基于 DCT 和混沌的图像隐藏技术①

黄慧青

(嘉应学院 数学学院, 梅州 514015)

摘 要: 提出一种基于 DCT 和混沌的图像隐藏算法. 首先利用混沌系统产生混沌序列对秘密图像进行加密, 然后利用 DCT 变换与混沌序列把秘密图像隐藏到载体图像中. 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;图像隐藏; DCT 变换

Image Hiding Technology Based on DCT and Chaos

HUANG Hui-Qing

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

Abstract: An improved image hiding technology based on DCT and chaos is presented. We use chaotic system to generate one chaotic sequence which is utilized to encrypt the secret image, and then we use DCT and chaotic sequence to realize the secret image hiding in the host image. Simulation results show that the algorithm has good security and hiding effect.

Key words: chaotic system; image scrambling; image hiding; DCT transfer

信息隐藏技术是 20 世纪 90 年代中期从国外兴起的一门集多学科理论与技术于一身的新兴技术领域, 图像隐藏技术是其分支之一. 由于混沌系统具有易生成、无序性以及遍历性等特点, 因此经常利用混沌系统产生的混沌序列对图像进行置乱与异或[1-4], 从而达到加密的效果. 而离散余弦变换具有一个很好的性质, 能把图像的主要能量集中在左上角, 从而只要把秘密图像隐藏在除左上角外的其它地方, 就能有效地减少载体图像的失真度.

本文在混沌加密的基础上, 结合二维离散余弦变换与混沌序列, 给出一种基于 DCT 和混沌的图像隐藏新方案. 实验结果表明, 该算法隐藏效果、安全性及还原效果良好.

1 二维离散混沌系统

二维离散混沌系统形式如下[5]:

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

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.

2 离散余弦变换

离散余弦变换又称 DCT 变换[6], 通过变换将时域图像信号映射到空间频率域, 使得图像在时域所表现出的能量发散形式变换为频域能量相对集中的形式, 以便与对图像信息进行各种处理. DCT 变换具有能量集中的作用, 将图像的主要能量集中在左上角. 因此, 在图像隐藏中保留左上角的主要能量信息, 将秘密信息嵌入到中高频的右下方, 就可以有效地减少载体图像的失真度.

二维离散余弦正变换的公式为:

① 收稿时间:2012-11-22;收到修改稿时间:2012-12-25

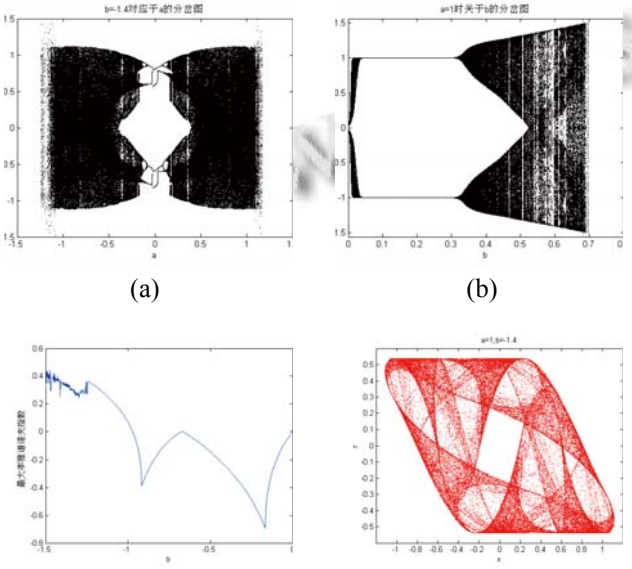
$$F(u,v)=c(u)c(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}f(x,y)\cos\frac{\pi(2x+1)u}{2N}\cos\frac{\pi(2y+1)v}{2N} \quad (2)$$

其中 $u,v=0,1,\cdots,N-1.c(u)=c(v)=\begin{cases}1/\sqrt{2} & u=0或v=0\\ 1 & u,v=1,2,\cdots,N-1\end{cases}$.

二维离散余弦反变换的公式为:

$$f(x,y)=\sum_{x=0}^{N=1}\sum_{y=0}^{N=1}c(u)c(v)F(u,v)\cos\frac{\pi(2x+1)u}{2N}\cos\frac{\pi(2y+1)v}{2N} \quad (3)$$

其中 $x,y=0,1,\cdots,N-1.c(u)=c(v)=\begin{cases}1/\sqrt{2} & u=0或v=0\\ 1 & u,v=1,2,\cdots,N-1\end{cases}$.



(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

3　算法原理

3.1 待隐藏图像预处理

待隐藏图像预处理是对待隐藏图像进行加密, 目的是提高算法的安全性, 经过预处理的待隐藏图像即使被检测出来, 破译者也无法获得待隐藏图像. 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通过填充边界使得行列相等).

