改进的分块算法在矩形图像加密中的应用*

孙劲光，汪 洁，姜文涛，孟祥福
（辽宁工程技术大学 电子与信息工程学院，辽宁 葫芦岛 125105）

摘 要：为提高图像加密算法抵御穷举攻击、统计分析攻击及差分攻击的能力，提出了一种改进的基于混沌的分块图像加密算法，并用于矩形灰度图像加密。该算法通过对外部密钥分组生成 Logistic 映射初始条件并迭代生成混沌序列，有效增强了密钥的敏感性。提出三向散布并结合像素值替代算法能够明显增强算法抵御差分攻击的能力；同时为增强算法的鲁棒性，采用反馈机制修改密钥。实验结果表明，该算法较二维混沌图像加密具有更高置乱度，且能够有效抵御穷举攻击、统计分析攻击及差分攻击。

关键词：分组密码；混沌序列；差分攻击；三向散布；图像加密
中图分类号：TP309.7 **文献标志码**：A **文章编号**：1001-3695(2013)01-0282-03
doi:10.3969/j.issn.1001-3695.2013.01.072

Application of improved blocking algorithm in rectangle image encryption

SUN Jin-guang, WANG Jie, JIANG Wen-tao, MENG Xiang-fu
(*School of Electronic & Information Engineering, Liaoning Technical University, Huludao Liaoning* 125105, *China*)

Abstract: In order to improve image encryption algorithm resistance ability to exaustive attack, statistical attack and differential attack, this paper put forward a modified block encryption algorithm based on chaos, and applied it to rectangle image encryption. This algorithm generated Logistic initial condition by block external keys and chaotic sequence iterately for strengthening the sensitivity of keys. It proposed three-direction dispersion combined with pixel value substitution algorithm to increase the resistance ability to differential attack obviously. Meanwhile, it used feedback mechanism to modify keys. The results show that it not only has higher scrambling degree than two-dimensional chaotic system of image encryption, but also resists exaustive attack, statistical attack and differential attack effectively.

Key words: block cipher; chaotic sequence; differential attack; three-direction dispersion; image encryption

目前，图像加密技术在许多领域发挥了重要作用，相关算法的研究在近几年显著增加。但图像加密仍面临很多未解决的问题，如果用户破译量化处理的加密矩阵或比较像素值就可以完成图像解密。统计分析攻击和差分攻击的抵御能力是衡量加密算法安全性的重要指标。保障秘密信息在网络通信和信息交换的过程中不被非法者盗用是图像加密技术的重要目的之一，在复杂攻击条件下增强加密算法鲁棒性是一个重要的研究课题。

为提高加密算法的鲁棒性，国内外学者相继提出了许多可行有效的图像加密算法[1~4]，其中经典的方法包括矢量量化(VQ)、对称块加密技术、混沌映射等，它们实现简单，但是抵御穷举攻击的能力较差。近年来许多学者利用混沌[5~7]对初始条件极其敏感等特性进行加密处理，并采用外部密钥扩充密钥量，但这同时带来了计算复杂度较高、置乱效率降低的问题。文献[8]提出基于混淆与扩散相结合的图像加密方案，但若要达到理想加密效果则需较多迭代次数与较长扩散时间。针对该问题，文献[9]提出一种基于三维 Chen 混沌系统的图像分块加密算法，提高了置乱效率，但算法对图像尺寸具有局限性。鉴于此，本文提出了一种适用于矩形图像的改进的分块加密算法。

1 混沌密钥的生成

1)分组密码的生成 首先随机选取 104 bit 外部密钥并分组，k_i 表示一个 4 bit 或 8 bit 密钥组。

$$K_1 = k_1 k_2 \cdots k_{13} (\text{in ASCII}) \tag{1}$$

$$K_2 = k_1 k_2 \cdots k_{26} (\text{in hexadecimal}) \tag{2}$$

将密钥组进一步分组，得到 K_1 的分组密码为

$$B_1 = (k_1, k_2, k_3), B_2 = (k_4, k_5, k_6)$$
$$B_3 = (k_7, k_8, k_9), B_4 = (k_{10}, k_{11}, k_{12}) \tag{3}$$

