基于激光散斑和 Henon 映射的图像加密方法

贺锋涛,张 敏,白 可,孙 力

(西安邮电大学 电子工程学院,陕西 西安 710061)

摘 要:为了提高图像在信息交换中的安全性与可靠性,提出一种将激光散斑和 Henon 映射混合应用于图像加密的新方法。激光散斑图像灰度分布具有随机性,采用 SCAN 语言将其扫描为不同的随机序列,该序列与 Henon 映射生成的序列求和形成新序列,新序列与待加密的原始图像按位异或实现加密。结果表明:该方法具有较好的加密效果,较强的密钥敏感性,较弱的相邻像素相关性,可抵御统计分析攻击。

关键词:激光散斑; Henon 映射; 随机序列; 图像加密

中图分类号:TN249 **文献标志码**:A **DOI**:10.3788/IRLA201645.0428003

Image encryption method based on laser speckle and Henon mapping

He Fengtao, Zhang Min, Bai Ke, Sun Li

(College of Electronic Engineering, Xi′an University of Post and Telecommunications, Xi′an 710061, China)

Abstract: In order to improve the security and reliability of the image in the information exchange, a new method was put forwards that laser speckle and Henon mapping were mixed and applied to the image encryption in this paper. Laser speckle image gray distribution was random, it could be scanned for difference random sequences by using the SCAN language. A sequence generated by this sequence with Henon mapping that sum modulo form a new sequence. Using the new sequence to made bit-wise exclusive or implement encryption with original images to be encrypted. The results showed that the method has a good encryption effect, strong key sensitivity and weak correlation of adjacent pixels, could against the statistical attack.

Key words: laser speckle; Henon mapping; random sequence; image encryption

收稿日期:2015-07-05; **修订日期**:2015-08-10

基金项目:国家自然科学基金(61201193)

作者简介:贺锋涛(1974-),男,副教授,博士,主要从事光电传感信息处理技术,信息高密度光存储等方面的研究。Email: hefengtao@xupt.edu.cn.

通讯作者:张敏(1990-),女,硕士生,主要从事激光应用方面的研究。Email:xiaobaizhang1990@126.com

0 引 言

随着多媒体通信技术日新月异的发展，人们对图像传输的需求也日益增加，图像安全和保密工作亦与日俱增。图像加密技术主要分为像素空间位置置乱和灰度值的置乱两类。基于图像空间位置置乱技术——如 Arond 变换[1]，Hilbert 曲线变换[1-2]，骑士巡游变换[3]，魔方变换[4]等，均具有或长或短的变换周期且并未改变图像的灰度统计特性，因此难以抵御统计分析的攻击。基于灰度值的置乱技术——如 Henon 映射[4-5]，Logistic 映射[5]，Lorenz 系统[6]等，均是利用没有随机扰动的装置(比如计算机)生成随机序列，难以抵御算法已知或算法穷举攻破。

近年来，混合图像加密技术逐渐成为研究热点。参考文献[7-9]初步提出混合加密理论，其仅利用算法混沌[10]实现，安全性较之前有所增加，但依旧无法满足人们的要求。参考文献[10]提出一种物理混沌的图像加密系统，其主要思想是利用模拟电路产生混沌序列实现加密。由于随机扰动的存在导致初始条件随机变化，提高了图像的保密性。文中将物理随机序列与算法混沌结合起来，利用激光散斑图像灰度分布的随机性，提出一种物理随机序列发生器激光散斑和 Henon 映射的混合图像加密方法。仿真结果表明，该方法具有较好的加密效果及较强的抗攻击能力。

1 激光散斑和 Henon 映射的基本概念

1.1 激光散斑成因及其特征

激光具有高亮度，方向性、单色性、和相干性好等特征。当使用激光作为光源照射粗糙物体表面时，粗糙物体表面可以看做是由许多独立的表面面积的组元相互叠加组成的，经表面面积的组元反射的子波在像面上发生干涉产生明亮相间的斑点，称之为散斑[11-12]，通过 CCD 采集到的激光散斑图像如图 1 所示。

