

引用格式:王勇,叶树成,王瑛. 双随机相位编码与 AES 结合的图片加密方案 [J]. 微电子学与计算机, 2020, 37(7): 71-77.
[WANG Y, YE S C, WANG Y. Image encryption scheme combining dual random phase encoding and AES[J]. Microelectronics & Computer, 2020, 37(7): 71-77.]

双随机相位编码与 AES 结合的图片加密方案

王 勇, 叶树成, 王 瑛

(广东工业大学 计算机学院, 广东 广州 510003)

摘 要: 针对双随机相位编码光学加密系统(DRPE)易于被密码分析的问题,提出了一种将双随机相位编码与 AES 结合的图片加密方案. 该算法的主要思想是首先利用四维超混沌系统迭代生成的混沌序列来设计随机相位版和 AES 目标密钥,以此扩大密钥空间和增强密钥随机性来提高系统安全性,其次通过在 DRPE 第二透镜输出面植入 AES 加密算法实现双重加密. 模拟仿真实验表明,与同类加密算法相比,该算法有效加强了加密系统密钥的随机性,使得密文的相关系数更低,同时克服了双随机相位编码第二透镜的无效性的不足,具有较高的安全性.

关键词: 超混沌系统;DRPE;AES;双重加密

中图分类号: TP3

文献标识码: A

文章编号: 1000-7180(2020)07-0071-07

Image encryption scheme combining dual random phase encoding and AES

WANG Yong, YE Shu-cheng, WANG Ying

(School of computers, Guangdong University of Technology, Guangzhou 510003, China)

Abstract: Aiming at the problem that the double random phase encoding optical encryption system (DRPE) is easy to be cryptographically analyzed, this paper proposes an image encryption scheme combining dual random phase encoding and AES. The main idea of the algorithm is to first design the random phase version and AES target key by using the chaotic sequence iteratively generated by the four-dimensional hyperchaotic system, thereby expanding Key space and enhanced key randomness to improve system security. A double encryption is implemented by implanting AES encryption algorithm on the second lens output surface of DRPE. Simulation experiments show that comparing to the similar encryption algorithms, the algorithm enhances the randomness of the encryption system key, and makes the ciphertext correlation coefficient lower, and also overcomes the invalidation of the second lens of the double random phase encoding, which has high security.

Key words: hyperchaotic systems ;DRPE ;AES ;double encryption

1 引言

图像加密技术是互联网安全领域的一个重要研究课题. 其中,光学系统由于其高速和并行处理的优点,在图像加密领域引起了广泛关注. Refregier 和 Javidi^[1]提出了双随机相位编码(DRPE)的开创性

成果,后来也有许多改进算法,例如通过在不同的光学变换域中实现 DRPE^[2]. 然而这些方案忽略了 DRPE 弱安全性的关键内部因素.

对此,为了解决 DRPE 中傅里叶域的密文安全问题,本文提出一种基于双随机相位编码和 AES 结合的图片加密方案,在 DRPE 第二透镜输出平面后

植入改进版 AES 加密算法,同时,利用超混沌系统来设计出随机相位版、AES 目标密钥和 S 盒,解决传统 AES 算法中密钥的固定性和 S 盒的不变性的缺点,扩大了系统密钥空间,有效提高系统整体的安全性。

2 算法原理

2.1 四翼超混沌系统

结合传统 Qi 系统的二次项和三次项,产生的新型数学模型为

$$\begin{cases} \dot{x} = a(y-x) + yz + yzw \\ \dot{y} = b(x+y) + xz - xzw \\ \dot{z} = -cz + ey + xyw \\ \dot{w} = -dw + xyz \end{cases} \quad (1)$$

