

## 基于频谱切割和二维 Arnold 变换的彩色图像加密算法

龚黎华, 曾绍阳, 周南润\*

(南昌大学 电子信息工程系, 南昌 330031)

(\*通信作者电子邮箱 zmr21@163.com)

**摘要:**针对多通道彩色图像加密算法传输负担大的缺陷,提出了基于频谱切割和二维 Arnold 变换的单通道彩色图像加密算法。该算法对原彩色图像的 RGB 分量分别进行不同分数阶次的分数傅里叶变换(FrFT),将各分量所得频谱信息进行切割,组合成一幅新的频谱;再用二维 Arnold 变换对组合频谱进行置乱,使三个分量的频谱信息充分混淆和扩散。密文为一幅灰度图像,在保留原彩色图像主要信息的同时,减小了传输负担。仿真结果与性能分析验证了该算法的加密效果和安全性。

**关键词:**分数傅里叶变换;频谱切割;二维 Arnold 变换;图像加密

**中图分类号:**TN918 **文献标志码:**A

## Color image encryption algorithm based on cutting spectrum and 2D Arnold transform

GONG Li-hua, ZENG Shao-yang, ZHOU Nan-run\*

(Department of Electronic Information Engineering, Nanchang University, Nanchang Jiangxi 330031, China)

**Abstract:** To reduce the heavy transmission burden of multichannel color image encryption algorithms, a single-channel color image encryption algorithm based on cutting spectrum and 2D Arnold transform was presented. In the proposed algorithm, the R, G, B components of the original color image were extracted, and their spectra were obtained separately by the Fractional Fourier Transform (FrFT) of different orders, followed by cutting their spectra to construct a new spectrum, then the combined spectrum was scrambled by the 2D Arnold transform to confuse and diffuse the spectrum information well enough. The encrypted image was a gray image, thus the transmission burden was reduced apparently while the main information of the original color image was kept. The simulation results and performance analyses verify the validity and the security of the encryption algorithm.

**Key words:** Fractional Fourier Transform (FrFT); cutting spectrum; 2D Arnold transform; image encryption

### 0 引言

彩色图像因其生动形象的特点,广泛应用于各行业各领域,因此彩色图像安全性受到越来越多的关注。常见的彩色图像加密方法是多通道彩色图像加密<sup>[1-2]</sup>。多通道加密需要多个光源和多套光学元件,使加密系统变得复杂,在增加实验难度的同时增加了系统的成本,因此单通道彩色图像加密成为彩色图像加密和多图像加密的重要手段和研究方向。杨晓苹等<sup>[3]</sup>提出基于双相位编码的单通道彩色图像加密,图像从 RGB 空间转换到 HIS 空间。I 分量作为相位编码的原始待加密图像,采用双随机相位加密技术对 S 分量加密后得到的相息图,与 H 分量一起构成对 I 分量加密的双相位,以实现彩色图像的单通道加密。多数彩色图像加密算法得到的密文仍然是彩色图像,而传输一幅彩色图像比传输一幅灰度图像往往需要付出更大的代价。

与文本信息不同,数字图像信息允许一定的图像失真度,只要图像失真度被控制在视觉不能觉察到的范围内。鉴于此,人们提出了基于频谱切割的彩色图像加密算法。2000 年 Unnikrishnan 等<sup>[4]</sup>提出基于分数傅里叶变换(Fractional Fourier Transform, FrFT)的双随机相位编码加密,利用 4f 加密系统,把两块统计无关的随机相位模板分别置于光学系统

的输入平面和加密平面,对原始图像信息和分数傅里叶域信息进行随机扰乱,在系统输出面得到平稳白噪声,即密文。此后,由于 FrFT 具有良好的时频特性,基于 FrFT 的图像加密新算法不断涌现<sup>[5-9]</sup>。FrFT 的阶次接近 1 时,图像的分数傅里叶谱的能量主要集中在中心的低频部分,利用这部分频谱信息就能恢复出原图像的主要信息<sup>[10-11]</sup>。本文讨论一种密文为灰度图像的单通道彩色图像加密算法,以减小多通道彩色图像加密算法的传输负担。

### 1 相关基础

Namias 型 FrFT 定义<sup>[10]</sup>为:

$$F^{\alpha}\{f(x)\} = \int_{-\infty}^{\infty} f(x) K_{\alpha}(x, x_{\alpha}) dx \quad (1)$$

