基于混沌系统的图像隐藏技术①

黄慧青

(嘉应学院 数学学院, 梅州 514015)

摘 要: 为了在保证隐藏信息不可见性的条件下, 尽可能地提高隐藏图像信息的安全性与抗干扰性, 提出一种基于混沌系统的图像隐藏技术. 先利用 Arnold 变换与混沌系统产生的混沌序列对待隐藏图像进行加密预处理; 然后利用 Logistic 混沌系统与图像分存技术把结果图像进一步隐藏起来; 最后应用评价指标对隐藏效果和安全性进行分析. 实验结果表明,该算法具有良好的安全性和隐藏效果.

关键词: 混沌系统; 图像置乱; 异或运算; 图像隐藏; 图像分存; Logistic 混沌映射

Image Hiding Technology Based on Chaos System

HUANG Hui-Qing

(School of Mathematics, Jiaying University, Meizhou 514015, China)

Abstract: To ensure the security and anti-disturbing of hiding image information under the conditions of visibility, An image hiding technology based on chaos systems was presented. Firstly, with the Arnold transform and the sequences generated by the chaos system, a hiding image was encrypted; then using Logistic chaos system and image sharing technique to hide the pre-encrypted image. The effect of hiding is also analyzed by using the method of accessing. Simulation results show that the algorithm has good safety and hidden effect.

Key words: chaotic system; image scrambling; XOR operating; image hiding; image sharing; Logistic chaotic map

计算机和通信技术的飞速发展, 使得信息的共享、传播变得越来越便捷, 但同时对一系列的信息安全问题提出了挑战. 而传统信息安全的保障手段——密码术并不能真正解决此类问题. 因此, 人们提出了信息隐藏技术. 信息隐藏技术是解决上述一系列信息安全问题的有效手段, 因此近年来信息隐藏技术成为人们研究的热点[1-6].

本文主要研究和讨论了基于混沌系统的图像隐藏技术, 提出了一种利用混沌加密和图像分存隐藏相结合的新方法. 该算法是先利用 Arnold 变换对待隐藏图像进行置乱[7,8], 然后利用混沌序列对其进行异或得到加密图像, 最后将加密图像隐藏到载体图像中. 实验结果证明, 该算法简单有效且具有很好的隐藏效果.

1 混沌系统

1.1 二维离散混沌系统

二维离散混沌系统形式如下[9]:

$$\begin{cases} x \to ax + \dfrac{3}{2}y, \\ y \to b(x - x^3). \end{cases} \tag{1}$$

其中 a, b 为系统参数. 对该系统作参数分岔图的数值实验, 固定参数 $b=-1.4$, 关于参数 a 的分岔图如图 1(a)所示, 固定参数 $a=1$, 关于参数 b 的分岔图如图 1(b)所示. 以 b 为参数对应的最大李雅谱诺夫指数的图为图 1(c). 图 1(d)是当 $a=1$, $b=-1.4$ 时系统的混沌吸引子. 从这些图形可以观察到, 整体上系统是稳定的, 局部是不稳定的; 混沌现象在很大的区域出现. 因此该二维映射系统可以用于信息的混沌加密.

1.2 Logistic 混沌系统[10-13]

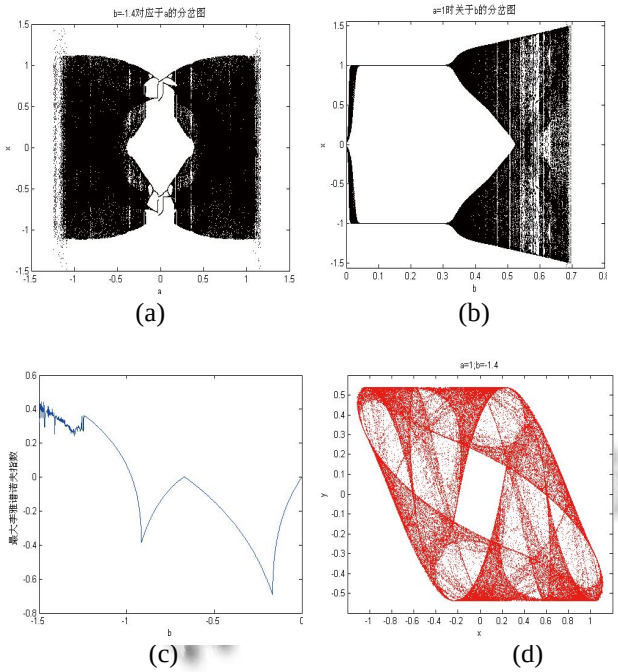
Logistic 混沌系统表述为:

$$a_{k+1} = \mu \cdot a_k \cdot (1 - a_k), k = 0,1,2,3,\cdots \tag{2}$$

其中, $3.569946\cdots \le \mu \le 4, a_0 \in (0,1)$. 这样, Logistic

① 收稿时间:2013-04-20;收到修改稿时间:2013-05-28

映射产生的混沌序列可以定义在上的伪随机序列.