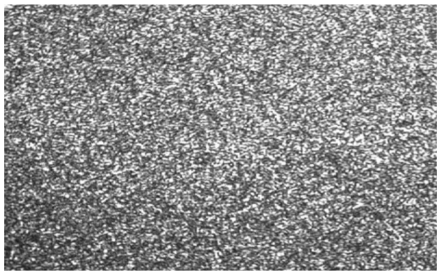


图 1 激光散斑图像

Fig.1 Laser speckle image

SCAN 语言是一种将二维数据转换为一维序列的方法，它可以产生大量的扫描路径或空间填充曲线，因此是一种有效的数据访问技术。由于激光散斑图像灰度分布具有的随机性[13]，可视为物理随机序列发生器。故可用 SCAN 语言[14-15]将其扫描为不同的随机序列。

1.2 Henon 映射

Henon 映射不止是一种简单的二维映射，而且也是一种非平凡二次方型非线性二维映射，但它的动力学性质已足够复杂，且存在唯一确定的单值解。

Henon 映射的方程及逆映射定义如公式(1)和公式(2)：

$$\begin{cases} x_{n+1}=-px_n^2+qy_n+1 \\ y_{n+1}=x_n \end{cases} \tag{1}$$

$$\begin{cases} x_n=y_{n+1} \\ y_n=(x_{n+1}+py_{n-1}^2-1)/q \end{cases} \tag{2}$$

为了适合图像数据流的特点，在加密算法中一般使用改进后的 Henon 映射及逆映射，如公式(3)和公式(4)：

$$\begin{cases} x_{n+1}=1-px_n^2+qy_n \bmod G \\ y_{n+1}=x_n \bmod G \end{cases} \tag{3}$$

$$\begin{cases} x_n=y_{n+1} \bmod G \\ y_n=(x_{n+1}+py_{n-1}^2-1)/q \bmod G \end{cases} \tag{4}$$

式中：G 为该类型图像最大的灰度值，如灰度图像 G=255。p=1.4，q=0.3 时映射系统处于混沌状态。

2 加密方法和仿真结果

2.1 加密方法

由于 CDD 采集的图像大小为 960×1 280，而待加密的原始图像相比散斑图像较小。因此可在散斑图像中随机选择和原始图像大小相同的区域，采用 scan 语言扫描为随机序列与 Henon 映射生成的混沌序列逐位求和取模形成新序列，该序列按位异或原始图像实现加密。其加密方法步骤如下：

(1) 输入待加密的原始图像 $I(m,n)$，其中 m，n为图像的行列维数；

(2) 给定 Henon 映射系统参数 a，b，初始值 x_1，y_1，由公式(3)迭代 $N-1$ 次($N=m\times n$)次，产生两组序列 $\{x_m\}$，$\{y_n\}$；

(3) $\{Z_{m*n}\}$交替读取$\{x_m\}$,$\{y_n\}$,即$\{Z_{m*n}\}=\{x_1,y_1,x_2,y_2,\cdots,x_m,y_n\}$;

(4) 在激光散斑图像以 I,J 为起始行列裁剪出大小为 $m\times n$ 的区域 K,用 SCAN 语言逐行扫描 K 的灰度值组成序列$\{T_{m*n}\}=\{K(1,1),K(1,2),K(1,3),\cdots,K(m,n)\}$;

(5) 将$\{Z_{m*n}\}$和$\{T_{m*n}\}$两个序列对应元素相加并求模,即 $N_i=(Z_i+T_i)\mathrm{mod}255$,$i=1,2\cdots m*n$,得到新序列$\{N_{m*n}\}$;

(6) 将新序列$\{N_{m*n}\}$排列为 $m\times n$ 的矩阵 Q,用其按位异或[16]原始图像,即 $P(i,j)=Q(i,j)\oplus I(i,j)$得到加密图像 P。

