294921857
i_t: 0.726727294921875)

图 1 Logistic 映射和复合映射

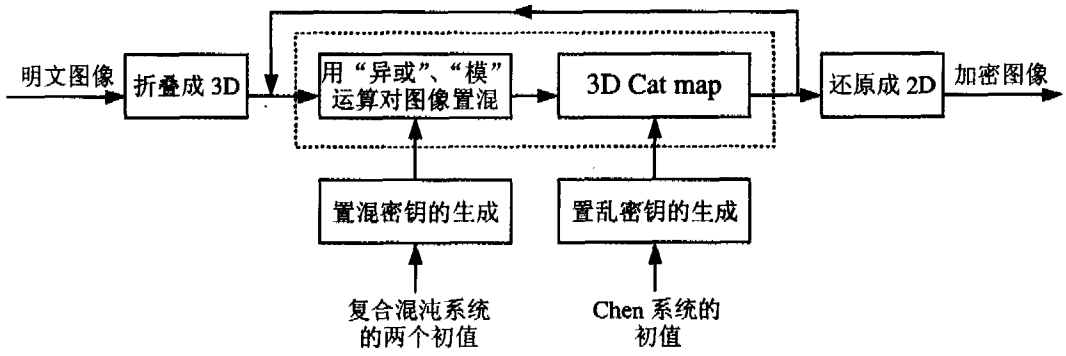


图 2 图像加密框图

2.4 图像的加密和解密过程

本文的加密算法框图如图 2。

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 2.2 节和文[1]。

(2)选定复合混沌系统的两个初始值(i_l,i_r)，按 2.3 节的方法对立方体图像进行置混。

(3)按第 2.2 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，可重复(2)、(3)两步多次。下面的实验中没有直接采用 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 $A^{(2)}$：

$$A^{(2)}=\begin{bmatrix}2080 & 11 & 21097\\ 14749 & 78 & 149596\\ 3787 & 20 & 38411\end{bmatrix} \tag{8}$$

其解密过程与加密过程类似，还原置乱过程，采用矩阵 $(A^{(2)})^{-1}$，还原置混过程，采用公式(7)的逆变换，如下：

$$I(k)=\{\{\phi(k)\oplus C(k)\oplus C(k-1)+N-\phi(k)\}\bmod N\}\bmod 256 \tag{9}$$

$C(k-1)$是前一位明文像素产生的密文像素，初始值 $I(0)=C(0)$，$C(0)$等于加密过程中的 $C(0)$，为任意的 0 到 255 之间的一个整数，$C(k)$是当前明文像素产生的密文像素。

3 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，并且其安全性不应该依赖于加密体制或算法的保密，而只依赖于密钥。针对本文提出的加密方案进行的各种安全性分析如下。

3.1 密钥空间分析

根据第 2 节的描述，在混沌密钥流的产生过程中，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，这将是一个非常大的数，使得穷举攻击不可能。

3.2 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：

①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；

②解密密钥的细微改变，其解密过程将失败。

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

$$CPCR=\frac{\sum_{i=1}^{W}\sum_{j=1}^{H}Difp(I(i,j),I'(i,j))}{W\times H} \tag{10}$$

