

文章编号:1001-9081(2009)11-2993-05

基于双混沌互扰系统的图像加密算法

胡勇辉, 李星野

(上海理工大学 管理学院, 上海 200093)

(jiangxi. hyh@163.com)

摘要:针对低维混沌系统有可能退化为周期问题,以及高维混沌系统计算量大的缺陷,提出基于双混沌互扰系统的图像加密算法。通过两个简单的 Logistic 映射间的互扰,构造一个双混沌互扰系统。双混沌互扰系统的最大特点是扰动项同时包括常数扰动项和随机扰动项,不仅保证了系统必要的复杂性,而且增大了系统参数的取值范围。以双混沌互扰系统作为序列密钥发生器,提出一种改进的二值序列量化方法。对二值序列做随机性检验和相关性分析的结果表明,该二值序列具有良好的伪随机性和相关性,适合作为加密密钥。将其应用于图像加密的仿真实验结果也表明,该二值序列能有效且安全地掩盖明文信息,取得了较好的加密效果。

关键词:Logistic 映射; 混沌互扰系统; 二值序列; 伪随机序列

中图分类号: TP309 文献标志码:A

Image encryption algorithm based on inter-perturbation of dual chaotic systems

HU Yong-hui, LI Xing-ye

(School of Business, University of Shanghai for Science and Technology, Shanghai 200093, China)

Abstract: An image encryption algorithm based on inter-perturbations of dual chaotic systems was proposed for the possible degradation of low-dimensional chaotic system and the high computing work of high-dimensional chaotic system. Dual chaotic system was constructed through inter-perturbations of two simple Logistic mappings. And the most prominent feature of inter-perturbations between chaotic systems was that perturbation included constant perturbation and random perturbation simultaneously, which not only ensured the necessary system complexity, but also increased the range of system parameters. Taking dual chaotic inter-perturbed system as sequence key generator, an improved quantization method for converting chaotic sequence to binary sequence was put forward. Random testing and correlation analysis were done on binary sequence. The results show that the binary sequence has good pseudo-randomness and correlation, and appropriate to be encryption key. Simulation results of image encryption applied with the binary sequence also show that the binary sequence can cover up plaintext effectively and safely, and good encryption results are achieved.

Key words: Logistic mapping; chaotic inter-perturbed system; binary sequence; pseudo random sequence

0 引言

混沌^[1]是一种貌似无规则的运动,在确定性非线性系统中,不需要任何外在因素即可出现类似随机的行为。混沌系统的演化对初始条件十分敏感,具有混沌序列的遍历特性,其吸引子的维数是分维,有着十分复杂的分形结构,因此经过长期演化后,系统将是不可预测的。由于混沌序列有如此特性,非常适合作为加密密钥,而混沌密码学也已成为现代密码学的重要研究内容。自从 1989 年首次以 Logistic 映射作为序列密钥发生器用于信息加密以来,低维混沌系统用于信息加密已得到广泛研究。但低维混沌系统有动力学特性相对简单、确定序列参数太少、密钥空间容量小、安全性不高等缺陷。有效的解决方法是采用超混沌系统(至少有两个混沌系统)作为密钥发生器,超混沌系统轨道不稳定方向越多,随机性越强,抗破译能力越高,增大了密钥空间。文献[2]中首先应用 Hyperhenon 映射产生混沌序列对明文图像置换加密,接着应用 Kawakami 映射产生的混沌序列对置换后的密文图像做魔方置乱,得到最终密文图像。文献[3]中结合 Logistic 映射和

分段线性混沌映射(Piecewise Linear Chaotic Map, PLCM),采用定义区间上的移位映射作为混沌随机数发生器,通过不同混沌系统迭代,增强了系统的复杂性。文献[4]中则采用四维混沌系统作为密钥发生器。以上的算法大部分是通过增加混沌系统的个数或是应用高维混沌系统来产生混沌序列。实际上增加系统的复杂度能增大混沌序列的复杂性,但是能否增加混沌序列的随机性还有待进一步研究。最近研究发现,简单混沌系统间的互扰能改变混沌系统的复杂性,更不易预测。文献[5]中利用两个混沌系统通过对序列值和控制参数的扰动产生混沌序列。但这种扰动过于简单,扰动方式也过于单一。