(a)　(b)

(c)　(d)

图 1　混沌系统的分岔图、李雅谱诺夫指数图及吸引子

2　图像隐藏技术处理

2.1 待隐藏图像的预处理

为了提高隐藏图像的安全性，首先应用 Arnold 变换对待隐藏图像进行置乱，然后再利用二维离散混沌系统产生的混沌序列对置乱后图像进行异或运算. 相应的预处理加密算法描述如下:

步骤 1: 输入大小为 $N\times N$ 的待隐藏图像 A(如果行列不相等的图像可以通过填充边界使得行列相等).

步骤 2: 对图像 A 的像素进行如下的 Arnold 坐标变换:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\bmod N) \tag{3}$$

将 Arnold 变换次数作为提取原始图像时的密钥 K.

步骤 3: 生成混沌序列. 用给定的两个初始值 x_0, y_0 迭代映射 T_0 次后，将得到的 x_{T_0} 与 y_{T_0} 赋给初始值 x_0, y_0. 用这两个新的初始值分别迭代映射 n 次($n > N\times N$)，得到两条长度为 n 的混沌序列 $\{x_i | i=1,2,\cdots,n\}$ 与 $\{y_i | i=1,2,\cdots,n\}$. 按照式(4)对这两个序列进行改进:

$$X_i = 10^k X_i - round(10^k X_i) \tag{4}$$

其中 X_i 可以是 x_i 或 y_i, k=3, $round(.)$ 为取最近整数运算. 得到 $\{u_i | i=1,2,\cdots,n\}$ 与 $\{v_i | i=1,2,\cdots,n\}$.

步骤 4 对置乱后的图像 A 进行异或，使其平均分布在一定区域内. 混沌序列 $\{u_i | i=1,2,\cdots,n\}$ 与 $\{v_i | i=1,2,\cdots,n\}$ 按照式(5)对这两个序列进行改进:

$$W_i = \bmod(round(10^k X_i), 256) \tag{5}$$

得到 $\{e_i | i=1,2,\cdots,n\}$ 与 $\{w_i | i=1,2,\cdots,n\}$. 应用 $\{e_i\}$ 和 $\{w_i\}$ 构造像素变换矩阵: 取序列 $\{e_i\}$ 或 $\{w_i\}$ 的某连续片断，该片断元素个数为 $N\times N$，重构为一个大小为 $N\times N$ 的矩阵 E. 用 E 与置乱后的图像 A 进行异或得到密图 D.

该算法的解密过程为加密过程的逆.

2.2 图像隐藏

在预处理图像的基础上，把预处理后得到的加密图像分存到载体图像中，实现图像的隐藏，相应的图像隐藏算法描述如下:

步骤 1: 任意选取一幅大小与待隐藏图像相同($N\times N$)的载体图像 B.

步骤 2: 将载体图像 B 采用线性放大 4 倍.

步骤 3: 将密图 D 与放大后的载体图像 B 转换为 8 位二进制序列.

步骤 4: 利用 Logistic 混沌系统产生一个元素 a_k，然后按照式(6)进行运算:

