

基于物理混沌的混合图像加密系统研究^{*}

晋建秀[†] 丘水生

(华南理工大学电子与信息学院, 广州 510640)

(2009 年 1 月 15 日收到; 2009 年 4 月 13 日收到修改稿)

初步实现了基于物理混沌的混沌和数据加密标准算法级联的混合图像加密系统, 基于该系统研究了级联加密与单级加密的抗统计分析能力, 以及不可预测性强弱不同的混沌信号在该系统中应用时密文特性的不同. 这种利用物理混沌不可预测性的混合加密系统, 不存在确定的明文密文映射关系, 而且密文统计特性也应优于(或大致相当)其他加密系统. 数值结果支持这一结论, 同时表明不可预测性较强的混沌系统其加密产生的密文相关性较弱.

关键词: 物理混沌, 图像, 级联加密

PACC: 0545

1. 引 言

混沌系统用于数据加密最早由英国数学家 Matthews 提出^[1]. 随着实时快捷的信息交流与信息安全之间矛盾的日益突出, 混沌通信和混沌加密技术成为国际电子通信领域的一个热门课题, 并在密码学领域内日益显示出一定的优越性和潜在的生命力^[2-7]. 混沌加密和常规加密各自具有不同的特点, 根据优势互补的原则提出了一种混合加密的原理方案^[8,9]. 除了唯密文攻击(穷举攻击)之外的一切基于确定的明文密文映射关系的攻击方法对该方案都将失效, 因此系统具有较高的安全性. 文献[10—12]初步研究了混合加密系统, 但没有利用物理混沌. 依据文献[8,9]的思想, 本文实现了基于物理混沌的混沌和数据加密标准 DES(data encryption standard)算法级联的混合图像加密系统原理方案, 并与其中任一单级加密密文进行了对比分析. 另外, 还研究了不可预测性强弱不同的混沌信号在该系统中应用时密文特性的差异. 研究结果对实际图像加密系统方案及信号源选择具有重要的理论意义和参考价值.

2. 物理混沌和算法混沌的基本概念

由一个混沌系统产生的混沌吸引子可分为算

法混沌和物理混沌两类. 利用没有随机扰动的数值计算装置(例如计算机)所产生的混沌吸引子属于算法混沌, 而利用具有随机扰动的物理实现装置(例如模拟电路)所产生的混沌吸引子属于物理混沌. 由于随机扰动的存在而初始条件随时改变, 物理混沌吸引子是不可预测的^[13](具有“过去和未来没有必然的联系”的性质^[14]). 对于算法混沌, 由于没有随机扰动, 其轨道完全取决于初值, 因而是可预测的. 因此, 基于物理混沌的保密通信系统是理想的具有高安全性的通信系统. 而算法混沌由于具有可复制、类噪声的优点广泛应用于混沌研究中; 但将其用于保密通信则系统安全性相对较差. 这是后者明显的不足.

值得指出的是, 对于物理混沌, 实际波形的测量值有一定的误差, 但混沌波形的近似仍然是混沌的. 这种“有限精度”效应与产生伪混沌序列的数字仿真系统具有实质性的不同^[13]. 前者没有改变原有的初值复杂性, 其影响相应于连续频谱的局部改变, 而后者则因丧失初值复杂性必然是可预测的.

3. 混合加密方案原理

初值敏感性、类随机性和不可预测性是混沌系统的主要特征, 也是其被应用于密码学的最根本原因. 混沌加密系统的主要优点是可以利用混沌信号

^{*} 国家自然科学基金(批准号:60372004)和华南理工大学自然科学基金(批准号:E5090790)资助的课题.

[†] E-mail: jxjin@scut.edu.cn

的不可预测性,主要缺点是没有解决密钥空间的设计问题;常规加密系统的主要优点在于具有成熟的密钥空间设计技术,而且其安全性较容易评估;而主要缺点是明文密文对的唯一对应而有可能被破译.因此由混沌加密器与常规加密器相结合构成的

混合加密系统,使两种加密器的优点可以互补,整个系统的抗攻击能力明显高于其中的任一加密器.

基于物理混沌的混合加密方案原理如图 1 所示.