本文采用了两个简单一维 Logistic 映射来实现混沌系统间的互扰,以此来解决低维混沌系统的动力学特性简单、密钥空间容量小、安全性不高等缺陷。混沌系统间互扰的最大特点是扰动项同时包括常数扰动项和随机扰动项,而随机扰动项的随机性由文献[6]中的二值序列量化算法决定,即将混沌序列值与混沌序列的平均值相比较来决定系统间的随机扰动。由文献[4]中量化算法得到的二值序列具有良好的随机

收稿日期:2009-05-27;修回日期:2009-07-29。 基金项目:上海市教育委员会科研项目(07ZZ94);上海市重点学科项目(S30501)。

作者简介:胡勇辉(1984-),男,江西高安人,硕士研究生,主要研究方向:数字图像处理、数字水印; 李星野(1958-),男,辽宁葫芦岛人,教授,主要研究方向:控制系统与建模、系统工程。

性,但该量化算法过于复杂,效率也很低,混沌序列中的 1 个实数值只能转换成二值序列中的 1 个 0、1 值,称之为一次一密。本文以双混沌互扰系统作为序列密钥发生器,由双混沌互扰系统产生混沌实值序列,并给出了一种改进的二值序列量化方法,将混沌实值序列转换成二值序列,而且混沌序列中的 1 个实数值就能转换成二值序列中的 8 个 0、1 值,称之为一次多密,密钥生成效率明显提高。试验结果表明该方法生成的二值序列具有良好的伪随机性和相关性,非常适合做加密密钥。将二值序列应用图像加密中,加密效果明显,密文图像的像素灰度值明显变得均匀,仿真实验结果也表明,该算法具有较高的安全性和较好的加密效果。

1 双混沌系统互扰方案及混沌实值序列生成

文献[7]中指出,在生态学中一些非常简单的确定性的数学模型却能产生看似随机的行为。如:

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

称之为人口方程,即著名的 Logistic 模型。其中 $x_n \in (0,1)$, 当控制参数 $3.569946\cdots \leq \mu \leq 4$ 时, Logistic 映射表现出混沌的特性。

1.1 双混沌系统互扰方案

从两个简单的 Logistic 映射混沌系统模型出发,设计混沌系统互扰方案,迭代映射如下:

$$\begin{cases} x(n+1) = (\mu_1 x(n)(1 - x(n)) + \\ cr_1 + sr_1(n+1)) \bmod 2 \end{cases} \quad (1)$$

$$\begin{cases} x(1) = x_0 \bmod 2 \\ y(n+1) = (\mu_2 y(n)(1 - y(n)) + \\ cr_2 + sr_2(n+1)) \bmod 2 \end{cases} \quad (2)$$

$$y(1) = y_0 \bmod 2$$

其中: \bmod 为求余运算; x_0, y_0 为混沌的初始值; cr_1, cr_2 为常数,称之为常数扰动项; $sr_1(n+1), sr_2(n+1)$ 为随机扰动项; μ_1, μ_2 是混沌系统的控制参数。

$$sr_1(n+1) = \begin{cases} \text{floor}(y(n) \times 10^{m1}) \times 10^{-n1}, & x(n) \geq \text{mean}(x) \\ 0, & \text{其他} \end{cases}$$

$$sr_2(n+1) = \begin{cases} \text{floor}(x(n) \times 10^{m2}) \times 10^{-n2}, & y(n) \geq \text{mean}(y) \\ 0, & \text{其他} \end{cases}$$

其中: floor 是向下取整运算; mean 是序列平均值; $m1, n1, m2, n2$ 为随机扰动项的控制参数。随机扰动项的随机性由混沌序列本身决定^[6],即将混沌序列值与混沌序列的平均值相比较。

当系统参数 $cr_1 = e^{0.3}, cr_2 = e^{0.4}, m1 = m2 = 2, n1 = n2 = 8$ 时,初值 $x_0 = 0.1, y_0 = 0.2$ 。Logistic 映射是在初始值

$x_0 \in (0,1)$, 控制参数 $3.569946\cdots \leq \mu \leq 4$ 条件下才出现混沌现象,但在本文的双混沌互扰方案中,对初始值的取值范围没有任何限制,混沌系统互扰映射在控制参数 $\mu_1 > 2, \mu_2 > 2$ 时各自都出现混沌现象, $x, y \in (0,2)$, 如图 1 的分岔图所示。