当式(1)中系统参数 $a=30, b=7, c=8, d=12, e=5$ 时,系统能够产生如图 1 所示的穿过零线的上下吸引子,形成真正的四翼吸引子。

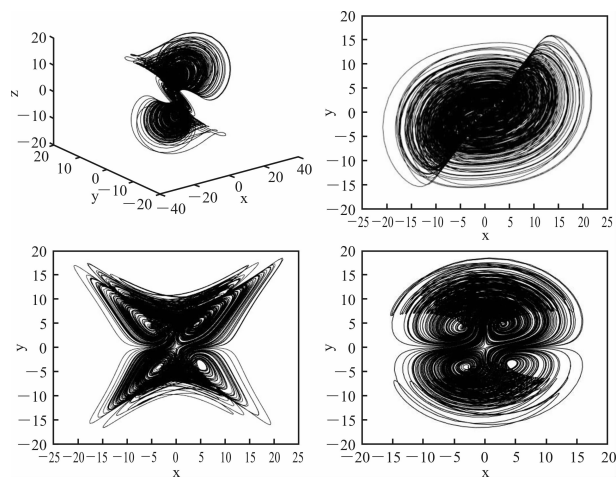


图 1 四翼混沌吸引子

经过计算,该系统产生的 4 个 Lyapunov 指数满足 $L_1 > L_2 > L_3 > L_4$ 的混沌系统要求。

2.2 AES 加密算法

传统的 AES 加密算法由于初始密钥的固定性,还有 S 盒的不变性,导致传统的密钥比较容易破解^[3]。本文对传统 AES 加密算法进行了相应的改进,通过结合明文特性的超混沌序列作为初始值,利用哈希表来设计出 S 盒并且通过前后置乱来产生密钥,然后进行 1 轮加密。算法分为 4 步:(1)字节代换:将状态矩阵每个值的后 4 位作为列坐标,前 4 位二进制作为行坐标,查询 S 盒对应的值进行替换;(2)行移位:对矩阵中第 i 行右移 i 个字节;(3)列混

合:通过 GF 二元乘法对状态矩阵与一组特定矩阵进行矩阵相乘;(4)轮密相加:将状态矩阵与密钥进行矩阵异或运算。AES 加密过程如图 2 所示。

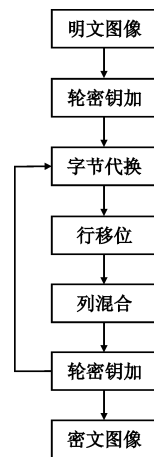


图 2 AES 算法加密过程

2.2.1 明文相关参数

对于一个像素大小为 $m \times n$ 的灰度图像,设 t 是与明文像素密切相关的控制参数, S 是图像所有像素值的和, avg 是图像所有像素值的平均值,其中:

$$\text{avg} = \frac{S}{m \times n} \quad (2)$$

$$t = m \times n + \text{mod}(\text{avg} \times 10^{12}, 8 \times (m + n)) \quad (3)$$

2.2.2 S 盒的设计

四翼超混沌系统通过公式(1)产生的混沌序列有可能出现重复元素值,为了避免此现象同时保留混沌序列的随机性,本文对 S 盒的构造进行改进,步骤如下:

Step1:先由四翼超混沌系统迭代产生混沌序列,从第 t 项后开始截取超混沌序列,选取其中 256 个元素值组成一个新序列 seq , seq 可表示为 $\text{seq} = \{s_1, s_2, s_3, \dots, s_{256}\}$ 。

Step2:创建一个长度同样是 256 的哈希表 H ,使用直接定址法将原序列 seq 的元素值插入到哈希表 H 中,处理冲突的方法是线性探测再散列,公式如下:

$$H_i = \text{mod}(s_i + 1, 256) \quad (4)$$

每当一个元素值插入到哈希表中,则将该元素在原 seq 序列中的值替换成其在哈希表中的索引值,并得到一个全新的序列 $\text{seq}' = \{s'_1, s'_2, s'_3, \dots, s'_{256}\}$,然后将序列 seq' 转换成 16×16 的矩阵作为 S 盒。

2.3 双随机相位编码 DRPE

双随机相位编码光学系统是采用标准的 $4-f$ 系

统来实现的,本文首先利用截取的超混沌序列作归一化处理产生两块随机相位版 RPM,将两块随机相位版分别置于光学系统的输入平面和傅里叶平面,分别扰乱原始明文图像 $f(x,y)$ 的空间信息和频谱信息,从而实现加密得到密文图像 $c(x,y)$,RPM1 和 RPM2 的相位调制函数分别用 $\exp[j2\pi t(x,y)]$ 和 $\exp[j2\pi b(\alpha,\beta)]$ 来表示,其中 x,y 表示空间坐标, α,β 表示频域坐标.加密公式如下:

$$c(x,y) = \text{IFT}\{\text{FT}[f(x,y) * \text{RPM1}] * \text{RPM2}\} \quad (5)$$

$$\text{RPM1} = \exp[j2\pi t(x,y)] \quad (6)$$

$$\text{RPM2} = \exp[j2\pi b(\alpha,\beta)] \quad (7)$$

式中,FT 和 IFT 表示傅里叶变换和傅里叶逆变换.加密过程如图 3 所示.

