

三维彩色图像加密的改进与实现

任晓奎¹, 马 超²

(1 辽宁工程技术大学 电子与信息工程学院, 辽宁 葫芦岛 125105;

2 辽宁工程技术大学 研究生学院, 辽宁 葫芦岛 125105)

摘 要: 针对三维空间上的彩色图像进行加密处理具有运算量和空间需求较大、加密效率较低的问题, 将彩色图像转换为三个层面上的二维灰度图像进行加工处理, 加快了加密速度. 为了提高算法的鲁棒性, 将混沌序列改进为一种均匀分布的序列, 得到了更理想的伪随机特性. 针对单一混沌加密算法安全性较差的问题, 将 Logistic 映射与 Chebyshev 映射相结合, 获得了复杂性较高的双混沌系统. 利用双混沌系统生成的混沌序列有效实现了像素混淆与扩散, 对图像加密方法进行了改进.

关键词: 三维空间; 彩色图像; 混沌; 图像加密

中图分类号: TP39

文献标识码: A

文章编号: 1000-7180(2015)01-0096-04

Improvement and Implementation of 3D Color Image Encryption

REN Xiao-kui¹, MA Chao²

(1 College of Electronics and Information Engineering, Liaoning Technical University, Huludao 125105, China;

2 School of Graduate, Liaoning Technical University, Huludao 125105, China)

Abstract: Encryption processing color images in 3D space on the computational complexity and space requirements for the larger, less efficient encryption problem, the color image is converted to three dimensions on a two-dimensional gray-scale image processing, thereby speeding up the encryption speed. In order to improve the robustness of the algorithm, the chaotic sequence turns to a homogeneous distribution of the sequence, to achieve more desirable characteristics of a pseudo-random. Logistic map and Chebyshev map for poor single chaotic encryption algorithm security problems, the combination of higher complexity of the dual chaotic system. Realization of the pixels confusion and diffusion effective with the chaotic sequence which generated by the dual chaotic system, the method of image encryption is improved.

Key words: 3D space; color image; chaos; image encryption

1 引言

采用原始 Logistic^[1] 进行图像加密具有易于实现、较好的类随机性, 以及稠密的周期点集等良好性质, 这些特性为密码系统的混合与扩散打下基础. 但是一些曾被广泛应用的经典的混沌密码方案对于现代密码体系来说不仅效率低下而且安全性也受到极大威胁. 因此, 需要进一步对原有密码系统进行分析, 在此基础上进行改进, 设计出可靠实用的加密方案是当务之急. 本文针对原始的 Chebyshev 和 Lo-

gistic 映射迭代生成的序列加以改进.

2 原始图像加密

原始图像加密采用的是一维离散动力系统 logistic 映射, 它表现出类随机性的行为. 它描述了在生态系统相对封闭的条件下, 某种昆虫随时间的变化规律并进行预测. 其中 $x_n \in (0, 1)$ 是决定系统某个时刻状态的变量. $\mu \in (0, 4)$ 称作分岔映射, 当满足条件 $3.569\ 945\ 6 \leq \mu \leq 4$ 时, 该函数的状态在平面坐标中是混沌的, μ 越接近 4 其随机性越好, 具有

类似噪声的平均分布特性. 经典的利用 Logistic 函数实现彩色图像加密^[1] 通常需要以下四个过程.

(1) 分离基色分量, 首先分离输入图像的基色分量, 根据式(1) 可以生成新的基色分量矩阵 I_R, I_G, I_B .

$$I_R = I(:, :, 1), I_G = I(:, :, 2), I_B = I(:, :, 3) \quad (1)$$

(2) 生成密钥, 因为需要满足混沌 Logistic 映射生成的密钥跟图像像素一一对应, 所以同样将混沌序列划分成三种形式, 它们的变量依次记作 x, y, z :

$$\begin{aligned} x_{n+1} &= \mu x_n (1 - x_n), y_{n+1} = \mu y_n (1 - y_n), \\ z_{n+1} &= \mu z_n (1 - z_n) \end{aligned} \quad (2)$$