通过混沌系统间的扰动后,双混沌互扰系统变得更复杂,更加不可预测。与常用的超混沌系统和高维混沌系统相比,本文构造的双混沌互扰系统具有以下优势:1) 构造混沌互扰系统时,可以任意选择相同或不同的多个混沌系统(不只限于两个混沌系统),构造方法灵活,且易于实现;2) 随机扰动项的随机性可以人为地控制,在不知道随机扰动项的随机性如何决定的情况下,对破译者来说亦增加了难度;3) 增加了系统参数的个数,扩展了初始条件的取值范围,进一步增大了密钥空间,安全性得到提高。

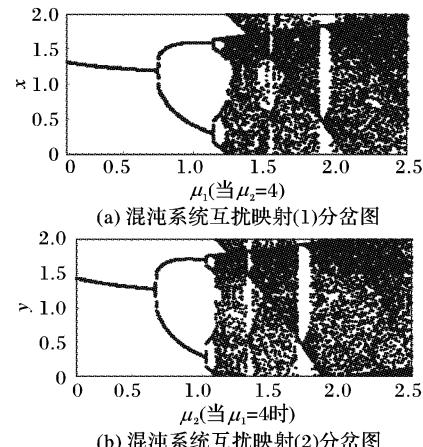


图 1 混沌系统互扰映射分岔图

1.2 混沌实值序列的产生

由两个简单的 Logistic 映射混沌系统经过常数扰动和随机扰动后,得到两个混沌序列分别为: $\{x: x^1, x^2, x^3, \dots, x^n\}$, $\{y: y^1, y^2, y^3, \dots, y^n\}$, 其中 n 为序列的长度。

定义 1 用于产生二值序列的混沌序列 z 为:

$$z(i) = \begin{cases} x(1000+j), & i = 2j-1 \\ y(1000+j), & i = 2j \end{cases}$$

式中 $j = 1, 2, 3, \dots$

最终混沌序列 z 是由 Logistic 映射互扰后得到的混度序列 $\{x: x^1, x^2, x^3, \dots, x^n\}, \{y: y^1, y^2, y^3, \dots, y^n\}$ 交叉组合而成,为了消除初始值对混沌序列过渡部分的影响,选取迭代 1000 次后的序列值构成最终混沌序列 z 。

当参数为 $\mu_1 = 60, \mu_2 = 70, cr_1 = e^{0.3}, cr_2 = e^{0.4}, m1 = m2 = 2, n1 = n2 = 8$, 初值 $x_0 = 0.1, y_0 = 0.2$ 时, 系统参数不变,只是初始值 x_0 或 y_0 发生 0.000 001 的微小变化,得到的混沌序列的差异相当明显。实验中选取了混沌序列的前 40 个序列值对比,如图 2 所示。

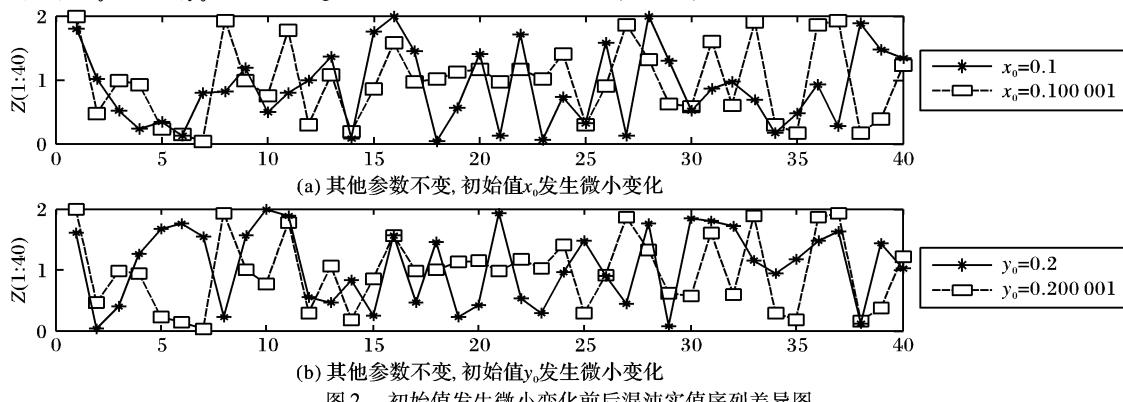


图 2 初始值发生微小变化前后混沌实值序列差异图

图 2 中, 实线表示的是初始值未发生变化的混沌序列值, 虚线表示的是初始值发生 0.000 001 微小变化后的混沌序列值, 实验结果也表明了由双混沌互扰系统产生的混沌序列对初始值具有十分的敏感性。