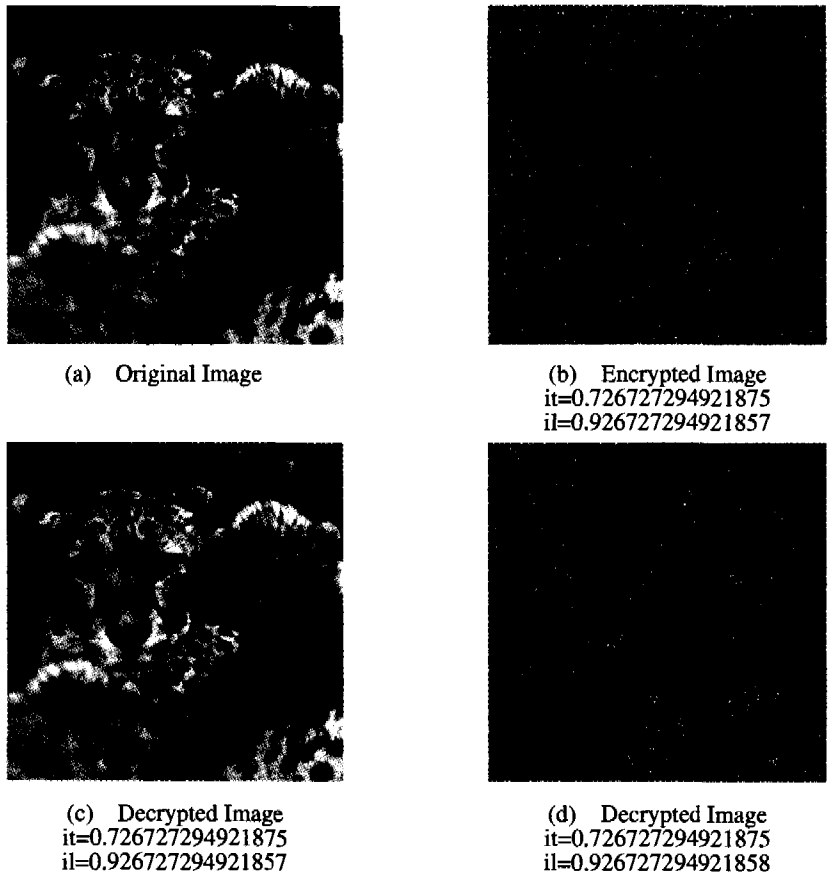
其中：

$$Difp(I(i,j),I'(i,j))=\begin{cases}1, & I(i,j)=I'(i,j)\\ 0, & I(i,j)\neq I'(i,j)\end{cases} \tag{11}$$

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(512X512 Pixels)，直接使用了文[2]中的矩阵 $A^{(2)}$(其 $\det(A^{(2)})=1$，见式(8))。对于 $C(0)$，直接取值 93。

(1)加密密钥敏感性测试(表 1 和图 4)。

(2)解密密钥敏感性测试(图 3)。



(a) Original Image

(b) Encrypted Image
it=0.726727294921875
il=0.926727294921857

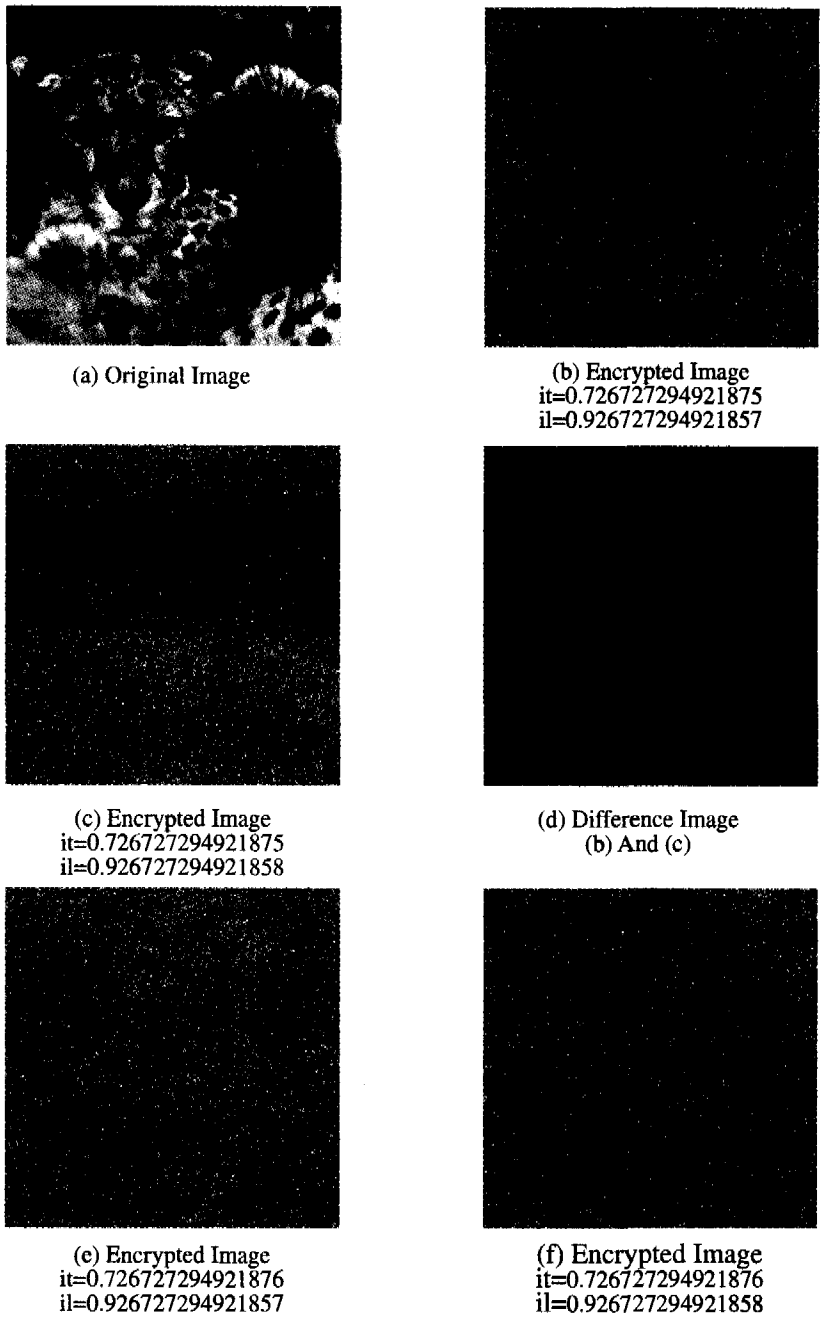
(c) Decrypted Image
it=0.726727294921875
il=0.926727294921857

