基于分数阶时延混沌神经网络的图像加密

孙甜甜，黄　霞，李玉霞
（山东科技大学 山东省机器人与智能技术重点实验室，山东 青岛 266590）

摘　要：基于分数阶时延混沌神经网络，提出了一种新的图像加密算法：利用混沌系统产生秘钥流，把时延和分数阶导数嵌入到秘钥系统中以增加算法的安全性；用像素异或和置换相结合的方法对原始图像进行加密。通过对加密后图像各像素的水平垂直相关性、信息熵、游程统计、灰度变化平均值、直方图均衡度、密钥灵敏度等数据的详细分析，验证了该加密算法的安全性和有效性。

关键词：图像加密；分数阶；混沌系统；时延；神经网络

中图分类号：TP309.7　　**文献标志码**：A　　**文章编号**：1672-3767(2014)01-0098-06

Image Encryption Based on Delayed Fractional-order Chaotic Neural Networks

Sun Tiantian, Huang Xia, Li Yuxia
(Key Laboratory for Robot and Intelligent Technology of Shandong Province, Shandong University of Science and Technology, Qingdao, Shandong 266590, China)

Abstract: In this paper, a new image encryption scheme was proposed based on a delayed fractional-order chaotic neural networks. In the process of generating a key stream, the time delay and fractional derivative were embedded in the proposed scheme to improve the security. All pixels of original image were encrypted by combining method exclusive OR and replacement. This scheme was described in detail with security study including analysis of correlation, information entropy, run statistic, mean-variance gray value, histogram equalization degree and key sensitivity. Experimental results show that the newly proposed image encryption scheme possesses high security.

Key words: image encryption; fractional-order; chaotic system; delay; neural networks

由于图像信息形象生动，比文字蕴涵更大的信息量，因而被人类广泛利用，成为人类表达信息的重要手段之一。在传统的密码学研究领域，并没有单独将图像作为一种特殊的明文形式来考虑其加密特性。例如，DES(data encryption standard)[1]和 AES(advanced encryption standard)[2]等著名的加密算法，将所有的输入明文看作二进制流来进行加密，以保证加密的透明性，即加密算法不用考虑输入明文的具体类型。由于图像数据具有数据量大、数据的二维空间分布、能量的不均匀分布、原始图像数据存在大量冗余等特性[3]，使得传统加密算法对图像加密并不适用。

混沌系统具有对初始条件的极度敏感性及运动轨迹的非周期性，非常适用于图像加密。1989 年，英国数学家 Matthews 提出了将混沌系统用于数据加密的思想，Fridrich 在 1997 年首次将其应用于图像加密[4]。基于混沌的图像加密技术是近年来才发展起来的一种加密技术[5]，它把待加密的图像信息看作是按照某种编码方式的二进制数据流，利用混沌信号来对该数据流进行加密。

分数微积分理论已有 300 多年的历史，但分数阶和混沌系统的结合是近几年才出现的热点。近年来的

收稿日期：2013-10-10
基金项目：国家自然科学基金项目(61004078, 61273012)
作者简介：孙甜甜(1986—)，女，山东济南人，硕士研究生，主要从事保密通信方面的研究. E-mail: sttdxl@gmail.com
黄　霞(1978—)，女，山东泰安人，副教授，博士，主要从事混沌系统的同步与控制方面的研究.
E-mail: huangxia.qd@gmail.com

研究已经证实，分数阶方程比整数阶方程能更有效更精确地模拟现实世界。与整数阶混沌系统相比，分数阶混沌系统更符合实际情况，更能反映系统的工程物理现象，是对整数阶系统的推广。此外，分数阶混沌系统具有更强的记忆功能和稳定性，特别适合描述各种材料的记忆和遗传等特性。

神经网络是由大量非线性神经元构成的动力学系统，具有高度复杂的混沌特性[6]。神经网络的最大特点就是能够模拟人脑生物神经网络的联想记忆功能[7]。时延神经网络最早由 Waibel 提出[8]，时延神经网络模型是在多层前馈神经网络模型中引入时间延迟器扩展而来。时延神经网络将时间信号序列的分类问题转化为多维曲线的分类问题，延迟单元的引入，使得神经元不但可以了解当前时刻的输入信息，还能了解过去时刻的输入信息，有利于生成更为丰富和复杂的分类界面。