其中  $\alpha$  阶 Fourier 变换的核函数  $K_{\alpha}(x, x_{\alpha})$  为:

$$K_{\alpha}(x, x_{\alpha}) = \begin{cases} \sqrt{1 - i \cot \theta_{\alpha}} \exp(i\pi(x_{\alpha}^2 \cot \theta_{\alpha} - 2xx_{\alpha} \csc \theta_{\alpha} + x^2 \cot \theta_{\alpha})), & \alpha \neq 2n \\ \delta(x + x_{\alpha}), & \alpha = 4n + 2 \\ \delta(x - x_{\alpha}), & \alpha = 4n \end{cases} \quad (2)$$

通常图像傅里叶频谱的能量主要集中在中心的低频部分,即可由傅里叶变换的低频部分重建原始图像。当分数阶

收稿日期:2012-03-24;修回日期:2012-05-29。

基金项目:国家自然科学基金资助项目(61141007, 61262084);江西省自然科学基金资助项目(2009GQS0080)。

作者简介:龚黎华(1977-),女,江西吉安人,实验师,硕士,主要研究方向:图像加密;曾绍阳(1989-),男,江西宁都人,主要研究方向:图像加密;周南润(1976-),男,江西吉安人,教授,博士,主要研究方向:网络与信息安全。

接近1时,经过FrFT以后,中间部分的频谱包含了图像的大部分信息,可以基本描述图像,解密时使用一半的频谱即可有效恢复出原始图像<sup>[10-11]</sup>。对FrFT域进行频谱切割,将其高频部分用0代替,再将多个图像的频谱组合成新的频谱,能缩减数据量,提高加密效率。该方法牺牲的图像细节信息在视觉上差异很小。假设函数 $I(x,y)$ 在 $(x,y)$ 内没有零值, $x \in [-L_x, L_x], y \in [-L_y, L_y]$ ,函数 $I(x,y)$ 的二维FrFT为:

$$\psi(u,v) = \text{FrFT}[I(x,y)]; u \in [-L_u, L_u], v \in [-L_v, L_v] \quad (3)$$

其中 $L_u, L_v$ 限制了输出函数 $\psi(u,v)$ 中变量 $u$ 和 $v$ 的幅度。 $\psi(u,v)$ 的频谱切割方程<sup>[12]</sup>为:

$$\psi'(u,v) = \begin{cases} \psi(u,v), & |u| < k_x L_u \text{ 且 } |v| < k_y L_v \\ 0, & \text{其他} \end{cases} \quad (4)$$

其中 $k_x$ 和 $k_y$ 为区间(0,1)内的切割系数。

Arnold变换是一种点的位置移动变换,即单位矩阵内各点唯一地变换到单位矩阵内的另一点。对于数字图像,二维Arnold变换形式<sup>[13]</sup>为:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N; x, y \in \{0, 1, \dots, N\} \quad (5)$$

其中 $N$ 是图像矩阵的大小。数字图像的位置移动是将 $(x,y)$ 处像素对应的灰度值移动至 $(x',y')$ 处。遍历原图像的所有点之后,便产生一幅置乱的新图像。Arnold变换具有周期性,当迭代到某一步时,将重新得到原始图像。对数字图像迭代地使用离散Arnold变换,即将前一次变换输出 $(x',y')$ 作为下一次Arnold变换的输入,直到图像“杂乱无章”,即变成类似噪声的无意义图像,以达到置乱的效果。

## 2 本文的彩色图像加密算法

对于 $N \times N \times 3$ 的彩色图像,加密算法的步骤如下:

1) 提取原始彩色图像的RGB分量。

2) 对RGB分量分别进行FrFT。

$$\begin{cases} F^{\alpha,\beta}[R(x,y)] = R(u,v) \\ F^{\alpha,\beta}[G(x,y)] = G(u,v) \\ F^{\alpha,\beta}[B(x,y)] = B(u,v) \end{cases} \quad (6)$$

3) 按相应的切割系数对RGB三个分量的FrFT频谱进行切割,将切割得到的频谱 $\psi_1, \psi_2$ 和 $\psi_3$ 组合在一起,得到 $N \times N$ 的二维组合频谱图 $\psi$ 。

$$\begin{cases} \psi_1 = R(u,v), & (u,v) \in S_1 \\ \psi_2 = G(u,v), & (u,v) \in S_2 \\ \psi_3 = B(u,v), & (u,v) \in S_3 \end{cases} \quad (7)$$