(d) Decrypted Image
it=0.726727294921875
il=0.926727294921858

图 3 解密密钥敏感性测试

表 1　不同初始条件加密后，加密图像的像素灰度变化率

两个初始条件	it=0.726727294921875 il=0.926727294921857	it=0.726727294921875 il=0.926727294921858	it=0.726727294921876 il=0.926727294921857	it=0.726727294921876 il=0.926727294921858
灰度值变化的像素	0	260105	262105	260122
CPCR	0	99.222%	99.985%	99.229%



(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)

(e) Encrypted Image
it=0.726727294921876
il=0.926727294921857

(f) Encrypted Image
it=0.726727294921876
il=0.926727294921858

图 4　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，本文的算法具有很好的密钥敏感性。

3.3　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（整个图像的像素灰度值相同）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]。这主要是文[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。而在本文的算法中，从式(1)和(2)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：

$$n_1 = 4 \cdot \left(\frac{k \cdot (k-1)}{2}\right) = 2k \cdot (k-1) \qquad (12)$$

在本文的算法中，如果取式(2)的 $Q=128$，则从 φ 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：

$$n_2 = 4 \cdot 2^{6(k-1)} \tag{13}$$

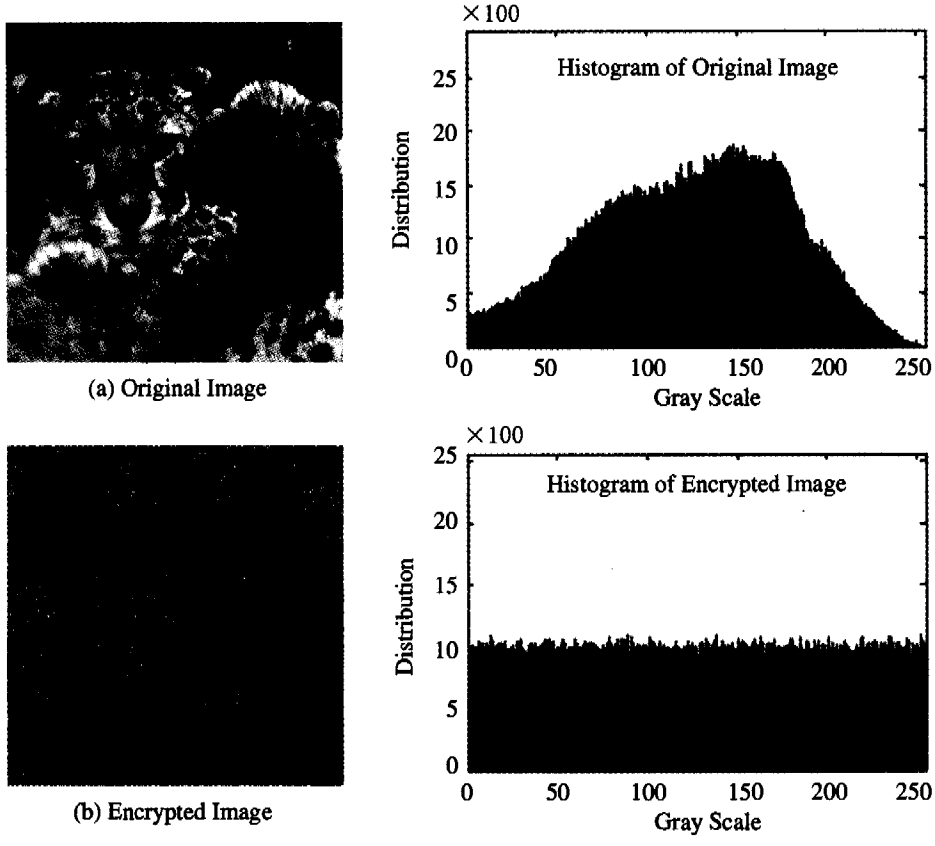


图 5

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。

3.4 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，本文的算法不仅具有良好的抗选择明文攻击能力，同时也具有良好的抗统计分析攻击能力。

