

文章编号:1001-9081(2010)01-0198-05

一种新的离散混沌同步保密通信方案

潘 勃,李 骞,冯金富,徐建军,李 斌,陶 茜

(空军工程大学 工程学院,西安 710038)

(panbo581@sohu.com)

摘 要:系统地分析了一种新的 TD-ERCS 离散混沌系统产生的伪随机序列的复杂性,仿真验证了 TD-ERCS 离散系统是复杂性稳定的全域性离散混沌系统。在此基础上,提出基于 TD-ERCS 离散系统构造伪随机序列的双信道保密通信方案。在该方案中,发送端利用混沌驱动器产生混沌密钥和遮掩信号,基于混沌的伪随机序列发生器(CPRNG)将驱动离散系统产生的混沌序列转化为加密密钥序列,并对信息信号先加密再遮掩。获得加密信号后使用一个信道传输,利用另一信道传输系统同步的单变量同步信号。理论分析和数值实验验证了该方案在密钥安全性和算法复杂性方面性能良好,且易于软件实现。

关键词:相空间;混沌同步;Limpel-Ziv 算法;Logistic 迭代;遮掩信号

中图分类号: TP393.08 **文献标志码:** A

Encryption approach to chaotic synchronization communication by TD-ERCS discrete system

PAN Bo, LI Qian, FENG Jin-fu, XU Jian-jun, LI Bin, TAO Qian

(Engineering College, Air Force Engineering University, Xi'an Shaanxi 710038, China)

Abstract: The complexity of chaotic pseudo-random sequences generated by the new TD-ERCS discrete chaotic system was analyzed in detail, and the simulation results show that TD-ERCS is a discrete chaotic system with the great steady complexity. On the basis of this, the authors presented a double-channel encryption approach to generate chaotic pseudo-random sequences based on TD-ERCS discrete chaotic system. In this approach, the chaotic oscillator at the transmitter was used to generate digital key and masking signal, and chaotic sequence generated by the driver system was turned into encryption keys in CPRNG. The information signals were first encrypted by the key and then masked by the masking signal. The masked signals were transmitted through one channel, the other channel was used to transmit the single variable which was coupled to the receiver to drive two chaotic oscillators to synchronize. The simulation results show that the theoretical analysis is in accordance with the experimental result. The cryptosystem is of higher level of security, synchronization and algorithm complexity, and it can be easily implemented by software.

Key words: phase space; chaotic synchronization; Limpel-Ziv algorithm; Logistic iteration; masking signal

0 引言

混沌同步应用于保密通信是近些年来引起非线性动力学和信息科学界广泛关注的一个研究领域^[1]。国内学者相继提出了多种混沌保密通信方案^[2-4]。常采用低维混沌系统(也是自然系统)如 Logistic、tent、Chebyshev 等设计流密码、分组密码和 Hash 函数,但就混沌系统自身来说,仍存在某些安全缺陷^[5-7]。

文献[8-9]中基于混沌安全性条件构造了一类新的混沌系统:基于切延迟的椭圆反射腔映射系统(Tangent-Delay Ellipse Reflecting Cavity map System, TD-ERCS)。本文试图应用这一新的混沌系统构造基于混沌的伪随机序列发生器(Chaos-based Pseudo-Random Number Generator, CPRNG),设计出一种新的应用于无线电通信的数据加密通信方案。该方案保留了 CPRNG 系统理论上的安全性,且不需要驱动信号在信道中传输,从而避免了攻击者利用截获的驱动信号重构

发送端动力学系统之后检测出被隐藏在其中的消息的可能性,同时提高了传输效率。另外,本方案易于用软件实现,且由于使用了 CPRNG 系统,使通信的安全性获得了一定改善。