其中 $S_1, S_2$ 和 $S_3$ 表示相应的切割系数所限制的频谱范围。

4) 利用二维Arnold变换对组合频谱 $\psi$ 进行置乱,即利用式(5)遍历 $\psi$ 的所有点完成一次Arnold置乱,以此类推对每次变换所得结果进行Arnold变换,直到完成所设定的迭代次数。迭代次数可作为密钥。迭代完成后, $\psi$ 被置乱为 $\psi'$ 。

$$\psi' = T[\psi] \quad (8)$$

5) 对 $\psi'$ 进行随机相位编码,与第2)步一起构成双随机相位加密。对于实值的输入图像,双随机相位编码加密过程中真正起作用的是第二块随机相位模板,将第2)步中的相位模板看作相位全0的模板。

$$\psi''(u',v') = F^{\alpha,\beta}[\psi'(u,v) \exp(ip(u,v))] \quad (9)$$

其中 $\psi''(u',v')$ 和 $p(u,v)$ 分别为密文图像和随机相位掩模。

解密过程与加密过程相反,进行随机相位解码后利用二维Arnold变换的周期性恢复出组合频谱,从中提取出RGB三个分量的FrFT频谱,不足部分填充0,再对其进行分数傅里叶逆变换,解密出原始彩色图像的RGB分量,三者的组合就是解密图像。

## 3 仿真与分析

在Matlab平台上对大小为 $512 \times 512$ 的彩色图像Lena进行仿真。第2)步和第5)步中FrFT的 $x$ 和 $y$ 方向上的阶次分别设为 $\alpha = 0.9$ 和 $\beta = 0.5$ ;频谱切割时RGB三个分量的比例为1:1:2;二维Arnold变换的迭代次数设定为200;生成随机相位模板的种子 $seed = 0.55$ 。图1为正确密钥加解密结果,图(d)为将频谱进行随机相位编码后所得的图像(即密文图像);图(e)为随机相位解码后的频谱。图2为错误密钥的解密图像,由图可知,本文算法对各个密钥的敏感性较强,只要其中一个密钥错误,都无法正确解密出原始图像。

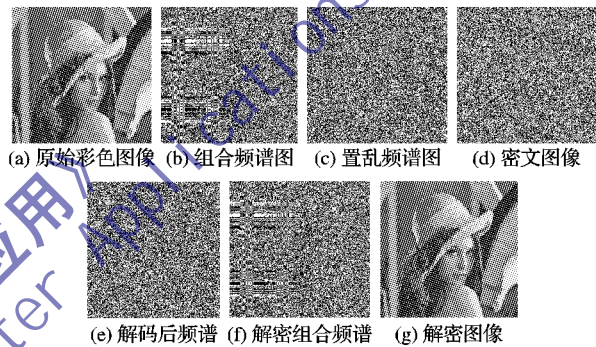


图1 正确密钥解密过程结果

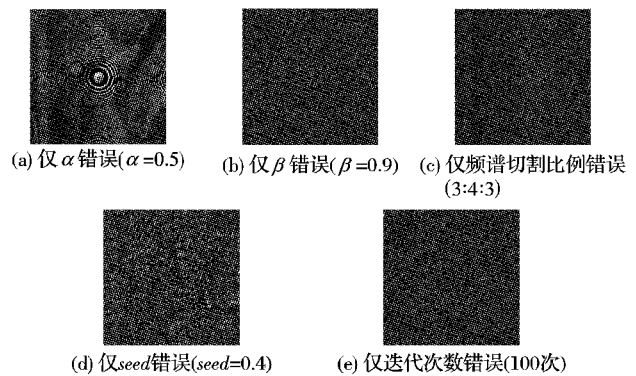


图2 错误密钥的解密图像

为了考察频谱切割比例对系统解密的影响,本文对不同频谱切割比例的解密图像进行分析。

1) 分数阶不都接近于1。

设加密密钥为: $R$ 分量 $x$ 和 $y$ 方向上FrFT的分数阶分别为0.9,0.95; $G$ 分量 $x$ 和 $y$ 方向上FrFT的分数阶分别为0.8,0.85; $B$ 分量 $x$ 和 $y$ 方向上FrFT的分数阶分别为0.7,0.75。不同频谱切割比例下的解密图像如图3所示。对于彩色图像Lena来说,频谱切割的分数阶不都接近于1时, $B$ 分量占的比例较大, $R$ 和 $G$ 分量占的比例较小时,解密图像与原始图像的差异较小,解密效果较好,即 $B$ 分量比 $R$ 和 $G$ 分量来说更加重要。因此,频谱切割时要得到最佳的解密效果应该尽量多地截取 $B$ 分量的频谱,少截取 $R$ 和 $G$ 分量的频谱。不同的彩色图像具有不同的颜色特点,各颜色分量的重要程度也不同,因此应根据原图像的颜色特点进行频谱切割。