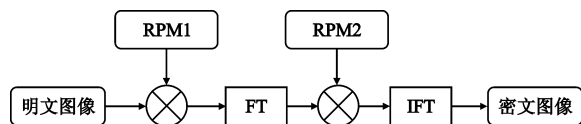


图 3 DRPE 加密过程

2.4 加密和解密原理

2.4.1 加密原理

本文选取 256×256 的灰阶图像作为明文图像,然后将明文图像转换成对应大小的矩阵,其中元素值的取值范围是 $[0,255]$.加密算法过程如图 4 所示,步骤如下:

Step1:为四翼超混沌系统设置初始值 x,y,z,w ,设循环次数 len 为 $2 * 256 * 256$,在每次循环中,利用四阶龙格库塔法对公式(1)进行求解,得到一组新的数据 $\{x,y,z,w\}$,通过公式(8)计算状态变量 s ,其中 $\text{floor}(x)$ 表示取小于或等于 x 的最大整数;当 $s=0$ 时,将 $\{x,y,z,w\}$ 插入序列 D 中;当 $s=1$ 时,将 $\{y,x,z,w\}$ 插入序列 D 中;当 $s=2$ 时,将 $\{z,y,w,x\}$ 插入序列 D 中;当 $s=3$ 时,将 $\{w,z,y,x\}$ 插入序列 D .如此循环 len 次,得到一个原始超混沌序列 D .

$$s = \text{mod}(\text{floor}(\sqrt{x^2 + y^2 + z^2 + w^2}), 4) \quad (8)$$

Step2:通过公式(9)对原始超混沌序列 D 进行改造,然后利用公式(3)得到的控制参数 t ,从第 t 项开始截取序列,目的是消除暂态效应带来的不良影响,得到一个新的超混沌序列 K .

$$K(i) = \text{mod}(\text{floor}((|D_i| - \text{floor}(|D_i|)) \times 1012), 256) \quad i = 1, 2, \dots \quad (9)$$

Step3:利用超混沌序列 K 构造两个随机相位

版和 AES 密钥,随机相位版 RPM1 和 RPM2 大小各取 $[256, 256]$,密钥矩阵 Keys 大小应该是 $[256, 256 \times 2]$,获取 K 中 256×256 个数据作为第一组并存入 RPM1 中,同样地取第二组 256×256 个数据并存入 RPM2 中,取同样长度的第三和第四组数据填入密钥矩阵中.

Step4:按照 2.3 中的流程将原始明文图像与第一个随机相位版 RPM1 进行一次空域滤波,然后经过傅里叶变换,继续利用第二个随机相位版 RPM2 进行频域滤波,最后经过傅里叶逆变换操作得到初步加密图像.

Step5:将初步加密图像进行 AES 二次加密.先将密钥矩阵的第 0 到 255 列组成的第一个加密密钥 key 与明文图像进行异或运算,得到一个状态矩阵 A_1 .

Step6:对状态矩阵进行字节代换,根据前面 2.2.2 节中的方法构造 S 盒,然后将状态矩阵每个元素值取二进制值,其中后 4 位转为十进制后作为列坐标,同样地前 4 位转十进制后作为行坐标,对应 S 盒的值进行替换,得到状态矩阵 A_2 .

Step7:进行行移位:对状态矩阵中每一行进行一次右移处理,其中第 n 行右移 n 个字节,得到下一个状态矩阵 A_3 .

Step8:进行列混合:将状态矩阵 A_3 与矩阵 $[02, 03, 01, 01; 01, 02, 03, 01; 01, 01, 02, 03; 03, 01, 01, 02]$ 进行矩阵相乘,其中涉及的乘法和加法都是定义在基于 $\text{GF}(2^8)$ 上的二元运算,采用行优先的方式相乘后得到状态矩阵 A_4 .

