**Computer Science and Application** 计算机科学与应用, 2018, 8(1), 30-34
Published Online January 2018 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2018.81005

Hans汉斯

# Color Digital Image Scrambling Algorithm Based on Linear Transformation

**Wuming Liu, Siting Yu*, Yongshen Zhang, Menglu Lai, Yaojuan Liu**

School of Mathematics and Computational Science, Guilin University of Electronic Technology, Guilin Guangxi
Email: *1250875535@qq.com

Received: Jan. 2nd, 2018; accepted: Jan. 16th, 2018; published: Jan. 25th, 2018

## Abstract

**There are some problems that traditional color digital image scrambling algorithm has: small key space, weak anti-attack and low encryption intensity. In this paper, we present a new algorithm of color digital image scrambling algorithm based on linear transformation. In order to achieve the purpose of pixel scrambling, it randomly generates three matrices, operates with the three *RGB* matrices of the original color digital image, and then it will disrupt the position of the pixel scrambling. The simulation results show that the algorithm can change the gray image features of image, and has the advantages of stability, strong randomness and strong anti-attack.**

## Keywords

**Digital Image, Image Scrambling, Linear Transformation**

# 基于线性变换的彩色数字图像置乱算法

**刘武明，喻思婷*，张永燊，赖梦露，刘瑶娟**

桂林电子科技大学，数学与计算科学学院，广西 桂林
Email: *1250875535@qq.com

收稿日期：2018年1月2日；录用日期：2018年1月16日；发布日期：2018年1月25日

## 摘　要

**针对传统的彩色数字图像置乱算法存在的密钥空间小，抗攻击性弱，加密强度低等问题，本文提出了一种新的基于线性变换的彩色数字图像置乱算法。该算法使用3个随机生成的矩阵与原彩色数字图像的三个RGB矩阵进行运算，既改变了像素值又改变了像素的位置，达到像素置乱的目的。仿真结果表明，该**

*通讯作者。

文章引用: 刘武明, 喻思婷, 张永燊, 赖梦露, 刘瑶娟. 基于线性变换的彩色数字图像置乱算法[J]. 计算机科学与应用, 2018, 8(1): 30-34. DOI: 10.12677/csa.2018.81005

**算法能够改变图像的灰度图像特征，具有稳定性，随机性强，抗攻击性强等优点。**

## 关键词

**数字图像，图像置乱，线性变换**



## 1. 引言

随着信息化发展越来越深入，人们对网络的依赖性越来越强，图像、语音、视频等信息通过网络传播，进而带来的就是这些信息的安全问题，如何解决对图像进行加密，从而保证图像完整且安全的被接收这一问题成为越来越被人们关注的焦点，因此某些具有特殊意义的信息进行加密是一个值得深入研究的课题。对于图像信息的加密而言，置乱技术可以看做图像信息隐藏的基础工作，它通过算法置乱，打乱原图像的像素特征，造成视觉上的混淆，从而使图像原有的信息得到隐藏。

目前，较为熟悉的置乱方法有基于像素位置的置乱算法，该方法是把当前像素位置的影响扩散到后面的像素，而最初的像素位置则由混沌序列来决定，则像素位置置乱效果不仅与加密钥匙有关，而且与图像本身的特性有关，使图像变得杂乱无章，达到增加图像置乱的复杂性。如魔方变换[1]，幻方变换[2]，仿射变换[3]等方法都是基于像素位置的置乱算法。其次是基于像素值改变的置乱算法，该方法又分为低维和高维的置乱变换，如 Arnold 变换[4]，Fibonacci 变换[5]等。其中，基于像素位置改变的置乱算法简单，只是像素位置发生改变，而像素总数，直方图，灰度值并没有发生变化，因此该类算法的安全性相对来说较差。而基于像素值改变的置乱算法较为复杂，该算法并不改变像素的位置和顺序，而是对像素值进行处理，从而达到置乱的目的，它依赖于置乱的次数来达到好的置乱效果，耗时较大。尽管图像置乱算法已有一些研究成果[6] [7] [8] [9]，但还需我们不断更新继续研究。因此，对于这些问题，我们研究了新的彩色数字图像置乱算法。

本文提出了一种基于线性变换的彩色数字图像置乱算法。通过随机矩阵与原数字图像的矩阵进行运算，随机矩阵使得置乱后的图像矩阵具有较大的随机性，这种方法既改变了像素值又改变了像素的位置，置乱效果较好，而且易于实现。通过逆变换矩阵对置乱图像进行还原，由于置乱后的图像矩阵具有较大的随机性，使得秘钥空间非常大。在面对暴力攻击时，还原的可能性微乎其微，因此该算法具有较高的安全性。