2 混沌二值序列的产生

由混沌实值序列转换为二进制序列的方法有多种。文献[6]中将混沌序列值与混沌序列平均值进行大小比较, 然后量化成 0,1 二值序列。文献[8]中用混沌系统生成两个混沌序列, 比较两个序列对应项的大小, 然后量化成 0,1 二值序列。文献[4]中基于一个四维混沌系统生成四个混沌序列, 将混沌序列划分小区间, 接着在小区间内取平均值后与 0 比较小, 然后量化成二值序列。

本文采取的二值量化算法如下:

- 1) 设定双混沌互扰系统的初始值 x_0, y_0 , 经过系统迭代映射产生混沌序列 z ;
- 2) 提取混沌序列 z 中每个混沌实值小数部分的 2、4、6 位, 组成一个新的 3 位整数, 比如: $0.372\ 685\ 189 \rightarrow 765$, 由这些整数组成新的整数序列 I' ;
- 3) 将整数序列对 256 求余预算, 即 $I' = \text{mod}(I, 256)$, 比如 $765 \rightarrow 253$, 这样就得到一个新的整数序列 I' , 且序列 I' 每个值都在区间 $[0, 255]$;
- 4) 将得到的整数序列 I' 转换成二进制序列 $\{I': 253 \rightarrow 11111101\}$, 这样就完成了由混沌序列 z 到二值序列 S 的转换;

所得到的整数序列 I' 的直方图如图 3 所示。

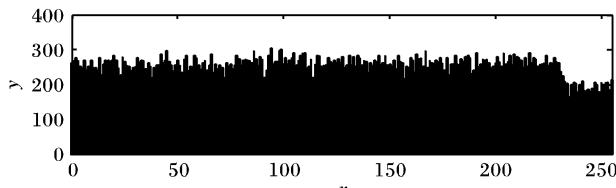


图 3 混沌序列转换成整数序列 I' 的直方图

可以看出, 整数序列 I' 中分布不够均匀, 区间 $[225, 255]$ 的数明显偏少, 这将影响图像加密效果。因此对量化算法进行改进, 改进的量化算法如下:

- 1) 设定双混沌互扰系统的初始值 x_0, y_0 , 经过系统迭代映射产生混沌序列 z ;
- 2) 提取混沌序列 z 中每个混沌实值小数部分的 2、4、6 位, 组成一个新的 3 位整数, 比如: $0.372\ 685\ 189 \rightarrow 765$, 由这些整数组成新的整数序列 I_1 ; 提取混沌序列 z 中每个混沌实值小数部分的 3、5、7 位, 组成一个新的 3 位整数, 比如: $0.372\ 685\ 189 \rightarrow 281$, 由这些整数组成新的整数序列 I_2 ;
- 3) 将整数序列 I_1, I_2 分别对 256 求余预算, 即 $I'_1 = \text{mod}(I_1, 256)$, 比如 $765 \rightarrow 253$; $I'_2 = \text{mod}(I_2, 256)$, 比如 $281 \rightarrow 25$ 。这样就得到两个新的整数序列 I'_1, I'_2 , 且序列 I'_1, I'_2 的每个值都在区间 $[0, 255]$ 内;
- 4) 将得到的整数序列 I'_1, I'_2 的每个整数都转换成二进制, 例如 $\{I'_1: 253 \rightarrow 11111101\}, \{I'_2: 25 \rightarrow 00011001\}$ 。分别提取二进制序列后面 4 位交叉排列, 组成新的二进制序列 S , 那么就有 $\{S: 1101 \oplus 1001 \rightarrow 11100011\}$, 以及与二值序列 S 对应的整数序列 I ;

改进后得到的二值序列转换成整数序列 I 的直方图如图 4 所示。可以看出, 改进后得到的整数序列 I 更加均匀。

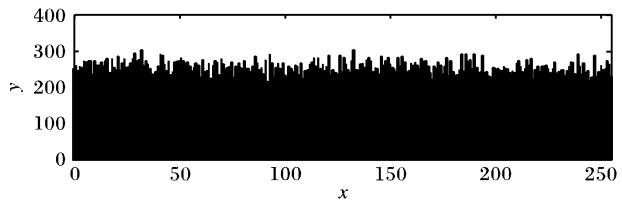


图 4 改进后的混沌序列转换成整数序列 I 的直方图

3 混沌伪随机二值序列的随机性分析

根据 Shannon 理论, 若加密密码序列是完全随机的, 则该加密系统是不可破解的。在数字实现方式下, 由于存在有限精度效应, 得到的序列密码并非完全随机的, 是伪随机序列。为了确保混沌伪随机二值序列 S 可以作为安全的加密密钥, 需要通过随机性检验。