神经网络可以展现丰富的动力学行为，时延神经网络的混沌现象在保密通信应用中显示出巨大的优势和广阔的前景，本研究将分数阶时延神经网络中的混沌应用到图像加密中，探索此种方法在图像加密中的安全性和有效性。

1 基本定义和定理

分数阶微积分是一种将普通的微积分推广到任意实数阶的基本运算，记为${}_aD_t^\alpha$。连续的分数阶微积分算子可以定义为[9]：

$$ {}_aD_t^\alpha = \begin{cases} \dfrac{\mathrm{d}^\alpha}{\mathrm{d}t^\alpha}, & \alpha > 0 \\ 1, & \alpha = 0 \\ \displaystyle\int_a^t (\mathrm{d}\tau)^\alpha, & \alpha < 0 \end{cases} 。 \tag{1} $$

目前，三种最常用的分数阶微分定义分别是：Grünwald-Letnikov 定义[10]，Riemann-Liouville 定义[11]和 Caputo 定义[12]。

Grünwald-Letnikov 定义下的分数阶微分[10]通过将整数阶求导定义中的二项式系数推广到用 Gamma 函数表示，得到：

$$ x(t) = \sum_{k=0}^{[\alpha]-1} x^{(k)}(0)\frac{t^k}{k!} + \frac{1}{\Gamma(\alpha)}\int_0^t (t-\xi)^{\alpha-1} f(\xi, x(\xi), x(\xi-\tau))\mathrm{d}\xi 。 $$

定义中的二项式系数可以利用 Γ 函数表示为：$\binom{\alpha}{j} = \dfrac{\alpha!}{j!\ (\alpha-j)!} = \dfrac{\Gamma(\alpha+1)}{\Gamma(j+1)\Gamma(\alpha-j+1)}$，其中：$\Gamma(z) = \int_0^\infty \mathrm{e}^{-t}t^{z-1}\mathrm{d}t$，$\Gamma(z+1) = z\Gamma(z)$ 是对阶乘的推广。

本研究使用 Adams-Bashforth-Moulton 预估-校正算法[13]，能保证 $O(h^{1+\alpha})$ 阶代数精度，适用于求解具有常延时的分数阶时滞微分方程。

考虑分数阶时滞微分方程：

$$ D_t^\alpha x(t) = f(x(t), x(t-\tau), t), t \in [0, T], 0 < \alpha < 1; $$
$$ x(t) = g(t), t \in [-\tau, 0] 。 \tag{2} $$

由 Volterra 方程可知：

$$ x(t) = \sum_{k=0}^{[\alpha]-1} x^{(k)}(0)\frac{t^k}{k!} + \frac{1}{\Gamma(\alpha)}\int_0^t (t-\xi)^{\alpha-1} f(\xi, x(\xi), x(\xi-\tau))\mathrm{d}\xi 。 \tag{3} $$

取 $t_n = nh, n = -l, -l+1, \cdots, -1, 0, 1, \cdots, N$。其中，$l$，$N$ 为正整数，满足 $T = Nh, \tau = lh$。令 $x_h(t_j) = g(t_j)$，$j = -l, -l+1, \cdots, -1, 0$，则可得到：

$$ x_h(t_j - \tau) = x_h(jh - lh) = x_h(t_{j-l}), j = 0, 1, \cdots, N; $$

$$ x_h(t_{n+1}) = \sum_{k=0}^{[\alpha]-1} x^{(k)}(0)\frac{t_{n+1}^k}{k!} + \frac{h^\alpha}{\Gamma(\alpha+2)} f(t_{n+1}, x_h^p(t_{n+1}), x_h^p(t_{n+1-l})) + $$

$$\frac{h^{\alpha}}{\Gamma(\alpha+2)}\sum_{j=0}^{n}a_{j,n+1}f(t_j,x_h(h_j),x_h(t_{j-l}))。\tag{4}$$

