

doi: 10.11830/ISSN.1000-5013.201702020



采用混沌系统的 HIS 彩色图像加密算法

郭献洲, 刘文文, 张相梅

(河北工业大学 理学院, 天津 300401)

摘要: 为了增强对数字彩色图像信息安全的有效保护, 给出一种基于医院信息系统(HIS)的彩色图像加密算法. 首先, 使用混沌序列控制对亮度层的位平面排序; 然后, 对排序后每一个位平面采用改进的置乱算法; 最后, 恢复到像素平面以完成加密. 该算法相比于基于 RGB 系统的加密算法, 减小了时间复杂度, 且不降低加密算法的安全性能. 仿真结果表明: 该算法的密钥空间大、秘钥敏感性强, 对统计分析和剪切攻击具有较好的抵抗能力.

关键词: 图像加密; 混沌系统; 位平面; 医院信息系统; 分块排序

中图分类号: TP 391.41; TP 393 **文献标志码:** A **文章编号:** 1000-5013(2017)02-0241-04

HIS Color Image Encryption Algorithm Using Chaos System

GUO Xianzhou, LIU Wenwen, ZHANG Xiangmei

(School of Science, Hebei University of Technology, Tianjin 300401, China)

Abstract: In order to protect digital color image's safety, one color image encryption algorithm for hospital information system (HIS) space is proposed in this paper. First of all, use chaotic sequence to control the bit-plane of luminance layer, then use the improved scrambling algorithm on each sorted bit-plane, finally, retrieve them into pixel plane. This algorithm has less time complexity compared to the traditional algorithm in RGB space, meanwhile, has good safety performance. The simulating results show that this algorithm has a large space of keys, good key sensitivity, also has ability to resist the statistical analysis and shearing attacks.

Keywords: image encryption; chaos system; bit-plane; hospital information system; block sorting

为了增强对数字彩色图像信息安全的保护, 研究者们提出了一些改进的加密算法, 传统的二维 Arnold 变换被扩展到三维及更高的维度^[1], 新型的三维混沌映射^[2]也被提出用于数字图像的加密算法. 同时, 将数字图像进行分块、扩散, 再配合使用混沌序列构造的混沌网^[3]或仿射变换与 Logistic 混沌映射^[4]的加密算法也具有较好的扩散加密效果. 区别于基于 RGB 系统的彩色图像加密算法, Guo 等^[5]将彩色图像在医院信息系统(hospital information system, HIS)下加密, 针对携带较多视觉信息的亮度层, 采用较其另两层而言安全性能更好但相对复杂的算法, 兼顾了安全性能和算法复杂度上的双重优势. 本文在已经提出的数字图像加密算法^[6-11]的基础上, 给出一种基于 HIS 的彩色图像加密算法.

1 HIS 的彩色图像加密算法

首先, 将 RGB 彩色图像转换到 HIS 系统下; 然后, 对 3 个分量分别完成加密操作; 再将其重新转换

收稿日期: 2017-02-14

通信作者: 郭献洲(1976-), 男, 副教授, 博士, 主要从事应用数学、数学计算的研究. E-mail: xianzhou_guo@hebut.edu.cn.

基金项目: 国家自然科学基金资助项目(11301132, 11171087)

到 RGB 系统下,以完成整体加密.其中,亮度层使用一种基于位平面和混沌序列的分块加密算法,而在色度和饱和度两层采用时间复杂度低的猫映射加密算法.关于猫映射文中不再赘述.

针对亮度层,文中改进的加密算法包括 2 个步骤,即基于位平面排序的像素置换和一种改进的基于混沌序列和位平面分块的像素置乱.

1.1 基于位平面排序的像素置换

为摒弃了时间复杂度高的异或等运算,结合混沌序列,使用对计算机而言时间复杂度较低的排序操作进行像素置换,算法采用以下 5 个步骤.

步骤 1 得到明文图像的尺寸 $N \times N$,通过密钥控制 Chebyshev 映射进入混沌状态,并生成一组混沌序列,去掉其前面若干项后保留 N 项记为 X .