1 TD-ERCS 离散混沌系统

1.1 TD-ERCS 离散混沌系统模型

文献[8]给出了 TD-ERCS 离散混沌系统的定义,其映射表达为:

$$\begin{aligned}x_n &= -\frac{2k_{n-1}y_{n-1} + x_{n-1}(\mu^2 - k_{n-1}^2)}{\mu^2 + k_{n-1}^2} \\k_n &= \frac{2k'_n - k_{n-1} + k_{n-1}k_n'^2}{1 + 2k_{n-1}k'_n - k_n'^2}; n = 1, 2, 3, \dots \\k'_{n-m} &= -\frac{x_{n-m}}{y_{n-m}}\mu^2; m \leq n \\y_n &= k_{n-1}(x_n - x_{n-1}) + y_{n-1}\end{aligned} \quad (1)$$

其中:系统参数 $\mu \in (0, 1]$; $|x_n| \leq 1$, $|y_n| \leq 1$; m 为整数,代

收稿日期:2009-05-15;修回日期:2009-08-30。

作者简介:潘勃(1983-),男(满族),辽宁清原人,博士研究生,主要研究方向:武器系统抗干扰技术研究、混沌保密通信;李骞(1981-),男,湖南新化人,博士研究生,主要研究方向:武器系统抗干扰技术研究、武器系统控制与仿真;冯金富(1964-),男,江苏泰兴人,教授,博士生导师,主要研究方向:武器系统控制系统与仿真、多源信息融合;徐建军(1978-),男,吉林榆树人,博士研究生,主要研究方向:计算机视觉;陶茜(1983-),女,安徽萧县人,博士研究生,主要研究方向:信息系统工程、智能决策。

表切线延迟; k'_{n-m} 为延迟 m 后椭圆切线的斜率; k_0 可由入射角 a 确定。显然,给定系统参数值 μ, m ,初值 x_0 和 a ,就可以求出 $y_0, k_0, k'_{0 \leq m < n}$ 的状态称为过渡状态; $m \geq n$ 的状态称为正常状态;当 $m \geq 1$ 时,系统有切线延迟操作,系统是混沌的;当 $m = 2, 3, 4, 5, 6, \dots$ 时,系统可获得一组混沌序列 $\{x_n, k_n\}$ 。

1.2 TD-ERCS 系统的动力学特性仿真

近年来,随着混沌伪随机序列构造的确定性和非线性等动力学特性逐渐被人们所认识,相继出现了一些基于相空间重构方法对通信实施预测干扰的研究报道^[5-6]。因此,初始

条件的敏感性只是混沌系统用于信息加密的必要条件而不是充分条件,本文着重考察 TD-ERCS 的迭代点分布和相空间分布情况。

设定初值 $x_0 = 0.5624, a = 0.6545$,系统参数 $\mu = 0.6452, m = 2$,迭代1000次,TD-ERCS系统处于混沌状态,绘制出 TD-ERCS 迭代轨迹如图1(d)所示,图1(a)、(b)、(c)分别为虫口映射、Henon映射和文献[12]中的组合映射;绘制出 TD-ERCS 相空间分布如图2所示,图2中的(a)~(d)分别对应于图1的相空间分布。

