基于电流传输器的网格多涡卷混沌吸引子在混合图像加密中的研究*

林愿[1)2)] 王春华[1)†] 徐浩[1)]

1) (湖南大学信息科学与工程学院, 长沙 410082)

2) (湖南工程学院电气信息学院, 湘潭 411104)

(2012 年 6 月 13 日收到; 2012 年 7 月 6 日收到修改稿)

该文提出了一种新的基于第二代电流传输器 (CCII) 的网格多涡卷混沌吸引子产生器, 用于物理混沌加密和高级加密标准 (AES) 加密的混合图像加密算法. 因 CCII 比普通运放有更好的频率特性和更大的动态范围, 能产生频率更高, 动力学特性更复杂的多涡卷物理混沌信号. 基于 CCII 的多涡卷物理混沌加密和 AES 加密的混合加密系统, 不存在确定的明文密文映射关系, 密文统计特性也应优于其他加密系统. 基于该算法研究了混合加密和单级加密的抗统计分析能力, 以及涡卷数目不同的混沌信号在该算法中应用时密文统计特性的不同. 完成了基于 CCII 的混沌电路设计与硬件实现, 对加密系统进行了数值仿真, 仿真结果与理论分析一致, 同时表明涡卷数目越多的混沌系统其加密产生的密文相关性越弱.

关键词: 电流传输器, 物理混沌, AES, 混合图像加密

PACS: 05.45.Ac, 05.45.Gg

1 引 言

随着多媒体技术的飞速发展, 信息的安全与保密显得越来越重要, 而图像以其直观性、可操作性和大信息量而成为多媒体保密通信中的重要信息载体, 为保护数字图像的安全, 人们提出了许多传统的加密算法, 如数据加密标准 DES 和 AES 等. 传统加密系统的主要优点在于具有成熟的密钥空间设计技术, 且其安全性较易评估, 主要缺点在于明文密文对唯一对应而有可能被破译 [1]. 近年来, 随着混沌理论和应用的快速发展, 许多基于混沌理论的图像加密方案被提出, 基于混沌的加密方案在安全性、速度、复杂度和计算能力等方面表现出优良特性 [2−8]. 然而单一混沌系统面临的最严重的问题是当用数字计算机实现时, 由于有限精度效应, 其混沌动力学特性的快速退化. 因而用轨道简单混沌系统构成的密码直接加密明文, 能从混沌轨道提取有用信息来破解密码 [9]. 根据优势互补的原则, 可将常规加密和混沌加密相混合, 使得除了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对混合加密方案都失效, 因此系统具有较高的安全性 [10], 文献 [11, 12] 初步研究了混合加密系统, 但采用的是没有随机扰动的数值计算装置 (例如计算机) 所产生的算法混沌, 实质上是伪混沌序列, 因其轨道完全取决于初值, 因而是可预测的. 文献 [13] 提出采用物理实现装置所产生的物理混沌加密和 DES 加密来实现混合图像加密, 但采用的物理装置是将普通运放作为有源器件, 来产生双涡卷混沌吸引子, 由于普通运放存在带宽不够宽、转换速率较低以及动态范围不够大等缺点, 难以产生真正适应于保密通信的高频率多涡卷混沌信号 [14,15]. 而且是与 DES 混合加密, 相对而言, AES 的 128 密钥比 DES 的 56 密钥强 1024 倍, 且加密

* 国家自然科学基金 (批准号: 61274020) 和湖南省高校重点实验室开放基金 (批准号: 12K011) 资助的课题.

† E-mail: wch1227164@sina.com

效率更高 [16]. 本文提出一种新的方案, 采用电流传输器作为有源器件来产生网格多涡卷混沌吸引子, 用于物理混沌加密与 AES 加密的混合加密算法. 设计的多涡卷混沌信号比双涡卷混沌信号具有更复杂的动力学特性, 保密性能更好. 完成了基于电流 CCII 的多涡卷混沌电路的设计与硬件实现, 实现电路结构简单, 偏置电压较低, 工作频率较高. 对加密系统进行了数值仿真, 并与其中任一单级加密密文进行了比较分析, 还研究了涡卷数目不同的混沌信号在该混合加密算法中应用时密文特性的不同. 研究结果对混沌信号源的选取及实际图像加密方案的选择具有重要的理论意义与参考价值.

2 基于电流传输器的混合图像加密方案

提出的基于电流传输器产生网格多涡卷混沌吸引子, 用于物理混沌加密和 AES 加密的混合图像加密算法的方案原理框图如图 1 所示.

方案中混沌电路采用电流传输器作为有源器件, 能产生适合保密通信的高频率的多涡卷混沌信号, 从安全性角度考虑, 多涡卷混沌系统比双涡卷混沌系统具有更复杂的相空间, 因此用它设计加密系统能够获得更高的安全性 [17]. 我们充分利用多涡卷物理混沌的不可预测性, 又保留了 AES 作为常规加密系统具有成熟的密钥空间等特性, 使两种加密器优势互补, 整个系统的抗攻击能力高于其中任一级加密器. AES 算法主要包括三个方面: 轮变化、圈数和密钥扩展. AES 不管是从安全性、效率，还是密钥的灵活性等方面都优于 DES, 在今后将逐步代替 DES 而被广泛应用, 因此本方案选择与 AES 进行混合加密.