Step9:进行轮密钥加运算,将状态矩阵 A_4 与密钥 key 进行异或运算,其中密钥 key 是由密钥矩阵 Keys 取第 256 到 $256+255$ 列组成.最后得到最终密文,将其转化成最终的加密图像.

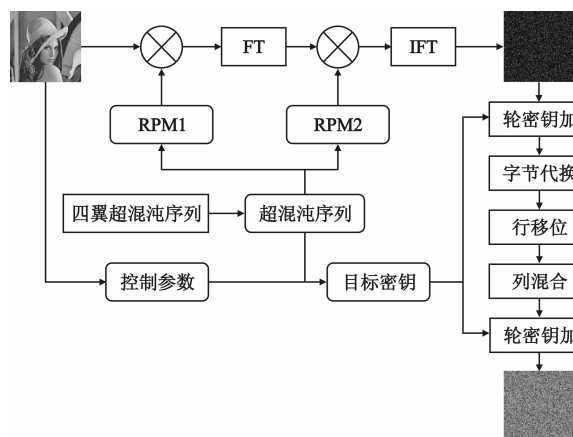


图 4 加密过程

2.4.2 解密原理

解密过程是加密过程的逆过程,先对密文图像进行 AES 解密,先用 Step9 的同一段密钥进行轮密钥加运算,接着进行逆列混合,其中逆相乘的矩阵 $[14, 11, 13, 09, 09, 14, 11, 13, 13, 9, 14, 11, 11, 13, 9, 14]$,然后进行逆行移位,即向左移动元素,接着字节代换逆操作,其中逆 S 盒由 S 盒计算得出,再进行一次轮密钥加得到一次解密图像,然后对解密图像执行 DRPE 解密进行二次解密,同样地 DRPE 解密过程是加密过程的逆过程,但是其中 RPM1 和 RPM2 的相位调制函数变为 $\exp[-j2\pi n(x,y)]$ 和 $\exp[-j2\pi b(\alpha,\beta)]$. 解密过程如图 5 所示.

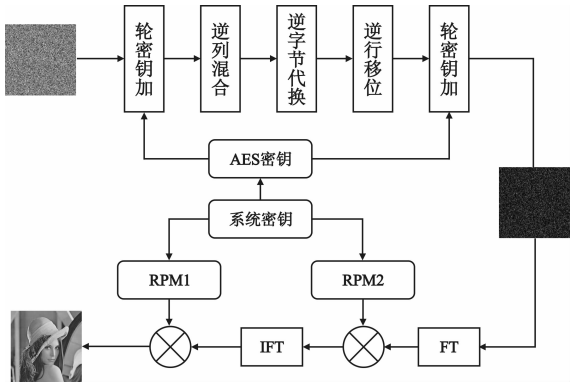
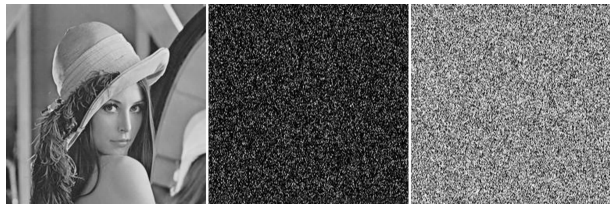


图 5 解密过程

3 实验仿真及性能分析

3.1 算法仿真

本文为了方便验证,仿真实验的明文图像选择了尺寸为 256×256 的 Lena 灰度图像,仿真实验的环境是 Matlab2016a. 设超混沌系统初始值为 $x=1, y=1, z=1, w=1$. 加密后的加密图像如图 6 所示,加密效果表现良好.



(a)Lena 第一次加密的密文图像(左二)

(b)Lena 最终密文图像(右一)