(3) 像素置换过程. 依据式(3) 生成的基于混沌的序列 x, y, z 并依次置换基色分量矩阵, 过程主要由两部分构成:

① 因为式(2) 生成序列值的范围在 $[0, 1]$ 内, 而图像矩阵的值在 $[0, 255]$ 闭区间. 因此需要将式(2) 生成的序列转化为灰度矩阵并记作 G_x, G_y, G_z , 如式(3) 所示.

$$\begin{aligned} G_x &= \text{round}(x \times 256), G_y = \text{round}(y \times 256), \\ G_z &= \text{round}(z \times 256) \end{aligned} \quad (3)$$

② 输入待加密图像中分离的基色分量矩阵 I_R, I_G, I_B , 将灰度矩阵 G_x, G_y, G_z 与基色分量像素值执行式(4) 所示的的异或运算最终得到密文, 实现图像像素的置换.

$$\begin{aligned} C_R &= \text{bitxor}(I_R, C_x), C_G = \text{bitxor}(I_G, C_y), \\ C_B &= \text{bitxor}(I_B, C_z) \end{aligned} \quad (4)$$

(4) 合并彩色分量. 最后对上述加密分量按照式(5) 进行合并, 获得完整加密的彩色图像. 具体过程如图 1 所示.

$$C(:, :, 1) = C_R, C(:, :, 2) = C_G, C(:, :, 3) = C_B \quad (5)$$

3 改进的彩色图像加密

3.1 密钥和初始条件的获取

为了实现密钥的获取进而生成初始条件, 首先计算获得的原始彩色图像所占用的空间, 将其表示为 $[M \times N \times C]$. 然后将原始图像 P 记作 $P = \{P_1, P_2, \dots, P_{M \times N}\}$ 并分成三个颜色分量 R, G, B , 则 $P = \{P_1 = P_1R, P_2 = P_1G, P_3 = P_1B, P_4 = P_2R, \dots, P_i, \dots, P_h = P(M \times N)B\}$. 最后设置生成密钥的条件, 由外部变量(时间戳 p_time) 和内部变量(密码变量 p_pass) 以及某些图像本身具有的性质共同构成. 算法按照上述条件并基于 MD5 算法分别生成两

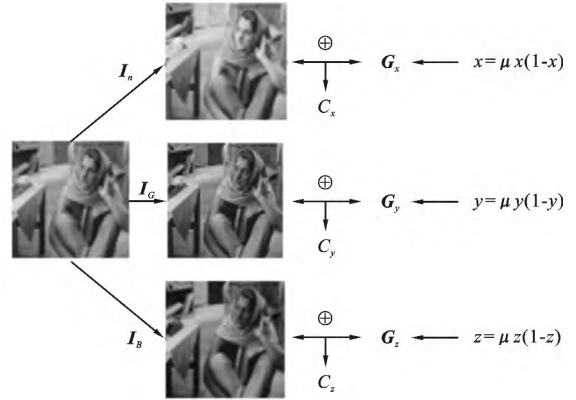


图 1 原始实现彩色图像的加密流程

组密钥, 每组均是由 32 位十六进制的数构成. 为了获得初始条件和参数, 分别将每组密钥除以一较大的素数再执行模加运算, 除以素数的目的是使得小数的位数较长一些, 从而增大算法的密钥空间^[2]. 生成素数的公式如式(6) 所示.

$$A = (n-1) \div 2 * \{ \lfloor [m(n+1) - (n!+1)^2] - 1 \rfloor - [m(n+1) - (n!+1)^2 + 1] + 1 \} \quad (6)$$

式中, A 表示生成的素数, 实数参数 m, n 的取值范围需要满足 $m > 1, n \geq 4$, 本文实验取值为: $m = 2, n = 4$, 此时 $A = 592$. 考虑到计算机具有精度效应, 因此输出的初始条件和系统参数均取 15 位有效数字. 该过程具体步骤如图 2 所示.