步骤 2 按照值大小将步骤 1 所得 X 进行升序排列,得到另一组序列记为 Y .

步骤 3 将明文像素平面拆分为位平面,按照 $N \times 8N$ 结构拼接后将每一行与 X 的项进行关联,再按照 X 中的各项在 Y 中的对应位置关系,对位平面上各与其相关联的行进行重排序.

步骤 4 选取另一组混沌序列中 $8 \times N$ 项按照步骤 1 到步骤 3 对拼接位平面的各列进行重新排序.

步骤 5 将经过行列重新排序的位平面恢复到像素平面.

1.2 基于混沌序列和位平面分块的像素置乱

置乱算法将经过基于位平面排序的像素置换算法处理的灰度图像拆分为 8 个位平面,配合混沌序列对各平面进行以下 6 个操作.

步骤 1 利用 Logistic 混沌系统生成一组序列,从某项开始选取连续的 4 个值,配合该位平面的第一轮置乱使用.

步骤 2 构造 4 个集合,即 $A=\{x|x \bmod 4=0, x \in \mathbf{N}^+\}, B=\{x|x \bmod 4=1, x \in \mathbf{N}^+\}, C=\{x|x \bmod 4=2, x \in \mathbf{N}^+\}, D=\{x|x \bmod 4=3, x \in \mathbf{N}^+\}$,与后面提出 4 种排序方法一一关联.

步骤 3 将步骤 1 所得 4 个混沌值乘以 256 后,分别判定到 4 个集合中.

步骤 4 将上一轮置乱后的位平面按后面提出的扩散方法分为 4 个等份区域,与步骤 1 所得 4 个混沌值一一关联.

步骤 5 对分块后各位平面上的点进行扩散穿插及排序,方法如后面提出的扩散方法所述.排序时,对位平面上不同区域的点采用不同的方法.该点所处区域在步骤 4 中关联的混沌值,被判决到步骤 2 中的哪一个集合,就对该点使用步骤 2 中与该集合关联的方法进行排序,遍历位平面上的所有点.

步骤 6 从已生成的混沌序列中选取本轮置乱所使用的项之后的 4 个连续项,重复步骤 3 到步骤 5 的过程,直到完成指定迭代次数.

1.2.1 扩散方法 将每一个位平面分别在行和列进行二等分,将会得到 4 个分块,将左上部分的点穿插到整个位平面的奇数行和奇数列;将右上角的部分的点穿插到整个位平面的奇数行和偶数列;将左下角的部分的点穿插到整个位平面的偶数行和奇数列,将右下角部分的点穿插到整个位平面的偶数行和偶数列上,至此,将完成位平面上所有点的一次扩散和穿插.

1.2.2 集合判定方法 将每轮置乱所需的从混沌序列得到的若干值分别乘以 256 后取整,再将其逐个判定到步骤 2 的 4 个集合之一.

1.2.3 排序方法 置乱算法对每轮分块扩散后的点进行不同的重新排序,这里一共设计了 4 种方法:1) 行与列都按照原本的正序排列;2) 行按照原来本的正序排列,列按照原本的倒序排列;3) 行按照原来本的倒序排列,列按照原本的正序排列;4) 行与列都按照原本的倒序排列.

2 实验结果及分析

对色度和饱和度层采用猫映射加密,密钥为迭代次数 30.亮度层采用 HIS 的彩色图像加密算法,对位平面排序使用 Chebyshev 混沌序列,将控制行和列排序的两个序列的初始值和参数分别选择如下: x_0, y_0 均为 0.48, k, v 均为 3.777 777,则记位平面置乱时的迭代次数 $T=90$.在基于混沌序列和位平面分块的像素置乱算法中,用 8 组 Logistic 序列分别控制 8 个位平面的排序,将这 8 个 Logistic 映射的初

始值分别表示为 $x_{1,0}, x_{2,0}, x_{3,0}, x_{4,0}, x_{5,0}, x_{6,0}, x_{7,0}, x_{8,0}$ ；参数变量分别表示为 $\mu_1, \mu_2, \mu_3, \mu_4, \mu_5, \mu_6, \mu_7, \mu_8$ ，各参数选值如表 1 所示. 由此得到加密图像和亮度层加密直方图, 如图 1, 2 所示.

