

基于 Bezier 曲线的数字图像加密研究

李晴晴^{1,2}, 杭后俊^{1,2}, 尹天乐¹

(1. 安徽师范大学 计算机与信息学院, 安徽 芜湖 241000;

2. 网络与信息安全安徽省重点实验室, 安徽 芜湖 241000)

摘要:分析了数字图像加密在国内外的发展现状和面临的问题,在此基础上深入讨论并提出了一种基于有理二次 Bezier 曲线的数字图像加密算法。根据该曲线内权因子的特殊性质给出了一个有理映射函数,经计算当权因子在一定范围内取值时,该映射具有正的 Lyapunov 指数,即具有混沌性质。随后利用其混沌特性生成混沌序列进而构造加密因子与像素灰度进行运算并置换,最终得到加密图像。该算法不仅保留了一维混沌系统形式简单的特点,而且具有加密解密效率高的优点。通过对直方图、相邻像素之间的相关性及信息熵等进行的详细分析可以看出,该算法安全性高,加密图像的灰度直方图较为均匀,加密图像中相邻像素之间的相关性强度显著降低。仿真结果表明该算法取得了较好的加密效果。

关键词:混沌系统;有理 Bezier 曲线;权因子;加密因子

中图分类号:TP309.7

文献标识码:A

文章编号:1673-629X(2019)04-0091-04

doi:10.3969/j.issn.1673-629X.2019.04.019

Research on Digital Image Encryption Based on Bezier Curve

LI Qing-qing^{1,2}, HANG Hou-jun^{1,2}, YIN Tian-le¹

(1. School of Computer and Information, Anhui Normal University, Wuhu 241000, China;

2. Anhui Provincial Key Laboratory of Network and Information Security, Wuhu 241000, China)

Abstract: We analyze the development status and problems of digital image encryption at home and abroad. On the basis, we discuss in depth and propose a digital image encryption algorithm based on rational quadratic Bezier curves. According to the special property of the inner weight factor, a rational mapping function is given. When the weight factor is evaluated in a certain range, the mapping has a positive Lyapunov exponent, that is, it has the property of chaos. Then, the chaotic sequence is generated by the mapping function. The pixel gray values are replaced by the encryption factor, and the encrypted image is obtained finally. The algorithm proposed not only maintains the virtue of simple form, but also has high efficiency because of the encryption and decryption algorithm both are the same one. Finally, the gray histogram and the correlation between adjacent pixels and the entropy are analyzed in detail. The proposed algorithm has high security. The gray histogram of the encrypted image is more uniform, and the intensity of the correlation between adjacent pixels in the encrypted image is significantly reduced. The simulation shows that the proposed algorithm achieves better encryption effect.

Key words: chaos system; rational Bezier curve; weight; encryption factor

0 引言

由于网络环境本身的复杂性和易变性,使得信息在网络中传输时的安全问题愈加突出^[1]。据不完全统计,网络中传播的信息,大约有百分之七十是以数字图像形式体现出来的,因此数字图像加密技术就成了研究的热点问题。现在常用的图像加密算法中,基于现代密码体制的图像加密^[2-3]、基于矩阵变换/像素置换的图像加密^[4-5]、基于秘密分割与秘密共享的图像加

密^[6-7]等由于图像数据存在大量冗余,像素之间具有很强的相关性,图像具有特定的数据格式等特点,并不能完全满足图像加密的要求^[8]。而混沌系统由于自身的特殊性质如对初始条件和参数高度敏感,随机性强,遍历性等使其非常适合图像加密^[9-14]。现在很多基于混沌系统的图像加密算法以时间和空间换加密强度的思想,大多采用复杂的加密算法和变换流程来获取更高效的加密指标,这样自然导致加密解密速度慢、算法

收稿日期:2018-04-30

修回日期:2018-08-08

网络出版时间:2018-12-20

基金项目:安徽省高等学校自然科学研究重点项目(KJ2017A326)

作者简介:李晴晴(1994-),女,硕士研究生,研究方向为计算机图形学、数字图像处理;杭后俊,副教授,硕导,CCF会员(12645M),研究方向为计算机图形学、计算机辅助几何设计、数字图像处理等。