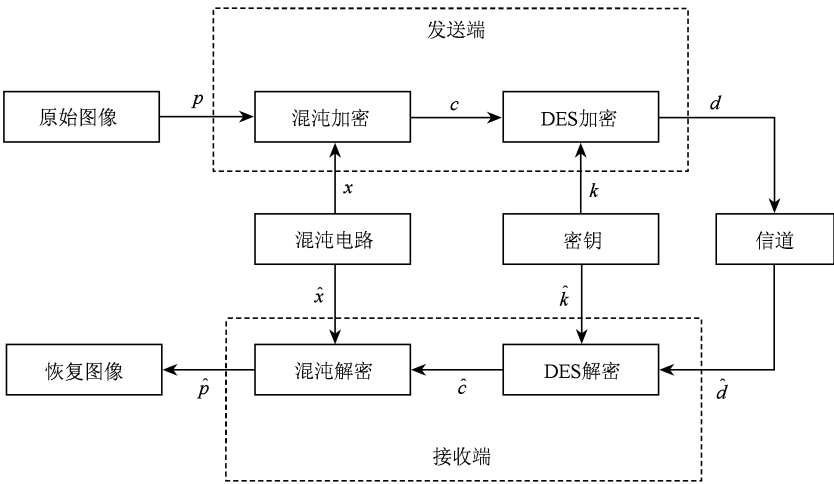


图 1 混合加密方案原理框图

DES 是一种较为典型的分组密码算法^[15],使用一个 56 位的密钥以及附加的 8 位奇偶校验位,产生最大 64 位的密钥大小.使用 Feistel 技术,将加密的信息块分成各 32 位的两组,使用子密钥对其中一半应用循环功能,然后将其输出与另一半进行“异或”运算;接着交换这两半.这是一个迭代的分组密码,共进行 16 次循环.

混合加密算法的主要步骤如下:
1)混沌电路产生的连续信号经采样得到序列 x_i , x_i 经过一定变换得到 x_j ,由 x_j 构成的 x 对原始信息 p 加密,得到混沌加密密文 c ,

$$c = p \oplus x,$$
其中 $x_j = \text{round}(K(x_{1i}^2 + x_{2i}^2 + x_{3i}^2)^{1/2} + \lambda) \bmod 255$ 表示 $K(x_{1i}^2 + x_{2i}^2 + x_{3i}^2)^{1/2} + \lambda$ 对 255 取整后的余数, $K = 3000, \lambda = 127$.

2)密文 c 经过常规加密技术 DES 在密钥 k 加密下得到加密密文 d ,

$$d = f_k(c) = f_k(p \oplus x),$$
其中 $f_k(\cdot)$ 表示经密钥 k 加密下密文 c 到 d 的映射.

3)将加密密文 d 经信道传送,接收端收到信号 $\hat{d}$,

$$\hat{d} = d.$$

4)接收端首先对 $\hat{d}$ 进行解密,在密钥 $\hat{k}$ 解密下得到解密密文 $\hat{c}$,

$$\hat{c} = f_{\hat{k}}^{-1}(\hat{d}),$$
$$\hat{k} = k.$$

5) $\hat{c}$ 经过混沌信号 $\hat{x}$ 解密,得到恢复信息 $\hat{p}$,

$$\hat{p} = \hat{x} \oplus \hat{c} = \hat{x} \oplus f_{\hat{k}}^{-1}(\hat{d}).$$

除了唯密文攻击之外,常规加密算法的所有已知攻击方法(如直接针对 DES 的差分分析和线性分析)的基本条件是某些唯一对应的明文密文对^[15].由于采用硬件实现的混沌系统,前级密钥信号 x 是不可预测的,因而其输出 c 是随机变化的,故不存在唯一对应的明文密文对.这是前级的优点.混合级联加密系统的后级(常规加密器)因其输入不可预测而不可能有唯一对应的明文密文对(输入-输出对),其关键在于由物理混沌产生的 x 不能用算法描述^[13].这样,上述的已知攻击方法在原理上不可能击破混合加密系统中的常规加密器.由此可见,前级优点弥补了后级的弱点,而显著增强了后级的安全性.在上述系统的后级不可击破的情况下,要获得其输入信号 c 是不可能的,而目前已知的利用频谱分析、系统识别等破译方法对于前级的攻击也就无能为力.因此,这一方案的安全性能容易评估,不存在比唯密文攻击更加有效的破译方法.

4. 混沌信号的产生

本实验应用的混沌信号分别为 Lorenz 物理混

沌、Chua 物理混沌和 Lorenz 算法混沌. Lorenz 和 Chua 电路^[16,17] 分别如图 2 和图 3 所示,基波频率均设计为 3 kHz,参数选择已在图中标示.