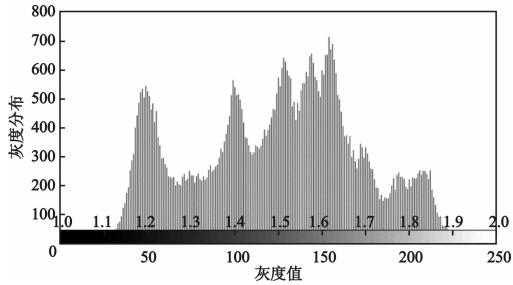
图 6 加密图像

3.2 算法统计特性分析

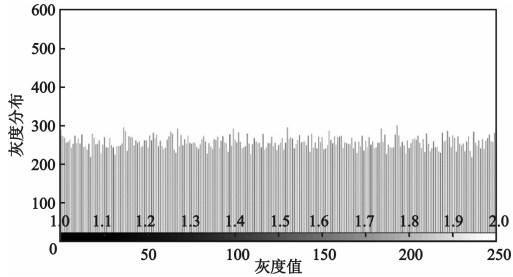
3.2.1 直方图分析

把图像中各灰度级像素出现的频率通过图表的形式展示,这就是灰度图像的直方图分析,其中

横坐标表示灰度级,纵坐标表示灰度级频率,目的在于反映图像灰度分布的情况. 如果一个灰度图像的直方图是均匀分布的,则该图像无法提取出任何有价值的信息,从而证明该加密图像的效果是很好的. Lena 图像加密前后的灰度直方图如图 7 所示. 显然,明文图像的直方图分布明显不均匀,而加密后的密文图像的直方图分布相对均匀,由此可以看出其对于隐藏明文图像分布特性的效果显著.



(a)Lena 明文图像灰度直方图



(b)Lena 密文图像灰度直方图

图 7 Lena 明文与密文图像灰度直方图

除了通过直方图分析,本文还将计算直方图方差来展示直方图均匀程度,直方图方差越小,则表示图像的像素点灰度值分布越均匀. 方差计算公式如式(10):

$$\text{Var}(Z) = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n \frac{1}{2} (z_i - z_j)^2 \quad (10)$$

式中, Z 是直方图像素值向量, $n = (1, 2, 3, \dots, 256)$. Lena 的明文图像和密文图像的直方图方差分别是 42 378 和 252. 很明显,密文图像的直方图方差远远小于明文图像的直方图方差,而且与文献[4]对比,本加密算法加密后的密文图像直方图方差更小,证明加密效果非常好.

3.2.2 算法统计学分析

分别对水平方向,垂直方向和对角方向,在明文图像和密文图像随机的提取相邻的像素值,用来测试相关性,并计算每组数据的相关系数. 相关系数的计算公式见公式(11) ~ (14):

$$\bar{x} = \frac{1}{N} \sum_{i=1}^N x_i$$

(11)

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

(12)

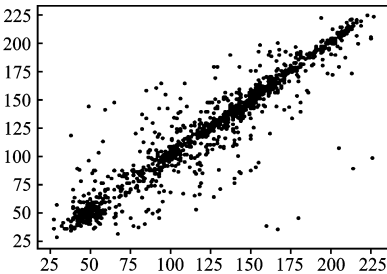
$$\text{Conv}(x,y) = \frac{1}{N} \sum_{i=1}^N (x_i - \bar{x})(y_i - \bar{y})$$

(13)

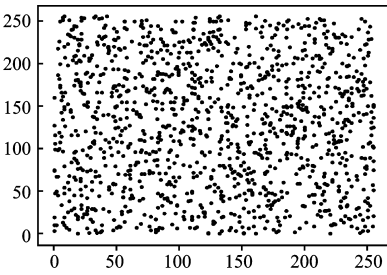
$$\gamma_{xy} = \frac{\text{Conv}(x,y)}{\sqrt{D(x)} \sqrt{D(y)}}$$

(14)

式中, γ_{xy} 表示两个相邻像素的相关系数, x,y 表示相邻两个像素的像素值. 在实验中分别从明文和密文图像随机抽取 1 500 组水平方向的相邻像素, 然后用这些数据描绘出明文和密文图像水平方向相邻像素的关系图, 如图 8 所示. 正如图 8 中所显示的, 明文图像的相邻像素之间的相关性非常高, 而加密后的密文相邻像素之间则几乎没有关系.



(a)明文图像水平方向关系图



(b)密文图像水平方向关系图

图 8 明文与密文水平方向关系图

继续分别从 Lena 明文和密文图像随机抽出 1 500组垂直方向和对角方向的相邻像素, 并计算每个方向上的相关系数和平均值, 表 1 给出了对照结果, 显然, 明文图像在各个方向上的相关系数都接近于 1, 而密文图像的相关系数却非常趋向于 0. 而表 2 给出了密文相关系数在每个方向上与文献[5-8]的实验结果的对比结果. 可见相比于同类算法, 本加密算法拥有更低的密文相关系数, 证明本算法具有很好的加密效果, 同时能够充分地抵抗统计分析攻击.