网络出版地址: <http://cnki.net/kcms/detail/61.1450.TP.20181220.1035.030.html>

的复杂性高等缺陷,加密效率不如一维系统。

Bezier 曲线是一种由控制点控制的多项式曲线,具有诸多优良性质,广泛应用于形状设计中。研究表明,单位区域内的二次曲线映射可以产生混沌序列^[15-17],而有理二次 Bezier 曲线可以精确表示二次圆锥曲线^[18]。基于这一理论,文中提出了一种基于有理二次 Bezier 曲线的数字图像加密算法。根据有理二次 Bezier 曲线的内在特性,提出了一个一维有理映射函数,当内权因子在一定范围内取值时,该迭代函数具有混沌特性,产生混沌序列,进而构造加密因子与像素灰度进行运算并置换,最终得到加密图像。

1 有理二次 Bezier 曲线

根据 CAGD 理论^[13],有理二次 Bezier 曲线

$$p(u) =$$

$$\frac{(1-u)^2\omega_0\mathbf{b}_0 + 2u(1-u)\omega_1\mathbf{b}_1 + u^2\omega_2\mathbf{b}_2}{(1-u)^2\omega_0 + 2u(1-u)\omega_1 + u^2\omega_2}, 0 \leq u \leq 1 \quad (1)$$

精确表示二次圆锥曲线,可由 $k = (\omega_0\omega_2)/\omega_1^2$ 的取值范围进行分类:

$$k = \begin{cases} \in (1, +\infty) & \text{椭圆弧} \\ 1 & \text{抛物线弧} \\ \in (0, 1) & \text{双曲线弧} \end{cases}$$

对于标准型,可用内权因子 ω_1 进行分类:

$$\omega = \begin{cases} \in (1, +\infty) & \text{双曲线弧} \\ 1 & \text{抛物线弧} \\ \in (0, 1) & \text{椭圆弧} \end{cases}$$

有理二次 Bezier 曲线具有如下重要特性:

(1) 如果保持其余权因子、所有控制点不变,让 ω_1 在某个范围内变化,就会得到一族曲线。再固定参数 u ,则这一族曲线上参数 u 相同的点位于一条直线上。

(2) 如果曲线上点 p 的切线平行于弦 $\overline{b_0b_2}$,称 p 为二次曲线的肩点。肩点的参数为 $u = 1/(1 + \sqrt{\frac{\omega_2}{\omega_0}})$ 。特别的,对于标准型,肩点的参数 $u = 1/2$ 。

2 基于 Bezier 方法的图像加密算法

2.1 加密系统

据式 1 可知,由控制点 $b_0 = [0, 0]$, $b_1 = [0.5, (1 + \omega)/\omega]$, $b_2 = [1, 0]$ 确定的标准型有理二次 Bezier 曲线为:

$$\begin{cases} x(u) = \frac{u(1-u)\omega + u^2}{(1-u)^2 + 2u(1-u)\omega + u^2} \\ y(u) = \frac{2u(1-u)(1+\omega)}{(1-u)^2 + 2u(1-u)\omega + u^2} \end{cases}, 0 \leq u \leq 1$$

万方数据

(2)

显然,该曲线上点的 x 坐标取值范围为 $x \in [0, 1]$,而 y 最大值为曲线上肩点的 y 值,即 $y_{\max} = y(0.5) = 1$,所以 y 坐标取值范围为 $y \in [0, 1]$ 。

$\forall x_0 \in (0, 1)$, $\forall \omega > 0$,根据内权因子对曲线形状的影响特性,构造如下一维有理映射函数:

$$x_{n+1} = \frac{2x_n(1-x_n)(1+\omega)}{(1-x_n)^2 + 2x_n(1-x_n)\omega + x_n^2} \quad (3)$$

李雅普诺夫指数 (Lyapunov) 是评判一个系统是否具有混沌性质的重要指标, $\text{Lyapunov} > 0$ 说明该系统具有混沌特性。对任意一维映射 $x_{n+1} = f(x_n)$,其李雅普诺夫指数的计算方式如下:

$$\lambda = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left| \frac{df(x)}{dx} \right|_{x=x_i} \quad (4)$$

