

基于混沌系统的 DNA 图像加密算法

徐光宪, 郭晓娟*

(辽宁工程技术大学 电子与信息工程学院, 辽宁 葫芦岛 125105)

(*通信作者电子邮箱 1070533530@qq.com)

摘要:为了解决数字图像加密算法复杂度、安全性较差的问题,提出一种基于混沌系统的 DNA 融合图像加密算法。首先利用 Baker 变换对图像进行置乱以读取 DNA 序列;再由 Logistic 混沌映射产生混沌序列,从而对 DNA 序列进行混沌加密。该算法对初值具有很好的敏感性,抗统计、抗差分攻击能力强。仿真结果表明:所提算法不仅实现简单,而且加密效果好,安全性高。

关键词:混沌系统;DNA 序列;Baker 变换;Logistic 映射;图像加密

中图分类号: TP309.7 **文献标志码:** A

DNA image encryption algorithm based on chaotic system

XU Guangxian, GUO Xiaojuan*

(School of Electronic and Information Engineering, Liaoning Technical University, Huludao Liaoning 125105, China)

Abstract: In order to solve the problems of digital image encryption algorithm including scheme complexity and poor security, a DNA fusion image encryption algorithm based on chaotic system was proposed. Firstly, the image was scrambled by Baker transform to obtain the DNA sequence. Then, Logistic map was used to generate chaotic sequence. Finally, the DNA sequence was encrypted. The method has good sensitivity to initial values and strong ability of anti-statistical and anti-differential attacks. The simulation results show that the algorithm is not only simple, but also has good encryption effect and high security.

Key words: chaotic system; DNA sequence; Baker transform; Logistic map; image encryption

0 引言

信息化社会的飞速发展使计算机多媒体技术得到了广泛应用。然而,数字媒体的安全却始终是一个亟待解决的问题,尤其针对数字图像而言,如何保证其信息的安全性更是一项重大研究课题。1994 年,Adleman^[1]首次提出 DNA 计算这一思想,为图像加密领域开辟了新的研究方向。而随后的相关研究亦能证明,DNA 计算确实能够很好地解决数字图像的信息安全问题。

2008 年 Gao 等^[2]提出基于多个混沌系统的图像加密算法,该算法实现了像素位置置乱和像素值的变换,提高了算法的安全性;但他们的加密方案被文献^[3]的算法破译。2009 年 Ning^[4]提出了一种伪 DNA 加密算法,该算法实现了信息的有效加密;但这种算法只能运用于文字信息,不能用于加密数字图像信息。2010 年薛香莲^[5]提出了一种基于 DNA 序列与多混沌映射的数字图像加密算法,该算法利用 DNA 序列与 Cubic 映射、Logistic 映射融合加密图像;但是加密后图像的像素相关性高,安全性差,实现过程复杂。2011 年 Zhang 等^[6]提出基于 Hao 分形法的图像加密算法,将 DNA 序列操作应用到加密过程,提高了安全性。2012 年张鑫等^[7]提出基于 Baker 变换的扩频水印算法,利用了 Baker 变换具有置乱周期

长和置乱效果好的优势。2013 年刘乐鹏等^[8]提出了一种改进的数字图像加密算法,该算法有较好的加密效果;但安全性需要进一步提高。

基于上述分析,本文提出一种图像融合加密算法,将 Logistic 混沌映射、Baker 变换与 DNA 序列相结合对数字图像进行加密。本文算法实现简单,加密效果好,能充分保证数字图像加密后安全性高。

1 理论知识

1.1 混沌理论和 Logistic 映射

混沌系统有许多特性,如对初始条件的敏感性被认为是一个加密算法的密钥发生器中的一个基本部分^[9]。Logistic 映射的数学表达形式如下:

$$x_{n+1} = \mu x_n (1 - x_n) \quad (1)$$

其中 $0 \leq \mu \leq 4$ 为分叉参数。混沌动力学的研究表明,在 $3.569\,945\,6 \dots \leq \mu \leq 4$ 时,Logistic 映射为混沌状态。