解密算法与加密算法互为逆向运算。在得到加密图像与正确的密钥 I,J,x_1,y_1 的情况下,只需要进行加密过程的逆向操作便可以解密出正确的原始图像。

2.2 仿真结果

为了测试该加密方法的性能,利用 MATLAB 对其进行仿真。像素为 256×256 的 lena.bmp 作为原始图像。在密钥 I=400,J=400,x_1=0.5,y_1=0.5 的条件下对该图像进行加密。对其加密测试结果如图 2 所示。

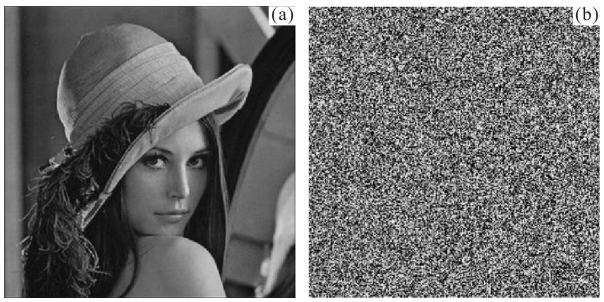


图 2 原始图像加密测试结果

Fig.2 Original image encryption test results

3 安全性分析

3.1 密钥空间分析

对于传统的 Henon 加密方法,其系统迭代过程一般采用 IEEE754 浮点数标准。假设 $x_1=0.x_{11}x_{12}x_{13}\cdots x_{15}$,$y_1=0.y_{11}y_{12}y_{13}\cdots y_{15}$,所以该方法的密钥空间大约为 10^{30}。文中所用方法密钥包括系统初始值 x_1、y_1、截取位置 I、J,其密钥空间可达到 10^{40},且其关键在于散斑图像具有不可复制性,即使在密钥已知的情况下,得不到经安全信道传输的散斑图像,依旧无法解密。故该方法具有较大的密钥空间及安全性。

3.2 灰度直方图

灰度直方图是反映一副图像灰度分布有序性的图表,其横坐标表示灰度值,纵坐标表示的该灰度值的像素数对整幅图像的像素数的比率。Lena.bmp 图像在加密前后的灰度直方图如图 3 和图 4 所示。由图 3 和图 4 可知:原始图像的灰度集中在中间区域,两边区域接近 0,而加密图像的灰度则打破了这种分布呈现均匀分布。因此,该方法可以较好的抵御统计分析和差分解密攻击。

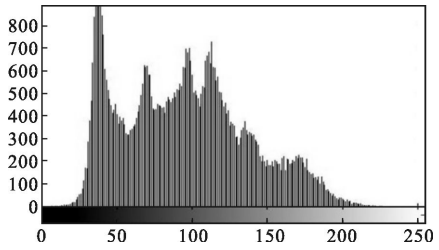


图 3 原始图像灰度直方图

Fig.3 Original image gray histogram

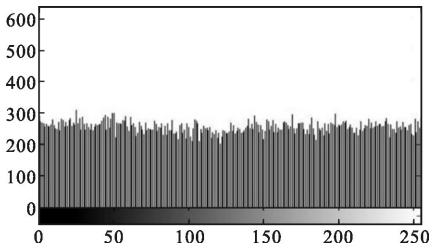
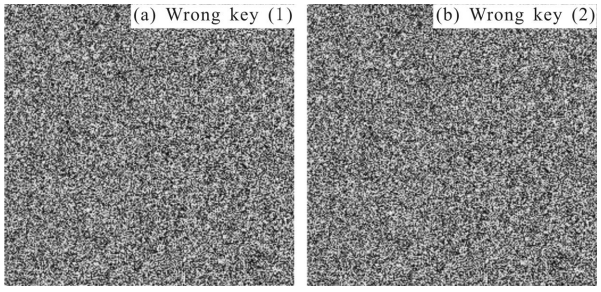


图 4 加密图像灰度直方图

Fig.4 Encrypted image gray histogram

3.3 密钥敏感性分析

为了检验该方法的密钥敏感性,稍微调整 I,J,x_1,y_1 的值,即以错误密钥 (1) I=401,J=400,x_1=0.5,y_1=0.5;(2) I=400,J=401,x_1=0.5,y_1=0.5;(3) I=400,J=400,x_1=0.45,y_1=0.5;(4) I=400,J=400,x_1=0.5,y_1=0.45 分别作为解密密钥,解密后图像完全不可知如图 5 所示。



