文章编号:1672-058X(2014)11-0050-06

基于复合混沌及 LSB 的图像加密和隐藏技术*

张玉明[1,2], 刘家保[1,3]

(1.东南大学 复杂系统与网络科学研究中心,南京 210000; 2.芜湖职业技术学院 电气工程学院,
安徽 芜湖 241001;3.安徽新华学院 公共课教学部,合肥 230088)

摘 要:给出了一个基于复合混沌及 LSB 的图像加密和隐藏技术的方法,该方法首先利用 Logistic 映射和 Tent 映射进行复合产生混沌映射,用明文彩色图像的灰度信息来控制复合混沌的参数,产生的混沌序列对彩色图像进行加密,然后把加密图像用 LSB 算法嵌入到二个或多个载波图像中进行传输;实验和仿真结果表明:该方法具有隐藏效果好、密钥敏感性强、鲁棒性高等特点。

关键词:复合混沌;图像加密;图像隐藏;LSB

中图分类号:TP391 **文献标志码**:A

0 引 言

进入 21 世纪,人们获取信息(包括文本、图像、音频、视频等)的一个重要渠道来自互联网,然而互联网数据易受人为攻击,如信息的篡改、信息窃取、信息泄露等,一些重要的信息,特别是涉及国家安全或公司利益或个人利益的重要信息不能在网络上直接传播[1,2]。因此,保密通信技术引起了许多研究者浓厚的兴趣,越来越成为世界科学研究的热点。

混沌系统是一种非线性动力系统,由于其对初始条件和系统参数非常敏感,具有遍历性和伪随机性等特点[3-5],非常适合对图像的加密和隐藏,但简单的混沌映射易受到攻击破解.本文主要研究基于复合混沌及 LSB 的图像加密和隐藏技术,用 Logistic 映射和 Tent 映射进行复合产生新的混沌映射,加大攻击和破解的难度,同时用明文彩色图像的灰度信息来控制复合混沌的参数,产生的混沌序列对彩色图像进行加密,使得用已知明文进行攻击变得不可能。由于图像信号有较大的冗余度[4,5],把经过预处理的加密图像用 LSB (Least Significant Bit)算法嵌入到一个像素高于明文图像 8 倍的载波图像或多个载波图像中进行传输,则嵌入了水印的载波图像看不出变化,不会引起攻击者的注意.实验和仿真结果表明,该方法具有隐藏效果好、密钥敏感性强、鲁棒性高等特点。

1 复合混沌映射分析及参数控制

复合混沌映射有很多的复合方法,具有很高的复杂性,本文用 Logistic 映射和 Tent 映射进行复合产生混沌映射,对比分析比较 Lyapunov 指数表明:复合混沌映射对初始条件更具有敏感性。同时用明文彩色图像

收稿日期:2014-04-23;**修回日期**:2014-05-27.

* **基金项目**:安徽省高等学校省级自然科学基金项目(KJ2013B105).

作者简介:张玉明(1968-),男,安徽芜湖人,副教授,从事混沌系统、图像处理和保密通信研究.

的灰度信息进行参数控制,不同的明文产生不同混沌序列,依赖于明文且更具有随机。

1.1　复合混沌映射

Logistic 映射定义为[6]

$$x_{n+1} = \mu x_n(1 - x_n) \qquad 0 < x_n < 1, 0 < \mu \leqslant 4 \tag{1}$$

Tent 映射定义为[6]

$$x_{n+1} = 1 - 2 \mid x_n \mid \qquad -1 < x_n \leqslant 1 \tag{2}$$

将式(1)代入式(2)进行复合,得到新的复合映射,选择合适的 μ 值可以进入混沌状态,即

$$x_{n+1} = 2\mu \mid x_n \mid (1 - 2 \mid x_n \mid) \qquad -1 < x_n < 1, 0 < \mu \leqslant 2 \tag{3}$$

1.2　Lyapunov 指数对比分析

Lyapunov 指数可以表征系统运动的特征,是衡量系统动力学特性的一个重要定量指标,它表征了系统在相空间中相邻轨道间收敛或发散的平均指数率[6]。一个正的 Lyapunov 指数,意味着在系统相空间中,无论初始两条轨道的间距多么小,其差别都会随着时间的演化而成指数率的增加而达到无法预测,形成混沌现象。Lyapunov 指数越大,混沌特性越明显,混沌程度越高[4]。

Lyapunov 指数定义为[6]

$$\lambda = \lim_{N \to \infty} \frac{1}{N} \sum_{i=0}^{n-1} \ln \mid F'(x_i) \mid \tag{4}$$