$$k = \bmod(a_k, 8) + 1 \tag{6}$$

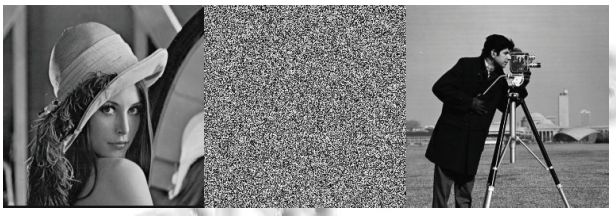
得到一个大于等于 1 而小于等于 8 的整数 k，若 k 为奇数则把密图的灰度值用二进制表示，从高位到低位依次记为第 1 位，第 2 位，……，第 8 位. 取 D 中像素点的灰度二进制表示的第 k 位开始把 8 位二进制分成 4 组替换在 B 相应图像区域左上、右上、左下、右下灰度值二进制表示的低二位(如当 k=3 时，取 D 中像素点的灰度二进制表示的第 3、4 位替换 B 相应图像区域左上点灰度值二进制表示的低二位；取 D 中像素点的灰度二进制表示的第 5、6 位替换 B 相应图像区域右上点灰度值二进制表示的低二位；取 D 中像素点的灰度二进制表示的第 7、8 位替换 B 相应图像区域左下点灰度值二进制表示的低二位；取 D 中像素点的灰度二进制表示的第 1、2 位替换 B 相应图像区域右下点灰度值二进制表示的低二位)；若 k 为偶数则把密图的灰度值用二进制表示，从低位到高位依次记为第 1 位，第 2 位，……，第 8 位. 取 D 中像素点的灰度二进制表示的第 k 位开始把 8 位二进制分成 4 组替换在 B 相应图像区域左上、右上、左下、右下灰度值二进制表示的低二位.

步骤 5: 将所得的结果转换为载体图像的数据矩阵, 恢复图像格式并输出.

3 实验结果与分析

3.1 实验结果

为了验证以上方法的隐藏效果, 选取 256×256 的 lena 图像作为待隐藏图像, 256×256 的 cameraman 图像作为载体图像. 在 MATLAB7.0 编程环境下, 设置二维离散混沌系统初始值分别为 x_0=0.01, y_0=0.01 及 T_0=2000. 错误密钥为 x_0=0.01, y_0=0.0100000000000001, 图像隐藏与恢复效果如图 2.



(a)待隐藏图像 (b)预处理后图像 (c)载体图像

(d)隐藏后混合图像(e)正确恢复图像(f)错误密钥恢复图像

图 2 图像隐藏与恢复效果

由图 2 可见, 由于混沌序列对初始值非常敏感, 即使初始值有微小的变化也无法对图像进行正确恢复.

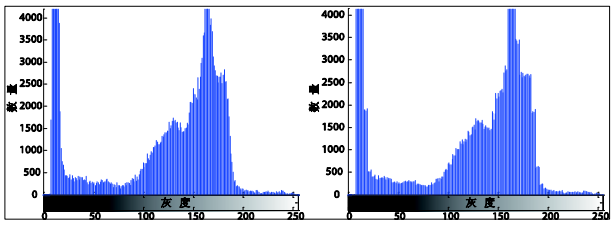
3.2 实验分析

3.2.1 密钥空间

一个好的隐藏加密算法应该使其密钥空间足够大从而使得强行攻击不可行, 理论计算表明当一个算法的密钥空间不小于 2^{128} 时, 该算法是安全的. 本文提出的加密算法中, 只考虑二维离散混沌系统的参数与初始值用作密钥, 其中 x_0, y_0, a, b 为双精度型, 精度为 10^{-16}, T_0 迭代次数为 16 比特整数型, 所以密钥空间为 $10^{16}\times10^{16}\times10^{16}\times10^{16}\times2^{16}=6.5536\times10^{68}$. 远大于 2^{128}, 因此使用穷举攻击解密图像几乎是不可能成功的.

3.2.2 统计分析

将载体图像的直方图与混合图像的直方图进行对比, 观察嵌入预处理密图后, 图像直方图的统计特性是否有改变. 图 3 为载体图像和混合图像的直方图.



载体图像直方图 混合图像直方图

图 3 载体图像和混合图像的直方图

为了进一步对图像隐藏的效果进行衡量, 我们引用峰值信噪比(Peak Signal-to-Noise Ratio, PSNR)和均方根误差(Root Mean Squared Error, RMSE)来衡量载体图像和混合图像之间的客观保真度[14-16]. 对于载体图像 B 与混合图像 G 的峰值信噪比定义为

$$PSNR=10\log10\left[\frac{M\times N\times255^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}[B(i,j)-G(i,j)]^2}\right] \tag{7}$$

峰值信噪比 PSNR 作为图像客观保真度准则, 它的值越大, 说明混合图像的保真度越好, 这两个图像越像.

载体图像 B 与混合图像 G 的均方根误差定义为

$$RMSE=\left[\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}[B(i,j)-G(i,j)]^2\right]^{\frac{1}{2}} \tag{8}$$

均方根误差越小, 说明两幅图像越相似.