混合加密算法的主要步骤如下:

1) 混沌电路产生的多涡卷混沌信号经采样得到序列 x_i, x_i 经过变换得到 0—255 之间的整数序列 x_j, $x_j = \mathrm{round}[c(x_{1i}^2 + x_{2i}^2 + x_{3i}^2)^{1/2} + d] \mathrm{mod} 256$, 其中 $c = 3000$, $d = 128$, round 表示取整数. 由 x_j 构成的密钥流 x 对原始信息流 p 进行混沌流密码加密得到密文 c: $c = p \oplus x$.

2) 密文 c 进行 AES 加密得到密文 d.

3) 将密文 d 经信道传输, 接收端收到信号 $\hat{d}$, $\hat{d} = d$.

4) 接收端首先对 $\hat{d}$ 进行 AES 解密, 在解密密钥 $\hat{k}$ 下解密得到解密密文 $\hat{c}$.

5) $\hat{c}$ 经解密密钥 $\hat{x}$ 解密得到解密信息流 $\hat{p}$.

AES 具有足够的安全性, 除了明文密文对唯一对应这个缺陷, 没有已知的方法能攻击 AES[16], 我们采用电流传输器作为有源器件产生物理混沌信号, 经采样后仍然是混沌的. 这种有限精度效应没有改变原有的初值复杂性, 只改变了连续频谱的局部, 与产生伪混沌序列的数字仿真系统具有实质性的不同 [13]. 对于原始信息流 p, 由于物理混沌产生的密钥流 x 是不可预测的, 因而密文 c 是随机变化的, 再经 AES 加密后产生密文 d, p 和 d 由于 c 的不可预测性而不可能唯一对应. 这样, 在原理上混合加密系统中的 AES 加密是不可攻破的了. 前级显著增强了后级的安全性. 在上述系统的 AES 加密这一级不可击破的情况下, 就无法获得其输入信号也就是混沌加密的输出信号 c, 这样利用频谱分析、系统识别等目前已知的破译方法对于混沌加密这一级的攻击也就无能为力. 因此, 这一加密方案不存在比穷举攻击更加有效的破译方法.

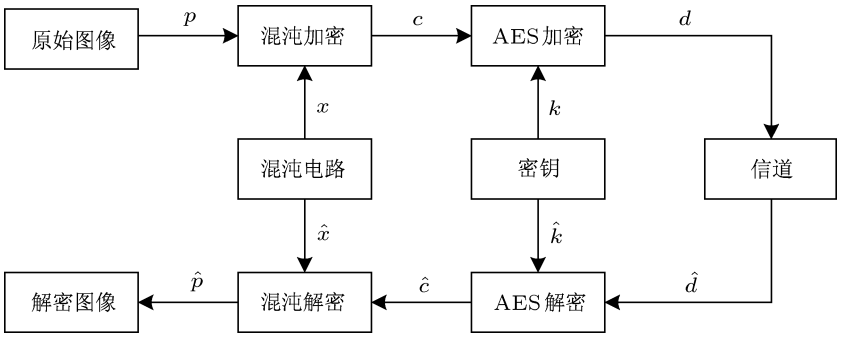

图 1 基于电流传输器的混合图像加密方案原理框图

3 基于电流传输器的网格多涡卷混沌信号的产生

考虑三阶自治非线性系统:

$$\begin{aligned}\dot{x} &= y - f(y),\\ \dot{y} &= z,\\ \dot{z} &= -a(x+y+z-f(x)),\end{aligned} \tag{1}$$

其中 x, y, z 是状态变量, a 是正实数, $f(x)$ 是非线性项, 我们设计为阶梯函数序列, 对应涡卷数目为奇数或偶数的表达式分别为

$$\begin{aligned}f(x) =& A_x\Bigg[\sum_{i=0}^{(Nx-3)/2}(\mathrm{sgn}(x+(2i+1)A_x)\\ &+\mathrm{sgn}(x-(2i+1)A_x)\Bigg], \quad N_x \geqslant 3,\end{aligned} \tag{2}$$

$$\begin{aligned}f(x) =& A_x[-\mathrm{sgn}(x)+\sum_{i=0}^{(Nx-2)/2}(\mathrm{sgn}(x+2\mathrm{i}A_x)\\ &+\mathrm{sgn}(x-2\mathrm{i}A_x))\Bigg], \quad N_x \geqslant 2,\end{aligned} \tag{3}$$

这里 $A_x > 0$,

$$\mathrm{sgn}(x) = \begin{cases} 1, & x > 0,\\ 0, & x = 0,\\ -1, & x < 0.\end{cases}$$

$f(y)$ 也能用 (2) 或 (3) 式来表示, 但要用 y 代替 x. 给定合适的参数 a, 系统 (1) 能产生 2 方向 $N_x \times N_y$ 网格涡卷混沌吸引子, 这里取 $a = 0.7$.