图 1 为根据式(4)计算并绘制的复合映射 Lyapunov 指数谱。在相同条件下,由式(3)确定的复合映射最大 Lyapunov 指数为 0.693 7,比 Logistic 映射的 0.691 2、Tent 映射的 0.577 6 要大。当 $\mu = 2$ 时,复合映射 Lyapunov 指数达到最大值,具有更好的初值敏感性,混沌特性明显。

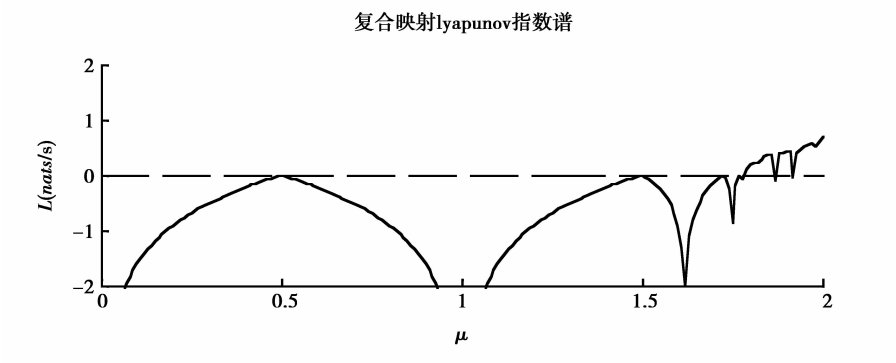


图 1　初值 $x_1 = 0.1$,迭代 2 000 点

1.3　参数控制

为了抵御对已知明文的攻击,增加密钥对明文彩色图像的敏感性,也就是一幅图像一种密钥,采用已知明文彩色图像的灰度信息来控制复合混沌的参数 μ:

$$\mu = 9/5 + \mathrm{bi2de}(\bigoplus_{i=1}^{M}\bigoplus_{j=1}^{N} g(i,j))/1\ 280 \tag{5}$$

式(5)中 bi2de 表示将二进制数转化为十进制数,⊕表示异或运算,$g(i,j)$ 为彩色图像在 (i,j) 点处的灰度值,实际操作中可以用 (i,j) 点处的 RGB 值中的一个或者组合,参数 μ 的取值范围在(1.8,2)之间,保证系统处于混沌状态,这样通过对参数 μ 的控制,明文彩色图像出现细微的变化就会得到不同的参数,效果相当于对密钥进行了局部修改,混沌序列对密钥是敏感的,最终导致算法对明文彩色图像足够敏感。

2 彩色(RGB)图像加密和隐藏的算法及实现

2.1 复合混沌序列的产生

给定待加密明文彩色BMP格式图像,假设其尺寸为 $M*N*3$,每个像素标记为 $p_{i,j,dim}$,i 对应行,j 对应列,$dim=1,2,3$,分别对应R,G,B。读取彩色明文图像,取出灰度图像,计算 $\bigoplus_{i=1}^{M}\bigoplus_{j=1}^{N} g(i,j)$ 的值并保存为 H,此值为8 bits二进制数,根据(5)式计算出 μ 值,给定 x_n 的初值 x_0,以 μ 和 x_0 为密钥key,代入复合混沌映射式(3),迭代 $(M-1)$ 次,得到混沌序列 $XL1(x_0,x_1,\cdots,x_{M-1})$;更换初值 x_0,再次代入复合混沌映射式(3),迭代 $(N-1)$ 次,得到混沌序列 $XL2(x_0,x_1,\cdots,x_{N-1})$;再次更换初值 x_0,第三次代入复合混沌映射式(3),迭代 $(M*N-1)$ 次,得到混沌序列 $XL3(x_0,x_1,\cdots,x_{MN-1})$。

2.2 彩色(RGB)图像的置乱和置换加密

对彩色(RGB)图像采用置乱和置换加密算法,其中置乱加密是对图像中的数据位置重新排列,数据值并没有改变;置换加密则是改变图像的数据值。

第1步,行坐标置乱,列不变。对混沌序列 $XL1(x_0,x_1,\cdots,x_{M-1})$,首先找出最大值及其在序列中的位置坐标 i,$i\in(1,2,\cdots,M)$,令 $p'_{k,j,dim}=p_{i,j,dim}$,同理找出混沌序列 $XL1$ 第二大的位置重复上述操作。