步骤 2: 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 ($n>N^2$), 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:

$$X_i=10^k X_i-round(10^k X_i) \quad (4)$$

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 3: 应用 $\{u_i\}$ 和 $\{v_i\}$ 构造置乱矩阵. 取序列 $\{u_i\}$ 的某连续片断(如 $100<k\le 100+N$), 该片断元素个数为 N, 生成 1 个行变换序列, 再对它们进行排序, 得到索引序列, 然后构造 1 个 $N\times N$ 的零矩阵, 将每行中对应的索引序列元素值的列的值变为 1, 构造出行置乱矩阵 M_1. 同理, 在 $\{v_i\}$ 中抽取 N 个元素, 构造出列置乱矩阵 M_2.

步骤 4: 对图像 A 进行空间置乱: $A=M_1\times A\times M_2$.

步骤 5: 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:

$$W_i=\mathrm{mod}(round(10^k X_i),256) \quad (5)$$

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^2, 重构为一个大小为 $N\times N$ 的矩阵 E_1. 利用同样的方法构造出大小为 $N\times N$ 的矩阵 E_2. 用 E_1 与置乱后的图像 A 进行异或得到密图 C.

该算法的解密过程为加密过程的逆.

3.2 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: 对密图 C 与放大后的图像 B 进行余弦正变换得到对应的 C_1 与 B_1.

步骤 4: 对密图 C_1 进行改造. 按照式(6)对 E_2 进行改进:

$$E=\mathrm{mod}(E_2,k)+3,(k为正整数) \quad (6)$$

然后对 C_1 中的每一个元素进行下面的运算:

$$C_1(i,j)=C_1(i,j)\times 10^{-E(i,j)} \quad (7)$$

使得 C_1 中的元素的值都小于 1.

步骤 5: 把 B_1 均分成左上、右上、左下、右下四块, 然后用混沌序列产生序列 $\{k_i\},\{k_j\}$ $(k_i,k_j=0,1)$ 按照式(8)运算把 C_1 隐藏到 B_1 中右上、左下、右下三块.

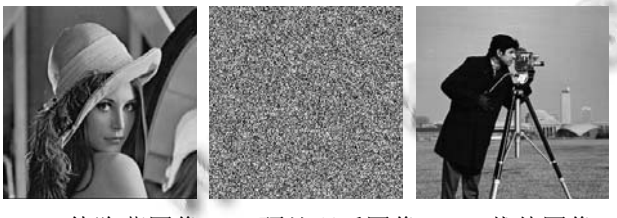
$$B_1(N\times k_i+i,N\times k_j+j)=B_1(N\times k_i+i,N\times k_j+j)+C_1(i,j) \quad (8)$$

其中当 ($k_i=k_j=0$时$k_i=k_j=1$) .

4 实验仿真结果

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 $T_0=2000, k=5$. 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.

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.

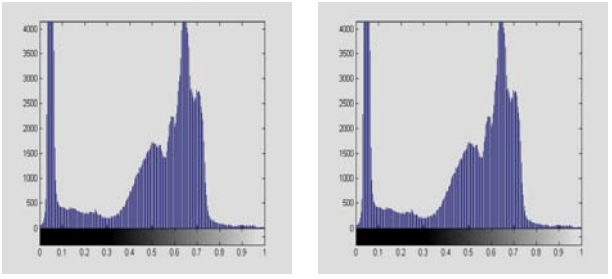


(a) 待隐藏图像 (b) 预处理后图像 (c) 载体图像

(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

直方图的分布能有效地反映隐藏效果的质量, 当直方图越一致则隐藏效果越佳. 因此为了观察算法的隐藏效果, 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归一化后的直方图.



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(PSNR)和均方根误差(RMSE)来衡量载体图像和混合图像之间的客观保真度[7-9]. 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. 而均方根误差越小, 说明两幅图像越相似. 表 1 列出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, 错误密钥恢复图像与待隐藏图像的对比, 以及正确密钥恢复图像与待隐藏图像的对比.

表 1 效果分析

	PSNR	RMSE
图 1(a)与图 1(b)	28.701889	9.363662
图 1(e)与图 1(d)	71.751470	0.065912
图 1(a)与图 1(e)	Inf	0
图 1(a)与图 1(f)	26.451428	12.133016

通过表 1 的实验结果可以看出, 与文献[4]载体图像与混合图像之间的 RMSE 与 PSNR 相比较, 本文的载体图像与混合图像之间的 RMSE 更小, PSNR 更大, 说明图像的隐藏效果比文献[4]更好; 正确密钥恢复图像与待隐藏图像之间的 RMSE 为 0, PSNR 无穷大, 说明算法能无失真地恢复隐藏图像.