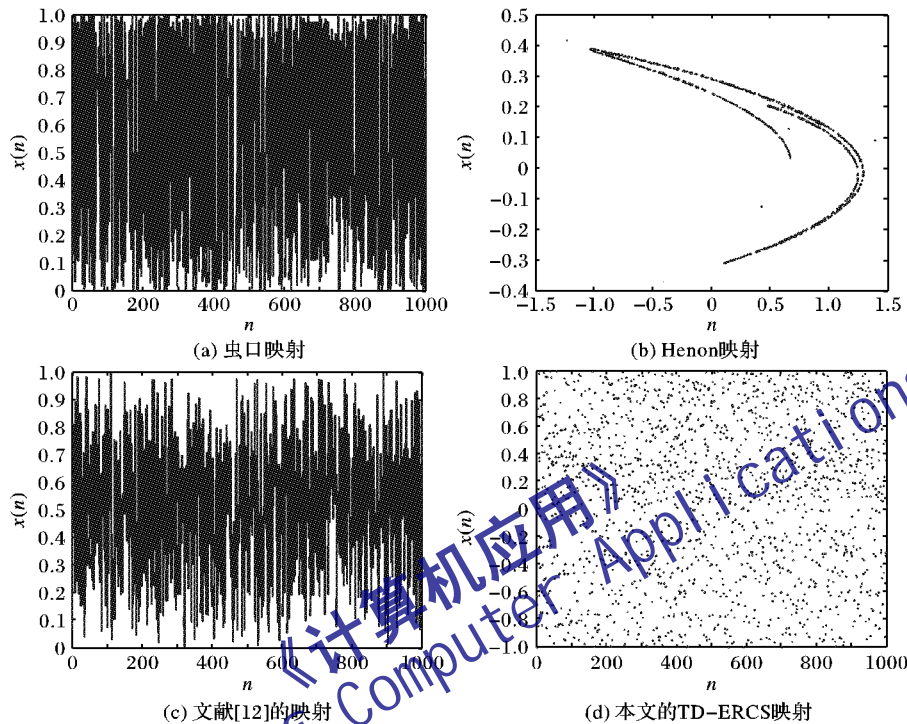


图1 4种映射的迭代轨迹

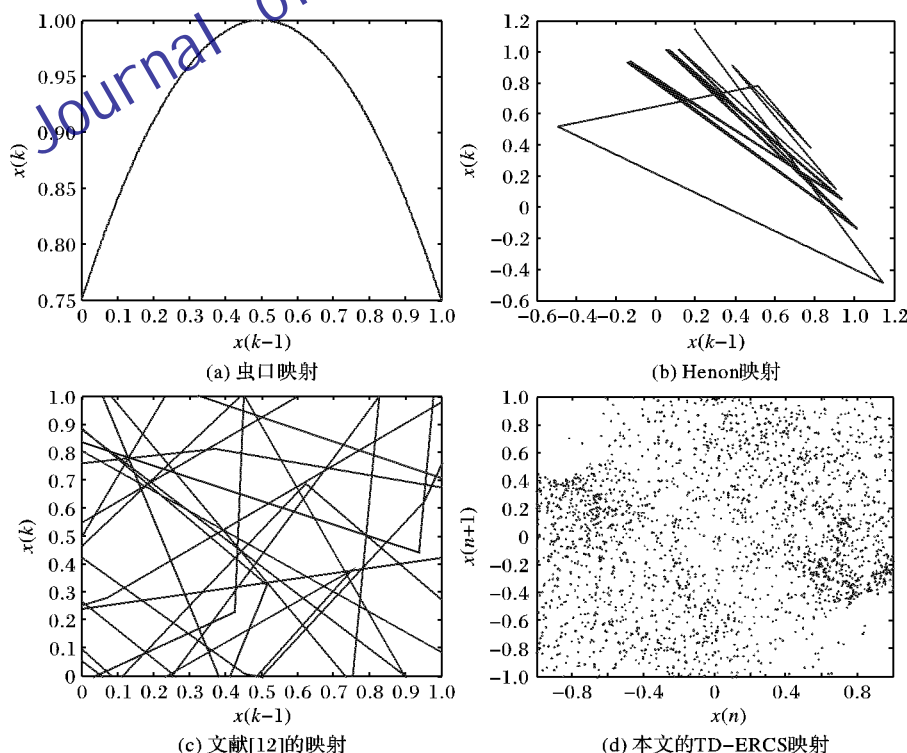


图2 4种映射的相空间分布

比较图1、2可以看出,TD-ERCS的混沌吸引子较虫口映射、Henon映射及组合映射射原形具有复杂的迭代轨迹,而且

不存在任何几何形状简单明晰的吸引子,点分布几乎充满了整个值域范围,表明用其进行信息加密将具有良好的安全性,

难以用重构预测方法破译。

2 基于 TD-ERCS 混沌映射加密方案

2.1 混沌伪随机序列发生器

传统的混沌伪随机序列发生器通常以系统初值作为密钥,通过数值计算在有限精度下实现混沌映射的迭代。由于混沌映射定义在实数域内,有限精度的数值计算必然引入舍入误差,相关研究表明^[3,10],这种基于有限精度数值计算的 CPRNG 在密码学意义上是不安全的。