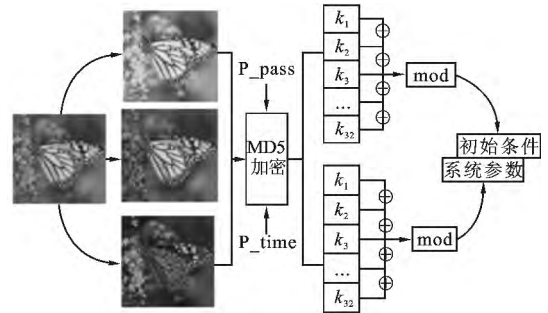


图 2 密钥和初始条件的生成

3.2 生成均匀的混沌映射

针对混沌映射的不均匀性, 采用下面方法做合理改进: (1) 混沌序列的放大和量化操作: 为了提高混沌序列具有的不规则特性, 首先采用小数点右移的方法, 相当于对整个序列乘以 10^n , 然后再对该值进行取整, 最后将两者做减法获得具有更加随机分布的序列, 如图 3 中(c)、(d) 所示, 变换后的序列值域的长度不变; (2) 混沌序列的第二次量化和模运算是再次对上述变换的序列取整, 由于彩色图像各分量的灰度级是 256, 所以需要把上面得到的序列

做一次映射, 最终改进的序列可以利用式(7)、(8)构成的数学模型进行描述.

$$X(i) = 10^m X(i) - \text{round}(10^m X(i)) \quad (7)$$

$$X(i) = \text{round}(X(i) + 0.5) \times 10^n \bmod 225 \quad (8)$$

式中, $X(i)$ 表示混沌序列, 整数参数 m 和 n 的作用是控制小数点移动位数, 通过大量实验得知, m 和 n 的取值范围在 $[0, 15]$ 之间, 令 $m = 10, n = 15$, 迭代次数为 150, 图 3(a)、(b)、(c) 表示对 Logistic 映射序列改进的过程, 图 3(d)、(e)、(f) 表示 Chebyshev 映射序列改进的过程. 图 3(c)、(f) 表示混沌序列改进后的分布情况, 可见改进的序列具有更理想的伪随机特性.

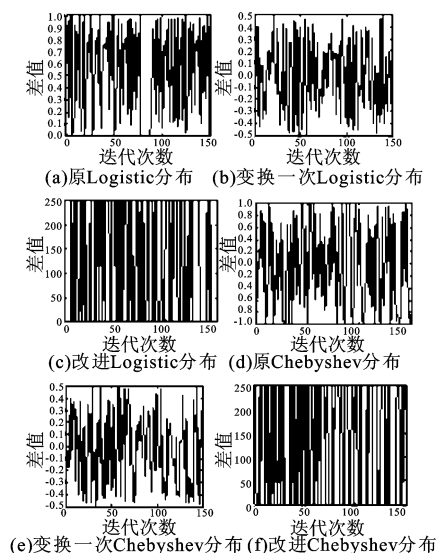


图 3 改进前和改进后状态对比图

把 MD5 算法生成的密钥代入均匀分布的双混沌映射^[2-4], 交替生成新的混沌映射序列 $C(x, y, z)$, 利用该映射实现像素的混淆和扩散, 对像素值逐点进行加密, 增强了系统的安全性和复杂性.

3.3 利用改进序列执行像素混淆和双向扩散

首先, 将获得的初始条件和系统参数分别代入 Logistic 和 Chebyshev 映射, 基于提出的均匀分布的双混沌系统, 交替生成新的混沌序列.