由此,文献^[8]提出了二维 Logistic 混沌映射,其表达式:

$$\begin{cases} x_{n+1} = \mu \alpha_1 x_n (1 - x_n) + \beta y_n \\ y_{n+1} = \mu \alpha_2 y_n (1 - y_n) + \beta x_n \end{cases} \quad (2)$$

其中: $\mu = 4$, $\beta = 0.1$, $\alpha_1 = \alpha_2 \in [0.65, 0.9]$, 系统进入混沌状态。

收稿日期: 2014-06-05; 修回日期: 2014-07-27。 基金项目: 辽宁省高等学校杰出青年学者成长计划项目(LJQ2012029)。

作者简介: 徐光宪(1977-), 男, 江苏盐城人, 副教授, 博士, 主要研究方向: 网络编码、信息处理; 郭晓娟(1988-), 女, 内蒙古乌兰察布人, 硕士研究生, 主要研究方向: 数字图像处理、信息安全。

1.2 DNA 序列加密

1.2.1 图像的 DNA 编码和解码

一个链 DNA^[10],由四个不同的基本核苷酸组成:腺嘌呤(A)、胸腺嘧啶(T)、胞嘧啶(C)和鸟嘌呤(G),这4种核苷酸能够结合在一起形成一条长序列,且A与T配对,C与G配对。通过规定A、C、G、T分别编码为00,01,10,11,这样的编码方案有24种,但只有8种编码方案满足Watson-Crick规则,如表1。假设规定A-00、T-01、C-10、G-11,如二进制序列10110100,DNA序列可以写成GTCA。

表1 DNA 序列的8种编解码映射规则

核苷酸	编码方案							
	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
C	10	01	11	00	11	00	10	01
G	01	10	00	11	00	11	01	10
T	11	11	10	10	01	01	00	00

1.2.2 DNA 序列的加减代数运算

随着DNA计算的飞速发展,一些研究人员提出基于DNA序列的某些生物学操作和代数运算,如加法运算。DNA序列加法和减法运算是源于在传统二进制中加法和减法^[11]。

对应于8种DNA编码方案,也存在8种DNA加法运算和8种DNA减法运算。如表2~3所示,从中可看出任何一个基因在每行或列中是唯一的,即加法运算和减法运算的结果有且只有一个。

表2 DNA 序列的加法运算

核苷酸	A	G	C	T
A	A	G	C	T
G	G	C	T	A
C	C	T	A	G
T	T	A	G	C

表3 DNA 序列的减法运算

核苷酸	A	G	C	T
A	A	T	C	G
G	G	A	T	C
C	C	G	A	T
T	T	C	G	A

1.3 Baker 变换

Baker变换^[12]是一种将连续的平面区域反复进行拉伸和折叠的变换技术,公式如下:

$$f(x, y) = \begin{cases} (2x, \lambda y), & 0 \leq x \leq 1/2 \\ (2x - 1, \lambda y + 1/2), & 1/2 < x \leq 1 \end{cases} \quad (3)$$

由于Baker变换的拉伸与折叠性以及图像的点阵特征,对数字图像进行置乱时,首先对图像 $G_{n \times m}$ 的各个像素按照混

沌随机序列进行两两配对,依次记为 $a(1), a(2), \dots, a(n)$,其中 $a(1) = 1, a(i)$ 与 $a(i-1)$ 进行配对(其中 i 为奇数)且 $a(1) < a(3) < \dots < a(n/2)$;其次对已经配对后的两行进行拉伸和折叠操作,其公式为:

$$F(r(i, j)) = \begin{cases} (i, 2j - 1), & i = 2\lambda, 1 < j \leq m/2 \\ (i - 1, 2j), & i = 2\lambda + 1, 1 \leq j \leq m/2 \\ (i - 1, 2n - 2j + 2), & i = 2\lambda, m/2 < j \leq m \\ (i, 2n - 2j + 1), & i = 2\lambda - 1, m/2 < j \leq m \end{cases} \quad (4)$$