表 1 Logistic 映射的初始值和参数

Tab. 1 Initial value and parameters of Logistic mapping

参数	$x_{1,0}$	$x_{2,0}$	$x_{3,0}$	$x_{4,0}$	$x_{5,0}$	$x_{6,0}$	$x_{7,0}$	$x_{8,0}$
数值	0.700 001	10.700 002	20.700 003	30.700 004	40.700 005	50.700 006	60.700 007	70.700 008
参数	μ_1	μ_2	μ_3	μ_4	μ_5	μ_6	μ_7	μ_8
数值	3.700 001	13.700 002	23.700 003	33.700 004	43.700 005	53.700 006	63.700 007	73.700 008

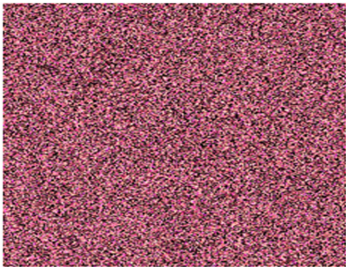


图 1 Lena 加密图像

Fig. 1 Encrypted image of Lena

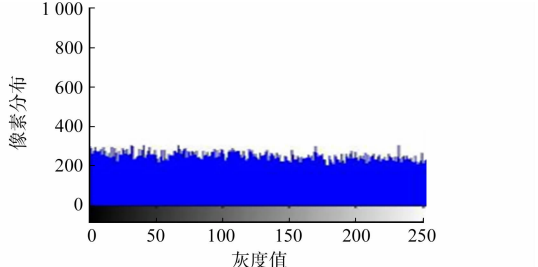


图 2 Lena 加密亮度层直方图

Fig. 2 Histogram of brightness layer of encrypted Lena

2.1 密钥安全性分析

文中算法包含 3 个方面的密钥: 1) 色度和饱和度层使用猫映射变换时, 迭代次数为 2 个整型密钥; 2) 算法 1.1 中两个混沌序列的初始值和参数为 4 个浮点型密钥; 3) 算法 1.2 中使用的 8 个 Logistic 序列初始值和参数及各层的置乱迭代次数 T 为 $2 \times 8 = 16$ 个浮点型和 1 个整型密钥. 混沌序列选择的起始位也可以作为一个整形密钥. 综合以上分析, 文中算法的密钥包括大量的浮点型密钥, 以及较多的整型密钥作为辅助加密, 因此, 认为该加密算法具有较大的密钥空间.

2.2 相邻像素相关性

分别计算加密前后的 RGB 各层的水平相邻、垂直相邻及对称轴相邻像素, 随机选取 1 000 组相邻点, 计算结果如表 2 所示.

表 2 相邻像素相关系数

Tab. 2 Correlation coefficients of adjacent pixels

方向	R 平面原始	R 平面加密	G 平面原始	G 平面加密	B 平面原始	B 平面加密
水平	0.946 8	-0.006 8	0.955 3	-0.021 3	0.910 4	-0.015 0
垂直	0.969 6	0.030 9	0.977 1	-0.006 4	0.935 8	0.029 6
对角线	0.907 4	0.017 0	0.915 2	0.001 5	0.870 7	-0.016 1

由表 2 可知: 该加密算法能较大地降低原始图像相邻像素之间的相关性.

2.3 密钥敏感性

评估亮度层加密算法的密钥敏感性, 对正确密钥加密的各层位平面分别使用表 3 中的错误密钥进行解密; 然后, 将解密位平面与对应的原始位平面进行异或运算以统计不同点的比例, 结果如表 4 所示.