利用上述方法, 我们得出了多组对比数据的 PSNR 和 RMSE 的数值并将其汇总后展示在表 1 中. 这其中包含了待隐藏图像与预处理后图像的对比, 载体图像和混合图像的对比, 以及错误密钥恢复图像与待隐藏图像的对比.

表 1 效果分析

	PSNR	RMSE
图 2(a)与图 2（b)	28.694839	9.371266
图 2(c)与图 2(d)	47.253182	1.106321
图 2(a)与图 2(e)	Inf	0
图 2(a)与图 2(f)	28.747958	9.314129

通过表 1 的实验结果可以看出, 载体图像与混合图像比较, RMSE 较小, PSNR 较大, 说明图像的隐藏效果很好.

3.2.3 抗干扰能力分析

秘密图像隐藏到载体图像后,只需要传输、存储混合图像. 但混合图像在传输过程中,很难避免一些必要的数据处理或人为攻击,如压缩、滤波、噪声污染及几何失真等,对一些比较常见的处理和攻击,文中也进行了实验测试. 图 4(a)是混合图像经过 1/4 剪切破坏后的图像, 图 4(b)所示是剪切后的混合图像的恢复图像. 图 4(c)对混合图像添加涂鸦, 图 4(d)为添加涂鸦后的恢复图像. 图 4(e) 为密图添加椒盐噪音后的解密图像,噪音强度为 4%. 测试结果表明,该算法具有较强的抗干扰能力.

(a)　(b)　(c)

(d)　(e)

图 4　算法抗干扰能力试验结果

4　结束语

本文提出了一种基于混沌系统的图像隐藏算法. 与文献[3]所给出的图像隐藏算法相比, 本文的算法具有更好的隐藏效果, 更大的密钥空间以及更高的安全性, 可以有效地抵抗统计分析以及剪切、涂鸦的攻击. 实验结果表明, 文中的算法具有很好的隐藏效果, 并且可以实现秘密图像的无损复原.

参考文献

1 张雪峰,范九伦.基于图像融合的数字图像隐藏技术.微电子学与计算机,2007,24(2):188–190.

2 张雪峰,范九伦.一种基于混沌系统的数字图像隐藏技术.计算机工程,2007,33(4):134–136.

3 李萌.一种基于超混沌的对数字化图像信息的隐藏加密方法.科学技术与工程,2009,9(4):905–910.

4 叶瑞松,兀松贤.一个对称的四维混沌系统及其图像隐藏应用.计算机技术与发展,2010,20(1):93–96.

5 甘甜,冯少彤,聂守平,朱竹青.基于分块离散小波变换的图像信息隐藏与盲提取算法.物理学报,2012,61(8):1–8.

6 周志刚,李苏贵.基于变参数混沌系统的数字图像隐藏技术.计算机应用,2009,29(11):2972–2976.

7 顾艳春,韩国强,沃焱,等.基于小波变换和置乱技术的二值水印新算法.计算机工程与设计,2008,29(15):4017–4019.

8 黄良永,肖德贵.二值图像 Arnold 变换的最佳置乱度.计算机应用,2009,29(2):474–476.

9 黄慧青.一个二维离散系统的分岔分析.嘉应学院学报,2010,28(5):22–26.

10 孙燕飞,王凤英,周运明,等.基于双混沌系统的数字水印技术.微电子学与计算机,2005,22(8):114–116.

11 Dan PP, Chau PM. Image encryption for secure internet multimedia applications. IEEE Trans. on Consumer Electronics, 2000, 46(8): 395–403.

12 肖迪,赵秋乐.一种基于 Logistic 混沌序列的图像置乱算法的安全分析.计算机应用,2010,30(7):1815–1817.

13 袁玲,康宝生.基于 Logistic 混沌序列和位交换的图像置乱算法.计算机应用,2009,29(10):2681–2683.

14 Chang CC, Hwang RJ. A new scheme to protect confidential image. 2004 IEEE Proc. of the 18th International Conference on A INA04. 2004.158–163.

15 Zhang JS, Tian L, Tai HM. A new watermarking method based on chaotic maps. IEEE International Conference on Multimedia and Expo. Taipei. 2004. 939–942.

16 王迤冉,王春霞,詹新生.一种图像加密算法的性能评定方法.微计算机信息,2006,22(30):313–314.