## 2. 基于线性变换的图像置乱算法

彩色数字图像可以看作 3 个二维矩阵，即 $R,G,B$ 三个二维矩阵，$RGB$ 各有 256 级亮度，用数字表示为从 0、1、2...直到 255。矩阵元素所在的行和列就是图像显示在计算机上诸像素点的坐标，元素的数值为该图像的 $RGB$ 值。依附图像数字化后得到的三个矩阵，通过改变每个矩阵元素的位置和数值，从而改变了原来的图像，达到了加密的作用，通过逆运算即可解密，从而隐藏了图像的信息。

设数字矩阵

$$R=\left(r_{ij}\right)_{k\times r},\ \left(i=1,2,\cdots,k,\ j=1,2,\cdots,r\right),$$

$$G=\left(g_{ij}\right)_{k\times r},\ \left(i=1,2,\cdots,k,\ j=1,2,\cdots,r\right),$$

$$B=\left(b_{ij}\right)_{k\times r},\ \left(i=1,2,\cdots,k,\ j=1,2,\cdots,r\right),$$

其中 $r_{ij},g_{ij},b_{ij}$ 为对应位置的红色，绿色，蓝色三种原色光的亮度值，每种原色光 256 级亮度，用数字表示为从 0、1、2...直到 255。

$$R'=P_1R \tag{1}$$

$$G'=P_2G \tag{2}$$

$$B'=P_3B \tag{3}$$

其中 $P_1,P_2,P_3$ 中 $p_{ij}\left(i=1,2,\cdots,k,\ j=1,2,\cdots,k\right)$ 是经过生成一个随机可逆矩阵， $P_x=\left(p_{ij}\right)_{k\times k}$ ，$\left(i=1,2,\cdots,k,\ j=1,2,\cdots,k,\ x=1,2,3\right)$， $P_x\neq E$ （$E$ 为单位阵)，依次与 $R=\left(r_{ij}\right)_{k\times r}$， $G=\left(g_{ij}\right)_{k\times r}$， $B=\left(b_{ij}\right)_{k\times r}$ 相乘后得到的对应的置乱矩阵 $R'=\left(r'_{ij}\right)_{k\times r}$， $G'=\left(g'_{ij}\right)_{k\times r}$， $B'=\left(b'_{ij}\right)_{k\times r}$ 对应位置的亮度值。

可知，经过置乱式(1)，(2)，(3)叠加后得到了一个既改变位置又改变原来的值的数字矩阵，误差量 $\Delta$ 将扩散到像素矩阵的每个元素，而且每个元素由三个不同的随机矩阵与对应的 $RGB$ 矩阵运算叠加而成的，每个 $RGB$ 矩阵即使改变微小的变化，但是叠加之后也是发生了巨大的改变，置乱变化对误差具有全局性和扩散性，所以每个微小误差就能导致整个图像的不可恢复，而且密钥是三个随机矩阵，这样密钥空间非常大，用暴力破解几乎不可能，可见该置乱方法具有很高的安全性。

该方法的解密是加密得到的 $R',G',B'$ 通过左乘对应的随机矩阵的逆，即：

$$R=P_1^{-1}R' \tag{4}$$

$$G=P_2^{-1}G' \tag{5}$$

$$B=P_3^{-1}B' \tag{6}$$

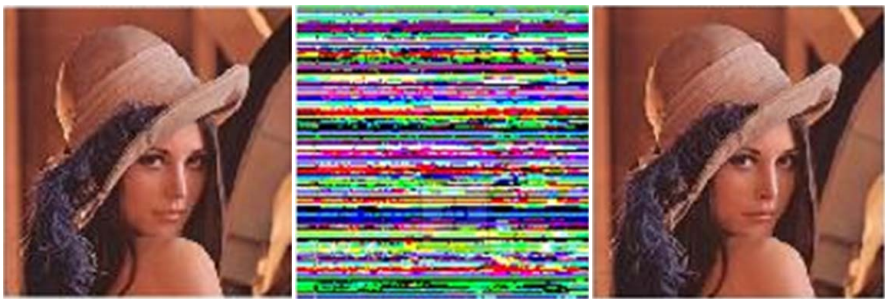
就得到了原来的 $R,G,B$，通过叠加就得到了原来的图像矩阵。

## 3. 仿真实验与分析

算法中用三个随机矩阵做密钥，这样密钥空间大，安全性更强，下面将用三个随机生成矩阵对经典的 Lena 图像进行置乱和还原，效果如图 1 所示：

由图 1 可见该方法置乱后可还原。

下面将分别对比一下图 2 原图像的灰度图和灰度直方图，图 3 加密图像的灰度图和直方图。灰度直方图(histogram)是灰度级的函数，它表示图像中具有每种灰度级的象素的个数，反映图像中每种灰度出现