其中：$a_{j,n+1}=\begin{cases}n^{\alpha+1}-(n-\alpha)(n+1)^{\alpha},j=0\\(n-j+2)^{\alpha+1}+(n-j)^{\alpha+1}-2(n-j+1)^{\alpha+1},1\leqslant j\leqslant n\\1,j=n+1\end{cases}$。

预估项 $x_h^p(t_{n+1})$ 可通过式(5)求得：

$$x_h^p(t_{n+1})=\sum_{k=0}^{[\alpha]-1}x^{(k)}(0)+\frac{1}{\Gamma(\alpha)}\sum_{j=0}^{n}b_{j,n+1}f(t_j,x_h(t_j),x_h(t_j-\tau))=$$
$$\sum_{k=0}^{[\alpha]-1}x^{(k)}(0)+\frac{1}{\Gamma(\alpha)}\sum_{j=0}^{n}b_{j,n+1}f(t_j,x_h(t_j),x_h(t_{j-l}))。\tag{5}$$

其中：$b_{j,n+1}=\frac{h^{\alpha}}{\alpha}((n+1-j)^{\alpha}-(n-j)^{\alpha})$。

2 分数阶时延神经网络混沌系统加密算法

2.1 系统的提出

本研究基于如下分数阶延时神经网络[14]：

$$D_t^{\alpha}\boldsymbol{x}(t)=-\boldsymbol{A}\boldsymbol{x}(t)+\boldsymbol{B}f(\boldsymbol{x}(t))+\boldsymbol{C}f(\boldsymbol{x}(t-\tau))+\boldsymbol{I}。\tag{6}$$

其中，$\boldsymbol{x}(t)=[x_1(t)\quad x_2(t)]^{\mathrm{T}}$，$f(\boldsymbol{x}(t))=[f(x_1(t))\quad f(x_2(t))]^{\mathrm{T}}$，$f(\boldsymbol{x}(t-\tau))=[f(x_1(t-\tau))\quad f(x_2(t-\tau))]^{\mathrm{T}}$，$\boldsymbol{I}=[\boldsymbol{I}_1\quad \boldsymbol{I}_2]^{\mathrm{T}}$，$\boldsymbol{A}=\begin{bmatrix}1&0\\0&1\end{bmatrix}$，$\boldsymbol{B}=\begin{bmatrix}2.0&-0.1\\-5.0&2.0\end{bmatrix}$，$\boldsymbol{C}=\begin{bmatrix}-1.5&-0.1\\-0.2&-1.5\end{bmatrix}$。输入输出函数选定为 $f(x)=\tanh x$，为了研究方便，下文中均令外部输入 $\boldsymbol{I}=0$。当 $\alpha=0.92$，$\tau=1$ 时，系统(6)的混沌吸引子如图 1 所示。

2.2 加密算法

1)加密方确定参数 τ_0，α 及初始值 x_0。

2)用分数阶延时神经网络混沌系统产生一个长度为 $M\times N$ 的混沌序列$\{x_1,x_2,\cdots,x_{M\times N}\}$，对混沌序列进行预处理，$x'_k=\frac{x_k}{\max\limits_{i=1,2,\cdots,M\times N}|x_i|}\times 2.56$，$k=1,2,\cdots,M\times N$，以使其取值范围为$[-2.56,2.56]$，取其绝对值后扩大 100 倍，然后以行序为主序构成矩阵 $\boldsymbol{A}$。