K_2 的分组密码为

$$B_5 = (k_1, \cdots, k_6), B_6 = (k_7, \cdots, k_{12})$$
$$B_7 = (k_{13}, \cdots, k_{18}), B_8 = (k_{19}, \cdots, k_{24}) \tag{4}$$

2)生成 Logistic 混沌序列密钥 本文采用 Logistic 映射，定义如式(5)所示。

$$x_{n+1} = 3.9999 x_n (1 - x_n) \tag{5}$$

为了计算初始条件 x_0，选择分组密码 B_1、B_6 并转换成二进制，$B_6 = k_{71} k_{72} k_{73} k_{74} k_{81} \cdots k_{84} k_{91} \cdots k_{94} k_{101} \cdots k_{104} k_{111} \cdots k_{124}$，$B_1 = k_{11} k_{12} \cdots k_{18} k_{21} k_{22} \cdots k_{28} k_{31} \cdots k_{38}$。其中，$k_{ij}$ 表示外部密钥第 i 组的二进制值。

$$x_{01} = (k_{11} \times 2^0 + k_{12} \times 2^1 + \cdots + k_{18} \times 2^7 + k_{21} \times 2^8 + k_{22} \times 2^9 + \cdots + k_{28} \times 2^{15} + k_{31} \times 2^{16} + k_{32} \times 2^{17} + \cdots + k_{38} \times 2^{23}) / 2^{24} \tag{6}$$

收稿日期：2012-06-15；**修回日期**：2012-07-26 **基金项目**：国家青年科学基金资助项目(61003162)

作者简介：孙劲光(1962-)，女，教授，博导，主要研究方向为图形图像、数据挖掘；汪洁(1987-)，硕士，主要研究方向为图像加密和数字水印(wj-0126@163.com)；姜文涛(1986-)，博士研究生，主要研究方向为图像与视觉信息计算；孟祥福(1981-)，男，讲师，博士，主要研究方向为 Web 数据库与 XML 个性化柔性查询.

$$x_{02} = \sum_{i=7}^{12}(k_i)_{10}/2^{24} \tag{7}$$

$$x_0(1) = (x_{01} + x_{02}) \bmod 1 \tag{8}$$

$$P_k = \mathrm{int}(31 \times (f_k - 0.1)/0.8 + 1) \tag{9}$$

同理对式(3)(4)采用不同方式组合,计算得到 16 个不同的 x_0,即 $x_0(1), x_0(2), \cdots, x_0(16)$。首先利用式(5)的 Logistic 映射迭代 200 次以去除暂留效应,然后得到随机序列 $\{x_{201}(1), x_{202}(1), x_{201}(2), x_{202}(2), \cdots, x_{201}(16), x_{202}(16)\}$,记做 $\{f_1, f_2, \cdots, f_k, \cdots, f_n \mid f_k \in [0.1, 0.9]\}$。最后利用式(9)将实数转换成整数序列。

2　加密算法描述

2.1　改进的分块加密算法

a)将 256 × 256 的原始图像四等分,分别记做 $I_{lu}^{(1)}(x,y)$、$I_{ru}^{(1)}(x,y)$、$I_{ld}^{(1)}(x,y)$、$I_{rd}^{(1)}(x,y)$(即按照左上、右上、左下和右下方向)。

b)水平散布。根据水平散布函数式(10)将子图像 $I_{lu}^{(1)}(x,y)$、$I_{ld}^{(1)}(x,y)$ 的像素均匀散布到子图像 $I_{ru}^{(1)}(x,y)$、$I_{rd}^{(1)}(x,y)$ 中。$k_i(i=1,2,3,4)$ 表示式(1)中的密钥;结果子图像分别记做 $I_{lu}^{(2)}(x,y)$、$I_{ru}^{(2)}(x,y)$、$I_{ld}^{(2)}(x,y)$、$I_{rd}^{(2)}(x,y)$。

$$\begin{aligned} I_{ru}^{(2)}(x,y) &= I_{ru}^{(1)}(x,y) \oplus \{[k_1 + I_{lu}^{(1)}(x,y)] \bmod 64\} \\ I_{rd}^{(2)}(x,y) &= I_{rd}^{(1)}(x,y) \oplus \{[k_3 + I_{ld}^{(1)}(x,y)] \bmod 64\} \end{aligned} \tag{10}$$