然后, 为了有效削弱图像的相邻像素相关性, 采用像素混淆算法有效改变了图像的像素值. 最后, 因为混淆的过程没有考虑到相邻像素之间的关系, 我们在算法中引入像素扩散^[5]有两个原因: 一方面, 像素值的有效扩散可以使离散化的混沌映射不可逆; 另一方面, 通过将明文图像像素散播到密文图像, 可以有效地改变图像的统计特征. 因此, 采用像素混淆与扩散相结合, 通过增强明文图像、密文图和密钥之间的复杂性, 可以有效提高系统抵御统计分析攻击

和选择明文攻击的能力. 利用如下公式分别实现像素点的水平方向和对角方向的扩散.

$$C^{(i+1)}(x+1, y, z) = \{[P(x, y, z) + C^{(i)}(x, y, z)] \bmod G\} \oplus C(x, y, z) \quad (9)$$

$$C^{(i+1)}(x+1, y+1, z) = \{[P(x, y, z) + C^{(i)}(x-1, y-1, z)] \bmod G\} \oplus C(x, y, z) \quad (10)$$

公式中 $C(x, y, z)$ 是采用双混沌映射混沌作用后的混沌序列, $P(x, y, z)$ 代表针对明文图像当前操作像素, G 表示图像的灰度级. 本文采用的是灰度级为 256 的图像进行实验, 初始值 $C(0)(0, 0, 0) = S$, S 为整数, 也是密钥的一部分, $C(i)(x, y, z)$ 是第 i 次加密后坐标为 (x, y, z) 的像素值, $1 \leq x \leq M-1, 1 \leq y \leq N-1$. 算法具体流程如图 4 所示.

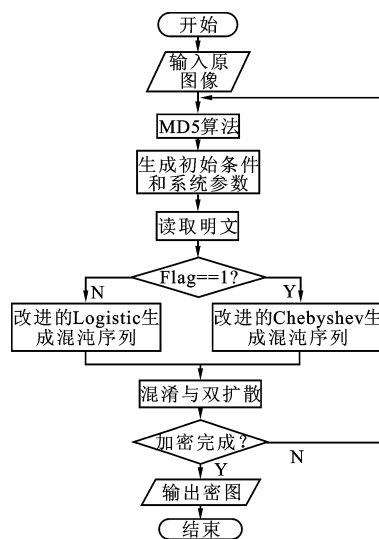


图 4 加密算法流程图

4 实验性能分析

4.1 实验分析

(1) 直方图分析: 图像中用来描述相同灰度级和它出现频数的统计图形称作直方图, 根据它的统计信息可分析算法对图像的扰动程度^[6-8]. 如图 5 所示, 其中(a)、(b)、(c)是 Monarch 图像各层灰度直方图, (c)、(e)、(f)为 Monarch 的加密图像各层灰度直方图.

图像加密前后的灰度直方图的差别很大, 说明算法改变了图像点分布的概率. 加密后灰度直方图分布均衡而平滑, 像素值个数平均值为 256, 灰度值均匀地在取值区间 $[0, 255]$ 范围内分布, 将原图像真实的分布规律打乱, 表明该算法对统计分析攻击的

抵抗能力较强.

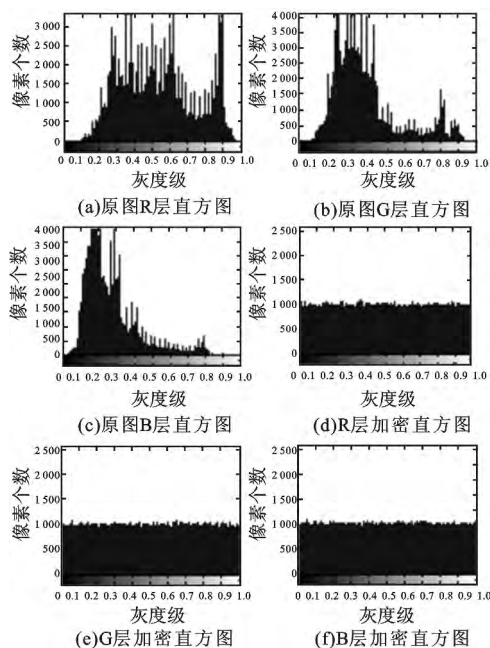


图 5 彩色图像三基色加密前后的直方图

(2) 图像相邻像素相关性分析: 图 6 展示的是 R 层在水平方向、G 层垂直方向和 B 层对角线方向的相邻像素相关性. 通过清晰的对比实验, 首先观察原始图像可以得出, 无论从哪个方向来衡量, 原始图像具有很强的线性关系, 像素在加密系统作用下均匀随机扩散, 打乱了真实图像的结构和特性, 说明系统降低相关性的能力较强, 因此该算法可以有效抵御统计攻击.