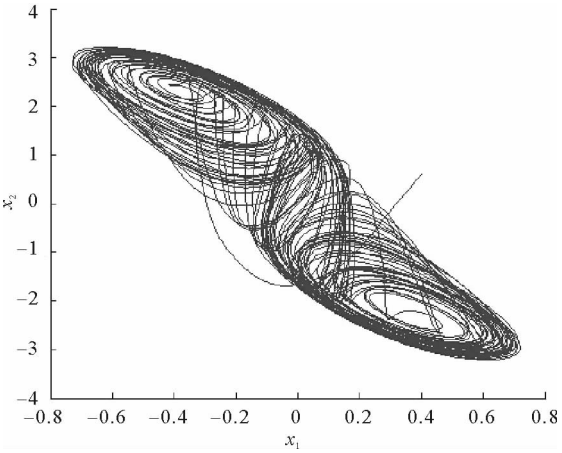


图 1 $\alpha=0.92$ 时分数阶时延神经网络(6)的混沌吸引子

Fig. 1 Chaotic attractor about delayed fractional-order chaotic neural networks when α is equal to 0.92

3)将矩阵 $\boldsymbol{A}$ 的转置与数字图像读取矩阵 $\boldsymbol{B}$ 的每一元素进行按位异或运算得 $\boldsymbol{C}$，因为根据按位异或运算的性质有：$x\oplus y\oplus y=x$，所以解密是容易的。

4)构造等差序列 Y:$\{1,2,\cdots,M\times N\}$，其中，M,N 为数字图像进行矩阵读取后矩阵的维数。将所产生的混沌序列构成的矩阵 $\boldsymbol{A}$ 的 $M\times N$ 个值由大到小进行排序，并对等差序列 Y 进行相应调整为 Y'，以记录其相应位置变化。

5)依据 Y' 对矩阵 $\boldsymbol{C}$ 进行相应调整为 $\boldsymbol{Z}$，其中 $\boldsymbol{Z}$ 是一个 $M\times N$ 的矩阵，即为加密后的图像。

2.3 实验数据

原始图像如图 2 所示。令延时时间 $\tau=1$ s，$\alpha=0.92$，初值条件为 $t\in[-1,0]$，$x_1(t)=0.4$，$x_2(t)=0.6$。应用上述加密算法得到加密图像如图 3 所示，很好地掩盖了原始图像的信息。

图 2　原始图像

Fig. 2　Original image

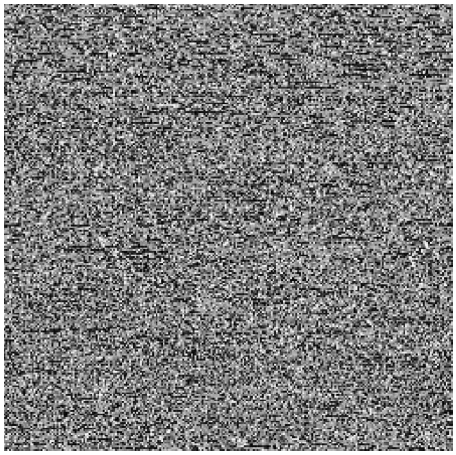


图 3　加密图像

Fig. 3　Encrypted image

3　安全性分析

为了验证该加密算法的安全性，对加密后的图像进行统计分析，对其相关性、信息熵、游程、灰度变化平均值、直方图均衡度、秘钥灵敏度等方面进行对比，观察此加密算法的有效性和安全性。