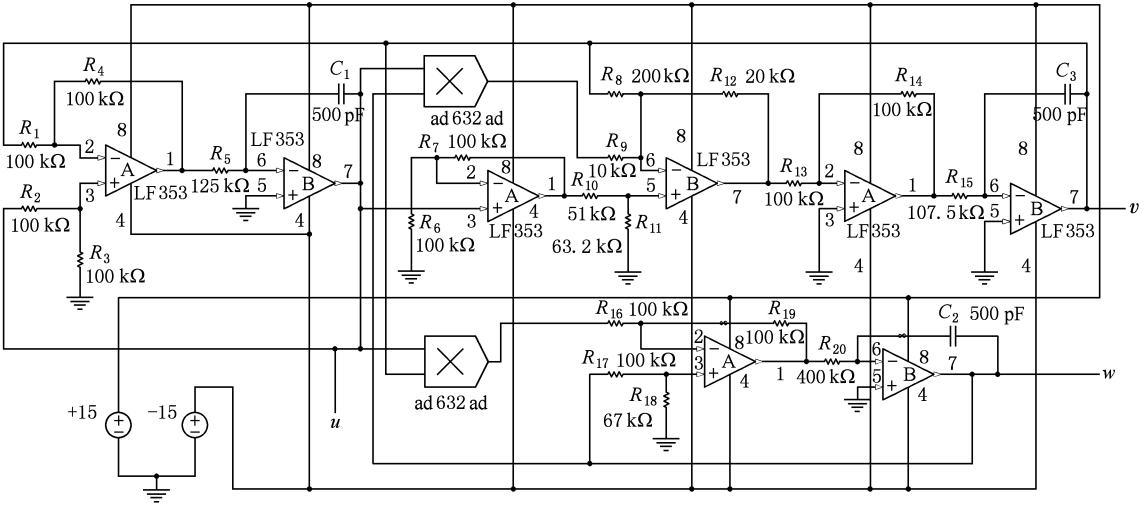


图 2 Lorenz 系统电路

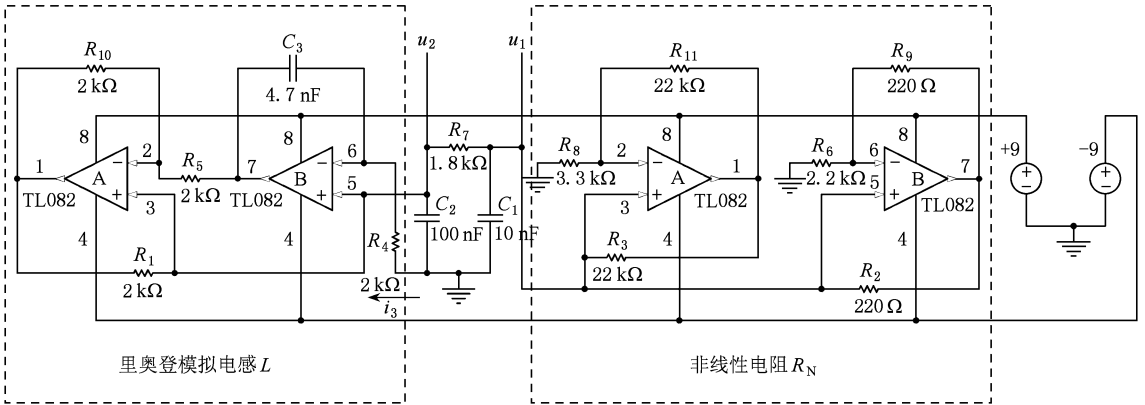


图 3 Chua 系统电路

Lorenz 电路状态方程为

$$\begin{aligned} \dot{u} &= \frac{1}{R_5 C_1} \left[\frac{R_4}{R_1} v - \frac{R_3}{R_2 + R_3} \left(1 + \frac{R_4}{R_1} \right) u \right], \\ \dot{v} &= \frac{R_{14}}{R_{15} C_2 R_{13}} \left[\frac{R_{11}}{R_{10} + R_{11}} \left(1 + \frac{R_{12}}{R_8} + \frac{R_{12}}{R_9} \right) \right. \\ &\quad \times \left(1 + \frac{R_7}{R_6} \right) u - \frac{R_{12}}{R_8} v - \frac{R_{12}}{R_9} u w \left. \right], \\ \dot{w} &= \frac{1}{R_{20} C_3} \left[\frac{R_{19}}{R_{16}} u v - \frac{R_{18}}{R_{17} + R_{18}} \left(1 + \frac{R_{19}}{R_{16}} \right) w \right]. \end{aligned} \quad (1)$$

Chua 电路状态方程为

$$\dot{u}_1 = \frac{u_2 - u_1}{RC_1} - \frac{f(u_1)}{C_1},$$

$$\begin{aligned} \dot{u}_2 &= \frac{u_1 - u_2}{RC_2} + \frac{i_3}{C_2}, \\ \dot{i}_3 &= \frac{-u_2}{L}, \end{aligned} \quad (2)$$

其中非线性电阻 R_N 的特性可表示为

$$\begin{aligned} f(u_1) &= G_b u_1 + 0.5 (G_a - G_b) \\ &\quad \times (|u_1 + E| - |u_1 - E|). \end{aligned}$$

分段线性转折点电压 E 及斜率 G_a, G_b 与元件参数关

系可表示为 $E = \frac{R_8}{E_8 + R_{11}} V_{sat}, G_a = \frac{-1}{R_8} - \frac{1}{R_6}, G_b =$

$\frac{1}{R_3} - \frac{1}{R_6}$, 其中, V_{sat} 为运放的输出饱和电压.

Lorenz 电路和 Chua 电路输出电压的时域波形分别如图 4(a) 和 (b) 所示,采样频率均取 500 kHz.