2) 分数阶都接近于 1。

选取 RGB 分量在  $x$  和  $y$  方向上 FrFT 的分数阶均为 0.9, 对应不同频谱切割比例的解密结果如图 4 所示。对 Lena 来说, 频谱切割的分数阶都接近于 1 时, 不同频谱切割比例的解密图像与原始图像非常接近, 这表明 3 个分量的重要性是相当的, 可以不考虑频谱切割的比例问题。



图3 分数阶不都接近于 1 时不同频谱切割比例下的解密图像



图4 分数阶都接近于 1 时不同频谱切割比例下的解密图像

算法的主要密钥为 FrFT 阶次和混沌序列的初值  $seed$ 。

1) 分数阶安全性分析。

设分数阶次偏差为  $\delta$ , 图 5 为不同分数阶偏差下的解密图像及其相应的均方误差曲线。由图 5 可知, 当  $\delta = 0.002$  时, 可以较好地解密出原始图像; 当  $\delta$  增大到 0.006 时, 虽然能够解密出图像的主要信息, 但此时彩色图像的颜色已发生严重失真; 当  $\delta$  增加到 0.01 时图像已成为一片混沌, 从解密图像无法得到原彩色图像的任何信息。随着分数阶偏差的增大, 均方误差 (Mean Square Error, MSE) 曲线急剧上升, 解密图像和原图像之间的差异越来越大, 表明分数阶次是敏感的密钥。

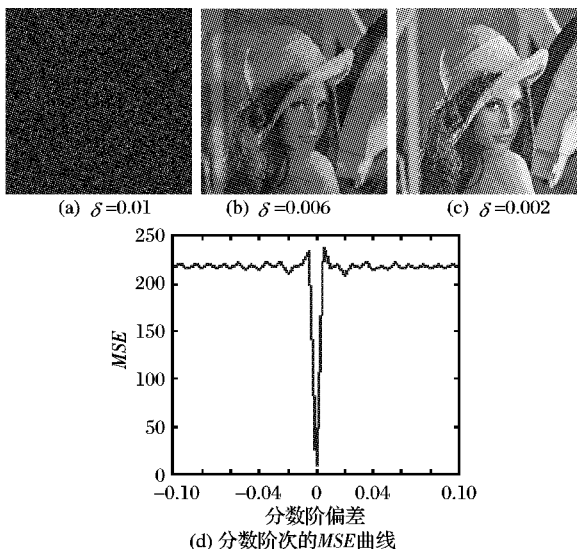


图5 不同分数阶下的解密图像

2)  $seed$  的敏感度分析

选取密钥  $seed = 0.55$ , 其他密钥均正确, 图 6 为当密钥  $seed$  偏差  $10^{-16}$  和  $10^{-17}$  时的解密图像及其相应的均方误差曲线。由图 6 可知, 当密钥  $seed$  偏差  $10^{-17}$  时, 可以解密出原始图像; 当密钥  $seed$  偏差  $10^{-16}$  时, 不能获取原始图像信息; 均方误差曲线的变化十分剧烈, 当发生微小偏差时, 均方误差值急剧增大, 说明  $seed$  为敏感的密钥, 只有当  $|seed - 0.55| < 10^{-16}$  时才能正确解密。

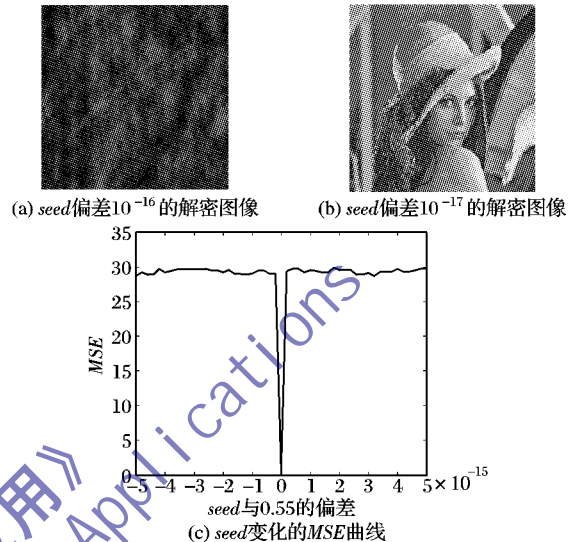


图6 不同  $seed$  下的解密图像

有效的图像加密算法需保证密文图像相邻像素间相关性足够小。在原始图像和密文图像中均随机选择 5000 个像素对, 其水平、垂直以及对角线方向相邻像素对的相关系数的计算公式<sup>[11]</sup>为:

$$C = \frac{\sum_{i=1}^N (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^N (x_i - \bar{x})^2 \sum_{i=1}^N (y_i - \bar{y})^2}} \quad (10)$$

其中:

$$\bar{x} = \frac{1}{N} \sum_{i=1}^N x_i$$

$$\bar{y} = \frac{1}{N} \sum_{i=1}^N y_i$$

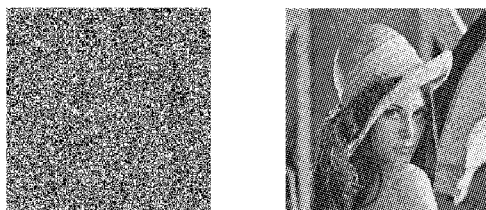
由表 1 可知, 密文图像相邻像素间的相关性要远小于原始图像相邻像素间的相关性, 这表明该图像加密算法能有效地解除原始图像相邻像素的相关性, 即该图像加密算法具有较强的抗统计分析能力。

表1 像素间的相关性

相关系数		原始图像	密文图像
水平相邻像素	R 通道	0.9902	-0.0042
	G 通道	0.9728	
	B 通道	0.9530	
垂直相邻像素	R 通道	0.9926	0.0160
	G 通道	0.9858	
	B 通道	0.9648	
对角线相邻像素	R 通道	0.9819	0.0036
	G 通道	0.9667	
	B 通道	0.9443	

图像在传输中会受到噪声的干扰。图 7 为在密文中加入

强度为5%的高斯白噪声的解密图像。受到噪声污染的密文图像经正确密钥解密后能够恢复原始图像的主要信息,但存在一定的失真,这表明本文算法具有一定的抗噪声能力。



(a) 加密图像加入5%的高斯白噪声 (b) 解密图像

图7 含噪声解密图像

## 4 结语

结合 FrFT 与混沌置乱技术,本文基于频谱切割提出了一种单通道彩色图像加密算法,并对其密钥空间、均方误差、相关性、抗噪声性能等进行了分析。该算法密文为灰度图像,具有多重密钥,可以抵御穷举攻击。仿真结果表明,加密图像相邻像素之间的相关性小,加密算法具有较强的抗统计分析能力、抗裁剪能力和抗噪声性能。