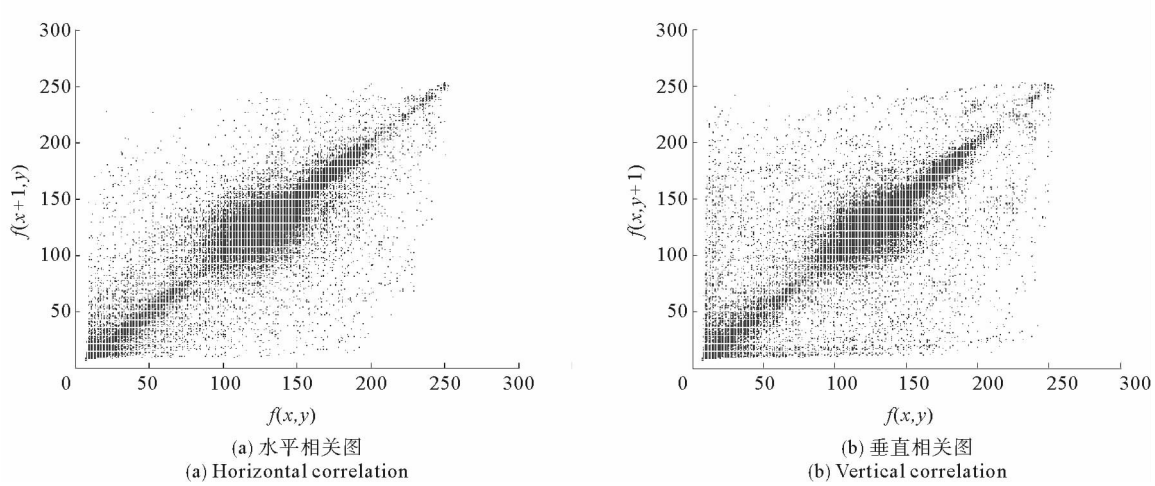
3.1　统计分析

相关性　对于加密后的图像，观察其水平方向和垂直方向各相邻像素之间的相关性。计算公式为：

$$E(x)=\frac{1}{P}\sum_{i=1}^{P}x_i;\ D(x)=\frac{1}{P}\sum_{i=1}^{P}(x_i-E(x))^2;$$

$$\mathrm{cov}(x,y)=\frac{1}{P}\sum_{i=1}^{P}(x_i-E(x))(y_i-E(y));\ \rho_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}}。$$

其中：x 和 y 分别表示两相邻像素值，P 为图像中的总像素值。图 4 表示加密前图像水平方向和垂直方向各相邻像素之间的相关性；图 5 表示加密后图像水平方向和垂直方向各相邻像素之间的相关性。



(a) 水平相关图
(a) Horizontal correlation

(b) 垂直相关图
(b) Vertical correlation

图 4　原始图像的水平相关和垂直相关图

Fig. 4　Horizontal correlation and vertical correlation of original image

信息熵 图像信息熵定义为

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i 。 \quad (7)$$

其中，p_i 表示图像中灰度值为 i 的像素出现的概率，n 为图像的灰度等级。

加密图像的信息熵越大，说明加密图像中灰度分布越均匀，攻击者从加密图像的灰度分布中得到的原图像信息就越少，加密算法的安全性就越高。

游程统计 游程统计量定义为

$$R = \frac{n}{M \times N} = \frac{\sum_{i=1}^{M} n_i}{M \times N}。 \quad (8)$$

其中，n_i 为第 i 行像素中的游程数。游程的定义为一串与像素灰度平均值保持相同大小关系的像素序列。

游程统计量的值增大时，说明灰度图像灰度游程总数 n 在增大，相应的灰度图像中相邻像素之间的灰度取值变化也就越剧烈，图像的混乱程度在增加。

灰度变化平均值 灰度变化平均值定义为

$$G = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} | B(i,j) - a |}{M \times N} 。 \quad (9)$$

其中：a 表示图像所有灰度值的平均值；$B(i,j)$表示原始图像读取矩阵 $\boldsymbol{B}$ 中第 i 行，j 列元素的值。

G 越大说明各像素与像素平均值之间的差距越大，初始图像像素集中区域的隐藏性越好。

直方图均衡度 直方图均衡度定义为

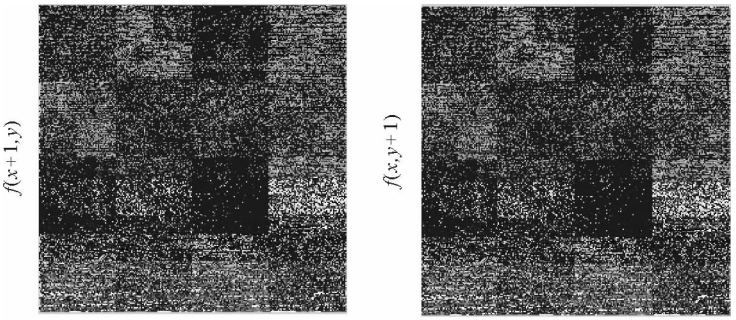
$$F = \frac{\sum_{i=1}^{255} (K(i) - \frac{M \times N}{256})^2}{M \times N} 。 \quad (10)$$