其中 $\lambda = 1, 2, \dots, n/2$ 。Baker变换如图1所示。

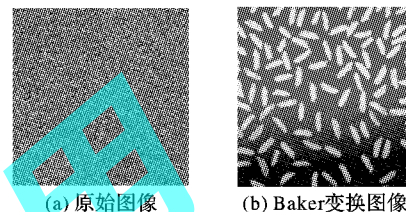


图1 Baker 变换

与Arnold置乱算法相比,Baker变换最大优点^[7]在于:Baker变换的置乱周期比较长;只需进行很少的变换次数就可以达到很好置乱效果;算法操作简便,运算速度快,而且图像的保密效果好。

2 加密方案设计

1) 设原图像为 G ,大小为 $N = a \times b$,则图像 G 表示为: $G = F(i, j)$ 。其中: $0 \leq i \leq a; 0 \leq j \leq b; (i, j)$ 表示像素点位置, $F(i, j)$ 表示该点处图像数据,则 $F(i, j)$ 可构成图像矩阵。

2) 根据内部设定的参数由式(3)构造二维Baker映射,然后由式(4)将图像矩阵进行置乱。

3) 置乱后的矩阵转变为相应的二进制序列,二进制序列编码为A、T、C、G分子表示序列,利用表1的方案2进行编码。

4) 给定参数 μ 值和初值 x_0, y_0 ,通过二维Logistic映射得到混沌序列 s_1, s_2 。

5) 利用索引函数对混沌序列 s_1, s_2 进行操作,排序的索引函数公式如下:

$$[ls_1 \quad fs_1] = \text{sort}(s_1) \quad (5)$$

其中: fs_1 是把 s_1 升序排列后的新序列, ls_1 是 s_1 的索引值。

6) 选择 s_1, s_2 的索引值组合通过表2进行加法运算。

7) 在图像加密的最后一步,DNA序列转变为二进制序列,再变为二进制矩阵,然后就得到了加密图像。

解密图像是加密图像的逆过程,需知道图像的置乱周期和DNA序列加密运用的减法运算和加法运算表才可解密图像。

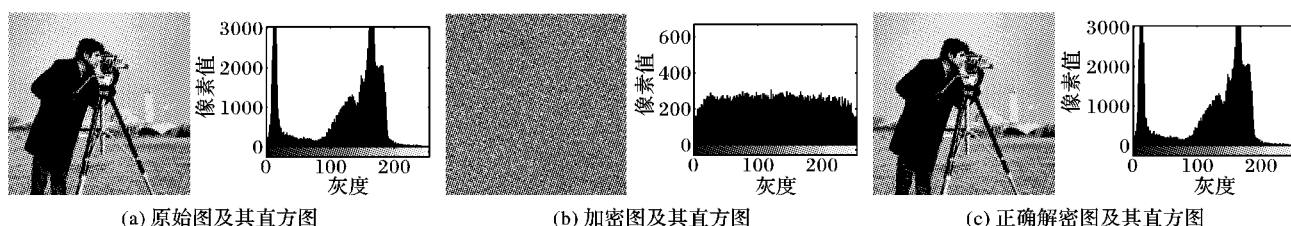


图2 加解密仿真结果

3 仿真结果及安全性分析

3.1 仿真结果

在产生混沌序列时用 501 次以后迭代形成的混沌序列,可以增加混沌序列的复杂性和提高加密安全性。如图 2 给出了仿真结果图及直方图。

3.2 统计特征分析

1) 直方图。

由图 2(a)、(b) 的直方图,图像加密前后的灰度分析,像素分布很均匀,与原图差别很大。

2) 相邻像素相关性。

相关系数的计算公式^[13]如下:

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \tag{6}$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N [x_i - E(x)]^2 \tag{7}$$

$$Cov(x, y) = \frac{1}{N} \sum_{i=1}^N [x_i - E(x)][y_i - E(y)] \tag{8}$$

$$g_{xy} = \frac{Cov(x, y)}{\sqrt{D(x)} \sqrt{D(y)}} \tag{9}$$

其中: x 和 y 分别代表图像中相邻 2 个像素值,且 g_{xy} 为相邻 2 个像素的相关系数。随机选取明文和密文中的相邻 1 000 对像素,计算相关系数,如表 4 及图 3 所示。