表 1 图像加密前后的相邻像素的相关系数

像素方向	水平方向	垂直方向	对角方向
Lena 明	0.952 2	0.962 6	0.935 2
Lena 密	0.000 83	−0.002 02	0.002 55
密文均值	0.000 85	0.001 1	0.003 2

表 2 密文相关系数平均值与其它文献的对比

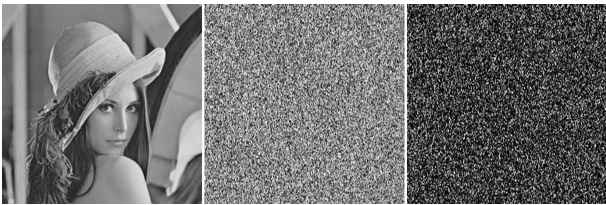
像素方向	水平方向	垂直方向	对角方向
密文平均值	0.001 2	0.001 1	0.003 2
文献[5]	0.009 6	0.034 2	0.020 5
文献[6]	0.002 0	−0.00 07	−0.001 4
文献[7]	0.001 9	0.003 8	−0.001 9
文献[8]	0.002 4	−0.000 6	0.001 2

3.3 抗差分攻击

本文分别从密钥的敏感性和明文敏感性两个方向来分析加密算法的抗差分攻击能力.

3.3.1 密钥敏感性分析

通常, 只要解密密钥发生变化, 解密图像就会产生显著变化, 称之为密钥敏感性. 通过实验仿真, 加密系统的密钥由两个随机相位版和 AES 目标密钥两种密钥组成, 采用正确的解密方式对 Lena 密文图像进行解密得到解密图像 A, 如图 9(a). 将 AES 密钥 $x_1=18$ 修改成 $x_1=18.000\ 01$, 其他的保持不变, 修改后解密图像如图 9(b). 即使密钥发生轻微变化, 最终也不能解密图像, 说明密钥敏感性很高. 将随机相位版 RPM2 中一个元素替换成 1, 其他的保持不变, 修改后解密图像如图 9(c). 显然, 改进后加密系统的密钥安全性很高.



(a)正确密钥解密图像 (b)错误 AES 密钥的解密图像 (c)错误随机相位版 RPM2 的解密图像

图 9 解密图像

3.3.2 明文敏感性分析

同样地, 明文敏感性越高, 算法的抗差分攻击能力就越强. 因此本文通过将平均值 avg 和控制参数 t 巧妙地混合在加密过程中, 使得就算明文发生轻微变化也会导致密文图像发生明显的变化, 有效提高了加密流程和明文图像之间的相关性.

典型的明文敏感性分析是通过参考归一化平均

变化强度(UACI)和像素值变化率(NPCR)实现的. 采用两张加密图像 H_1 和 H_2 , 其中 H_1 表示某明文图像的加密图像, H_2 表示该明文图像在随机位置改变像素值后的加密图像. 定义一个 $M \times N$ 大小的矩阵 P , 当 $H_1(i, j) = H_2(i, j)$ 时, $P(i, j) = 0$, 否则 $P(i, j) = 1$. NPCR 和 UACI 的公式如下:

$$\text{NPCR} = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N P(i, j) \times 100\% \quad (15)$$

$$\text{UACI} = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N \frac{|H_1(i, j) - H_2(i, j)|}{255} \times 100\% \quad (16)$$

本次实验先加密明文得到 H_1 , 再将其(1,1) 位置的像素值分别加减 1 得到 H_2 , 通过式(15) 和(16) 计算出像素值变化率和归一化平均变化强度, 表 3 给出了本文和文献[9-10] 的结果比较. 显然, 该算法对明文敏感性很强, 能够有效抵抗差分攻击.

表 3 明文敏感性对比

明文像素点变化	NPCR/%	UACI/%
(1,1)像素加 1	99.64	33.37
(1,1)像素减 1	99.59	33.39
文献[9]	99.58	33.25
文献[10]	99.57	27.35

3.4 经典攻击分析

根据攻击者对明文和密文等信息的了解情况, 典型的攻击方式可划为已知明文攻击, 选择密文攻击, 选择明文攻击和唯密文攻击这四种攻击方式.