正型第二代电流传输器 (CCII+) 是应用最广泛的电流传输器, 市面上的 CCII 只存在于电流反馈运算放大器 (CFOA) 如 AD844 中, 其内部结构是一个 CCII+ 串联一个电压跟随器, 具有高速和高转换率特性 [18]. 本文提出的混沌电路如图 2 所示, 将 AD844 配置成正负型二代电流传输器 (CCII±s) 来产生混沌信号, 电路结构比文献 [17, 19] 中采用运放实现要简单得多.

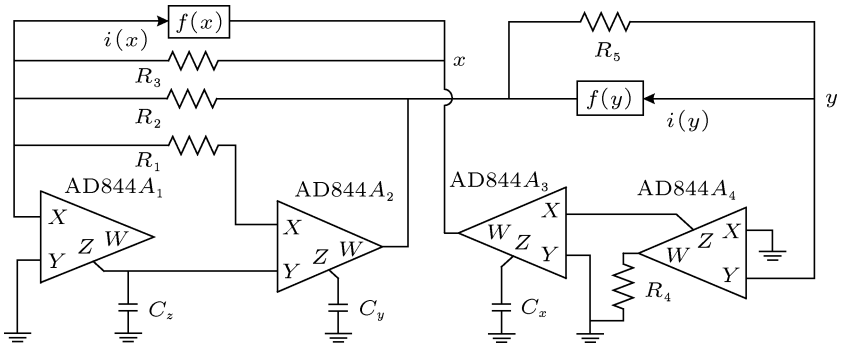

图 2 提出的由 CCII±s 构成的网格多涡卷混沌吸引子产生电路结构图

根据图 2 所示的电路图能严格的推出设计的网格多涡卷混沌电路所对应的动力学方程. 这里 AD844A3 串联 AD844A4 构成一个 CCII-. 考虑到 AD844 的输入输出端口的寄生参数, 其典型值为 $R_{yj} = 10$ MΩ, $R_{xj} = 50$ Ω, $R_{zj} = 3$ MΩ, $C_{yj} = 2$ pF, $C_{zj} = 4.5$ pF, $R_{wj} < 15$ Ω[17], 为了简化, 忽略寄生参数 R_{x1}, R_{w2} 和 R_{w3}, 我们能得到如下的非线性系统方程:

$$\begin{aligned}\dot{x} =& \frac{y}{R_5(C_x+C_{z3})} - \frac{\mathrm{i}(y)}{C_x+C_{z3}},\\ \dot{y} =& \frac{z}{(R_1+R_{x2})(C_y+C_{z2})},\\ \dot{z} =& -\frac{x}{R_3(C_z+C_{z1}+C_{y2})}\\ &-\frac{y}{R_2(C_z+C_{z1}+C_{y2})}\\ &-\frac{z}{(R_1+R_{x2})(C_z+C_{z1}+C_{y2})}\\ &+\frac{\mathrm{i}(x)}{C_z+C_{z1}+C_{y2}}.\end{aligned} \tag{4}$$

比较 (1) 和 (4) 式, 可得到下列关系式:

$$\begin{aligned}&a(C_z+C_{z1}+C_{y2}) = C_x+C_{z3} = C_y+C_{z2},\\ &R_5 = (R_1+R_{x2}) = R_3 = R_2\\ &\quad = \frac{1}{a(c_z+c_{z1}+c_{y2})},\end{aligned} \tag{5}$$

$$f(x) = R_3 \mathrm{i}(x)$$
$$f(y) = R_5 \mathrm{i}(y)$$

阶梯函数序列 $f(x)$ 和 $f(y)$ 采用 CCII+s 配置一个高增益的电压放大器来实现, 如图 3(a) 所示.