本文在研究文献[3,4,10]的基础上,提出了一种新型的随机序列发生器系统,该系统对原始密钥进行复合处理,得到粗粒化输出:

$$Y_n(k) = C(x_n(k)) \quad (2)$$

其中 $C(\cdot)$ 可以是复合运算或者非线性调制运算,本文分别由下面两式变换成均匀分布的伪随机序列:

$$\begin{cases} \theta_i = \frac{\arccos(x_i)}{\pi} \\ \beta_i = 0.5 + \frac{\arccos(k_i)}{\pi} \end{cases} \quad (3)$$

$$Y_n = C(x_n) = \begin{cases} 0, & x_n < 0.5 \\ 1, & x_n \geq 0.5 \end{cases} \quad (4)$$

$\{\theta_i\}$ 和 $\{\beta_i\}$ 具有稳定的均匀分布,且与初始条件和系统系数无关,按式(4)输出二进制伪随机序列 $\{X_n\}$ 。可以证明式(3)、(4)满足混沌构造随机数发生器的充分条件和附加条件^[10]。

2.2 加密方案

本文提出的利用混沌的伪随机序列发生器系统构成一个如图3所示的混沌通信加密/解密方案。密钥信道传输混沌同步驱动信号,发送端和接收端混沌系统之间的同步采用单变量单向耦合同步法^[1,4]。该方法只用一个混沌变量驱动,通信信道中只传送给用于同步的混沌信号,它不携带任何与传送数据有关的信息;通信信道传送加密信号。信息的加密与解密过程如下:

在发送端,利用离散 TD-ERCS 混沌系统产生出多组混沌序列,这些混沌序列经过本方案设计的 CPRNG 系统的处理后对应产生多组伪随机序列作为密钥序列,用这些密钥序列对明文数据按字节加密,然后对已加密信号使用 TD-ERCS 混沌系统的一个或多个状态信号进行一次或多次的信号遮掩,遮掩后的信号使用一个信道传输。密文数据通过调制后传输到接收端。

在接收端,利用对应的同步混沌系统和对应的 CPRNG 系统准确地重构密钥,对密文数据解密,从而不失真地还原明文数据。

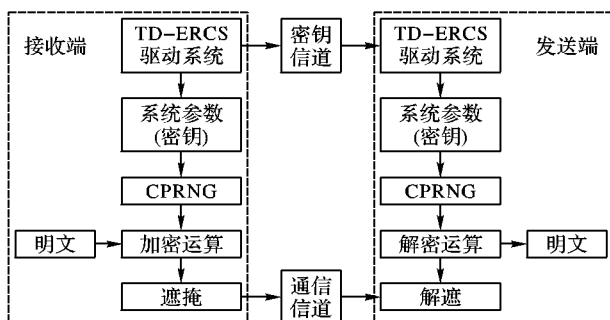


图3 基于 TD-ERCS 系统的保密通信方案

发送端的具体加密过程可描述为:选择混沌系统的一个状态变量生成密钥;把密钥与信息信号(数字信号)相异或,对信号加密;然后把加密后的信号与另一个混沌信号相加,实现对已加密信号的遮掩,这是对信息信号的二次加密,把遮掩后的加密信号送入信道传送。由式(2)设 $Y = \{y_1, y_2, \dots, y_n\}$ 为复合处理后的密钥序列,所需传输明文为 $M = \{m_1, m_2, \dots, m_n\}$,系统方程为:

$$c_n = (y_n + m_n) \bmod 2 \quad (5)$$

$$d_n = x_n + hc_n \quad (6)$$

x_n 是混沌系统的状态变量; c_n 是一次加密序列; h 为小常数; d_n 为通信信道中传送的信号。

解密过程可简单地描述为:首先在接收端恢复出与发送端的同步变量,用来解遮掩接收到的信号。同时,在接收端,用和发送端同样的非线性函数生成接收端的密钥。由式(8)可解调出信息信号。根据单向耦合的同步机理,解密过程是加密过程的逆运算,接收端系统方程为:

$$c_m = (d_n - z_k)/h \quad (7)$$

$$s_m = (c_m - x_m) \bmod 2 \quad (8)$$

其中: $Z = \{z_1, z_2, \dots, z_n\}$ 是接收端混沌系统的状态; x_m 是接收端密钥; c_m 是接收端的解遮掩信号; s_m 是解密后信号,即接收端解调出的信息信号。

在以往掩蔽法混沌同步通信方案中,驱动信号携带着该动力学系统的信息,用非线性预测、参数估计等技术^[5-7],可以检测出隐藏在驱动信号中的消息。相比之下,本方案具有以下两个优点:1)本方案中驱动系统和 CPRNG 系统只有间接的映射关系,攻击者只能从驱动信号获取驱动系统的动力学性质,估计驱动系统参数,无法估计 CPRNG 系统的参数;2)由于同步信号中不包含信息信号,同步驱动信号不会产生像混沌遮掩方法那样受到信息信号干扰的情况,可以保证快速准确地恢复同步信号。

3 密钥安全性和算法复杂性分析

混沌系统是混沌数字加密算法的“核”,研究混沌数字加密算法的安全性,首先必须研究混沌系统的安全性,只有确认混沌系统是安全的,才能保证构造的加密算法是安全的。文献[10]中指出安全的密码系统必须满足以下要求:1)由密钥序列组生成的密钥集应该足够大,且密钥应该近似等概率地随机产生;2)算法复杂度必须足够大。

3.1 密钥的安全性

文献[11]中通过控制 Logistic 迭代的参数和初值就能够从理论上得出无限多的伪随机序列。本文提出的驱动系统可控参数和遮掩密钥(密钥) x_0, a, m, μ 各含4个密钥,共8个密钥参数,理论上是文献[11]的4倍。所以可以通过控制不同参数的变化,可以是单一参数变化,也可以是几个参数组合的变化,扩大了生成二值序列的密钥空间,能够在理论上得到更多的伪随机序列码,进而增加了破译和预测的难度。

如果算法密钥空间为所有系统参数(主密钥)的乘积, $M = (x_0 am \mu)^k$,不妨设使用双精度为 $k = 32$,则该系统的参数空间为 $2^{32 \times 8} = 2^{256}$,相当于有近256位的密钥空间,就目前的计算条件来看,本系统可以有效地对抗穷举攻击。

3.2 基于 Lempel-Ziv 算法的复杂性分析

系统的行为复杂性是指系统产生的伪随机序列与随机序列的相似程度。为了分析 TD-ERCS 系统混沌序列的复杂性,采用 Lempel-Ziv 算法对 TD-ERCS 混沌伪随机序列的复杂性

进行分析和讨论。

文献[9-10,12]中的研究表明,几乎所有算法的复杂性都趋于一个常数,用归一化的 $C(n)$ 来测度伪随机序列的复杂性变换,完全随机的序列值都趋向于1,而周期性序列趋向于0,其余情况介于两者之间。归一化 $C(n)$ 反映了伪随机序列与随机序列等接近程度,其序列趋向于1,则表明该序列越趋近于随机序列,序列越复杂。

应用 Lempel-Ziv 算法对 TD-ERCS 系统产生的伪随机序列的复杂性进行计算,取系统参数 $\mu = 0.6452$, 结果如表1。

表1 伪随机序列复杂性分析

m	N			
	1000	2000	3000	4000
$m = 0$	0.073 2	0.064 1	0.049 5	0.023 1
$m = 1$	0.571 2	0.561 6	0.541 9	0.533 8
$m = 2$	0.922 3	0.914 5	0.911 2	0.907 6
$m = 3$	0.922 5	0.911 8	0.911 1	0.903 6
$m = 4$	0.922 5	0.909 4	0.908 7	0.901 3