其中, x_0 为系统的初始值; x_1, x_2, \dots 为每次的迭代值; n 为迭代次数。

对于有理映射函数,其李雅普诺夫指数为:

$$\lambda =$$

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \frac{2(1+\omega) |1-2x|_{x=x_i}}{[(1-x_n)^2 + 2x_n(1-x_n)\omega + x_n^2]^2} \quad (5)$$

经计算可得,内权因子 ω 至少在区间 $[0.7, 1.5]$ 上取值时 λ 大于零,即由式 3 产生的序列 $\{x_i\}$ ($i = 0, 1, 2, \dots$) 具有混沌特性。图 1 为该混沌序列产生过程的示意图。

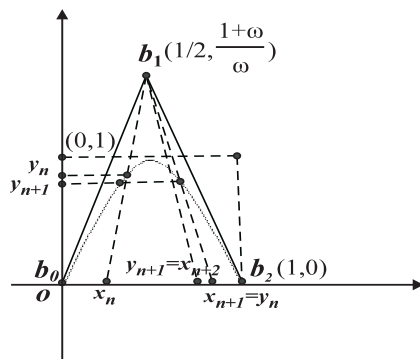


图 1 序列 $\{x_i\}$ ($i = 0, 1, 2, \dots$) 产生示意

2.2 加密算法

设明文图像 I 大小为 $m \times n$, $I(i, j)$ ($i = 1, 2, \dots, m, j = 1, 2, \dots, n$) 表示像素的灰度值。为了保证序列的混沌效果,可以预先对有理映射函数 (3) 迭代适当的次数 N , 比如 $N = 100$ 。依次读取图像 I 的每一像素 $I(i, j)$, 将有理映射函数 (式 3) 迭代 8 次所产生的实数序列在其最大值和最小值之间的每个数与其平均值 avg 进行比较, 若大于 avg 则对应位置 1, 否则置 0, 得到一个 8 位二进制序列, 称之为加密因子。再将该加密因子与当前像素灰度值进行异或运算, 并用运算的结果替代当前像素的灰度值, 从而得到密文图像。具体算法步骤如下:

(1) 设置初值 x_0 和 ω , 其中 $0 < x_0 < 1$, $\omega \in [0.75,$

- 1.55] ;
- (2) 对有理映射函数(式 3)进行 N 次预迭代;
- (3) 读取当前像素 $I(i,j)$;
- (4) 将有理映射函数迭代 8 次,得到一个 8 位加密因子 key;
- (5) 将 key 与图像当前灰度值 $I(i,j)$ 按位异或,并将运算的结果写入 $I(i,j)$;
- (6) 如果 $I(i,j)$ 是最后一个像素,转步骤 7,否则,转步骤 3;
- (7) I 即为密文图像;
- (8) 结束。

2.3 解密算法

解密算法和加密算法是一套算法,也就是说,采用文中算法进行加密的图像,用同样的算法即可对其进行解密。可以看出,文中算法具有复杂性低、加密效率高的优点。

3 仿真结果及分析

对文中算法进行仿真验证,取初始值 $x_0 = 0.01$, $\omega = 0.8$ 。这里用两张图片作为仿真用例,加密前后的对比图像如图 2 所示。



图 2 加密前后的对比图像

3.1 灰度直方图

灰度直方图是对图像中灰度级分布统计,直方图越均匀,抗统计分析能力越强。图 3 展示了图 2 中两幅图像加密前后的灰度直方图。可以明显看出,加密前后直方图变化很大,用该系统加密后图像直方图非常均匀。

3.2 密钥空间及安全性分析

该系统有两个参数, x_0 和 ω ,若运算精度按 10^{-16} 考虑,则系统初始条件组成的空间大小至少为 $10^{16} \times 10^{16} = 10^{32}$ 方数据,进行枚举攻击几乎是不可能的。