表 4 相邻像素相关性比较

相关系数	原始图像	Baker 置乱图像	加密图像
垂直方向	0.956 39	0.157 8	0.014 544
水平方向	0.948 03	0.210 3	-0.095 345
对角方向	0.903 27	0.055 1	0.005 915

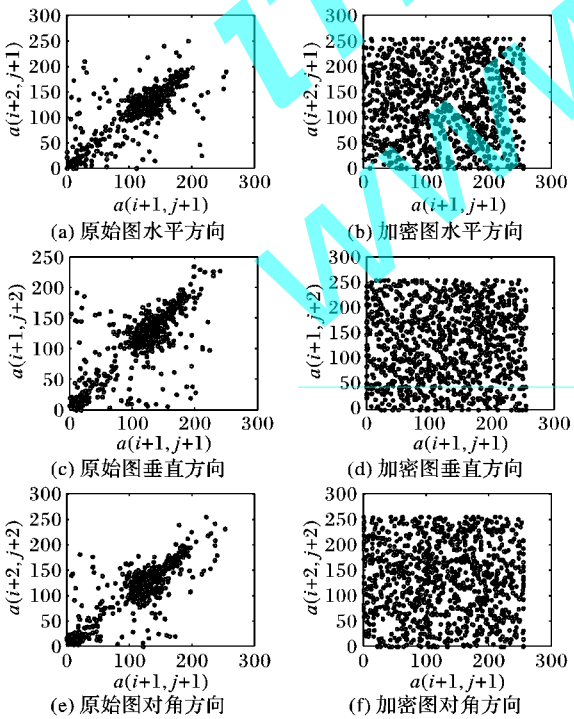


图 3 垂直、水平及对角方向相邻像素的相关性比较

3.3 敏感性分析

对一幅大小为 256 × 256 的图像进行测试。设置密钥参

数 $x_0 = 0.3, y_0 = 0.3, \mu = 4, \alpha_1 = \alpha_2 = 0.798\,171$ 。如图 4 所示,在解密过程中,只有 0.000 000 01 的差别,也不能恢复出原图像。

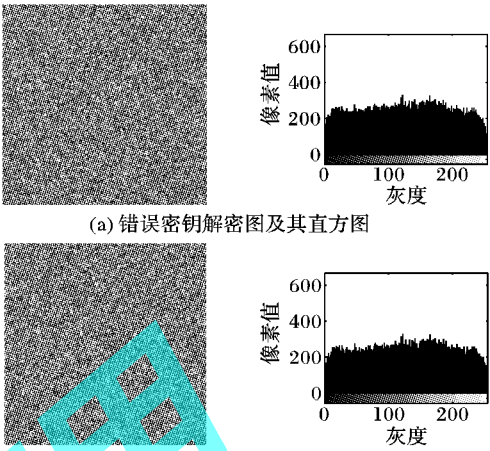


图 4 密钥敏感度对比

3.4 明文敏感性分析

差分攻击:原图像的一个微小改变能引起加密图像的巨大变化,攻击者能获得原始图像与加密图像之间的联系。通过 NPCR (Number of Pixel Change Rate) 与 UACI (Unified Average Changing Intensity) 来衡量^[14]。公式如下:

$$NPCR = \frac{\sum_y D(i, j)}{m \times n} \times 100\% \tag{10}$$

$$UACI = \frac{1}{m \times n} \left[\sum_y \frac{|C_1(i, j) - C_2(i, j)|}{255} \right] \times 100\% \tag{11}$$

其中: m, n 分别表示图像的行和列, C_1 与 C_2 分别为仅改变原图像的一个像素值而得到的不同加密图, $C_1(i, j)$ 与 $C_2(i, j)$ 表示在 (i, j) 坐标上的像素值。