3.4.1 图像的灰度值统计直方图

3.4.2 两个相邻像素的相关性

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：

$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{14}$$

其中：x,y 是相邻像素的灰度值。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 6)。在图 6(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 6(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。

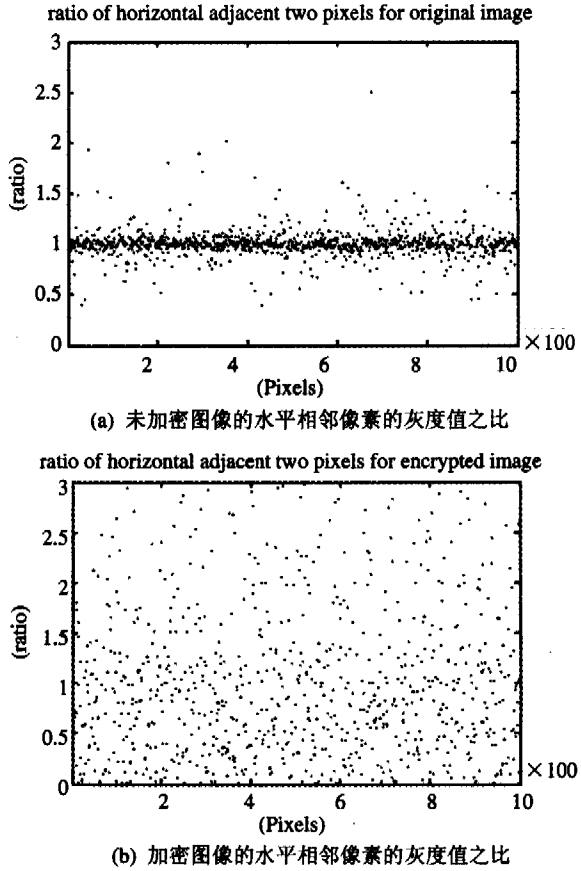


图 6 图像的水平相邻像素的相关性

(下转第 138 页)

我们通过调整个性参数来表达虚拟人的不同的个性。在开始对话之前，虚拟人的表情是平静的，随着交互的进行，虚拟人会改变它的情感表现。一个正向的激励并不意味一定展示出笑脸，因为情感心理状态的变化是按照一定概率出现的。但是，因为对立情感的相似度为0，一个激励不会引发出与激励状态截然相反的表情，如输入语音"你好"，虚拟人不会展示出悲哀的表情行为，这就避免了虚拟人表情行为的不可理解性。图3显示了虚拟人在交互期间的一些面部表情变化。

结论 本文提出了一个基于马尔可夫决策过程的情感计算模型，并且把这个模型应用到了一个虚拟人系统中。我们的目的并不是要探讨自然情感的发生机制，而在于探索交互虚拟人的情感处理方法，使交互过程显得更为自然。更进一步的工作是希望在系统中加入视觉反馈，如表情识别等。另外，我们也希望能够扩展这个情感计算模型，例如，加入动机模块和内部需求模块。