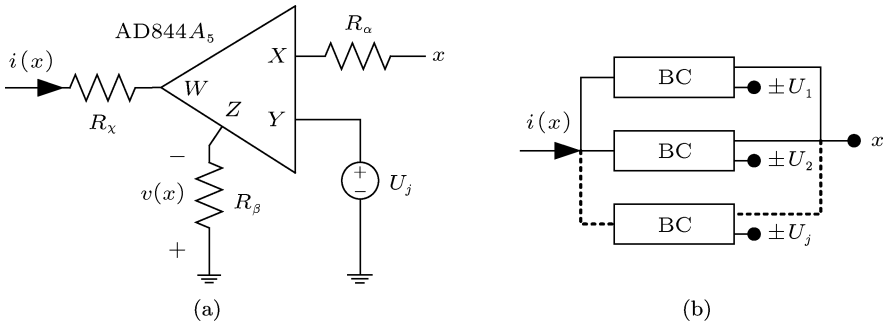

图 3 (a) 设计阶梯函数的基本单元电路; (b) 产生阶梯函数序列的一般结构

图 3 中, $i(x) \approx v(x)/R_\chi$. 为了减小 R_{x5} 和 R_{z5} 的影响, 我们固定 $R_\alpha = 1$ kΩ, $R_\beta = 1$ MΩ. 其他无源元件参数设置如表 1 所示. 我们将图 3(a) 所示的基本单元并联, 如图 3(b) 所示, 配置不同的比较电压 U_j, 能构造出复杂的阶梯函数序列电路, 产生数目不同的网格多涡卷混沌吸引子. 如要产生 2×2 网格涡卷吸引子, 需要一个基本单元用于设计 $f(x)$, 一个基本单元用于设计 $f(y)$. 要产生 3×3 网格涡卷吸引子, 需要两个基本单元并联用于设计 $f(x)$, 两个基本单元并联用于设计 $f(y)$. 实验中, 偏置电压设置为 ±5 V, 远低于文献 [13, 17, 19]. 图 4 和图 5 分别显示了 2×2 和 3×3 网格涡卷混沌吸引子 $x(t)$-$y(t)$ 平面上的相图.

表 1 图 2 中的无源元件的数值

无源元件	2×2 网格涡卷	3×3 网格涡卷
$C_x = 100$ uF	$\lvert E_{\mathrm{sat}}\rvert \approx 1.45$ V	$\lvert E_{\mathrm{sat}}\rvert \approx 1.45$ V
$C_y = 100$ uF	$R_{\chi x} = 22.5$ kΩ	$R_{\chi x} = 32$ kΩ
$C_z = 143$ uF	$R_{\chi y} = 45$ kΩ	$R_{\chi y} = 96$ kΩ
$R_1 = 10$ kΩ		
$R_2 = 10$ kΩ		
$R_3 = 10$ kΩ		
$R_5 = 10$ kΩ		

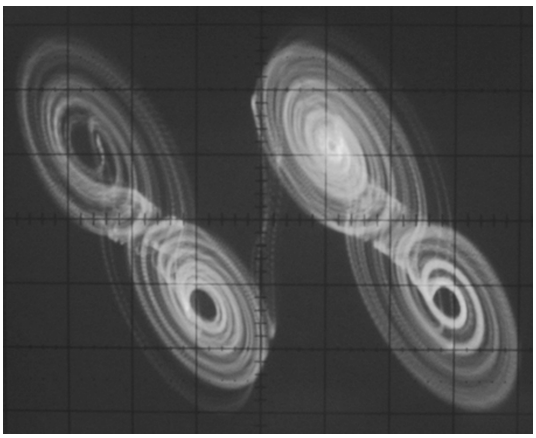

图 4 2×2 网格涡卷混沌吸引子的实验结果 (横坐标: 0.2 V/ 格, 纵坐标: 0.2 V/ 格)

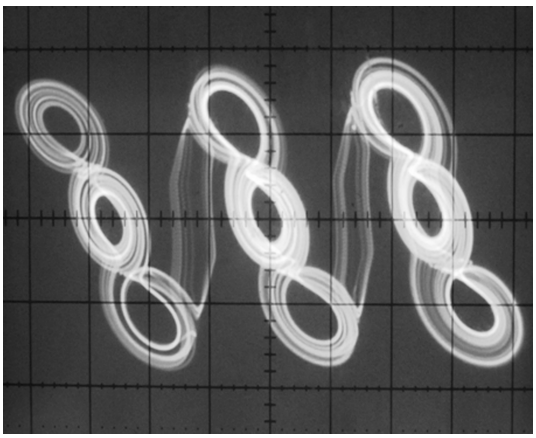

图 5 3×3 网格涡卷混沌吸引子的实验结果 (横坐标: 0.3 V/ 格, 纵坐标: 0.2 V/ 格)

CCII 有较好的高频特性, 可以通过尺度变换缩小 C_x, C_y, C_z 来提高系统的工作频率. 通过多次实验后, 我们发现同等条件下, 3×3 网格涡卷混沌吸引子的频率低于 2×2 网格涡卷混沌吸引子的频率. 这里只给出了当 $C_x = 100$ pF, $C_y = 100$ pF, $C_z = 143$ pF 时, 2×2 网格涡卷混沌吸引子的频谱, 如图 6 所示, 其中心频率达到了 105 kHz, 还能通过采用 CMOS 技术设计 CCIIs 来获得更高的频率 [14]. 远高于文献 [11] 中采用普通运放产生的混沌信号中心频率 3kHz, 本实验中采样频率取 500 kHz.

4 混合图像加密算法仿真结果

仿真过程采用 Matlab7.8 实现, 选取 256×256 的 Lena 灰度图作为原始图像, 如图 7(a) 所示, 混沌信号采用 2×2 网格涡卷混沌信号.