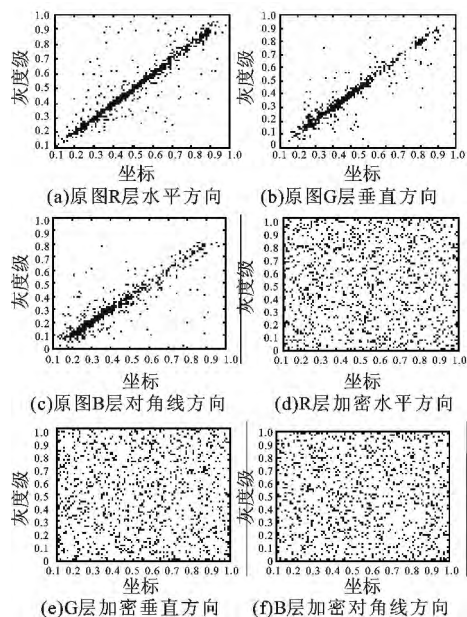


图 6 加密前后的水平、垂直、
对角线方向的相邻像素相关性

由上述实验得出, 相关性分析的实质是研究像素在加密系统作用下的扩散程度, 加密系统通过分散像素的冗余信息而达到削弱相关性的目的, 最终隐蔽明文的统计信息. 实验首先随机选择 2 000 个不同方向的相邻像素对进行测试, 根据相关系数计算公式, 最后结果如表 1 所示. 由表 1 中的数据得知, 原图像在任意方向的相关性都很大, 在加密系统的作用后在极大程度上降低了相关性, 几乎为零.

表 1 不同加密系统下相关系数值比较

相邻方向	原始图像	加密图像	混淆扩散算法	Logistic 彩色图像加密算法
水平	0.940 6	0.007 0	-0.004 8	0.032 4
垂直	0.943 6	0.085 5	0.028 3	-0.057 2
对角线	0.935 7	-0.047 4	-0.022 7	0.010 6

算法生成系统参数 $T_1(n) = O(n)$, 双混沌生成的序列 $T_2(n) = M \times N \times C = O(n_2)$, 像素混淆与扩散 $T_3(n) = 1 + 3 \times k \times (M - 1)(N - 1) \times C \times m + 1 = O(n_2)$, 因此得出最终的时间是 $T(n) = T_1(n) + T_2(n) + T_3(n) = O(n_2)$. 表 2 所示为将本文算法与经典的混淆扩散加密算法和经典的 Logistic 映射系统的彩色图像加密算法的执行时间进行对比. 通过分析得知本文提出的加密算法执行效率较高.

4.2 执行时间分析比较

设加密次数为 k , 本文主要分为三个部分, 因此分别计算它们的时间.

表 2 不同加密系统执行时间比较

算法执行时间	加密图像 Monarch(512×512)		
	改进算法	经典混淆扩散	Logistic 彩色图像加密
生成混沌序列	0.635 58	3.052 871	4.257 920
像素混淆或扩散时间	55.009 93	192.503 862	185.296 643
算法总时间	55.645 51	195.556 733	189.554 563

5 结束语

本文提出了一种基于混沌的混淆与双扩散相结合的图像加密新算法. 首先详细描述了算法具体的执行步骤, 然后针对加密方法的直方图和相邻像素之间的相关性以及执行效率进行分析, 最终得出结论, 该算法符合加密的基本要求, 而且对选择明文攻击的抵御能力较强, 大大提高了执行速度, 实验表明, 本方法安全有效, 基本达到了预期的效果.