c)垂直散布。利用垂直散布函数式(11)将子图像 $I_{ld}^{(2)}(x,y)$、$I_{rd}^{(2)}(x,y)$ 的像素均匀散布到 $I_{lu}^{(2)}(x,y)$、$I_{ru}^{(2)}(x,y)$ 中,结果子图像记做 $I_{lu}^{(3)}(x,y)$、$I_{ru}^{(3)}(x,y)$、$I_{ld}^{(3)}(x,y)$、$I_{rd}^{(3)}(x,y)$。

$$\begin{aligned} I_{lu}^{(3)}(x,y) &= I_{lu}^{(2)}(x,y) \oplus \{[k_3 + I_{ld}^{(2)}(x,y)] \bmod 64\} \\ I_{ru}^{(3)}(x,y) &= I_{ru}^{(2)}(x,y) \oplus \{[k_4 + I_{rd}^{(2)}(x,y)] \bmod 64\} \end{aligned} \tag{11}$$

d)同理,采用对角线扩散函数式(12)实现该方向散布。

$$\begin{aligned} I_{ld}^{(4)}(x,y) &= I_{ld}^{(3)}(x,y) \oplus \{[k_2 + I_{ru}^{(3)}(x,y)] \bmod 64\} \\ I_{lu}^{(4)}(x,y) &= I_{lu}^{(3)}(x,y) \oplus \{[k_4 + I_{rd}^{(3)}(x,y)] \bmod 64\} \end{aligned} \tag{12}$$

e)三向散布的原理如图 1 所示。根据式(9)转换的 $P_1P_2\cdots P_k$ 值对经过三向散布的子块中每个像素分别执行表 1 定义的替代操作。

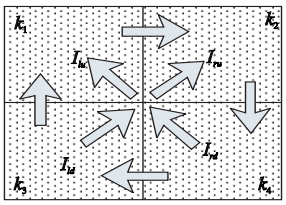

图1　三向散布示意图

表 1　整数序列值及其操作

$P_i \bmod 8 (1 \leqslant P_i \leqslant 32)$	采用的加密操作	$P_i \bmod 8 (1 \leqslant P_i \leqslant 32)$	采用的加密操作
1	循环左移一位 $p_i = p_i << 1$	5	$p_i = \mathrm{not}(p_i) \oplus (k_i \bmod 64)$
2	循环右移一位 $p_i = p_i >> 1$	6	$p_i = \mathrm{not}(p_i \oplus (k_i \bmod 64))$
3	所有位取反 $p_i = \mathrm{not}(p_i)$	7	循环左移一位后取反
4	$p_i = p_i \oplus (k_i \bmod 64)$	0	循环右移一位后取反

完成每个子块的替代操作后利用反馈机制修改密钥 $k_i = (k_i \oplus \overline{I_{i-1}}) \bmod 64, i = 2, \cdots, 5$;$\overline{I_i}$ 为第 i 块所有像素点的均值。

2.2　矩形图像的加密

待加密图像为 $M \times N (M > N)$ 的矩形灰度图像,令变量 J 满足 $0 < J < M, J \in \mathrm{Z}$,加密算法如下:将图像分成若干个 $N \times N$ 的正方形图像,记做 $I_0, I_1, \cdots, I_n$,根据式(13)设置图像的起始像素位置坐标为 $J_0, J_1, \cdots, J_n$。所有正方形图像的组合须涵盖整幅图像,每个像素至少加密一次,依次实现正方形图像的加密。

当 $N \leqslant M \leqslant (a+1)N$ 时

$$J_{a-i} = \begin{cases} 0 & i = a \\ \dfrac{(a-i)(M-N)}{a} & i = 0, 1, \cdots, a-1 \end{cases} \tag{13}$$

矩形加密算法的密钥为 $\mathrm{key}(C, J_0, J_1, \cdots, J_k, \cdots, J_n)$。其中:$C$ 为算法标志,即改进的分块置乱算法;$J_0, J_1, \cdots, J_n$ 为选取的正方形顶点;算法安全性取决于密钥空间的大小;采用 104 bit 外部密钥,即密钥空间为 2^{104}。因此在系统参数未知的情况下可以较好地抵御穷举攻击。