1) 频数检验。频数检验是用来测试序列中是否有大致相同数量的 0,1。设序列中 0 的个数为 n_0 , 1 的个数为 n_1 , 序列的长度为 n ($n = n_0 + n_1$)。计算检验统计量:

$$\chi^2 = (n_0 - n_1)^2 / n$$

将计算值与自由度为 1, 在检验的显著性水平下 $\alpha = 0.95$ 的 χ^2 分布, $\chi_{\alpha}^2(1) = 3.841$ 相比, 如小于则通过检验。

2) 扑克检验。扑克检验用来测试不同组合出现是否均匀及各自的频数。将序列划分为长度为 p 的分组, 则序列有可能出现 2^p 种排列方式。在加密过程中通常采用的单位是字节。所以实际试验中取 $p = 8$, 设各种组合出现的频数为: $\lambda_0, \lambda_1, \lambda_2, \dots, \lambda_{255}$ 。计算检验统计量:

$$\chi^2 = \frac{2^m}{\lambda} \sum_{i=0}^{2^m-1} (\lambda_i)^2 - \lambda$$

其中 $\lambda = \sum_{i=0}^{2^m-1} \lambda_i$, 将计算值与自由度 255, 在检验的显著性水平下 $\alpha = 0.95$ 的 χ^2 分布, $\chi_{\alpha}^2(255) = 279.2$ 相比, 如小于则通过检验。

3) 序列检验。序列检验用来检验转移概率是否合理, 即出现相同和不同相邻元素的概率是否大致相等。设 n_{00} 表示 00 的个数, n_{01} 表示 01 的个数, n_{10} 表示 10 的个数, n_{11} 表示 11 的个数。计算检验统计量:

$$\chi^2 = \frac{4}{n-1} \sum_{i=0}^1 \sum_{j=0}^1 (n_{ij})^2 - \frac{2}{n} \sum_{i=0}^1 (n_i)^2 + 1$$

将计算值与自由度 2, 在检验的显著性水平下 $\alpha = 0.95$ 的 χ^2 分布, $\chi_{\alpha}^2(2) = 5.991$ 相比, 如小于则通过检验。

设定参数 $cr_1 = e^{0.3}, cr_2 = e^{0.4}, m1 = m2 = 2, n1 = n2 = 8$, 初值 $x_0 = 0.1, y_0 = 0.2$, 用第 2 章的混沌二值序列改进的生成方法, 生成一个二值序列 S , 随机抽取长度不等的子序列进行随机检验, 试验结果表明全部通过随机性检验, 如表 1 所示。

4) 相关性分析。相关性测试也是混沌序列用于密码学的安全性指标的重要衡量标准之一, 自相关函数期望类似于 δ 函数, 而互相关函数接近于零。试验中从混沌二值序列 S 中随机抽取两个长度为 N ($N = 200\ 000$) 的子序列 S_1, S_2 。

$$\bar{S}_1 = \frac{1}{N} \sum_{i=1}^N S_1(i)$$

$$\bar{S}_2 = \frac{1}{N} \sum_{i=1}^N S_2(i)$$

自相关函数为:

$$Auto_r(k) = \frac{\frac{1}{N} \sum_{i=1}^N (S_1(i) - \bar{S}_1)(S_1(i+k) - \bar{S}_1)}{D(\bar{S}_1)}$$

互相关函数为:

$$Inter_r(k) = \frac{\frac{1}{N} \sum_{i=1}^N (S_1(i) - \bar{S}_1)(S_2(i+k) - \bar{S}_2)}{\sqrt{D(\bar{S}_1)} \cdot \sqrt{D(\bar{S}_2)}}$$

设定参数 $u_1 = 60, u_2 = 70, cr'_1 = e^{0.3}, cr_2 = e^{0.4}, m1 = m2 = 2, n1 = n2 = 8$, 初值 $x_0 = 0.1, y_0 = 0.2$, 生成一个二值序列 S 。由二值序列随机抽取子序列的自相关函数和互相关函数如图 5 所示, 试验结果表明序列具有良好的相关性。