由表1可见,当 $m = 0$ 时,TD-ERCS 系统的复杂性接近于0;当 $m = 1$ 时,TD-ERCS 系统的复杂性接近于0.45;当 $m = 2$ 时,TD-ERCS 系统的复杂性接近于0.55;当 $m \geq 3$ 时,TD-ERCS系统复杂性达到了0.9以上,系统复杂性大。而且,随着序列长度 N 的增长,复杂性的计算结果有减小的趋势,随着序列的不断增长,复杂性的计算结果逐渐趋于一个稳定值。在序列长度从3000增大到4000的过程中,复杂性变化不大。故当取 $N = 4000$ 时,Lempel-Ziv 算法计算结果趋于稳定。

4 图像保密通信仿真

假设信道为理想条件下,接收端接收到信号的同时,同步混沌发生器生成解密同步状态信号。用 x_n, d_n 生成密钥,并用 z_n 对 d_n 实行解遮掩。最后在接收端把解遮掩信号 c_m 与密钥 x_m 相异或解调出信息信号。

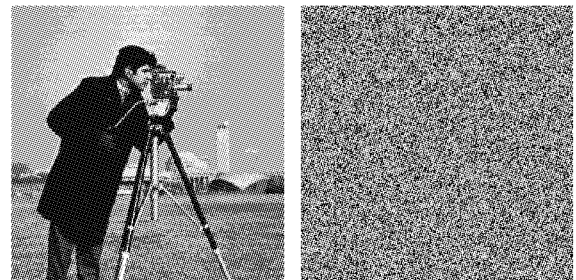
4.1 密钥敏感性

方案的整个程序在 Windows XP 操作平台下完成,软件使用 VC++ 6.0,具体参数如下:明文图像选取 Cameraman.tif,灰度值为256,大小 256×256 ,TD-ERCS 系统初始条件初值 $x_0 = 0.5624$, $a = 0.6545$,系统参数 $\mu = 0.6452$, $m = 2$,算法初始条件为迭代次数为1000次,混沌伪随机序列发生器按式(3)的非线性调制运算变换成均匀分布的伪随机序列,原图像和加密图像测试结果分别如图4(a)、(b)所示。

上述方案对遮掩参数和密钥参数是非常敏感的,参数略有差异,密文不能被成功遮掩和解密,只有参数完全一致时,才能准确解密。这进一步验证了本方案具有良好的双重抗破译性,该特性将有助于抵抗唯明文攻击。为了测试对密钥的敏感性,本文按以下步骤进行实验:

- 1) Cameraman 原始图像如图5(a),接收端解遮掩参数时, x_0 取0.5625,其他密钥参数不变,得到的解密图像见图5(b);
- 2) 对接收端的参数 x_0, a, m, μ 与发送端加密条件取值相同,得到的解密图像见图5(c);
- 3) 在接收端对密文解遮掩,但对 μ 进行微小扰动, u 取值为0.65450001,而其他迭代值不变,最终得到的解密图像见图5(d)。

从以上密钥敏感性分析结果看,当初始值误差为 10^{-8} 时,便产生不同的伪随机序列,也就是只要加密密钥和解密密钥有 10^{-8} 的误差时,就无法正确解密。同时每组密钥有五个值,它们在实数域中的取值不受任何限制,同时允许多次加密。