2.3　图像加密算法步骤

a)将矩形图像转换成正方形图像,并对每个正方形图像进行以下加密操作。

b)引入 104 bit 外部密钥,生成分组密码。

c)利用 Logistic 映射生成混沌序列密钥。

d)图像分块并对块进行散布操作,利用 b)生成的整数序列执行替代操作。

e)根据反馈机制完成密钥修改。

图像加密过程如图 2 所示,图像解密与之密钥相同但过程相反。

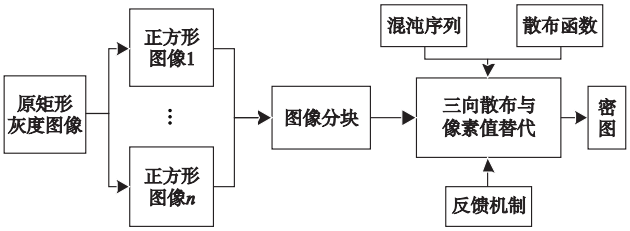

图2　完整的加密算法流程

3　实验与分析

图 3 描述了尺寸为 256 × 210 矩形灰度图像的加密过程。Fruit 灰度图像尺寸 $N < M < 2N < 5N$,根据式(13),计算起始坐标 $H_0 = 0, H_1 = 11.5, H_2 = 23, H_3 = 34.5, H_4 = 46$。

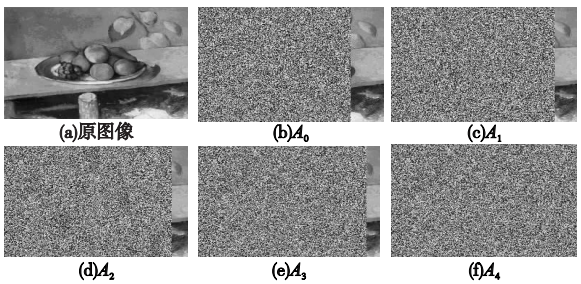

图3　矩形图像的加密效果

图 3(f)为所有正方形密图的混合结果,图像加密强度较大,增强了图像对已知明文攻击和已知密文攻击的能力。

此外,采用四个具有细微差别的密钥获得加密图像 A、B、C、D。通过分析表 2 数据得知本文算法具有较强的密钥敏感性。

key1:C8AD710B42CFD28F39E542BE62

key2:B8AD710B42CFD28F39E542BE62

key3:C8AD710B42CFD28F39E542BE63

key4:C8AD710B42CFE28F39E542BE62

表 2 不同密钥下加密图像的相关系数

方向	Fruit 图像					
	A,*B*	*A*,*C*	*A*,*D*	*B*,*C*	*B*,*D*	*C*,*D*
水平	0.009 40	0.005 90	0.007 45	0.006 74	0.000 82	0.003 30
垂直	0.007 41	0.000 26	0.006 13	0.000 26	0.004 93	0.008 10
对角	0.006 92	0.005 70	0.000 18	0.004 05	0.002 23	0.000 21

加密系统抵御差分攻击能力由算法对明文的敏感性决定，NPCR(net pixel change rate)和 UACI(unified average changing intensity)是衡量加密算法抵御差分攻击能力的重要指标。实验选取 200 组 Fruit 图像进行加密，并与文献[10]算法进行对比，实验数据如表 3 所示。

表 3 NPCR 和 UACI 值

组号	本文算法		文献[10]算法	
	NPCR	UACI	NPCR	UACI
12	0.999 925	0.329 192	0.625 062	0.127 960
42	0.999 936	0.331 547	0.828 510	0.310 526
107	0.999 901	0.342 984	0.881 933	0.256 844
146	0.999 980	0.328 933	0.813 505	0.170 564
189	0.999 250	0.329 432	0.619 974	0.324 885

由表 3 可见，本文算法对明文的敏感性强于文献[10]算法对明文的敏感性。因为文献[10]算法采用异或操作实现像素扩散，容易导致像素扩散不均匀；本文采用了基于分块的三向散布和像素替代相结合的方法，能够明显地消除单向散布中不能解决的相邻像素扩散不均匀现象，明文和基于混沌生成的密钥有效融合，密文达到较好的均匀性和随机性。理论和实验证明该算法具有较强的抵御差分攻击的能力。