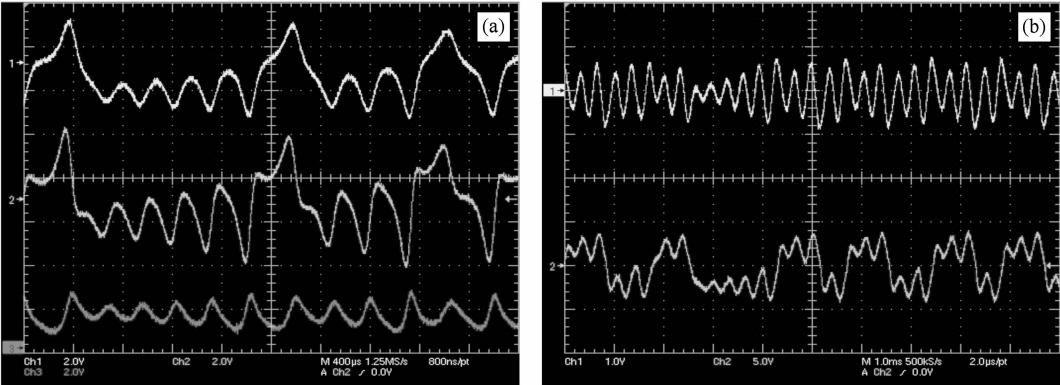


图4 混沌信号的时域波形 (a) Lorenz 电路, (b) Chua 电路

Lorenz 算法混沌的状态方程由物理混沌电路方程归一化得到,

$$\begin{aligned}\dot{x} &= \sigma(y - x), \\ \dot{y} &= \gamma x - y - 20xz, \\ \dot{z} &= 0.5375xy - bz,\end{aligned}\tag{3}$$

其中 $\sigma=1.72, \gamma=34.31, b=0.4312$, 系统时域波形及 x - z 平面相图如图 5 所示.

5. 算法仿真结果

先对涉及的多个不同加密系统予以说明. A 和 B 级联的加密系统以“A-B”标识, 如 Lorenz 物理混沌和 DES 级联的加密系统以“物理 Lorenz-DES”标识, “算法 Lorenz-DES”、“物理 Lorenz-算法 Lorenz”和“物理 Chua-DES”意义类同. 单级加密系统分别以“单级 DES 加密”、“单级物理 Lorenz 加密”和“单级算法 Lorenz 加密”标识, 其中“单级物理 Lorenz 加密”和“单级算法 Lorenz 加密”分别选用与“物理 Lorenz-DES”和“算法 Lorenz-DES”中第一级相同的加密算法和参数.

仿真过程采用 Matlab 7.5 实现并选取 160×160 的 Lena 灰度图作为加密图像, 如图 6(a) 所示. 混沌序列由图 2 所示 Lorenz 混沌电路产生, 各加密结果如图 6(b) 和 (c) 所示. DES 加密密钥为 “#(.5 + a/&”, 正确解密结果如图 6(d) 所示. 若解密密钥作微小变动为 “#).5 + a/&” 时, 解密结果如图 6(e) 所示. 即使解密密钥微小变动都不能得到正确的解密结果, 说明该算法对密钥具有较高的敏感度. 图 6(f) 为单级 DES 加密图像.

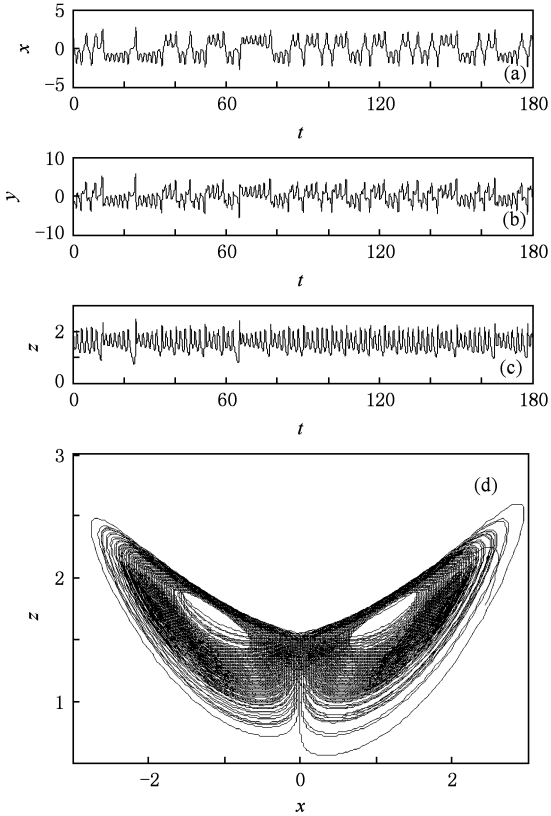


图5 Lorenz 算法混沌的时域波形及 x - z 平面相图 (a) x - t , (b) y - t , (c) z - t , (d) z - x

随机选取 1600 个像素点, 分别画出物理 Lorenz-DES 加密方案中原始图像和加密图像的水平相邻、垂直相邻和对角相邻像素的灰度关系, 如图 7 所示. 从图 7 可以看出, 加密前后图像的相邻像素相关性大大降低.