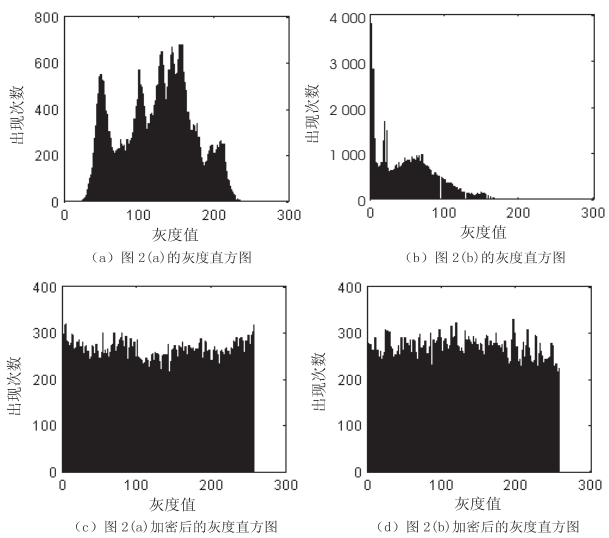


图 3 加密前后图像的灰度直方图

假如攻击者想破解图 2(a) 的加密图像,正确初始值为 $x_0 = 0.01$, $\omega = 0.8$ 。假若攻击者的猜测初值 $x_0 = 0.010\ 000\ 000\ 001$, $\omega = 0.8$,则解密图像如图 4(a) 所示;若攻击者猜测初值 $x_0 = 0.01$, $\omega = 0.799\ 999\ 999\ 99$, 则解密图像如图 4(b) 所示。可以看出,用文中模型加密的图片的安全性是非常高的。

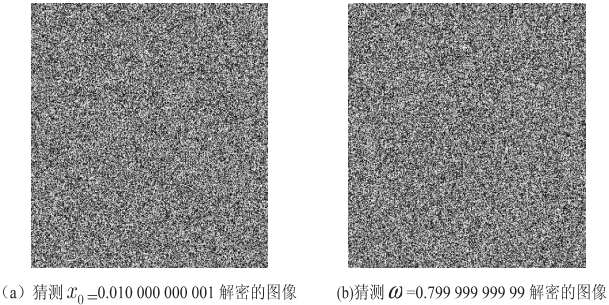


图 4 解密失败的图像

3.3 相关性分析

图像之所以不同于文本是因为图像像素间具有很强的相关性,攻击者会根据图像间的相关性进行统计分析,从而破解加密图像,所以,降低相关性是检验一个加密算法好坏的重要指标。因此,分别按水平方向、垂直方向以及对角线方向随机选取图像中的 50 行,50 列的像素进行相关性计算,随机次数为 5 次。以图 2(a) 为例,实验结果如图 5 所示。从仿真结果可以看出,相对于明文图片来说,像素间的相关性非常高,而在加密图片中像素的相关性的强度显著降低,具有非常好的加密效果,很好地满足了实际应用需求,有较高的实用价值。

分别求取该图像加密前后在三个方向上的相关系数,并且将经典的 Logistic 系统和 Chebyshev 同样用上述算法对图像进行加密后求取相关系数,对比结果如表 1 所示。可以明显看出,用同一算法实现三种不同的混沌系统,该系统加密后图像之间的相关性最小,安

全性更高。

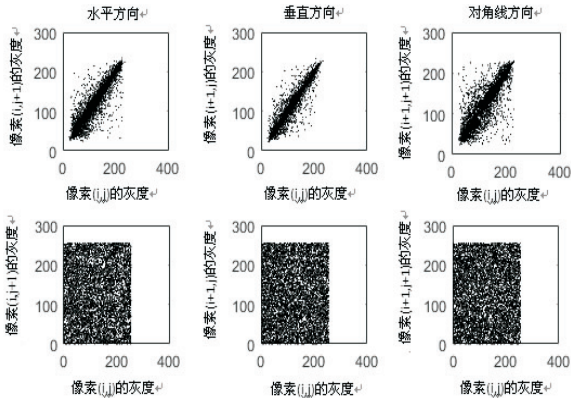


图 5 加密前后相关性对比图

表 1 加密前后相关系数对比

图 4(a)	加密前	加密后		
		Logistic	Chebyshev	文中系统
水平	0.947 1	0.041 1	0.007 4	6.684 9e-04
垂直	0.973 0	0.006 3	0.004 0	-0.001 0
对角线	0.929 5	0.008 4	0.002 5	-0.001 8

3.4 信息熵

信息熵是对信息随机性的度量,在图像中表示像素灰度值的随机性,图像的信息熵越大,信息的随机性越好。对任意图像 I,其信息熵计算公式如下:

$$H(I)=-\sum_{i=1}^Lp(x_i)\log_2p(x_i)$$
 (6)