表 1 混沌二值序列的随机性检验结果

序列长度	0 个数	1 个数	00 个数	01 个数	10 个数	11 个数	频数检验	扑克检验	序列检验
5000	2494	2506	1244	1250	1250	1255	0.0288	213.4512	0.0198
10000	4933	5067	2418	2515	2515	2551	1.7956	227.4272	2.1149
50000	24942	25058	12453	12488	12489	12569	0.2691	250.1882	0.3097
100000	50145	49855	25174	24971	24971	24883	0.8410	256.4595	0.9849
200000	100311	99689	50384	49927	49927	49761	1.9344	252.2701	2.3703

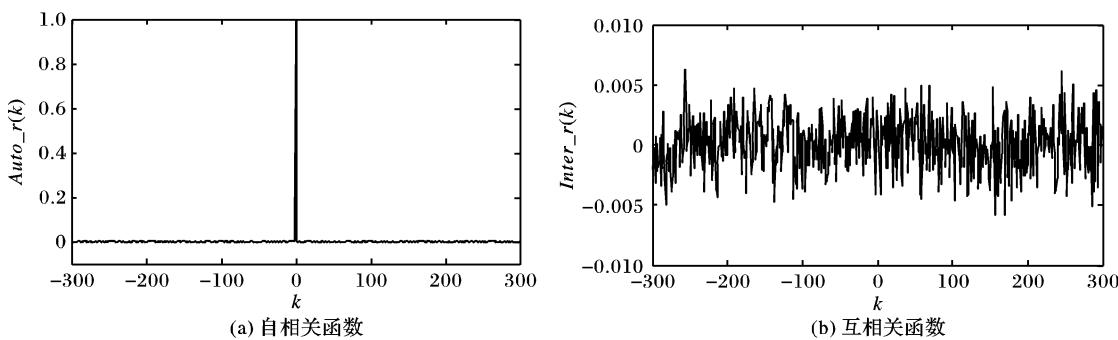


图 5 混沌二值序列随机性分析的相关性测试结果

4 加密流程及仿真试验

4.1 加密流程

1) 设定双混沌互扰系统的参数及初始值 x_0, y_0 , 经过系统迭代映射产生混沌序列 z 。

2) 置换: 由第 2 章的方法对混沌序列量化得到混沌二值序列 S , 同时将明文图像转换成二进制, 然后从混沌序列 S 中每次取 8 个数与明文图像像素二进制值“异或”运算, 最后转换成十进制整数, 这样就得到置换后的密文图像。

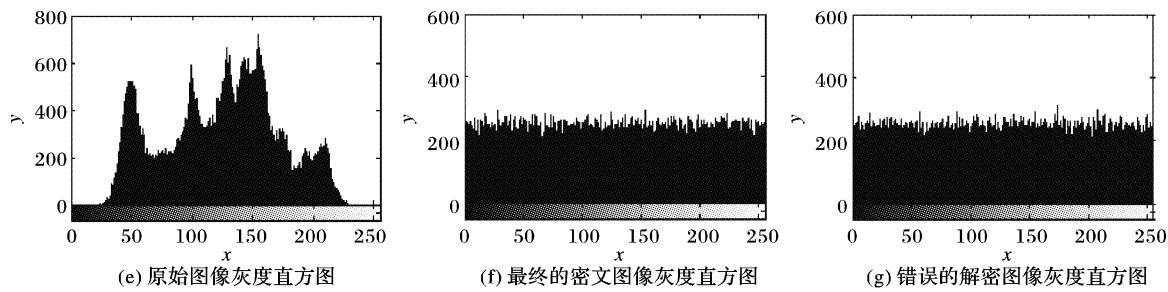
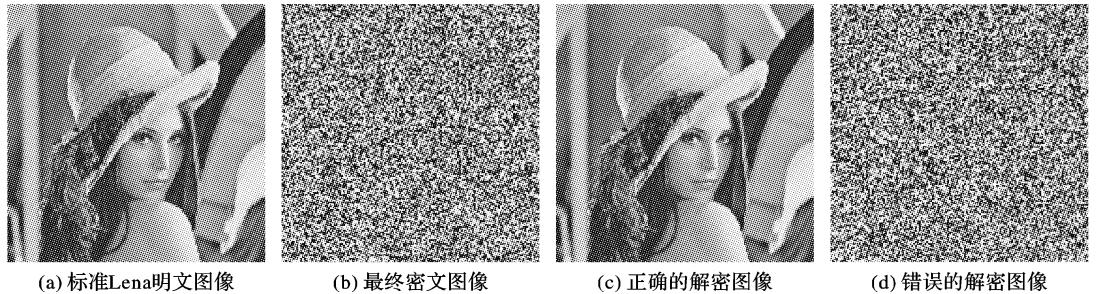