4.1 密钥敏感性分析

为了测试该混合加密算法对密钥的敏感性, 将 AES 的加密密钥设为 ′2b′ ′7e′ ′15′ ′16′ ′28′ ′ae′ ′d2′ ′a6′ ′ab′ ′f7′ ′15′ ′88′ ′09′ ′cf′ ′4f′ ′3c′, 正确解密结果如图 7(d) 所示. 若密钥某一位作细微变动, 比如变为 ′3b′ ′7e′ ′15′ ′16′ ′28′ ′ae′ ′d2′ ′a6′ ′ab′ ′f7′ ′15′ ′88′ ′09′ ′cf′ ′4f′ ′3c′ 时, 解密结果如图 7(e) 所示, 该混合加密算法保留了 AES 成熟的密钥空间特性, 对密钥有较高的敏感性, 任何一位稍有不同均不能正确解密. 而 AES 的密钥为 128 位二进制数, 所以 AES 的密钥空间为 2^{128}, 足以应对目前的实际需求.

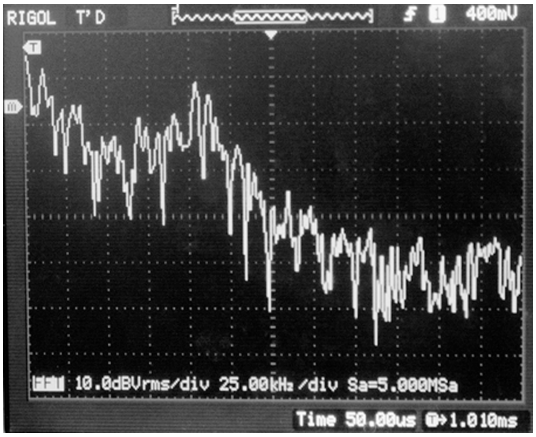

图 6 实验测量到的 2×2 网格涡卷混沌频谱

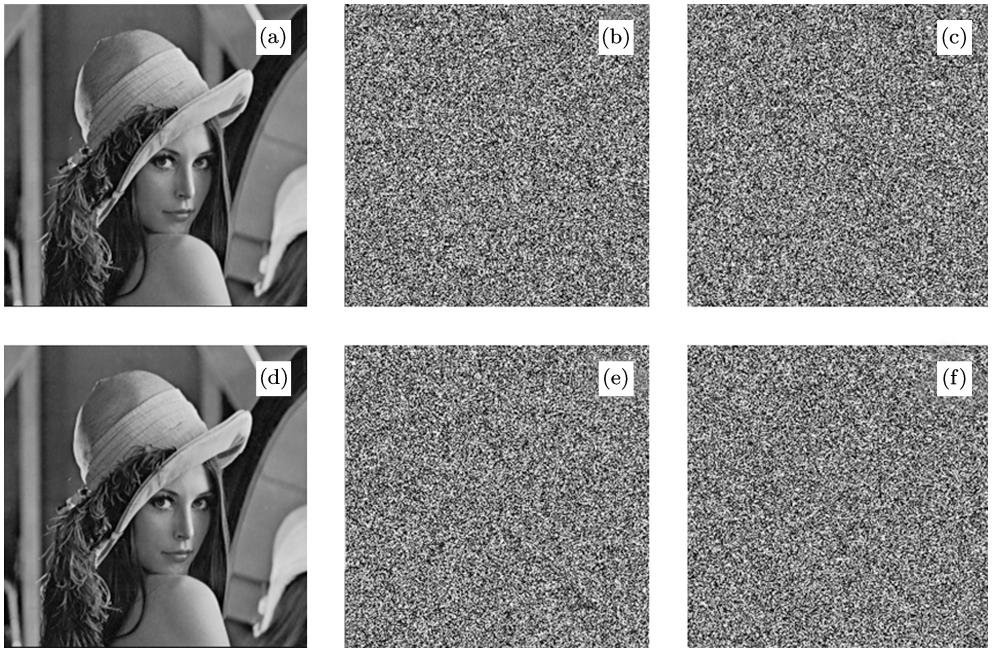

图 7 仿真结果 (a) 原始图像; (b) 物理混沌 AES 加密; (c) 单级 AES 加密; (d) 正确解密图像; (e) 错误解密图像; (f) 单级物理混沌加密

4.2 统计分析

4.2.1 灰度分布直方图

如图 8 所示, 从直观上来看, 混合加密图像的直方图与原始图像的直方图有很大的区别, 并且非常均匀, 表明密文的像素值在 [0—255] 范围内的取值概率均等, 即对整个密文空间呈均匀分布, 说明该混合加密算法能有效的防止统计攻击.