第2步,列坐标置乱,行不变。对混沌序列 $XL2(x_0,x_1,\cdots,x_{N-1})$,首先找出最大值及其在序列中的位置坐标 j,$j\in(1,2,\cdots,N)$,令 $p'_{k,l,dim}=p_{k,j,dim}$,同理找出混沌序列 $XL2$ 第二大的位置重复上述操作。

第3步,置换加密操作。混沌序列 $XL3(x_0,x_1,\cdots,x_{MN-1})$ 中的值为模拟量,设为 $x(n)$,对 $x(n)$ 进行模256运算得到 $ax(n)=\mathrm{mod}(x(n)*10^{15+\mu},256)$,接着把 $ax(n)$ 转换为8 bits二进制数设为 $dx(n)$,经过置乱的图像像素 $p'_{k,l,dim}$ 与 $dx(n)$ 进行逐位异或,得到置乱和置换后加密图像 $p''_{k,l,dim}$。

2.3 基于LSB技术的彩色(RGB)图像的隐藏实现

明文彩色图像经过混沌置乱和置换加密成密文图像后已经很安全,但是密文图像还是太引人注目,容易遭到破译者的好奇并实施攻击[4],把密文图像作为水印嵌入到载波图像中,由于图像信息本身的冗余度大,若选取的载波图像像素是密文图像像素的8倍,采用LSB(Least Significant Bit)算法,则嵌入了水印的载波图像基本看不出有什么变化,不会引起攻击者的注意。本文采用二个相同的载波图像,图像像素稍大于明文图像,可以体现隐藏实现的过程。

第1步,给定二个相同的载波图像Carry,假设其尺寸为 $M1*N1*3$,裁剪使其尺寸为 $M*N*3$,每个像素标记为 $C_{i,j,dim}$,i 对应行,j 对应列,$dim=1,2,3$,分别对应R、G、B。先将 $C_{1,1,dim}$ 与二进制数00000000B相与,即 $C_{1,1,dim}\wedge 00000000\mathrm{B}$,然后将 $C_{1,1,dim}$ 与 H 相或,即 $C_{1,1,dim}\vee H$,这样 H 的值就隐藏在 $C_{1,1,dim}$ 中供解密时使用。

第2步,将二个 $C_{i,j,dim}$(除了 $C_{1,1,dim}$)的低4位清0,即 $C_{i,,dim}\wedge 11110000\mathrm{B}$,清0后的 $C_{i,j,dim}$ 的低4位用来隐藏密文图像,分别标记为 $CL1C_{i,j,dim}$ 和 $CL2C_{i,j,dim}$。

第3步,将密文图像 $p''_{k,l,dim}$ 通过逻辑运算一分为二,并把图像信息放置于低4位,分别标记为 $CL1p''_{k,l,dim}$ 和 $CL2p''_{k,l,dim}$,$CL1p''_{k,l,dim}$ 和 $CL2p''_{k,l,dim}$ 为8 bits二进制数,高4位为0,低4为携带密文信息。

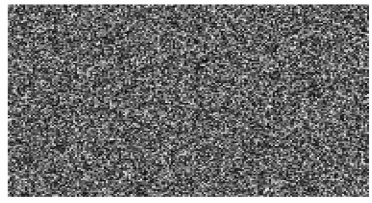
第4步,将密文图像 $p''_{k,l,dim}$ 隐藏到载波图像 $C_{i,j,dim}$ 中。即执行逻辑运算 $CL1p''_{k,l,dim}\vee CL1\mathrm{C}_{\mathrm{i,j},dim}$ 和 $CL2p''_{k,l,dim}\vee CL2C_{i,j,dim}$,得到最终隐藏加密图像设为 p_{end1} 和 p_{end2},这样完成了整个加密和隐藏过程。

3 试验结果

实验采用Matlab 8.1仿真平台,取220×331×3的仙人掌BMP图像作为明文图像,取300×450×3的飞机BMP图像作为载波图像,密钥选择 x_0 的初值对应3个序列分别是0.1,0.2,0.3,μ 值取决于明文图像,取值范

围在(1.8,2)之间,运行结果如图 2 所示,图 2(a)是待加密明文图像,图 2(b)是经过置乱和置换后待隐藏的密文图像,图 2(c)是载波图像,图 2(d)是成功加密并隐藏的最终结果图像。