由计算可知 NPCR 和 UACI 值如表 5 所示。可以了解到只要原图像发生微小的改变,会使加密图像接近 100% 的 NPCR 发生变化,加密后的图像平均变化在 30% (UACI) 以上。同时也说明明文图像的信息很好地扩散到了密文图像中,相比文献[6,8]算法具有很好的明文敏感性,对差分攻击有很好的鲁棒性。

表 5 Camera 图像明文敏感性分析比较

算法	NPCR	UACI
本文算法	99.71	36.87
文献[6]算法	89.19	31.22
文献[8]算法	90.77	28.96

4 结语

利用 Baker 变换置乱周期长与变换次数少、Logistic 映射的伪随机性与对初值的敏感性以及 DNA 序列算法加密简单且安全性好的优势,提出了一种新型的融合图像加密算法。本文算法克服了传统 Logistic 映射的安全性低及文献[6]和[8]复合加密算法的复杂性,算法思想及实现简单,加密效果好。同时,从仿真可知,该算法确保了安全性和有效性且有较强的鲁棒性。

(下转第 3183 页)

归纳的结果。但是,由于 EGG 使用边作为上下文,在文法的形式化上和产生式的形式上都与 RGG 不同。本文根据 EGG 的这一重要特性,推导出基于 EGG 的产生式选择无关条件。当 EGG 的产生式满足选择无关条件时,归纳的时间复杂度为多项式级的。

参考文献:

- [1] PFALTZ J, ROSENFELD A. Web grammars[EB/OL]. [2010-10-10]. <http://ijcai.org/Past%20Proceedings/IJCAI-69/PDF/054.pdf>.
- [2] ECONOMAKOS G, PAPA-KONSTANTINOU G, TSANAKAS P. An attribute grammar approach to high-level automated hardware synthesis[J]. Information and Software Technology, 1995, 37(9): 493 – 502.
- [3] COURCELLE B. An axiomatic definition of context-free rewriting and its application to NLC graph grammars[J]. Theoretical Computer Science, 1987, 55(2/3): 141 – 181.
- [4] ADACHI Y, KOBAYASHI S, TSUCHIDA K, *et al.* An NCE context-sensitive graph grammar for visual design languages[C]// Proceedings of the 1999 IEEE Symposium on Visual Languages. Piscataway: IEEE Press, 1999: 228 – 235.
- [5] JANSSENS D, ROZENBERG G. Graph grammars with neighbourhood-controlled embedding[J]. Theoretical Computer Science, 1982, 21(1): 55 – 74.
- [6] Le METAYER D. Describing software architecture styles using graph grammars[J]. IEEE Transactions on Software Engineering, 1997, 24(7): 521 – 533.
- [7] ZHAO C, KONG J, DONG J, *et al.* Pattern based design evolution using graph transformation[J]. Journal of Visual Languages and Computing, 2007, 18(4): 378 – 398.
- [8] DONG J, YANG S, ZHANG K. Visualizing design patterns in their applications and compositions[J]. IEEE Transactions on Software Engineering, 2007, 33(7): 433 – 453.
- [9] FLASINSKI M. Power properties of NLC graph grammars with a polynomial membership problem[J]. Theoretical Computer Science, 1998, 201(1/2): 189 – 231.
- [10] MARRIOTT K. Constraint multiset grammar[C]// Proceedings of the 1994 IEEE Symposium on Visual Languages. Piscataway: IEEE Press, 1994: 118 – 125.
- [11] GOLIN E J. A method for the specification and parsing of visual language[D]. Providence: Brown University, 1991.
- [12] REKERS J, SCHÜRR A. Defining and parsing visual languages with layered graph grammars[J]. Journal of Visual Languages and Computing, 1997, 8(1): 27 – 55.
- [13] ZHANG D, ZHANG K, CAO J. A context-sensitive graph grammar formalism for the specification of visual languages[J]. The Computer Journal, 2001, 44(3): 186 – 200.
- [14] KONG J, ZHANG K, ZENG X. Spatial graph grammars for graphical user interfaces[J]. ACM Transactions on Computer-Human Interaction, 2006, 13(2): 268 – 307.
- [15] ZENG X, HAN X, ZOU Y. An edge-based context-sensitive graph grammar formalism[J]. Journal of Software, 2008, 19(8): 1893 – 1901. (曾晓勤, 韩秀清, 邹阳. 一种基于边的上下文相关图文法形式化框架[J]. 软件学报, 2008, 19(8): 1893 – 1901.)