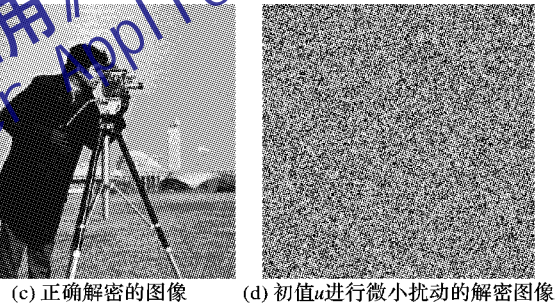


(a) Cameraman原始图像 (b) 加密后的密文图像

图4 加密前后的图像仿真结果



(a) 原始图像 (b) 加密后的密文图像



(c) 正确解密的图像 (d) 初值 α 进行微小扰动的解密图像

图5 密钥敏感性分析

4.2 灰度直方图比较

选用图4的明文图像(a)和密文图像(b)分析灰度值分布,相应的仿真结果如图6所示。

可以直观地看出,两幅图像的灰度统计值有着明显的差异,密文图像的灰度值分布趋于平均,这说明算法的灰度扩散是有效的。由此可见,加密后的图像统计分布完全被破坏,具有很好的抵御统计分析能力。

4.3 相邻两个像素相关性分析

通过比较明文图像与密文图像的相邻像素的相关性,可以考察算法对图像置乱的程度。分别对图5(a)、(b)的相邻像素的相关性进行测试,随机选取1000对水平竖直对角方向相邻像素,利用以下公式进行计算。

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

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

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

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

其中, x, y 代表随机选取的这1000对相邻像素的灰度值。测试的结果如表2所示,可看出加密后的图像与明文图像相比,其

相邻像素的相关性大大降低了。

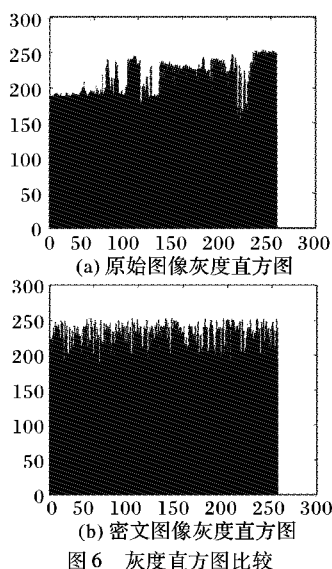


表2 明文、密文的像素相关性对比

方向	明文图像	密文图像
水平方向	0.9523	0.0563
竖直方向	0.9145	0.0175
对角方向	0.9378	0.0252

5 结语

本文提出了一种利用切延迟的椭圆反射腔映射混沌系统和双信道保密通信方法实现数据加解/密混沌保密通信方案。该方案采用切延迟的椭圆反射腔映射系统产生 CPRNG 系统的驱动序列,然后用按字节加密处理的方法对明文进行加密,在实现过程中又用到遮掩技术,相当于对信息信号进行了双

重加密,提高了保密通信系统的保密性;采用两信道传输方案,不仅提高了系统的抗扰性能,且进一步增加了密钥的复杂性;同步信号获取采用单变量单向耦合方法,工程上容易实现。因此,本文给出的方案是一种可靠且实用的混沌保密通信方法。

参考文献:

- [1] 郑会永. 混沌及混沌保密通信技术[J]. 中国图象图形学报, 1999, 3(12): 53-60.
- [2] SHORT K M. Steps towards unmasking secure communication [J]. International Journal of Bifurcation and Chaos, 1994, 4(4): 959-977.
- [3] 包浩明, 朱义胜. 基于分段抛物线映射的混沌加密方案[J]. 大连海事大学学报, 2008, 34(2): 53-60.
- [4] 龙敏, 丘水生. 离散超混沌同步保密通信系统的设计与分析[J]. 小型微型计算机系统, 2008, 29(5): 933-935.
- [5] 张家树, 肖先赐. 混沌时间序列的 Volterra 自适应预测[J]. 物理学报, 2000, 49(3): 403-408.
- [6] 张家树, 肖先赐. 用于低维混沌时间序列预测的一种非线性自适应预测滤波器[J]. 通信学报, 2001, 22(10): 93-98.
- [7] 郭进峰, 郭静波. 一种破译混沌直接序列扩频保密通信的方法[J]. 物理学报, 2008, 57(3): 1477-1483.
- [8] 孙克辉, 谈国强, 盛利元. TD-ERCS 离散混沌伪随机序列的复杂性分析[J]. 物理学报, 2008, 57(6): 3360-3366.
- [9] 盛利元, 闻江, 曹莉凌等. TD-ERCS 混沌系统的差分分析[J]. 物理学报, 2007, 56(1): 78-82.
- [10] 王蕾, 王美平, 王赞基. 一种新型的混沌伪随机数发生器[J]. 物理学报, 2006, 55(8): 3962-3968.
- [11] 米良, 朱中梁. 一种基于 Logistic 映射的混沌跳频序列[J]. 电波科学学报, 2004, 19(3): 333-337.
- [12] 徐茂智, 游林. 信息安全与密码学[J]. 物理学报, 2005, 54(9): 4031-4037.