图 6 图像加密解密的实验仿真

设定参数 $u_1 = 60, u_2 = 70, cr'_1 = e^{0.3}, cr_2 = e^{0.4}, m1 = m2 = 2, n1 = n2 = 8$, 初始值 $x_0 = 0.1, y_0 = 0.2$ 。按照 4.1 节的加密流程对明文图像加密, 得到最终的密文图像如图 6(b) 所示, 图 6(f) 是密文图像灰度直方图。通过原始图像与加密图像的灰度直方图对比可以看出, 加密图像的像素灰度直方

图非常均匀, 说明二值序列能有效地掩盖明文信息。文献 [9] 中提出了图像加密效果评价指标信息熵: 信息熵能度量出图像灰度值的分布, 灰度分布越均匀, 图像信息熵越大, 反映了图像的混乱程度。当且仅当所有像素值出现相同概率时, 信息熵取得最大值。根据信息熵指标来量化地度量本文

的图像加密算法效果,计算出原图像的信息熵 $H = 7.4473$;而最终加密图像的信息熵 $H = 7.9974$,对比文献[2]的最终加密图像的信息熵 $H = 7.9338$,本文最终加密图像的信息熵更接近理论上的最大值 8,这也表明了本文的图像加密算法效果更好。

图 6(c)是正确的解密图像,解密效果非常好。在系统参数不变,初始值 $x_0 = 0.1$, $y_0 = 0.200001$, y_0 发生微小变化,对密文图像解密,得到错误的解密图像如图 6(d)所示,图 6(g)是错误的解密图像灰度直方图。可见混沌序列对初始条件的敏感性,即使任意一个初始值的微小变化或系统参数值不正确,都将无法正确解密。

4.3 安全性分析

根据双混沌互扰系统的敏感性测试结果可知,必须正确输入所有密钥,即双混沌互扰系统的初始值 x_0 、 y_0 和系统参数 u_1 、 u_2 、 cr_1 、 cr_2 、 $m1$ 、 $m2$ 、 $n1$ 、 $n2$ 才能正确解密图像。因此,本文提出的图像加密算法总的密钥空间在 Matlab 7.0 试验平台上可达到 10^{90} ,其中参数 x_0 、 y_0 、 cr_1 、 cr_2 的密钥空间的数量级均为 10^{15} ;虽然并不是所有的系统参数 u_1 、 u_2 均能使双混沌互扰系统处于混沌状态,但综合考虑到参数 $m1$ 、 $m2$ 、 $n1$ 、 $n2$,因此可以确定由参数 u_1 、 u_2 、 $m1$ 、 $m2$ 、 $n1$ 、 $n2$ 共同决定的密钥空间的数量级为 10^{30} ;分析结果表明非授权者试图用穷举法破密,在有限的时间内是很难破密成功的。可以看出本文的加密算法具有很高的安全性。

5 结语

本文提出了以两个简单的 Logistic 映射构造一个双混沌互扰系统的图像加密算法,以简单的低维混沌系统通过互扰生成混沌序列,以此增大系统的复杂性和不可预测性。扰动项包括常数扰动项和随机扰动项,随机扰动项的随机性由混

(上接第 2992 页)

最后我们考虑 $V = g_2^\alpha g^{m \cdot f_{u\pi}(s) \cdot r_{u\pi}} \prod_{j=1}^n h^{r_j} g_j^{m \cdot r_{u\pi} + r_m}$,其中指数部分是随机的, g_2^α 是主私钥, m 是身份列表 R 和消息 m 的无碰撞 Hash 值。所有这些都没有提供任何有关实际签名人的信息。对于对手来说就等同于强力猜测。因此新的环签名方案是无条件匿名的。