当今主流的攻击方式就是选择明文攻击, 如果图像加密算法可以有效地抵抗选择明文攻击, 也就可以抵抗其他的攻击方式.

本文的加密算法对抵抗明文(密文)攻击有着显著的效果, 原因如下: 第一、本加密算法在密钥生成过程中引入与明文相关的控制参数 t , 使得即使有二维图像矩阵像素值全为 0 的情况, 混沌序列也不可能重复出现, 从而真正正确的密钥也无法被攻击者所获悉. 第二, 本文中 AES 加密算法使用随机的 S 盒和轮密钥, 就算攻击者使用非全为 0 的特殊明文攻击, 也能大大增加其破解难度, 使得基本无法破译. 第三, 第二次 AES 加密对 DRPE 中的第二透镜的有效保护, 攻击者无法通过强制傅里叶变换实现密文破解. 综上所述, 本文的加密算法能够有效地抵抗选择明文(密文)攻击.

4 结束语

由于现有双随机编码光学加密系统存在第二透镜的无效性的缺点, 导致加密图像容易被破解, 因此通过加入 AES 加密算法来提高加密系统安全性, 而且针对当前密钥空间小和固定不变的特性, 在系统中加入超混沌系统产生随机相位版和 AES 目标密钥, 使得密文的相关系数更低, 同时克服了传统算法上的不足. 本系统主要有以下三个特点: 第一方面, 通过结合传统 Qi 系统的二次项和三次项改进了超混沌系统; 第二方面, 结合明文特性的超混沌序列作为初始值, 来产生随机相位版和目标密钥, 大大增强了密钥的随机性, 解决了密钥固定不变的缺点. 第三方面, 通过正在 DRPE 系统中第二透镜输出面后面植入 AES 加密算法进行二次加密, 有效地保护了 DRPE 的后相位版, 使系统的安全性得到大大增强. 仿真实验结果表明, 这三个特点的优良结合使得加密算法具有较好的加密效果以及较高的安全性.

参考文献:

[1] HILIPPE P. Optical image encryption based on input plane and Fourier plane random encoding. [J]. Optics Letters, 1995, 20(7):767.

[2] SITU G , ZHANG J . Double random-phase encoding in the Fresnel domain. [J]. Optics Letters, 2004, 29 (14):1584-6.

[3] 陈在平,蔡鹏飞,董恩增. 基于超混沌 AES 图像加密算法:[J]. 吉林大学学报(信息科学版), 2013, 31(2): 158-164.

[4] ZHANG Y Q, WANG X Y. A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice[J]. Information Sciences, 2014, 273(8):329-351.

[5] WANG X Y, ZHANG Y Q, BAO X M. A novel chaotic image encryption scheme using DNA sequence operations[J]. Optics & Lasers in Engineering, 2015(73): 53-61.

[6] WANG X Y, GU S X, ZHANG Y Q. Novel image encryption algorithm based on cycle shift and chaotic system [J]. Optics & Lasers in Engineering, 2015 (68): 126-134.

[7] 杨志宏,屈双惠,张彩霞,等. 一个四翼超混沌系统在图像加密技术中的应用[J]. 西南大学学报(自然科学版). 2018, 40(5): DOI: 10. 13718/j. cnki. xdzk. 2018. 05. 025.

[8] 林青,王延江,王珺. 基于超混沌系统的图像加密算法

[D]. 中国科学(技术科学),2016,46(9),910-918.

[9] WANG X, LIU L, ZHANG Y. A novel chaotic block image encryption algorithm based on dynamic random growth technique[J]. Optics & Lasers in Engineering, 2015,66(66):10-18.

[10] ZHANG Y Q,WANG X Y. A new image encryption algorithm based on non-adjacent coupled map lattices [J]. Applied Soft Computing,2015(26):10-20.

作者简介:

王 勇 男,(1968-),博士,教授.研究方向为物联网、非结构化信息处理与智能计算.
E-mail: wangyong@gdut. edu. cn.

叶树成 男,(1993-),硕士研究生.研究方向为非结构化信息处理、混沌图像加密.

王 瑛 女,(1970-),高级工程师.研究方向为云计算与知识工程.