以上仿真结果一方面验证了算法的正确性, 另

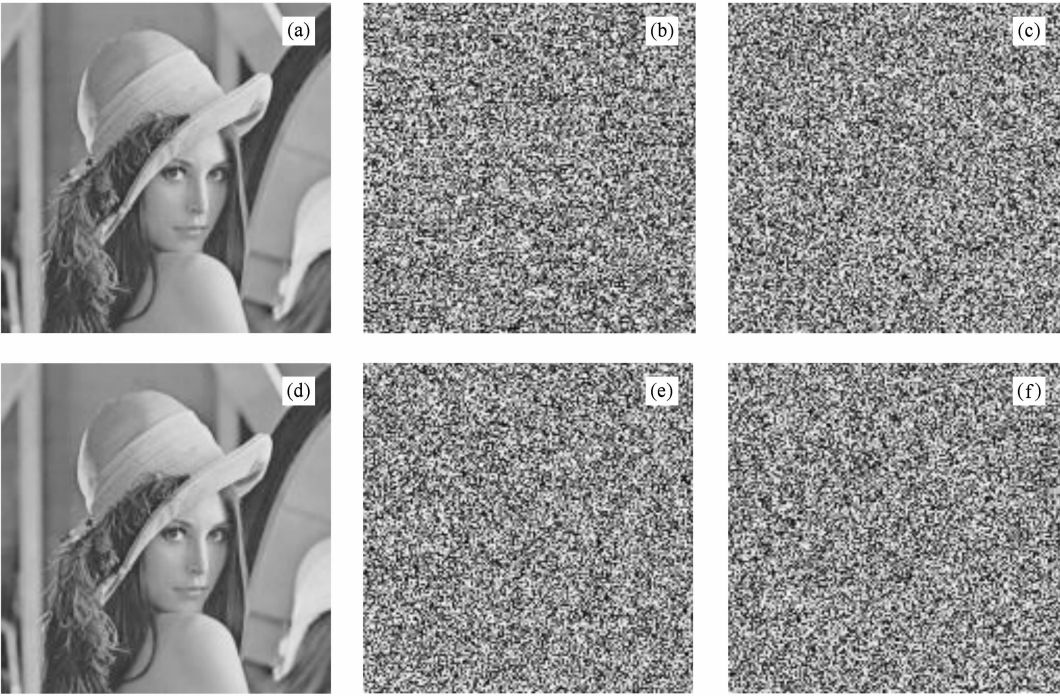


图 6 仿真结果 (a)原始图像,(b)单级物理 Lorenz 加密,(c)物理 Lorenz-DES 加密,(d)正确解密图像,(e)错误解密图像,(f)单级 DES 加密

一方面表明基于该方案的加密系统具有良好的扩散和混淆特性.

5. 1. 物理 Lorenz-DES 和单级加密特性的比较

5. 1. 1. 灰度分布直方图

图 8 所示为原始图像和各加密图像的灰度直方图.

直观上,图(c)灰度均匀性略优于图 8(b)和(d),说明两级级联的加密系统可以改善密文的灰度统计特性.

5. 1. 2. 相邻像素相关系数

选择部分像素进行相邻像素相关系数比较,仅能部分说明加密算法扩散和混淆的程度^[12,18]. 为了进行定量比较,本文选择计算整幅图像相关系数.

$C_{ov}(x,y)$ 表示 x,y 的协方差,定义为
 $C_{ov}(x,y) = E((x - E(x))(y - E(y)))$,
 R_{xy} 表示 x,y 的相关系数,定义为

$$R_{xy} = \frac{C_{ov}(x,y)}{\sqrt{D(x)} \sqrt{D(y)}},$$

式中 $E(x)$ 表示 x 的数学期望, $D(x)$ 表示 x 的方差. 在实际运算中,可通过下式进行:

$$E(x) = \frac{1}{n} \sum_{i=1}^n x_i, \tag{4}$$

$$D(x) = \frac{1}{n} \sum_{i=1}^n (x_i - E(x))^2, \tag{5}$$

$$\overline{C_{ov}}(x,y) = \frac{1}{n} \sum_{i=1}^n E((x_i - E(x))(y_i - E(y))). \tag{6}$$

物理 Lorenz-DES 和单级加密的相邻像素相关系数见表 1.

表 1 物理 Lorenz-DES 级联加密和单级加密相邻像素相关系数				
像素关系	原始图像	单级物理 Lorenz 加密	物理 Lorenz-DES 加密	单级 DES 加密
水平相邻	0. 868032	0. 035213	0. 000487	0. 002717
垂直相邻	0. 960027	0. 002469	0. 003681	0. 003740
对角相邻	0. 885254	0. 001659	-0. 000947	0. 001491

表 1 中数据说明:原始图像三个方向相关系数值从定量的角度反映了图 7 中相邻像素的相关程度,验证了算法的正确性. 级联加密系统相邻像素相关性与单级加密相比总体上有明显改善. 从相邻像素相关系数这一指标来看,单级 DES 加密和单级物理 Lorenz 混沌加密具有相似的特性,但加密速度却相差甚远. 单级 DES 加密耗时约为2209 s,而单级物理 Lorenz 混沌加密却仅需约0. 5 s. 级联加密时间即为两者之和. 因此,当图像加密实时性要求不高