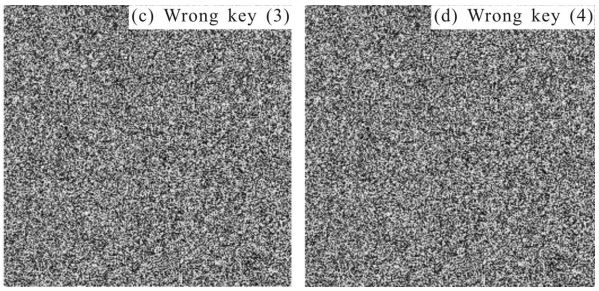


图 5 密钥敏感性测试结果

Fig.5 Encryption key sensitivity test results

只有在 I,J,x_1,y_1 均正确的情况下才可以正确的解密出原始图像如图 6 所示，可见该方法对密钥有较强的敏感性。

图 6 正确解密图像

Fig.6 Correct decrypted image

3.4 相邻像素相关性分析

相邻像素的相关性用来衡量一副图像中两个相邻像素的相关性，加密效果随着相关性的增大而变差。其定义如公式(5)：

$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}}$$

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

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

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{5}$$

式中：x,y 分别为相邻的两个像素；$D(x),E(x)$ 为 x 的方差和期望；$\mathrm{cov}(x,y)$ 为 x,y 的协方差。

计算图像 lena 和加密图像所有水平，垂直及对角线方向相邻像素的相关系数，如表 1 所示。

由表 1 可知：3 个方向相邻像素的相关性几乎接近 0。表明该方法去除了相邻像素之间的相关性，防止恶意攻击。

表 1 相关性分析

Tab.1 Analysis of the correlation

Relationship between pixels	Original image	Encrypted image
Horizontal	0.965 7	0.003 6
Vertical	0.979 7	−0.010 3
Diagonal	0.953 3	0.001 9

4 结 论

文中提出一种基于激光散斑和 Henon 映射的图像加密新方法。通过对原始图像加密仿真、灰度直方图、密钥敏感性分析及相关性分析表明该方法可以较好的实现对数字图像的加、解密，且具有较大的密钥空间，较强的密钥敏感度和较好的统计特性。利用激光散斑实现混合图像加密的思想，为散斑应用提供了新方向。同时利用 scan 语言获取更多的扫描方式作为随机序列，实现了安全性更高的加密方法。

参考文献：

[1] Ding Wei, Qi Dongxu. Digital image transformation and information hiding and disguising technology [J]. ***Chinese J Computer***, 1998, 21(9): 838-842. (in Chinese)
丁玮, 齐东旭. 数字图像变换及信息隐藏与伪装技术[J].计算机学报, 1998, 21(9): 838-842.

[2] Zhao Jie. Image segmentation based on Hilbert curve and wavelet transform [J]. ***Journal of Jilin Teachers Institute of Engineering and Technology***, 2013, 29(1): 77-80. (in Chinese)
赵杰. 基于 Hilbert 曲线和小波变换的图像分割[J]. 吉林工程技术师范学院学报, 2013, 29(1): 77-80.

[3] Zhong Keying. The file encryption algorithm based on the knight tour problem[J]. ***Software Guide***, 2011, 11(2): 40-42. (in Chinese)
钟克英. 基于骑士巡游问题的文件加密算法 [J]. 软件导刊, 2011, 11(2): 40-42.

[4] Dong Husheng, Lu Ping, Zhong Baojiang. Image encryption algorithm based on Henon Mapping and magic cube transformation [J]. ***Computer Application and Software***, 2014, 31(5): 291-294. (in Chinese)
董虎胜, 陆萍, 钟宝江. 基于 Henon 映射与魔方变换的图像加密算法[J]. 计算机应用与软件, 2014, 31(5): 291-294.