为客观评价本文算法应用于图像加密中的有效性，采用正方形图像完成如下实验。

置乱度(SM)能较好反映图像的置乱程度[11]，由图 4 可知，本文算法的置乱度随置乱次数的变化较二维混沌加密算法更加稳定。

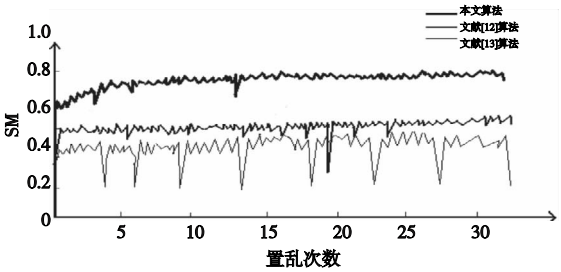

图4 置乱程度比较

统计分析攻击通常采用直方图或像素相关性信息来破译密钥。本文通过计算相关系数来衡量加密算法抵御统计分析攻击的能力，实验数据如表 4 所示。从表中数据可以看出，采用本文算法的密文图像相关系数比文献[13,14]密文图像的相关系数更低，表明本文算法更好地破坏了相邻像素相关性，密文达到了较好的均匀性和随机性。

表 4 相关系数比较

相邻方向	本文算法		文献[13]算法		文献[14]算法	
	Fruit	Lena	Fruit	Lena	Fruit	Lena
水平方向	-0.002 9	0.003 3	0.005 7	-0.010 6	-0.010 7	0.006 6
垂直方向	0.002 4	0.004 6	0.009 3	0.007 1	0.003 7	0.016 5
对角方向	-0.003 8	-0.002 4	-0.016 9	0.012 3	-0.038 1	0.020 4

4 结束语

为提高图像加密算法抵御穷举攻击、统计分析攻击及差分攻击的能力，提出一种改进的分块图像加密算法。利用混沌内在的随机性和对系统参数的敏感性增强算法的加密强度；提出三向散布方法，以降低像素相关性并增强抵御差分攻击的能力；同时采用反馈机制提高算法的鲁棒性。实验表明，该算法有效安全，可用于加密任意尺寸的矩形灰度图像。下一步将针对彩色矩形图像加密作进一步的研究。

参考文献：

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

[2] NAYAK C 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.

[3] PATIDAR V, PUROHIT G, SUD K K, *et al*. Image encryption through a novel permutation-substitution scheme based on chaotic standard map[C]//Proc of International Workshop on Chaos-Fractals Theories and Applications. 2010: 164-169.

[4] 刘金梅, 丘水生, 刘伟平. 基于超混沌系统的图像加密算法的安全性分析[J]. 计算机应用研究, 2010, 27(3): 1042-1044.

[5] YOON J W, KIM H. 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.

[6] JAMEI M K, ENYATIFAR R, HASSANPOUR H. Hybird model of chaotic signal and complete binary tree for image encryption[J]. International Journal of the Physical Sciences, 2011, 6(4): 837-842.

[7] MA Xin, FU Chong, LEI Wei-min, *et al*. A novel chaos-based image image encryption scheme with an improved permutation process[J]. International Journal of Advancements in Computing Technology, 2011, 3(5): 223-233.

[8] GOUMIDI D E, HACHOUF F. Modified confusion-diffusion based satellite image cipher using chaotic standard, Logistic and Sine maps[C]//Proc of the 2nd European Workshop on Visual Information Processing. 2011: 204-209.

[9] PENG Jun, ZHANG Du, LIAO Xiao-feng. A novel algorithm for block encryption of digital image based on chaos[J]. International Journal of Cognitive Informatics and Natural Intelligence, 2011, 5(1): 59-74.

[10] KADIR R, SHAHRIL R, MAAROF M A. A modified image encryption scheme based on 2D chaotic map[C]//Proc of International Conference on Computer and Communication Engineering. 2010: 1-5.

[11] 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.

[12] SATHISHKUMAR G A, BAGAN K B, SRIAAM N. Image encryption based on diffusion and multiple chaotic maps[J]. International Journal of Network Security & Its Applications, 2011, 3(2): 181-194.

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

[14] FATERI S, ENAYATIFAR R. A new method for image encryption via standard rules of CA and Logistic map function[J]. International Journal of Physical Sciences, 2011, 6(12): 2921-2926.