参 考 文 献

1 Buck R. The psychology of emotion. In: Mind and Brain. Dialogues in Cognitive Neuroscience, LeDoux J E, Hirst W, eds. New York: Cambridge University Press, 1986. 275～300
2 Sloman A, Beyond shallow models of emotion. Congnitive Processing, 2001, 1(1):530～539
3 Picard R. Affective Computing. Cambridge, Mass, London, England: MIT Press, 1997
4 Minsky M. The emotion machine. http://Web. media. mit. edu/～minsky/
5 Canamero L. Emotions and adaptation in autonomous agents: a design perspective. Cybernetics And Systems: An International Journal, 2001,32 :507～529
6 Breazeal C. Function meets style: insights from emotion theory applied to HRI. Systems, Man and Cybernetics, Part C, IEEE Transactions on, 2004,34:187～194
7 Ball G, Breese J. Emotion and personality ina conversational character. In: Cassell J, Sullivan J, Prevost S, et al, eds. Embodied Conversational Agents, Cambridge, MA: MIT Press, 2000
8 Kshirsagar S. A Multilayer Personality Model. In: SMARTGRAPH '02: Proceedings of the 2nd International Symposium on Smart Graphics, NewYork, NY, USA, ACM Press,2002. 107～115
9 Vlad O P, Vachkov G, fukuda T. Fuzzy emotion interpolation system for emotional autonomous agents. In: SICE 2002. Proceedings of the 41st SICE Annual Conference, Vol. 5. 2000. 3157～3162
10 El Jed M, Pallamin N, Dugdale J. Modelling character emotion in an interactive virtual environment. In: Proceedings of AISB 2004 Symposium: Motion, Emotion and Cognition. 29 March-1 April 2004
11 van Kesteren A J, op den Akker R, Poe M, et al. Simulation of emotions of agents in virtual environments using nerural networks. In: Jokiner K, Heylen D, Nijholt A eds. Learning to Behave: Internalising Knowledge. Twente Workshop on Language Technology 18(TWLT 18), Ieper, Belgium, November 2000. 137～147
12 王志良．人工心理学——关于更接近人脑工作模式的科学. 北京科技大学学报，2000，22(5):478～481
13 Xue Weimin, Wei Zhehua, Wang Zhiliang. The Research of Artificial Psychology Model. In: IEEE TENCON'02, Vol I. Beijing, China. October 2002. 691～693
14 Davidson R J, Abercrombie H, Nitschke J B, et al. Regional brain function, emotion and disorders of emotion. Current Opinion in Neurobiology, 1999, 9(2): 228～234
15 Plutchik R. The nature of Emotions. American Scientisr, 2001, 89:344～350
16 Allport G W. The Nature of Personality: Selected Papers, Addison-Wesley Press, Inc, 1950
17 Eysenck S, Eysenck H, Barrett P. A revised version of the psychoticism scale. Personality and Individual Di_erences, 6, 1985. 21～29
18 Costa P T, McCrae R R. Normal personality assessment in clinical practice: The NEO personality inventory. Psychological Assessment, 1992
19 Wilson I. The Artificial Emotion Engine. driving emotional behavior. In: AAAI Spring Symposium on Artificial Intelligence and Interactive Entertainment, 2000
20 Dolgov D A, Durfee E H. Resource Allocation and Policy Formulation for Multiple Resource-Limited Agents Under Uncertainty. In: Proceedings of the International Conference on Automated Planning and Scheduling, June 2004
21 kman E, Friesen W. Facial Action Coding System. Consulting Psychologists Press, 1977

(上接第90页)

结论 本文提出了一种新的基于复合离散混沌映射的对称加密算法，理论分析和仿真实验表明，本文的算法具有良好的密钥敏感性和很大的密钥空间，同时具有较好的抗统计攻击、差分攻击和选择明文攻击能力。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，因此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 Habutsu T, Nishio Y, Sasase I, et al. A secret key cryptosystem by iterating chaotic map. In: Lecture Notes Computer Science Advances in Cryptology—Euro Crypt'91, vol 547, 1991. 127～140
4 Pichler F, Scharinger J. Finite dimensional generalized Baker dynamical systems for Encrypt graphic applications. Lecture Notes in Computer Science, vol 1030, Springer, Berlin, 1996. 465～476
5 Masuda N, Aihara K. Cryptosystems with discredited chaotic maps. IEEE Trans Circuits Syst—I: Fundamental Theory and Application, 2002,49 (1):28～40
6 Yen J C, Guo J I. A new chaotic image encryption algorithm. In: Proceedings of the 1998 National Symposium on Telecommunications, December 1998. 358～362
7 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
8 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
9 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
10 Kocarev L, Jakimovski G. Chaos and cryptography: from chaotic maps to encryption algorithms. IEEE Trans Circ Syst——I2001, 48(2):163～169
11 Li SJ, Zheng X. Cryptanalysis of a chaotic image encryption method. In: IEEE Int Symposium Circuits and Systems, Scottsdale, AZ, USA, 2002
12 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
13 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
14 Alvarez G, Montoya F, Romera M, et al. Cryptanalysis of dynamic look-up table based chaotic cryptosystems. Physics Letters, 2004, A 326:211～218
15 Alvarez G, Montoya F, Romera M, et al. Cryptanalysis of anergodic chaotic cipher. Physics Letters, 2003, A 311:172～179
16 Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurc Chaos, 1998, 8(6): 1259～1284