表 3 错误解密乱密钥

Tab. 3 Wrong descramb keys

参数	$x_{8,0}$	μ_7	$x_{6,0}$	μ_5	$x_{4,0}$	μ_3	$x_{2,0}$	μ_1
数值	0.700 007 99	3.700 007 01	0.700 006 01	3.700 004 99	0.700 004 01	3.700 003 01	0.700 002 01	3.700 000 99

表 4 错误解密置乱相差比例

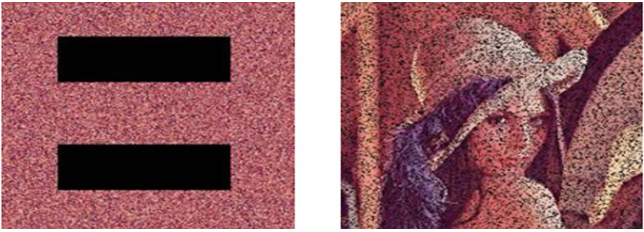
Tab. 4 Difference ratio between right and wrong descramb

位平面	8	7	6	5	4	3	2	1
比例/%	50.13	50.00	50.21	50.16	50.23	50.00	50.35	50.24

结果表明: 在使用该算法时, 只要任意密钥存在微小错误, 解密位平面将会与原本位平面产生较大差别(对于二值图像相差比例达到 50% 属于不相关), 可以认为该置乱算法具有较好的密钥敏感性.

2.4 抗剪切攻击

对遭受剪切攻击的加密图像进行正确解密,结果如图 3 所示. 由图 3 可知:加密图像遭受剪切攻击后,仍能从中恢复出原始图像较多的有用视觉信息,表明文中的加密算法能够较好地抵抗剪切攻击.



(a) 剪切 23%加密图像 (b) 剪切 23%恢复图

图 3 剪切图像及其恢复效果

Fig. 3 Sheared image and recovered result

3 结束语

通过理论分析和实验验证可知:文中算法具有较好的性能,同时,兼顾了降低整体算法的时间复杂度,但由于色度饱和度层所用算法较简单,安全性有一定的折扣,可以考虑配合使用安全性能更好的加密算法.

参考文献:

[1] 刘涛,肖汉. 基于三维 Arnold 变换的数字图像置乱改进算法[J]. 科学技术与工程,2009,9(6):1580-1583.

[2] 刘冰,潘大兵. 新三维混沌映射及其在数字图像信息加密中的应用[J]. 华侨大学学报(自然科学版),2015,36(6):655-658.

[3] 田岩,谢玉波,李涛,等. 一种基于分块和混沌网的图像置乱方法[J]. 中国图象图形学报,2007,12(1):56-60.

[4] 杨雪,于晓洋,邹奇峰,等. 基于仿射模变换的图像分块均匀加密算法[J]. 南京理工大学学报(自然科学版),2010,34(4):441-447.

[5] GUO Qing, LIU Zhengjun, LIU Shutian. Color image encryption by using Arnold and discrete fractional random transforms in IHS space[J]. Optics and Lasers in Engineering,2010,48(12):1174-1181.

[6] FU Chong, LIN Binbin, MIAO Yusheng, et al. A novel chaos-based bit-level permutation scheme for digital image encryption[J]. Optics Communications,2011,284(23):5415-5423.

[7] 鲍芳,李军,李旭. 基于高维广义猫映射的图像加密算法[J]. 西安理工大学学报,2012,28(2):193-197.

[8] ABUTURAB M R. Securing color information using Arnold transform in gyrator transform domain[J]. Optics and Lasers in Engineering,2012,50(5):772-779.

[9] ABUGHARSA A B, BASARI A S B H, ALMANGUSH H. A novel image encryption using an integration technique of blocks rotation based on the magic cube and the AES algorithm[J]. International Journal of Computer Science Issues,2012,9(4):41-46.

[10] LIU Zhengjun, XU Lie, LIU Ting, et al. Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains[J]. Optics Communications,2011,284(1):123-128.

[11] PALLAVI S, ASSOCIATE I, AVADHANI P S. Permutation based image encryption technique[J]. International Journal of Computer Applications,2011,28(8):45-47.

(责任编辑:黄晓楠 英文审校:吴逢铁)