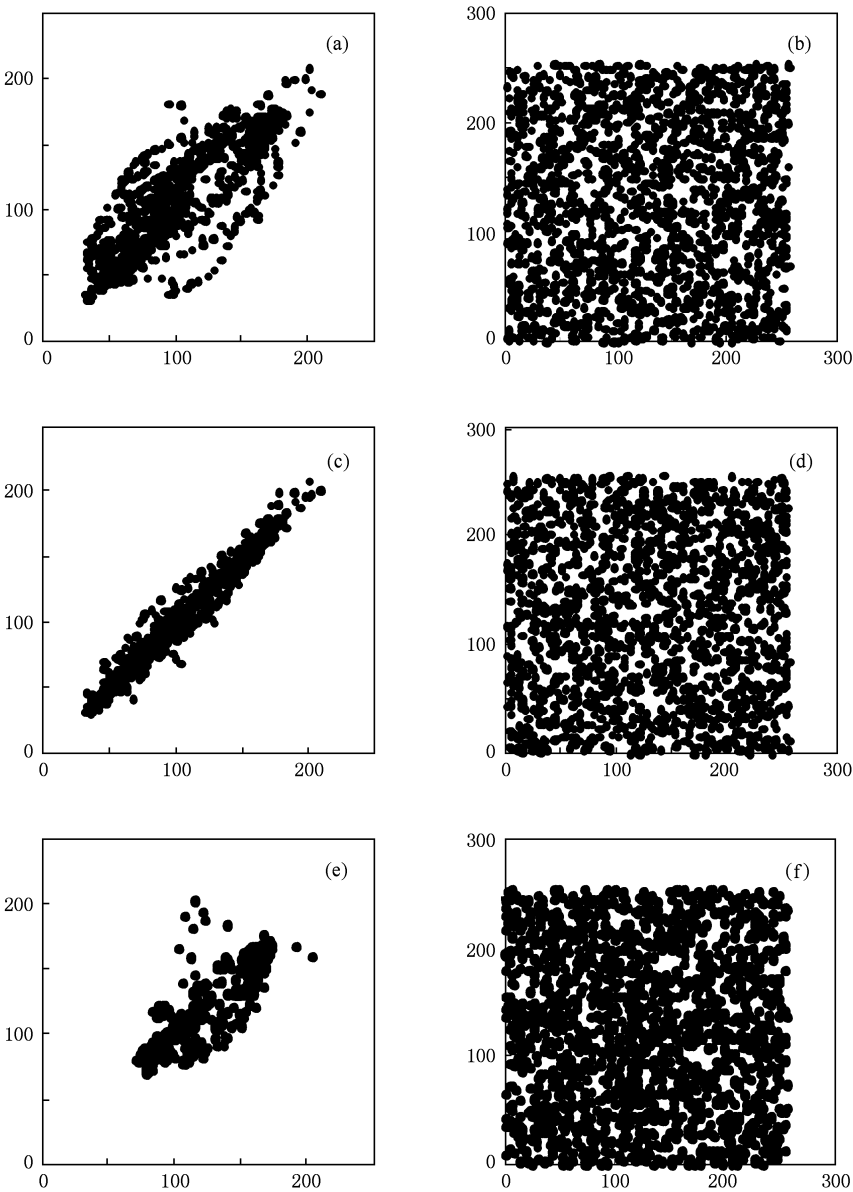


图7 相邻像素灰度相关性比较 (a)和(b)水平相邻,(c)和(d)垂直相邻,(e)和(f)对角相邻

时采取物理混沌-DES 级联的加密方案是合适的,可以充分利用两种系统的优点,获得较高的安全性.若需要兼顾加解密速度,则宜考虑以算法混沌代替DES,即采取“物理混沌-算法混沌”级联的加密系统,其中算法混沌系统主要任务在于形成一定的密钥空间.

表2 中列出了基于 Lorenz 系统的“物理 Lorenz-算法 Lorenz”级联加密各级密文的相关系数.由此可以看出,该级联加密系统同样可以改善密文相关性特性,但逊于物理 Lorenz-DES 加密方案,而加密速度却获得了极大改善,物理 Lorenz-算法 Lorenz 级联

加密系统耗时仅约1 s.后一种方案也因其实时性好而具有应用前景.

表2 物理 Lorenz-算法 Lorenz 级联加密密文相邻像素相关系数			
像素关系	原始图像	第一级输出	第二级输出
水平相邻	0.868032	0.035213	-0.006547
垂直相邻	0.960027	0.002469	0.0015817
对角相邻	0.885254	0.001659	-0.001462