5 结语

本文提出了一个基于身份的高效环签名方案,该方案的安全性基于标准模型下的计算性 Diffie-Hellman 假设。该体制充分挖掘了身份和公共参数之间的关系,与最近提出的标准模型下基于身份的环签名^[10-11]相比较,签名阶段运算量减少了约 $1/2$,环签名的验证阶段仅需要 2 个双线性对运算($e(g_1, g_2)$ 可以预计算)和群 G_1 上的 n 个指数运算加上群 G_2 上的一个指数运算,并且新的签名体制具有较短的公开参数。

参考文献:

- [1] SHAMIR A. Identity-based cryptosystems and signature schemes [C]// CRYPTO '84, LNCS 196. Berlin: Springer-Verlag, 1984: 47–53.
- [2] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairings [C]// CRYPTO 2001: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, LNCS 2139. Berlin: Springer-Verlag, 2001: 213–229.
- [3] WANG LING-LING, ZHANG GUO-YIN, MA CHUN-GUANG. A survey of ring signature [J]. Frontiers of Electrical and Electronic Engineering in China, 2008, 3(1): 10–19.
- [4] CHAUM D, van HEVST E. Group signatures [C]// EUROCRYPT91, LNCS 547. Berlin: Springer-Verlag, 1991: 257–265.
- [5] MIRACL. Multiprecision integer and rational arithmetic C/C++ library [CP/OL]. [2009-03-18]. <http://indigo.ie/mscott>.
- [6] BENDER A, KATZ J, MORSELLI R. Ring signatures: Stronger definitions, and constructions without random oracles [C]// TCC 2006: Third Theory of Cryptography Conference, LNCS 3876. Berlin: Springer-Verlag, 2006: 60–79.
- [7] WATERS B. Efficient identity-based encryption without random oracles [C]// EUROCRYPT 2005, LNCS 3494. Berlin: Springer-Verlag, 2005: 114–127.
- [8] CARMENISCH J, LYSYANSKAYA A. Signature schemes and anonymous credentials from bilinear maps [C]// CRYPTO 2004, LNCS 3152. Berlin: Springer-Verlag, 2004: 56–72.
- [9] AU M H, LIU J K, YUEN T H, et al. ID-based ring signature scheme secure in the standard model [C]// IWSEC 2006: The First International Workshop on Security, LNCS 4266. Berlin: Springer-Verlag, 2006: 1–16.
- [10] 王玲玲, 张国印, 马春光. 标准模型下基于双线性对的前向安全环签名方案[J]. 电子与信息学报, 2009, 31(2): 448–452.

沌序列本身决定,即将混沌序列值与混沌序列的平均值相比来实现系统间的随机扰动。与现有的以高维混沌系统作为随机数发生器相比较,本文提出的方案不仅增加了系统的参数个数和复杂性,而且同时扩展了系统的控制参数和初始值的取值范围,这使得密钥空间容量大大增加。另外提出了一种改进的二值序列量化方法,并对二值序列作了随机检验和相关性分析,大量实验结果表明该方法生成的二值序列具有良好的伪随机性和相关性,密钥生成效率高。将二值序列应用于图像加密,实验表明该算法具有较高的安全性和较好的加密效果。

参考文献:

- [1] LI T Y, YORKE J A. Period three implies chaos [J]. American Mathematical Monthly, 1975, 82: 958–992.
- [2] 李鹏, 田东平. 基于超混沌序列的数字图像加密算法[J]. 微电子学与计算机, 2008, 25(3): 4–7.
- [3] 吕宁, 孙广明, 张宇. 基于多混沌系统的图像分组密码设计[J]. 计算机应用, 2008, 28(9): 2263–2266.
- [4] 程东升, 叶瑞松. 基于四维混沌系统生成二值序列的方法及其加密应用[J]. 计算机应用, 2008, 28(3): 677–685.
- [5] 向菲, 邱水生. 基于混沌系统互扰的流密码设计[J]. 物理学报, 2008, 57(10): 6132–6138.
- [6] 孙绣花, 戴跃伟, 王志铨. 混沌序列产生方法及其在图像加密中的应用[J]. 南京师范大学学报, 2004, 4(1): 56–78.
- [7] MAY R. Simple mathematical models with very complicated dynamics [J]. Nature, 1976, 261: 459–469.
- [8] 赵莉, 张雪峰, 范九伦. 一种改进的混沌序列产生方法[J]. 计算机工程与应用, 2006, 42(23): 31–33.
- [9] 王迤冉, 王春霞, 詹新生. 一种图像加密算法的性能评定方法[J]. 微计算机信息, 2006, 22(30): 313–314.