(a)明文图像



(b)加密图像

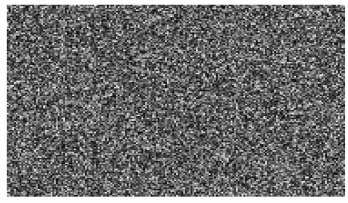
(c)载波图像

(d)隐藏加密结果图像

图 2　明文图像加密和隐藏结果

解密是加密的逆过程,首先恢复 p_{end1} 或 p_{end2} 中的(1,1,dim)像素值 H,根据式(5)计算出 μ 值,再根据密钥 x_0 的 3 个初值代入复合混沌映射式(3)产生 3 个同样的解密序列 $XL1$,$XL2$,$XL3$ 用于解密。从 p_{end1} 和 p_{end2} 中通过逻辑运算抽取低 4 位并进行合并得到加密图像,用 $XL3$ 序列与加密图像异或完成反置换,再用 $XL2$,$XL1$ 序列完成置乱的逆过程即得到原明文图像.解密结果如图 3 所示,图 3(a)为用正确的密码进行解密得到正确的结果并成功解密,图 3(b)为使用错误的密钥,序列 1 的初值 x_0=0.100 000 000 000 001 进行解密的结果,解密失败。

(a)解密成功



(b)解密失败

图 3　解密结果

4　算法安全性分析

一个好的图像加密和隐藏算法应具有很高的安全性,能有效抵御各种形式的攻击,如蛮力攻击、已知明文攻击、选择明文攻击等[7,8]。本文分析了密钥空间、直方图分析、明文依赖的敏感性分析。

4.1　密钥空间分析

密钥由 μ 和 x_0 二个参数构成,其中 x_0 在混沌序列产生过程中出现 3 次,设混沌系统的初值均为 15 位有效数字,则密钥空间为 $10^{15}\times10^{15}\times10^{15}\times10^{15}=10^{60}>2^{128}$,本算法具有足够的密钥空间,可以有效抵御蛮力攻击。

4.2　直方图分析

一个好的图像加密和隐藏算法能够有效抵抗统计分析攻击,这就要求加密图像应该具有良好的均匀分布[4,9]。图 4 为明文图像的 R、G、B 直方图,从图 4 中可以看出不服从均匀分布。图 5 为密文图像的 R、G、B