(下转第 104 页)

号,提取水印时不需要原始载体图像和原始水印的参与,是一种盲水印算法.仿真实验表明,提出的算法具有较好的透明性和鲁棒性.与采用同样的嵌入方法在彩色图像的 R 分量中嵌入水印相比,提出的算法具有更好的抵抗攻击的性能.

参考文献:

- [1] 邹长华,谭世恒,林土胜.基于混沌置乱和混沌加密的 DCT 域数字水印算法[J].微电子学与计算机,2011,28(5):58-62.
- [2] 熊祥光.基于量化和关系的图像水印算法[J].微电子学与计算机,2013,30(9):71-74.
- [3] 李涛,孙锐,徐彩臣.基于 Contourlet 域伪 3D-DCT 变换的视频水印[J].电子测量与仪器学报,2011,25(8):734-740.
- [4] 刘旺,姜守达,孙圣和.基于三维 DCT 变换的体数据鲁棒数字水印嵌入算法[J].电子学报,2005,33(12):2174-2177.
- [5] 孙克辉,包善琴.小波变换和子采样在彩色图像水印中的应用[J].中南大学学报:自然科学版,2011,42(2):404-408.
- [6] 熊祥光,王力,瞿云云.基于整数小波变换的彩色视

频水印算法[J].微电子学与计算机,2013,30(4):41-45.

- [7] 李晓强,薛向阳.基于多通道的彩色图像水印方案[J].计算机学报,2004,27(9):1238-1244.
- [8] Bami M, Bartolim F, Piva A. Multichannel watermarking of color images[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2002, 12(3): 142-156.
- [9] Hui Y H, Cheng H Y, Wen H H. A video watermarking technique based on pseudo-3-D DCT and quantization index modulation[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(4): 625-637.
- [10] Rao K, Yip R. Discrete cosine transform: algorithms, advantages, applications[M]. Boston: Academic Press Inc., 1990.

作者简介:

熊祥光 男,(1984-),硕士,讲师,CCF 会员(E200022762M).研究方向为数字水印和图像处理. E-mail:xxg0851@163.com.

韦立 男,(1981-),副教授,博士.研究方向为计算复杂性理论,图像处理.

(上接第 99 页)

参考文献:

- [1] 陈国亮,杨凌,张海桥.基于 logistic 混沌序列的彩色图像加密方法[J].甘肃科技,2012,28(14):23-25.
- [2] 郑凡.基于混沌的数字加密应用技术研究[D].吉林:吉林大学,2008.
- [3] 阚兢.基于混沌的数字图像的加密方法研究[D].太原:太原理工大学,2007.
- [4] 李玲,王伟男,李建杰,等.基于 Logistic 映射和超混沌的自适应图像加密算法[J].微电子学与计算机,2012,29(1):42-46.
- [5] 赵怀勋,程甲.基于三维超混沌系统的彩色图像加密算法[J].微电子学与计算机,2010,27(2):72-74.
- [6] Tomas Pevny, Patrick Bas, Jessica Fridrich. Steganalysis by subtractive pixel adjacency matrix[J]. IEEE Transaction on Information Forensics and Security, 2010, 5(2): 215-224.
- [7] Sahar Mazloom, Amir-Masud Eftekhari-Moghadam.

Color Image crypto system using chaotic maps[C]// Computational Intelligence for Multimedia, Signal and Vision Processing (CIMSIVP) Rajasthan, India: IEEE, 2011: 142-147.

- [8] Indrakanti S P, Avadhani P S. Permutation based image encryption technique[J]. International Journal of Computer Applications, 2011, 28(8): 45-47.
- [9] Jamei M K, Enyatifar R, Hassanpour H. Hybrid model of chaotic signal and complete binary tree for image encryption[J]. International Journal of the Physical Sciences, 2011, 6(4): 837-842.

作者简介:

任晓奎 男,(1965-),副教授.研究方向为通信与计算机应用. E-mail:machao198491@163.com.

马超 男,(1984-),硕士研究生.研究方向为通信与计算机应用.