### 参考文献:

- [1] JOSHI M, CHANDRASHAKHER K, SINGH K. Color image encryption and decryption using fractional Fourier transform [J]. Optics Communications, 2007, 279(1): 35-42.
- [2] CHEN LIN-FEI, ZHAO DAO-MU. Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms [J]. Optics Express, 2006, 14(19): 8552-8560.
- [3] 杨晓苹,高丽娟,王晓雷,等.基于双相位编码的单通道彩色图像加密[J].物理学报,2009,58(3):1662-1666.
- [4] UNNIKRISHNAN G, JOSEPH J, SINGH K. Optical encryption by double-random phase encoding in the fractional Fourier domain [J]. Optics Letters, 2000, 25(12): 887-889.
- [5] ZHU BANG-HE, LIU SHU-TIAN. Optical image encryption based on the generalized fractional convolution operation [J]. Optics Communications, 2001, 195(5/6): 371-381.
- [6] TAO RAN, MENG XIANG-YI, WANG YUE. Image encryption with multiorders of fractional [J]. IEEE Transactions on Information Forensics and Security, 2010, 5(4): 734-738.
- [7] ZHOU NAN-RUN, DONG TAI-JI, WU JIAN-HUA. Novel image encryption algorithm based on multiple-parameter discrete fractional random transform [J]. Optics Communications, 2010, 283(15): 3037-3042.
- [8] CHEN LIN-FEI, ZHAO DAO-MU, GE FAN. Gray images embedded in a color image and encrypted with FRFT and Region Shift Encoding methods [J]. Optics Communications, 2010, 283(10): 2043-2049.
- [9] 王雅庆,周尚波.基于分数阶 Fourier 变换的数字图像加密算法研究[J].计算机应用研究,2011,28(7):2738-2741.
- [10] 刘正君.分数阶变换及其在图像加密和滤波中的应用[D].哈尔滨:哈尔滨工业大学,2007.
- [11] 龚黎华.基于混沌映射与 FrFT 的单通道彩色图像加密算法[D].南昌:南昌大学,2011.
- [12] LIU ZHENG-JUN, LI QIU-MING, DAI JING-MIN, et al. A new kind of double image encryption by using a cutting spectrum in the 1-D fractional Fourier transform domains [J]. Optics Communications, 2009, 282(8): 1536-1540.
- [13] 黄仿元.基于 Arnold 变换的图像置乱算法及实现[J].贵州大学学报,2008,25(3):277-278.
- [4] 武汉大学学报:理学版,2011,57(5):444-448.
- [5] 万里红,孙燮华,林旭亮.三维 Hilbert 曲线在图像置乱中的应用[J].计算机工程,2011,37(2):227-229.
- [6] 吕政,唐海萍,陈海虹.基于三维置乱的加密算法及效果分析[J].通信技术,2009,42(4):159-162.
- [7] 农盛功,周满元.基于三维空间的图像加密算法[J].计算机系统应用,2010,19(8):87-91.
- [8] 柏森,曹长修.亚仿射变换的性质及其应用[J].计算机辅助设计与图形学报,2003,15(2):205-208.
- [9] 卢斌,王冰.基于改进亚仿射变换的图像信息隐藏算法[J].计算机工程,2011,37(11):164-167.
- [10] 邹玮刚,洪春勇.一种亚仿射变换的快速构造法及其性质与应用[C]//第十二届全国图像图形学学术会议论文集.北京:清华大学出版社,2005:117-120.
- [11] 柏森,曹长修.图像置乱程度研究[C]//第3届信息隐藏全国学术研讨会论文集.西安:西安电子科技大学出版社,2001:75-81.
- [12] 商艳红,李南,邹建成. Fibonacci 变换及其在数字图像水印中的应用[J].中山大学学报:自然科学版,2004,43(增刊2):148-151.
- [13] 卢振泰,黎罗罗.一种新的衡量图像置乱程度的方法[J].中山大学学报:自然科学版,2005,44(增刊):126-129.
- [14] 李志伟,陈燕梅,张胜元.基于 SNR 的数字图像置乱程度评价方法[J].厦门大学学报:自然科学版,2006,45(4):484-487.
- [15] 顾国生,刘富春.基于混沌映射的图像 Contourlet 编码加密算法[J].计算机应用,2011,31(3):771-774.

(上接第2598页)

$r_{xy}^d = 0.9800$ ,置乱16次后的加密图像的  $r_{xy}^h = 0.0237$ ,  $r_{xy}^v = 0.1259$ ,  $r_{xy}^d = 0.0783$ 。由此可见,明文图像中高度相关的相邻像素,在密文图像中几乎没有相关性。这说明明文图像的统计特性已被扩散到密文中,加密算法具有良好的扩散性。

## 5 结语

通过对三维亚仿射变换的定义与图像排列变换的规律分析,给出了一种三维亚仿射变换的快速构造法,并用实例对三维亚仿射变换的性质和用于图像置乱的周期性进行了研究,首次给出了伪周期和奇异点的概念。三维亚仿射变换用于图像置乱不仅增加了置乱时的密钥参数选择,同时由于变量之间的组合情况非常灵活,提高了图像置乱后的保密性和信息隐藏的抗攻击能力。因此增加了图像信息的安全性,同时具有很好的置乱效果,能很好地隐藏原始图像的信息,对图像的置乱加密有一定的应用研究价值。

### 参考文献:

- [1] 齐东旭,邹建成,韩效宥.一类新的置乱变换及其在图像信息隐藏中的应用[J].中国科学:E辑,2000,30(5):440-447.
- [2] 齐东旭.矩阵变换及其在图像信息隐藏中的应用研究[J].北方工业大学学报,1999,11(1):24-28.
- [3] 吴晏升,王介生,刘慎权.图像的排列变换[J].计算机学报,1998,21(6):514-519.
- [4] 刘婷,闵乐泉.基于 Arnold 变换的图像置乱密码的安全性分析