直方图,从图5中可以看出本文算法产生的密文图像基本服从均匀分布,可以有效抵抗统计分析攻击。

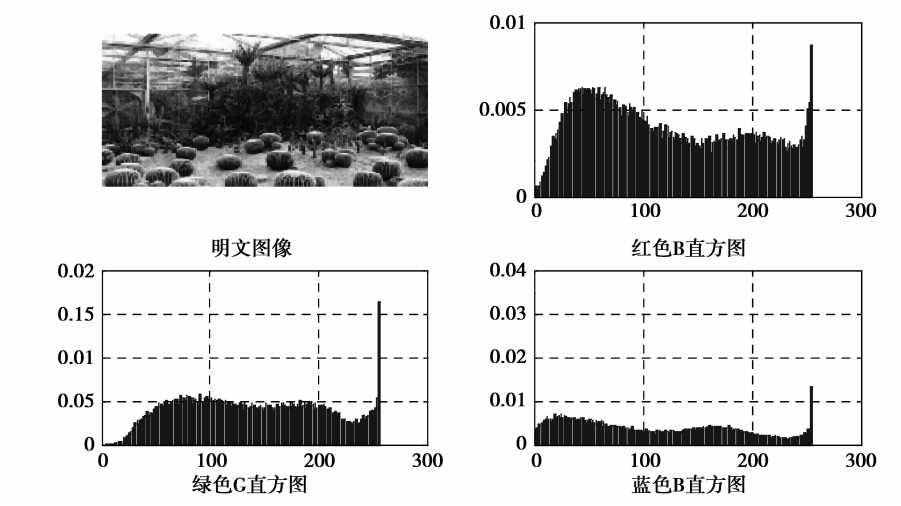


图4 明文图像直方图

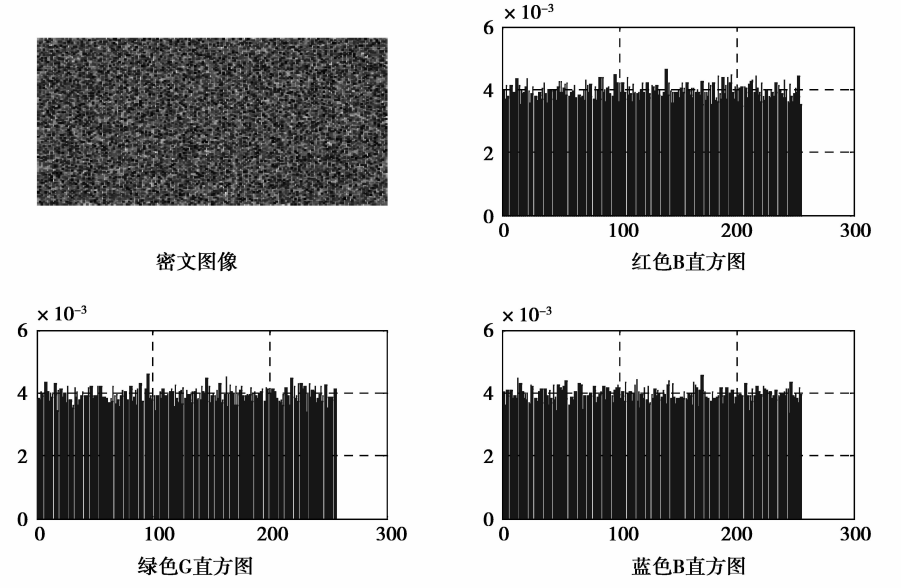


图5 密文图像直方图

4.3 明文依赖的敏感性分析

随机选取仙人掌BMP明文图像中的某个像素点进行修改,本文选取(10,10,*dim*)点,将该点灰度像素值减1。对修改前后的图像使用相同密钥进行加密,得到的加密序列完全不同,加密图像也不同。说明即使明文有微小的变化,得到的密文也完全不同,加密算法对明文依赖的敏感性高。可以有效地抵抗已知明文攻击,说明本算法具有很高的鲁棒性。

5 结 语

本文用一维Logistic映射和Tent映射进行复合产生新的混沌映射,用明文彩色图像的灰度信息来控制复合混沌的参数,利用3个不同的初值产生的3个不同混沌序列对彩色图像进行置乱和置换加密,加密后的密文图像利用LSB技术隐藏到二个或多个载波图像中,形成了一种新的彩色图像加密算法。多次仿真实验和安全性分析结果表明,本算法密钥空间大、对明文依赖的敏感性高、具有良好的均匀分布特性,可以有效

抵御对密钥的蛮力攻击、已知明文攻击、选择明文攻击及其他形式的攻击,具有很高的安全性和鲁棒性,利用本算法加密的图像可以安全地在网络上传输,特别适合于企业产品设计研发初期在网络上的传输。

参考文献:

[1] SMID M E , BRANSTAD D K.Data encryption standard: past and future[J].Proceedings of the IEEE, 1988,76(10):550-559

[2] RHOUMA R,SAFYA B. Cryptanalysis of a new image encryption algorithm based on hyper-chaos[J]. Physics Letters A 2008 (372):5973-5978

[3] WEI Xiaopeng, GUO Ling.A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system [J]. The Journal of Systems and Software, 2012(85):290-299

[4]CAO Yang. A New Hybrid Chaotic Map and Its Application on Image Encryption and Hiding[J]. Mathematical Problem in Engineering 2013,13(1):15-18

[5] 王丽娜.网络多媒体信息安全保密技术[M].武汉:武汉大学出版社,2003

[6] 廖晓峰. 混沌密码学原理及其应用[M].北京:科学出版社,2009

[7] 张小华,刘芳,焦李成. 一种基于混沌序列的图像加密技术[J]中国图象图形学报:工程技术版,2003,8(4):374-378

[8] 邱应强,张育钊,杜吉祥,郭荣新.一种用于矢量量化压缩图像的信息隐藏新方法[J].电子与信息学报,2008,30(7):1695-1699

[9] 易开祥,石教英.数字水印技术研究[J].中国图像图形学报,2001,6(2):111-117

An Image Encryption and Hiding Technique Based on Composite Chaos and LSB

ZHANG Yu-ming[1,2] , LIU Jia-bao[1,3]

(1.Research Center for Complex System and Network Science, Southeast University, Nanjing 210000, China;
2. School of Electrical Engineering, Wuhu Institute of Technology, Anhui Wuhu 241001, China;
3. Department of Public Course Teaching, Anhui Xinhua College, Hefei 230088, China)

Abstract: An image encryption and hiding technique based on composite chaos and LSB is proposed, this method firstly uses Logistic mapping and Tent mapping to be composited to produce chaos mapping, the parameters of the composited chaos are controlled by grey-level information of plain color image, then the produced chaos sequence encrypts the color image, and then the encrypted image is embedded into two or multiple carry images to be transmitted by LSB algorithm. Experiment and simulation results indicate that this method has the feature of good hiding effect, strong encryption-decryption sensitivity and high robustness and so on.

Key words: composite chaos; image encryption; image hiding; LSB

责任编辑:代小红