(上接第 3179 页)

参考文献:

- [1] ADLEMAN L M. Molecular computing of solutions to combinatorial problems[J]. Science, 1994, 266(5187): 1021 – 1024.
- [2] GAO T, CHEN Z. Image encryption based on a new total shuffling algorithm[J]. Chaos, Solitons and Fractals, 2008, 38(1): 213 – 220.
- [3] ARROYO D, LI C Q, LI S J, *et al.* Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm[J]. Chaos, Solitons and Fractals, 2009, 41(5): 2613 – 2616.
- [4] NING K. A pseudo DNA cryptography method[EB/OL]. [2012-10-10]. <http://arxiv.org/pdf/0903.2693v1.pdf>.
- [5] XUE X. Research on digital image encryption based on DNA sequence and multi-chaotic maps[D]. Dalian: Dalian University, 2010. (薛香莲. 基于 DNA 序列与多混沌映射的数字图像加密技术研究[D]. 大连: 大连大学, 2010.)
- [6] ZHANG Q, ZHOU S, WEI X. An efficient approach for DNA fractal-based image encryption[J]. Applied Mathematics and Information Sciences, 2011, 5(3): 445 – 459.
- [7] ZHANG X, XU G, FU X. Research on spread spectrum watermarking algorithm resisting image-cropping based on baker's transformation[J]. Application Research of Computers, 2012, 29(6): 2246 – 2248. (张鑫, 徐光宪, 付晓. 基于面包师变换的抗剪切扩频水印算法研究[J]. 计算机应用研究, 2012, 29(6): 2246 – 2248.)
- [8] LIU L, ZHANG X. Image encryption algorithm based on chaos and bit operations[J]. Journal of Computer Applications, 2013, 33(4): 1070 – 1073, 1099. (刘乐鹏, 张雪峰. 基于混沌和位运算的图像加密算法[J]. 计算机应用, 2013, 33(4): 1070 – 1073, 1099.)
- [9] JIANG J, YIN Z. The advantages and disadvantages of DNA password in the contrast to the traditional cryptography and quantum cryptography[J]. Science and Technology Vision, 2012(24): 24 – 27. (蒋君, 殷志祥. DNA 密码对比传统密码学与量子密码学的优势与不足[J]. 科技视界, 2012(24): 24 – 27.)
- [10] RAHIMOV H, BABAEI M, HASSANABADI H. Improving middle square method RNG using chaotic map[J]. Applied Mathematics, 2011, 2(4): 137 – 141.
- [11] SADEG S, GOUGACHE M, MANSOURI N, *et al.* An encryption algorithm inspired from DNA[C]// Proceedings of the 2010 International Conference on Machine and Web Intelligence. Piscataway: IEEE Press, 2010: 344 – 349.
- [12] BAO G, JI S, SHEN J. Magic cube transformation and its application in digital image encryption[J]. Journal of Computer Applications, 2002, 22(11): 23 – 25. (鲍官军, 计鸣, 沈建冰. 魔方变换及其在数字图像加密中的应用[J]. 计算机应用, 2002, 22(11): 23 – 25.)
- [13] HAN F, ZHU C, HU Y. New colour image encryption algorithm based on high-dimension chaotic system[J]. Journal of Computer Applications, 2007, 27(8): 1888 – 1890. (韩凤英, 朱从旭, 胡玉平. 一种基于高维混沌系统的彩色图像加密新算法[J]. 计算机应用, 2007, 27(8): 1888 – 1890.)
- [14] HUANG J. Research on the secure chaos-based image encryption algorithm[D]. Changsha: Changsha University of Science and Technology, 2010. (黄金. 安全混沌图像加密算法的研究[D]. 长沙: 长沙理工大学, 2010.)