其中, L 表示图像的灰度级; $p(x_i)$ 表示第 i 个像素灰度值所占的比例。

图像信息熵的理想值是 8。选取图 2(a)为示例,表 2 是分别采用 Logistic 映射、Chebyshev 映射和文中算法对原图和加密图像求取的图像信息熵的对比结果。可以看出,该系统加密后图像的信息熵更接近 8。

表 2 加密前后信息熵对比表

图 4(a)	加密前	加密后		
		Logistic	Chebyshev	文中系统
信息熵	7.453 2	7.883 9	7.985 2	7.987 1

4 结束语

Bezier 曲线广泛应用于工程设计中,将 Bezier 方法应用于图像处理是一项具有实际意义的工作。因此,文中提出一种基于有理二次 Bezier 曲线的数字图像加密算法,保留了一维混沌系统形式简单的特点。由于加密和解密是一套算法,所以该算法具有复杂性低、加密效率高的优点。通过仿真测试表明,利用该算法加密的图像,其灰度直方图较为均匀,加密图像中相邻像素之间的相关性强度与传统加密算法相比显著降低,取得了较好的加密效果。该方法对于将 Bezier 方

法应用于图像处理的其他问题也具有一定参考价值。

参考文献:

[1] 何泾沙. 信息安全导论[M]. 北京:机械工业出版社,2011.

[2] 陈燕梅,张胜元. 基于 AES 的数字图像置乱方法[J]. 中国图象图形学报,2006,11(8):1077-1080.

[3] NORCEN R,UHL A. Selective encryption of the JPEG2000 bitstream[C]//Proceedings of communications and multi-media security. Berlin:Springer,2003:194-204.

[4] 徐 亚,张绍武. 基于 Arnold 映射的分块双层自适应扩散图像加密算法[J]. 中国图象图形学报,2015,20(6):740-748.

[5] LIU Zhengjun,GONG Min,DOU Yongkang,et al. Double image encryption by using Arnold transform and discrete fraction alangular transform[J]. Optics and Lasers in Engineering,2012,50(2):248-255.

[6] 李昌刚,韩正之,张浩然. 图像加密技术综述[J]. 计算机研究与发展,2002,39(10):1318-1324.

[7] SASAKI M,WATANABE Y. Visual secret sharing schemes encrypting multiple images[J]. IEEE Transactions on Information Forensics and Security,2018,13(2):356-365.

[8] 张晓强,王蒙蒙,朱贵良. 图像加密算法研究新进展[J]. 计算机工程与科学,2012,34(5):1-6.

[9] 廖琪男,卢守东,孙宪波. 结合超混沌序列和移位密码的数字图像加密算法[J]. 小型微型计算机系统,2015,36(2):332-337.

[10] 黄冬梅,耿 霞,魏立斐,等. 基于 Henon 映射的加密遥感图像的安全检索方案[J]. 软件学报,2016,27(7):1729-1740.

[11] ABANDA Y,TIEDEU A. Image encryption by chaos mixing [J]. IET Image Processing,2016,10(10):742-750.

[12] CHEN Guanrong,MAO Yaobin,CHUI C K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos,Solitons and Fractals,2004,21(3):749-761.

[13] PAK C,HUANG Liliang. A new color image encryption using combination of the 1D chaotic map[J]. Signal Processing,2017,138:129-137.

[14] ZHANG Yong,TANG Yingjun. A plaintext-related image encryption algorithm based on chaos[J]. Multimedia Tools and Applicaions,2018,77:6647-6669.

[15] LAI Dejian,CHEN Guanrong. Generating different statistical distributions by the chaotic skew tent map[J]. International Journal of Bifurcation and Chaos,2000,10(6):1509-1512.

[16] GÓRA P,BOYARSKY A. On the significance of the tent map[J]. Internationa Journal of Bifurcation and Chaos,2003,13(5):1299-1301.

[17] 于万波,杨灵芝. 二次函数混沌特性分析及其图像加密应用[J]. 计算机工程,2013,39(4):5-8.

[18] 施法中. CAGD&NURBS[M]. 北京:高等教育出版社,2013.