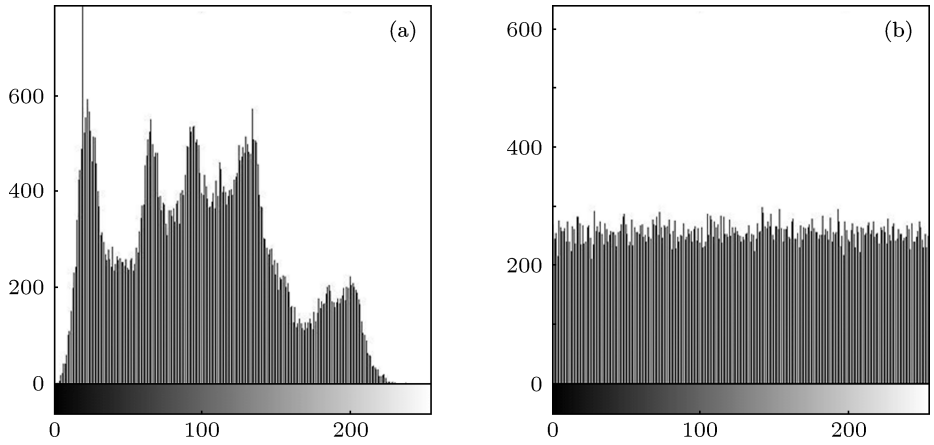

图 8 原始图像及经物理混沌 -AES 加密图像灰度直方图比较 (a) 原始图像; (b) 加密图像

4.2.2 相关性分析

数字图像中各个像素不是相互独立的, 其相关性很大, 这说明大块区域中的灰度值相差不大, 因此图像的冗余度很大. 图像加密的一个目标之一就是减小图像相邻像素相关性, 主要包括水平像素、垂直像素和对角线像素间的相关性. 显然, 相关性越小, 说明图像加密效果越好, 安全性越高.

图 9 所示分别为原始图像和经物理混沌 -AES 混合加密后的图像相邻像素在垂直方向、水平方向和对角方向上的相关性. 从原始图像和加密图像的相邻像素相关性可以部分说明该加密算法的扩散和混淆的程度.

为了定量比较混合加密和单级加密的抗统计分析能力, 本文选择计算整副图像的像素相关系数 ρ_{xy}, 计算如下:

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

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

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_j - E(y)), \tag{8}$$

$$\rho_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)\cdot D(y)}}, \tag{9}$$

其中 x 和 y 分别表示图像中相邻两个像素点的像素值, ρ_{xy} 为相邻两个像素点的相关系数. 表 2 所列分别为原始图像、经 AES 单级加密图像、经单级物理混沌加密图像和经物理混沌 -AES 混合加密图像的相邻像素之间按水平、垂直和对角 3 个方向根据式 (9) 计算所得的相关系数.

表 2 中数据说明: 原始图像的相邻像素高度相关, 相关系数接近于 1. 物理混沌 -AES 混合加密系统相邻像素相关性与单级 AES 加密、单级物理混沌加密相比总体上有明显改善, 接近于 0, 其相邻像素已基本不相关, 这说明原始图像的统计相关性已经被扩散到随机的密文图像中了, 验证了该混合加密算法的正确性.

4.3 涡卷数目不同的混沌信号对图像密文统计特性的影响

混沌系统的涡卷数目越多, 相空间越复杂, 因此用它设计加密系统能够获得越高的安全性 [17]. 为了研究涡卷数目不同的混沌信号对密文特性的影响, 我们改变图 2 中产生 $f(x)$ 和 $f(y)$ 的基本单元的个数, 使之产生 3×3 网格涡卷, 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. 2×2 和 3×3 网格涡卷算法混沌 -AES 加密和物理混沌 -AES 加密密文的各相关系数比较见表 2 和表 3. 从表中数据可以看出: 经涡卷数目相同的物理混沌 -AES 加密的图像各方向相关系数均小于经算法混沌 -AES 加密的情形; 经涡卷数目越多的算法混沌 -AES 加密的图像各方向相关系数均小于涡卷数目少的算法混沌 -AES 加密的情形; 经涡卷数目越多的物理混沌 -AES 加密的图像各方向相关系数均小于涡卷数目少的物理混沌 -AES 加密的情形.