原图像　　加密后　　解密后

**Figure 1.** Lena image scrambling and reduction map
**图 1.** Lena 图像置乱和还原图

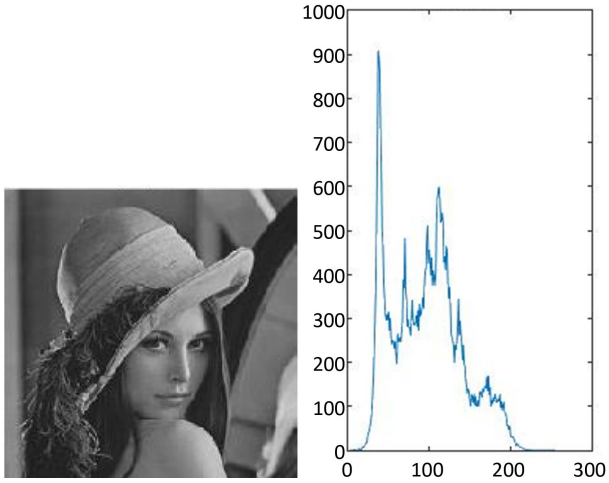



**Figure 2.** The gray and grayscale histograms of the original image
**图 2.** 原图像的灰度图和灰度直方图

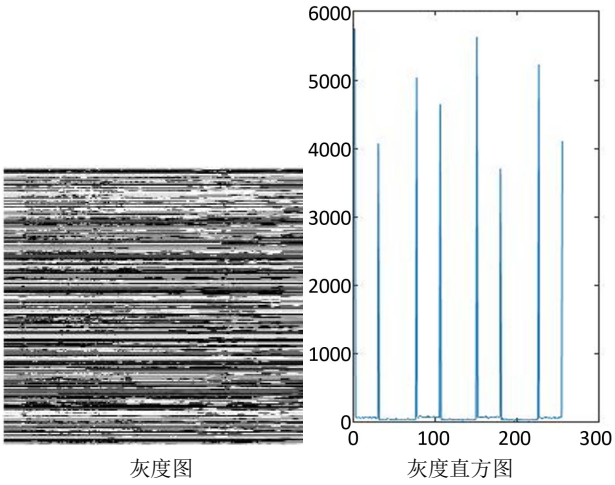



**Figure 3.** The grayscale and histogram of the encrypted image
**图 3.** 加密图像的灰度图和直方图

的频率。灰度直方图的横坐标是灰度级，纵坐标是该灰度级出现的频率，是图像的最基本的统计特征。原图像的灰度值分布较为均匀，而加密后的灰度值峰值起伏较大，而且较为集中，这样证明了置乱的效果，已经改变了像素值，不容易攻击，因为攻击分散在每个像素点，可见该算法的抗攻击性较强。

## 4. 结语

本文提出了一种基于线性变换的彩色数字图像置乱算法。仿真实验结果表明，该算法产生的密钥空间大且随机不受限制，因此，算法在加密解密上的安全性方面比较好，而且在攻击实验中表明，具有较强的抗攻击性，比较适合于在网络上对图像进行加密处理。

## 基金项目

国家自然科学基金项目(11561015; 11761024)，广西自然科学基金项目(2016GXNSFFA380009; 2016GXNSFAA380074; 2017GXNSFBA198082)。

## 参考文献 (References)

[1] 董虎胜, 陆萍, 钟宝江. 基于 Hénnon 映射与模仿变换的图像加密算法[J]. 计算机应用与软件, 2014, 31(5): 291-294.

[2] 王冬梅, 黄琳, 王金荣. 幻方变换加密数字全息图[J]. 浙江工业大学学报, 2007, 35(1): 116-118.

[3] 文昌辞, 王沁, 刘向宏. 基于放射和复合混沌的图像加密新算法[J]. 计算机研究与发展, 2013, 50(2): 319-324.

[4] 龚黎华, 曾绍阳, 周南润. 基于频谱切割和二维 Arnold 变换的彩色图像加密算法[J]. 计算机应用, 2012, 32(9): 2599-2602.

[5] 袁玲, 康宝生. 基于 Logistic 混沌序列和位交换的图像置乱算法[J]. 计算机应用, 2009, 29(10): 2681-2683.

[6] 段雪峰, 关健, 丁勇, 刘云波. 基于多组混沌序列的彩色数字图像置乱算法[J]. 计算机工程,2012, 38(9): 114-120.

[7] 汪太月, 戴燕青. 数字图像置乱算法的研究与比较[J]. 湖北理工学院学报, 2017, 33(4): 425-430.

[8] 郭婷婷, 娄岩, 刘佳, 王艳华. 基于 Rossler 变换的图像置乱算法[J]. 辽宁师范大学学报, 2017, 40(1): 41-46.

[9] 江帆, 吴小天, 孙伟. 基于稀疏矩阵的 Arnold 数字图像加密算法[J]. 计算机应用, 2015, 35(3): 726-731.