5 结束语

本文提出一种基于 DCT 和混沌的图像隐藏算法, 利用离散余弦变换的性质, 在 DCT 域的中高频部分嵌入加密后的待隐藏图像, 以实现图像的隐藏功能. 实验仿真结果表明, 文中的算法比文献[4]具有更好的隐藏效果, 并且可以实现秘密图像的无损复原, 具有一定的应用价值.

参考文献

1 苏莉萍,刘亮.一种基于 Logistic 混沌系统的图像加密新算法.电脑与信息技术,2006,14(5):26–28.

2 Ye RS, Huang HQ. A Novel Image Shuffling and WatermarkingScheme Based on Standard Map. Proc IEEE International Conference on Information Engineering and Computer Science.Wuhan, China, December 2009: 832–835.

3 叶瑞松,陈永洪.基于 Arnold 变换的混沌轨道遍历性的数字图像加密.微计算机应用,2009,30(9):14–21.

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

5 黄慧青.一个二维离散系统的分岔分析.嘉应学院学报,

(下转第 118 页)

用，成本较低，另一方面，还可结合精装修房建设，由购房人自由选择装修方案，减少二次装修，见表 1 和如图 9 所示.

表 1 售楼处数字沙盘名称和功能

名称	作用和功能
LED 楼盘模拟数字沙盘	显示楼盘的三维效果，类似普通沙盘
超大触屏显示器 1（左）	主要显示楼盘的更详细三维的信息，使每一栋楼的信息更加详细，如电梯位置、型号，户型结构；当然顾客也可以根据自己喜好从开发商提供的模拟精装修样板房模型库中，选择自己喜欢的装修风格。
超大触屏显示器 2（右）	与超大触屏显示器 1（左）相同
超大触屏显示器 3（后）	主要三维显示该楼盘周边情况。如距市中心、学校、医院、超市、公交站点距离等。

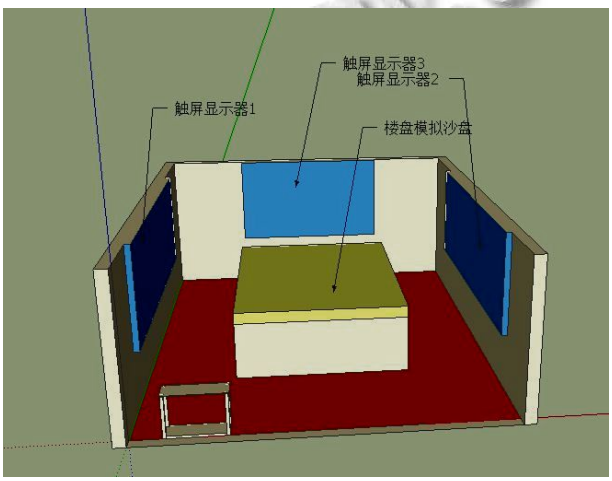


图 9 模拟售楼中心

5.3 数字导航

人类对于空间的定位有两种模式，一是直接定位，二是相对定位. 完全采用 GPS 导航仪由于坐标往往存在误差，只能成为人类导航的辅助工具，因而无法实现无人驾驶. 如能够将特征建筑坐标及建筑形态存储于导航仪中，先由导航仪识别特征建筑，再由特征建筑定位目标建筑，就可实现汽车无人驾驶.

6 结语

采用上述方法建模，不仅成本低，且速度快. 项目组以扬州科技学院扬子津校区(560 亩)为例，进行了对比试验：采用本方法建模时间仅需 96 工时，成本约 1 万元，而采用传统方法则需 192 工时，成本约 4 万元. 当然本方法与传统方法相比缺陷在于精度相对较低，这主要是以 Google Earth 为数据源带来的负效应，通过遥感技术的不断发展，高分辨率影像得到普及，这一缺陷终将在技术层面得到解决.

参考文献

1 王彤,等.基于 Google Earth 的数字校园 WebGIS 系统的专题制图.计算机应用与软件,2010,27(6):242–243.
2 朱兴洲,等.基于 ArcGIS Engine 的 3 维校园地理信息系统设计与开发.测绘与空间地理信息,2011,34(5):26–30.
3 邓彩群,等.基于 ArcScene+Sketchup 的小区三维可视化研究与实现.城市勘测,2011,(2):52–55.
4 洪清锋,等.基于 Google SketchUp 和 ArcGIS 建立校园三维可视化的方法探讨.数字技术与应用,2011,(11):174–175.

(上接第 107 页)

2010,28(5):22–26.
6 余成波.数字图像处理及 MATLAB 实现.重庆:重庆大学出版社,2007.
7 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.
8 Zhang JS, Tian L, Tai HM. A new water- marking method based on chaotic maps. IEEE International Conference on Multimedia and Expo.Taipei, 2004: 939–942.
9 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.