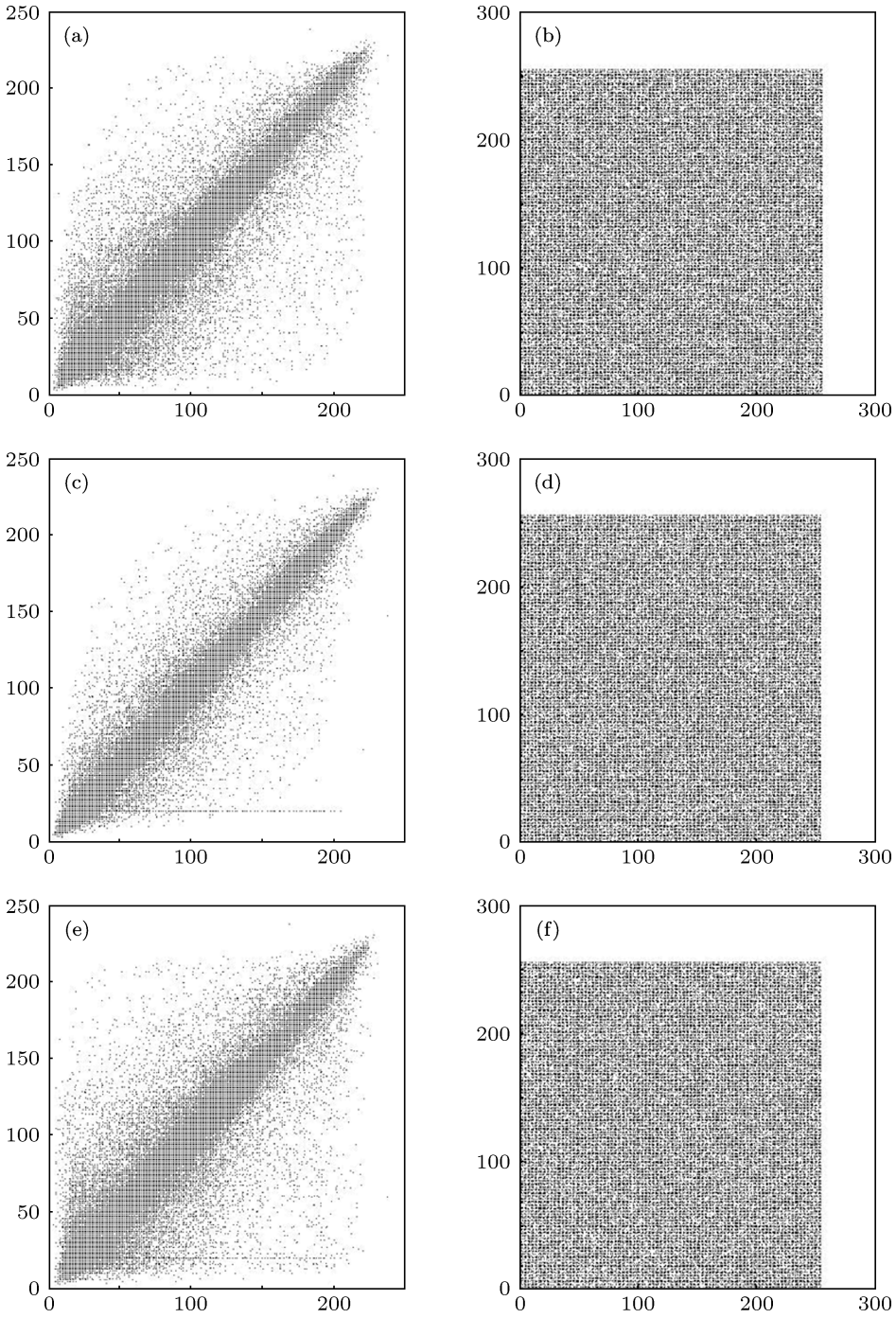

图 9 相邻像素相关性比较 (a) 与 (b) 水平相邻; (c) 与 (d) 垂直相邻; (e) 与 (f) 对角相邻

表 2 原始图像、AES 加密、物理混沌加密、物理混沌 -AES 混合加密密文相关系数比较

像素关系	原始图像	单级 AES 加密	单级物理混沌加密 (2 × 2)	物理混沌 (2 × 2) -AES 加密
水平相邻	0.941692	−0.003129	0.020316	−0.001144
垂直相邻	0.964861	0.002284	−0.003257	−0.000704
对角相邻	0.914658	0.001328	0001579	0.000629

表 3 原始图像和 2 × 2 和 3 × 3 网格涡卷混沌 -AES 加密密文相关系数

像素关系	原始图像	算法混沌 (2 × 2) -AES 加密	算法混沌 (3 × 3) -AES 加密	物理混沌 (3 × 3) -AES 加密
水平相邻	0.941692	0.002000	−0.001865	−0.001023
垂直相邻	0.964861	−0.003125	−0.002876	−0.000654
对角相邻	0.914658	0.000895	0.000786	0.000579

本文提出的方案与文献 [13] 提出的方案相比较, 从相邻像素相关系数这一指标来看, 文献 [13] 中加密图像的水平相邻、垂直相邻、对角相邻像素相关系数分别为 0.000487, 0.003681, −0.000947, 本方案中采用 3 × 3 网格涡卷物理混沌 -AES 加密方案在这一指标上有改善.

从加密速度来看, 我们使用 2.7 GHz Intel 双核处理器, 2 G 内存的计算机系统, 在 MATLAB7.8 软件平台下进行物理混沌 -AES 混合图像加密仿真, 原始图像为 256 × 256 的 Lena 灰度图, 单级物理混沌加密时间约为 0.3s, 单级 AES 加密时间约为 37s, 混合加密时间为两者之和 37.3s. 当图像加密实时性要求不高时, 采用该方案的软件实现是合适的. 若要兼顾加密速度和加密质量, 则宜考虑物理混沌 -AES 混合加密的硬件实现. 因为物理混沌加密是将采样到的混沌序列与信息流进行逐位异或运算, 其硬件实现是实时的, 而 AES 加密的硬件实现比其软件实现快很多, 能满足图像加密实时性要求 [20].