从以上分析可以得出,混沌加密和常规加密级联的主要原因在于两种不同加密体制的优势互补,密文特性总体也有明显改善,从而验证了文献

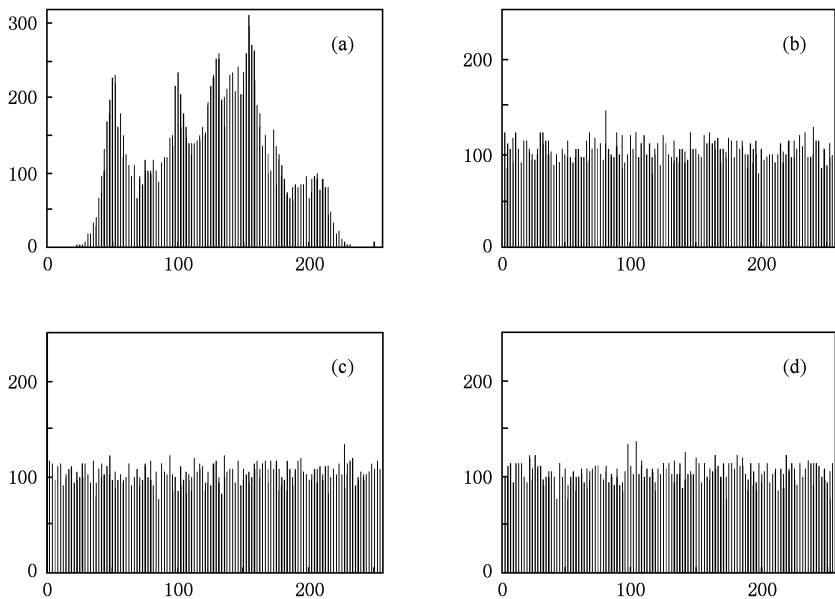


图 8 原始图像及加密图像灰度直方图比较 (a)原始图像,(b)单级物理 Lorenz 加密,(c)物理 Lorenz-DES 加密,(d)单级 DES 加密

[8,9]中提出的该方案的基本原理.

5.2. 不可预测性强弱不同的混沌信号对图像密文特性的影响

同一系统的物理混沌不可预测性强于算法混沌^[13];Lorenz 系统不可预测性强于 Chua 系统. 为了研究不可预测性强弱不同的混沌信号对密文特性的影响,我们选择改变图 1 方案中的混沌系统,并用相邻像素相关系数作为指标来分析比较密文特性的不同.

首先比较物理 Lorenz-DES 加密和算法 Lorenz-DES 加密的密文特性. 将物理 Lorenz 加密系统的混沌信号改为由 Lorenz 算法混沌产生,得到算法 Lorenz 加密系统. 单级物理 Lorenz 加密和单级算法 Lorenz 加密密文的各相关系数比较见表 3,物理 Lorenz-DES 加密和算法 Lorenz-DES 加密的密文相关系数比较见表 4.

表 3 单级物理 Lorenz 加密和单级算法 Lorenz 加密密文相邻像素相关系数

像素关系	原始图像	单级物理 Lorenz 加密	单级算法 Lorenz 加密
水平相邻	0. 868032	0. 035213	0. 073158
垂直相邻	0. 960027	0. 002469	-0. 004562
对角相邻	0. 885254	0. 001659	-0. 006999

表 4 物理 Lorenz-DES 加密和算法 Lorenz-DES 加密密文相邻像素相关系数

像素关系	原始图像	物理 Lorenz-DES 加密	算法 Lorenz-DES 加密
水平相邻	0. 868032	0. 000487	-0. 005076
垂直相邻	0. 960027	0. 003681	0. 004683
对角相邻	0. 885254	-0. 000947	0. 005077

从表 3 和表 4 可以看出:经单级 Lorenz 算法混沌加密后的图像各方向相关系数均大于物理混沌加密的情形;级联 DES 后算法 Lorenz-DES 加密系统密文各相关系数同样明显大于物理 Lorenz-DES 的情形. 重复进行不同基频的多组实验或者将系统换为 Chua 系统,也可得出与此一致的结论.

其次比较物理 Lorenz-DES 加密和物理 Chua-DES 加密特性. 加密方案和算法仿真的相关参数与物理 Lorenz-DES 相同. Chua 混沌序列由图 3 所示的 Chua 电路产生. 表 5 分别列出了两种加密系统各级密文相邻像素相关系数.

表 5 物理 Lorenz-DES 加密和物理 Chua-DES 加密密文相邻像素相关系数

像素关系	原始图像	物理 Lorenz-DES 加密		物理 Chua-DES 加密	
		第一级输出	第二级输出	第一级输出	第二级输出
水平相邻	0. 868032	0. 035213	0. 000487	0. 058051	0. 005760
垂直相邻	0. 960027	0. 002469	0. 003681	0. 005181	-0. 001077
对角相邻	0. 885254	0. 001659	-0. 000947	0. 007755	0. 008295

表 5 表明,单级物理 Lorenz 加密密文相关系数均小于单级 Chua 加密相关系统,且总体上物理

Lorenz-DES 加密密文特性明显优于物理 Chua-DES 系统加密密文特性.

综合以上分析可知,不可预测性越强的混沌信号用于加密时其密文相关性越弱,反之亦然.