其中，$K(i)$表示灰度值为 i 的像素个数。F 越小，说明灰度直方图的均匀程度越好。

通过对以上统计量的分析，得到加密后图像的各个统计量的数值，与加密前统计量数值进行比较，如表 1 所示。

3.2 鲁棒性分析

为了验证加密算法的鲁棒性，对密文图像进行污损和噪声攻击，实验结果如图 6 所示。加密图像受到涂鸦污染和 5%椒盐噪声污染之后，仍能解密出原始



(a) 水平相关图 $f(x,y)$ (a) Horizontal correlation
(b) 垂直相关图 $f(x,y)$ (b) Vertical correlation

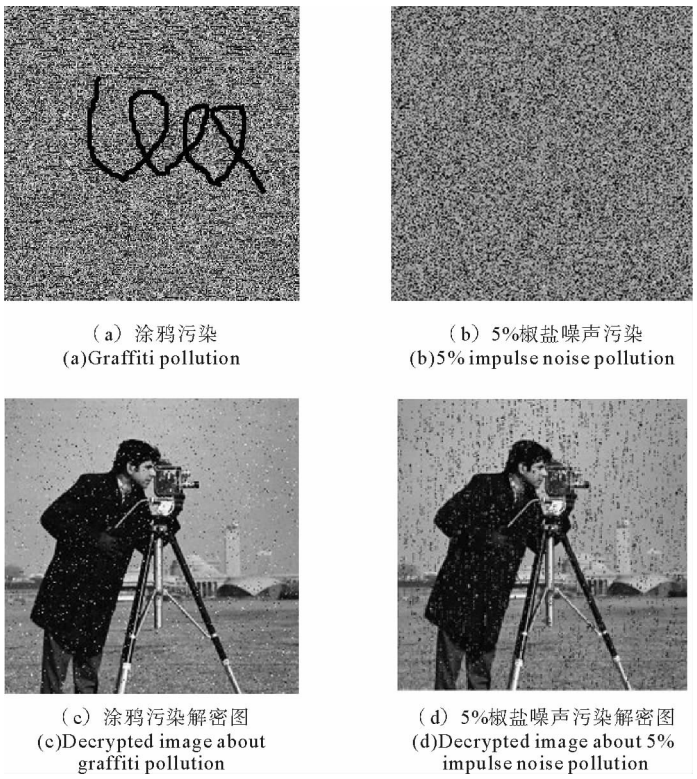
图 5 加密图像的水平相关和垂直相关图

Fig. 5 Horizontal correlation and vertical correlation of encrypted image

表 1 加密前后图像各统计量分析表

Tab. 1 The statistic analysis about original image and encrypted image

统计量对比	H	G	F	R
加密前	4.858 8	0.003 9	433.489 5	0.088 4
加密后	5.474 1	57.264 9	37.014 3	0.444 8



(a) 涂鸦污染 (a)Graffiti pollution
(b) 5%椒盐噪声污染 (b)5% impulse noise pollution
(c) 涂鸦污染解密图 (c)Decrypted image about graffiti pollution
(d) 5%椒盐噪声污染解密图 (d)Decrypted image about 5% impulse noise pollution

图 6 涂鸦污染、噪声攻击及其解密图

Fig. 6 Graffiti pollution, glitch attacks and their decryption figure

图像，表明该算法有较好的鲁棒性。

3.3 密钥灵敏度

在进行解密时，只需解密方知道加密参数 x_0，α 和 τ 的取值即可，而传输过程中加密参数被捕获的概率极小。若取 $x_1(t)=0.400\ 001$，$x_2(t)=0.6$，$\alpha=0.92$，$\tau=1$所得到的破译图像如图 7 所示，完全不同于原始图像。即此种加密算法的密钥空间为 $O(10^{24})$，在无时延 τ 时，分数阶神经网络的密钥空间为 10^{18}，而对于整数阶图像加密算法的密钥空间仅为 10^{12}，由此可见，该系统较整数阶有更大的密钥空间。对于计算速度为每秒 1 000 万亿次的计算机，解密时间为 $10^{12}\ \mathrm{s}\approx 3.17\times10^{4}\ \mathrm{a}$，可见此种加密算法完全有能力克服利用大规模穷尽搜索办法破译图像的弊端。