[5] Dong Husheng, Lu Ping. Scheme of image encryption based on Logistic chaos system and magic cube transformation[J]. ***Computer Era***, 2012, 11: 12-15. (in Chinese)
董虎胜, 陆萍. 基于 Logistic 混沌系统与魔方变换的图像加密方案[J]. 计算机时代, 2012, 11: 12-15.

[6] Wang Ying, Zhen Deling, Ju Lei. Digital image encryption algorithm based on Lorenz chaotic system [J]. ***Journal of University of Science and Technology Beijing***, 2004, 26(6): 678-682. (in Chinese)
王英, 郑德玲, 鞠磊. 基于 Lorenz 混沌系统的数字图像加密算法[J]. 北京科技大学校报, 2004, 26(6): 678-682.

[7] Fan Yi, Liu Xiongying, Qiu Shuisheng. Chaos based image secure communication combined with conventional encryption algorithm[J]. ***Computer Engineering***, 2005, 31(20): 44-45. (in Chinese)
范艺, 刘雄英, 丘水生. 混沌加密与常规加密复合的图像保密通信系统[J]. 计算机工程, 2005, 31(20): 44-45.

[8] Long Min. Qiu Shuisheng, Peng Fei. Design of a complex encryption scheme based on RSA algorithm and hyperchaos [J]. ***Chinese Journal of Radio Science***, 2006, 21(1): 74-78. (in Chinese)
龙敏, 丘水生, 彭飞. 基于 RSA 算法和超混沌的复合加密方案[J]. 电波科学学报, 2006, 21(1): 74-78.

[9] Xiang Fei, Xiao Huijuan, Qiu Shuisheng. The design scheme of image secure communication system based on CNN and DES [J]. ***Journal of South China of Technology***, 2007, 35 (9): 31-34. (in Chinese)
向菲, 肖慧娟, 丘水生. 基于 CNN 和 DES 的图像保密通信系统设计方案[J]. 华南理工大学学报, 2007, 35(9): 31-34.

[10] Jin Jianxiu, Qiu Shuisheng. Research on image encryption system based on chaotic Physical [J]. ***Acta Physica Sinica***, 2010, 59(2): 792-799. (in Chinese)
晋建秀, 丘水生. 基于物理混沌的混合图像加密系统研究[J]. 物理学报, 2010, 59(2): 792-799.

[11] Liu Jia, He Fengtao. High-resolution 405 nm laser microscopic imaging[J]. ***Journal of Applied Optics***, 2011, 32 (4): 806-809. (in Chinese)
刘佳, 贺锋涛. 高分辨率 405 nm 激光显微成像系统研究[J].应用光学, 2011, 32(4): 806-809.

[12] Wang Xiaolin, He Fengtao, Jia Qiongyao, et al. Laser speckle control based on optical fiber vibration [J]. ***Laser Technology***, 2014, 38(2): 177-180. (in Chinese)
王晓琳, 贺锋涛, 贾琼瑶, 等. 基于光纤振动的激光散斑抑制控制[J]. 激光技术, 2014, 38(2): 177-180.

[13] Pappu R, Recht B, Taylor J, et al. Physical one-way functions[J]. ***Science***, 2002, 297(5589): 2026-2030.

[14] Maniccan S S, Bourbakis N G. Lossless image compression and encryption using SCAN [J]. ***Pattern Recognition***, 2001, 34(6): 1229-1245.

[15] Maniccan S S, Bourbakis N G. Image and video encryption using scan patterns [J]. ***Pattern Recognition Agent Based Computer Vision***, 2004, 37(4): 725-737.

[16] Zhu Congxu, Chen Zhigang, Ouyang Wenwei. A new image encryption algorithm based on general Chen′s chaotic system [J]. ***J Cent South Univ***, 2006, 37(6): 1142-1148. (in Chinese)
朱从旭, 陈志刚, 欧阳文卫. 一种基于广义 Chen′s 混沌系的图像加密新算法 [J]. 中南大学学报, 2006, 37(6): 1142-1148.