6. 结 论

基于物理混沌的混沌加密和常规加密级联的混合加密方案是一种不存在确定明文密文映射关系的、具有较高安全性的加密系统,原理上可以抵

抗除了唯密文攻击之外的其他破译方法. 本文建立了基于该方案的图像加密系统,并对密文统计特性进行了研究. 结果表明:混沌-DES 级联加密系统的密文统计特性明显优于单级加密系统,在兼顾系统安全性与加解密速度方面具有较高的性能. 同时,不可预测性强弱不同的混沌信号在实际加密应用时密文相关性不同,不可预测性越强的信号产生的密文相关性越弱,反之亦然. 这些结论对于混沌图像加密方案选择和信号源选取及其他保密通信中的应用具有重要的参考价值.

[1] Matthews R A J 1989 *Cryptologia* **XIII** 29

[2] Pecora L M, Carroll T L 1990 *Phys. Rev. Lett.* **64** 821

[3] Gotz M, Kelber K, Schwarz W 1997 *IEEE Trans. CAS- I* **44** 963

[4] Dachsel F, Schwarz W 2001 *IEEE Trans. CAS- II* **48** 1498

[5] Kocarev L 2001 *IEEE Circ. Sys. Mag.* **1** 6

[6] Xiang F, Qiu S S 2008 *Acta Phys. Sin.* **57** 6132 (in Chinese)
[向 菲、丘水生 2008 物理学报 **57** 6132]

[7] Li N, Li J F 2008 *Acta Phys. Sin.* **57** 6093 (in Chinese) [李 农、李建芬 2008 物理学报 **57** 6093]

[8] Qiu S S, Chen Y F, Wu M, Ma Z G, Yu S M, Liu X Y 2002 *J. South China Univ. Technol (Natl. Sci. Ed.)* **30** 75 (in Chinese) [丘水生、陈艳峰、吴 敏、马在光、禹思敏、刘雄英 2002 华南理工大学学报(自然科学版) **30** 75]

[9] Qiu S S, Chen Y F, Wu M, Ma Z G, Long M, Liu X Y 2006 *J. Circ. Sys.* **11** 98 (in Chinese) [丘水生、陈艳峰、吴 敏、马在光、龙 敏、刘雄英 2006 电路与系统学报 **11** 98]

[10] Long M, Qiu S S, Peng F 2005 *Comp. Eng. Appl.* **41** 168 (in Chinese) [龙 敏、丘水生、彭 飞 2005 计算机工程与应用 **41** 168]

[11] Long M, Qiu S S, Peng F 2006 *Chin. J. Radio Sci.* **21** 74 (in Chinese) [龙 敏、丘水生、彭 飞 2006 电波科学学报 **21** 74]

[12] Xiang F, Xiao H J, Qiu S S 2007 *J. South China Univ. Technol (Natl. Sci. Ed.)* **35** 31 (in Chinese) [向 菲、肖慧娟、丘水生 2007 华南理工大学学报(自然科学版) **35** 31]

[13] Jin J X, Qiu S S, Xie L Y, Feng M K 2008 *Acta Phys. Sin.* **57** 2743 (in Chinese) [晋建秀、丘水生、谢丽英、冯明库 2008 物理学报 **57** 2743]

[14] Brown R, Chua L O 1996 *Int. J. Bifur. Chaos* **6** 219

[15] Zhang Z Z 2004 *Introduction to Modern Cryptography* (Beijing: Beijing University of Posts and Telecommunications Press) pp2, 3, 106—113 (in Chinese) [章照止 2004 现代密码学基础 (北京:北京邮电大学出版社) 第 2,3,106—113 页]

[16] Cuomo K M, Oppenheim A V, Strogatz S H 1993 *IEEE Trans. CAS- II* **40** 626

[17] Kennedy M P 1993 *IEEE Trans. CAS- I* **40** 657

[18] Peng F, Qiu S S, Long M 2005 *J. South China Univ. Technol (Natl. Sci. Ed.)* **33** 20 (in Chinese) [彭 飞、丘水生、龙 敏 2005 华南理工大学学报(自然科学版) **33** 20]

Cascaded image encryption systems based on physical chaos^{*}

Jin Jian-Xiu[†] Qiu Shui-Sheng

(*School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510640, China*)

(Received 15 January 2009; revised manuscript received 13 April 2009)

Abstract

A cascaded encryption scheme using physical chaos is realized primarily, which combines chaotic encryption with data encryption standard. The difference of statistical properties of cipher text is studied for two cases. One case is that the ciphertexts come from different schemes, i. e. the cascaded and the single-stage ones, respectively. The other is that the ciphertexts are generated by chaotic signals with different unpredictability in the same scheme. Because physical chaos is adopted in this system, there is no assured relationship between plaintexts and ciphertexts, and the statistical characteristics of ciphertexts should be better than (or about equal to) that of any other encryption system. The experimental results support this conclusion, and show that the stronger unpredictability of chaotic signals causes the weaker correlation of ciphertexts.

Keywords: physical chaos, image, cascaded encryption

PACC: 0545

^{*} Project supported by the National Natural Science Foundation of China (Grant No. 60372004) and the Natural Science Foundation for the Youth of South China University of Technology, China (Grant No. E5090790).

[†] E-mail: jxjin@scut.edu.cn