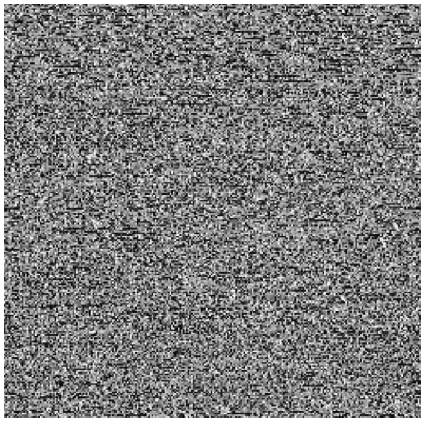


图 7 错误的解密结果图

Fig. 7 Wrong decryption result

4 结束语

提出了一种新的基于分数阶时延神经网络中混沌系统的图像加密方法。在该系统中，不仅将初始值 x_0 作为密钥，阶数 α 和时延 τ 都可以作为密钥，大大增加了密钥空间和破译难度。同时，本研究利用像素异或和置换相结合的方法对原始图像进行加密，该算法中每个明文进行两次加密运算，较好地改变了加密后相邻像素之间的相关性和像素灰度。仿真实验表明，该加密算法具有较好的统计特性、鲁棒性以及密钥敏感性等密码学特性。

参考文献：

[1]李连. 信息安全中的 DES 加密算法[J]. 现代电子技术，2005(9)：118-120.
Li Lian. Information security of DES encryption algorithm[J]. Modern Electronics Technique，2005(9)：118-120.

[2]何明星，林昊. AES 算法原理及其实现[J]. 计算机应用与研究，2002(12)：61-63.
He Mingxing，Lin Hao. AES algorithm principle and implementation[J]. Computer Application and Research，2002(12)：61-63.

[3]廖晓峰，肖迪，陈勇，等. 混沌密码学原理及其应用[M]. 北京：高等教育出版社，2009：38-38.

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

[5]张雪锋，范九伦. 两个新的数字图像加密效果评价准则[J]. 计算机科学，2010，37(2)：264-268.
Zhang Xuefeng，Fan Jiulun. Two new criterion to evaluate the efficacy of the digital image encryption[J]. Computer Science，2010，37(2)：264-268.

[6]Wolfeam S. Cryptography with cellular automata[C]//Lecture Notes in Computer Science，Advances in Cryptology：Proceedings of the Crypto' 85. Berlin：Springer-Verlag，1986，218：429-431.

[7]Hopfield J J. Neural networks and physical system with emergent collective computertational abilities[J]. Proceedings of the National Academy of Sciences，1982，79(2)：2554-2558.

[8]Waibel A，Hanazawa T，Hinton G. Phoneme recognition using time delay neural networks[J]. IEEE Transactions on Acoustics，Speech and Sigual Proceesing，1989，37：328-339.

[9]Butzer P L，Westphal U. An introduction to fractional calculus[M]. Singapore：World Scientific，2000：5-12.

[10]Miller K S，Ross B. An Introduction to the fractional calculus and fractional differential equations[M]. New York：John Wiley & Sons Inc.，1993：80-85.

[11]Oldham K B，Spanier J. The fractional calculus[M]. New York：Academic Press，1974：23-27.

[12]Podlubny I. Fractional differential equations[M]. New York：Academic Press，1999：216-218.

[13]李瑞遐，何庆林. 微分方程数值方法[M]. 上海：华东理工大学出版社，2005：30-33.

[14]Lu H T. Chaotic attractors in delayed neural networks[J]. Physics Letters A，2002，298(2/3)：109-116.

（责任编辑：吕文红）