5 结 论

提出了一种新的基于电流传输器产生网格多涡卷混沌吸引子, 用于物理混沌加密和 AES 加密的混合图像加密算法, 我们对基于电流传输器的网格多涡卷混沌电路进行了设计与硬件实现, 所设计的混沌电路结构简单, 偏置电压较低, 产生的混沌信号频率较高. 基于电流传输器的物理混沌加密和 AES 加密的混合加密算法, 不存在确定的明文密文映射关系, 具有较高的安全性, 原理上可抵抗除了穷举攻击之外的一切破译方法. 文中对混合加密系统进行了数值仿真, 结果显示: 该混合加密算法的密文统计特性明显优于单级加密系统, 在综合考虑安全性与加密速度方面具有较高的性能. 同时, 表明涡卷数目越多的混沌系统其加密产生的密文相关性越弱. 这些结论对于混沌信号的产生与选取、混沌图像加密方案选择及其他保密通信中的应用具有重要的参考价值.

[1] Fu C, Lin B B, Miao Y S, Liu X, Chen J J 2011 *Opt. Commun.* **284** 5415

[2] Tang G, Liao X F 2005 *Chaos Soliton. Fract.* **23** 1901

[3] Zhang L H, Liao X F, Wang X B 2005 *Chaos Soliton. Fract.* **24** 759

[4] Xiang T, Wong K W, Liao X F 2007 *Chaos* **17** 12

[5] Pareek N K, Patidar V, Sud K K 2006 *Image Vision Comput.* **24** 926

[6] Wong K, Kwok B, Law W 2008 *Phys. Lett.* A **372** 2645

[7] Wang J, Jiang G P 2011 *Acta Phys. Sin.* **6** 060503 (in Chinese) [王静, 蒋国平 2011 物理学报 **6** 060503]

[8] Liu Y R, Wu Z M, Wu J G, Li P, Xia G Q 2012 *Acta Phys. Sin.*

61 024203 (in Chinese) [刘宇然, 吴正冒, 吴加贵, 李萍, 夏光琼 2012 物理学报 **61** 024203]

[9] Ashraf A Z, Abdulnasser A R 2011 *Commun. Nonlinear Sci Numer Simulat.* **16** 3721

[10] 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]

[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 Ch inese) [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 2010 *Acta Phys. Sin.* **59** 792 (in Chinese) [晋建秀, 丘水生 2010 物理学报 **59** 792]

[14] Sanchez L C, Trejo G R, Munoz P J M, Tlelo C E 2010 *Nonlinear Dyn.* **61** 331

[15] Yang Z M, Zhang J, Ma Y J, Bai Y L, Ma S Q 2010 *Acta Phys. Sin.* **59** 3007 (in Chinese) [杨志民, 张洁, 马永杰, 摆玉龙, 马胜前 2010 物理学报 **59** 3007]

[16] Zhang Z Z 2004 *Introduction to Modern Cryptography* (Beijing: Beijing University of Posts and Telecomm unications Press) p106 (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 106 页]

[17] Sanchez L C 2011 *Appl. Math. Comput.* **217** 4350

[18] AD844 Data sheet, http://www.analogdevices.org [2012-6-2]

[19] Zhang C X, Yu S M 2009 *Acta Phys. Sin.* **58** 0120 (in Chinese) [张朝霞, 禹思敏 2009 物理学报 **58** 0120]

[20] Ming H J, Zih H C, Jian H C, Yan H C 2007 *Microprocess Microsy***91** 102

Grid multi-scroll chaotic attractors in hybrid image encryption algorithm based on current conveyor*

Lin Yuan[1)2)] Wang Chun-Hua[1)†] Xu Hao[1)]

1) (*College of Information Science and Engineering, Hunan University, Changsha* 410082*, China*)

2) (*College of Electrical & Information Engineering, Hunan Institute of Engineering, Xiangtan* 411104*, China*)

(Received 13 June 2012; revised manuscript received 6 July 2012)

Abstract

In this paper we propose a novel grid-scroll chaotic attractor generator based on the second generation current conveyor(CCII), which is used for hybrid image encryption of physical chaos encryption and advanced encryption standard (AES) encryption algorithm, because CCII has a higher speed and larger dynamic range than ordinary operational amplifier and can generate multiscroll physical chaotic signal with higher frequency and more complex dynamics properties. The hybrid encryption system of multiscroll physical chaos encryption and AES encryption based on the CCII, does not assure the relationship between plaintext and ciphertext, and the statistical characteristics of ciphertexts in this algorithm should be better than those of any other encryption system. The difference in statistical property of cipher text between the two cases is studied. One case is that the ciphertexts come from different schemes, i. e. the hybrid and the single stage ones, respectively, and the other is that the ciphertexts are generated by chaotic signals with different numbers of scrolls in the same algorithm. We design and implement the chaos circuit based on CCII, and simulat the encryption system. The results shown that they are in agreement with the theoretical analyses, and that the bigger number of scrolls chaotic system causes the weaker correlation of ciphertexts.

Keywords: current conveyor, physical chaos, AES, hybrid image encryption

PACS: 05.45.Ac, 05.45.Gg

* Project supported by the National Natural Science Foundation of China (Grant No. 61274020), and the Open Fund Project of Key Laboratory in Hunan Universities (Grant No. 12K011).

† E-mail: wch1227164@sina.com