(上接第189页)

表2列出了本文改进的直方图平移算法和文献[2]的直方图平移算法在多个阈值下的嵌入率和 PSNR 值,其中所用的直方图为色彩分量间预测误差差值直方图,实验对象为 200×200 Lena 彩色图像的 BG 分量组合。实验结果表明: T 越小,需平移的差值越多,改进算法的效果越明显。

表2 不同阈值下嵌入率和 PSNR 值对比实验(图像 Lena)

阈值 T	本文算法			单分量预测误差扩展		
	嵌入率	PSNR(B)/dB	PSNR(G)/dB	嵌入率	PSNR(B)/dB	PSNR(G)/dB
0	0.164	56.74	57.78	0.159	55.19	55.80
1	0.382	54.48	54.34	0.377	53.74	53.80
2	0.459	53.33	53.07	0.455	53.09	52.90
3	0.482	52.78	52.61	0.478	52.72	52.53

4 结语

针对 Tian 差值扩展算法和 Thodi 直方图平移算法的缺点,提出一种基于色彩分量间预测误差差值扩展的彩色图像无损数据隐藏算法。该算法将差值扩展量分散到两个色彩分量中,减少了对图像的修改,含印图像质量明显提高,同时,对差值直方图平移技术作了改进,进一步提高嵌入率和图像质量。隐藏数据的提取和图像恢复均不需要原始图像,并在提取数据后能够无损地恢复原始图像。该算法在不可见性和嵌入容量方面取得了较好的效果,在军事、法律和医学等领域具有广泛的应用前景。下一步的工作是,改进或者完全不用定

位图,进一步提高图像质量和嵌入容量。

参考文献:

- [1] TIAN JUN. Reversible data embedding using a difference expansion [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(8): 890-896.
- [2] THODI D M, RODRIGUEZ J J. Expansion embedding techniques for reversible watermarking [J]. IEEE Transactions on Image Processing, 2007, 16(3): 721-730.
- [3] ALATTER A M. Reversible watermark using the difference expansion of a generalized integer transform [J]. IEEE Transactions on Image Processing, 2004, 32(8): 1147-1156.
- [4] 陈开英, 胡永健, 李健伟. 利用差值扩展进行可逆数据隐藏的新算法[J]. 计算机应用, 2008, 28(2): 455-459.
- [5] 邓世文, 刘焕平, 叶宏宇. 基于 Laplacian 残差扩展的可逆嵌入算法[J]. 计算机工程与应用, 2008, 44(3): 110-113.
- [6] 彭德云, 王嘉祯. 基于错误控制编码的差值扩展可逆数字水印[J]. 计算机工程, 2007, 33(21): 18-20.
- [7] 祝玉新, 孙星明, 杨恒伏. 基于 Harr 小波的彩色图像可逆水印算法[J]. 计算机应用研究, 2007, 24(6): 165-169.
- [8] 杨边, 陆哲明, 徐殿国, 等. 基于邻近像素的低复杂度预测矢量量化图像压缩编码算法[J]. 电子学报, 2003, 31(5): 707-710.
- [9] 曹文伦, 彭国华, 秦洪元, 等. 利用色彩分量相关性的彩色图像分形编码方法[J]. 计算机工程与应用, 2004, 40(22): 51-55.