一种基于混沌和分数阶傅里叶变换的图像加密算法*)

杨 倬[1] 冯久超[1] 方 勇[2]

(华南理工大学电子与信息学院 广州 510641)[1] (上海大学通信与信息工程学院 上海 200072)[2]

摘 要 基于混沌及分数阶傅里叶变换,提出一种对灰度图像的加密算法,并对算法进行仿真实现,结果表明该加密算法加密速度快,效果良好,密钥空间大,具有较强的实用性。

关键词 分数阶傅里叶变换,混沌序列,图像加密

Image Encryption Algorithm Based on Chaos and Fractional Fourier Transform

YANG Zhuo[1] FENG Jiu-chao[1] FANG Yong[2]

(School of Electronic and Information, South China University of Technology, Guangzhou 510641, China) [1]

(School of Communication and Information Engineering, Shanghai University, Shanghai 200072, China)[2]

Abstract Based on chaos and fractional Fourier transform, a gray-image encryption algorithm is proposed and simulated in this paper, the results show that this algorithm is easy to implement with fast speed of encryption, large key space and great practicability.

Keywords Fractional fourier transform, Chaotic sequence, Image encryption

1 引言

随着 Internet 与多媒体技术飞速发展,多媒体通信逐渐成为人们进行信息交流的重要手段,许多信息都需要用图像形式进行传输,图像的信息安全与保密已成为人们关注的焦点。

目前,将混沌序列和现有的加密算法有机结合产生的混沌加密技术被认为是很有前途的加密新算法[1],已有许多基于离散余弦变换(Discrete Cosine Transform, DCT)实现算法。随着分数阶傅里叶变换(Fractional Fourier Transform, FRFT)经 Ozaktas 和 Mendlovics 于 1993 年首次引入到光学系统以来[2],由于它提供了一种新的信号表征方法[3],已受到人们的广泛关注,并在光信息处理和数字信号处理等领域展开了对离散分数阶傅里叶变换(Discrete Fractional Fourier Transform, DFRFT)的研究。

近几年来,人们开始利用混沌及分数阶傅里叶变换的相关特性对图像进行加密方面的研究。何俊发等人[4]分别用积分表达式得到的快速离散分数傅里叶变换算法[5]和基于厄米高斯函数展开的离散分数傅里叶变换算法[6],对图像的 x,y 方向实施不同阶的分数阶傅里叶变换得到了加密图像;然而,当反变换与正变换阶数都接近时,能看到原图像的部分轮廓信息;为此,王银花等人[7]采用了图像空间域混沌置乱和频率域分数阶傅里叶变换,实现图像双重加密,进一步增强了安全性,但是该方法为理论上的研究,离实际应用还有一定的距离。为此,本文提出了一种基于混沌及分数阶傅里叶变换的灰度图像加密算法,并最终形成可传输的彩色加密图像。

2 二维分数阶傅里叶变换

2.1 分数阶傅里叶变换的定义

分数阶傅里叶变换是傅里叶变换的广义形式,它表示信号从时间域到频率域变化过程中信号所呈现的特征[8],即从时间域和频率域同时表示信号旋转 $\pi/2$ 分数倍时的信号特征。设连续信号为 $x(t)$,令 $\alpha=\frac{p\pi}{2}$,则其一维 p 阶分数阶傅里叶变换定义为[9]:

$$X_p(u)=\int_{-\infty}^{+\infty}x(t)K_p(t,u)\mathrm{d}t \tag{1}$$

式中 $p\in(-2,2]$(或 $\alpha\in(-\pi,\pi]$),$K_p(t,u)$ 为 FRFT 的变换核:

$$K_p(u,t)=\begin{cases}\sqrt{\frac{1-j\cot\alpha}{2\pi}}\exp\left(j\frac{u^2+t^2}{2}\cot\alpha-\frac{jut}{\sin\alpha}\right) & \alpha\neq n\pi\\ \delta(t-u) & \alpha=2n\pi\\ \delta(t+u) & \alpha=(2n\pm1)\pi\end{cases} \tag{2}$$

其反变换为:

$$x(t)=\int_{-\infty}^{+\infty}X_p(u)K_{-p}(t,u)\mathrm{d}u \tag{3}$$

2.2 二维离散分数阶傅里叶变换

对一维分数阶傅里叶变换进行推广,可以得到高维的分数阶傅里叶变换。这里简单介绍用于灰度图像加密的二维离散分数阶傅里叶变换。

离散信号 $x(p,q)$ 的二维正向和反向的 DFRFT 计算如下[10]:

$$X_{\alpha,\beta}(m,n)=\sum_{p=0}^{M-1}\sum_{q=0}^{N-1}x(p,q)K_{\alpha,\beta}(p,q,m,n) \tag{4}$$

$$x(p,q)=\sum_{p=0}^{M-1}\sum_{q=0}^{N-1}X_{\alpha,\beta}(m,n)K_{-\alpha,-\beta}(p,q,m,n) \tag{5}$$

因为二维变换核是可分离的,于是有:$K_{\alpha,\beta}=K_\alpha\otimes K_\beta$($\otimes$ 表示张量积),这里 K_α 和 K_β 分别是两个一维 DFRFT 的变换核,α,β 分别为 x 和 y 方向的变换阶数。

*)国家自然科学基金(60572025),教育部基金("新世纪优秀人才"基金:NCET-04-0813),广东省自然科学基金研究项目(04205783,07006496)和上海市重点学科开放基金(T0102)资助项目。杨 倬 硕士研究生;冯久超 教授,博士生导师;方 勇 教授,博士生导师。

3 算法概述

本文的加密算法主要由二维离散分数阶傅里叶变换、混沌置乱和RGB分量映射三个步骤组成，前两个步骤对原始灰度图像进行二次加密，第三个步骤用生成彩色加密图像的方法来存储二次加密图像数据，以实现传输，如图1所示。

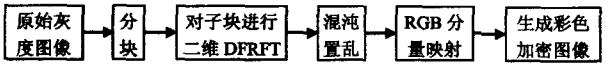


图1 加密算法框架

算法的主要步骤如下。

步骤1 先对原始灰度图像进行分块，然后对每个子块进行二维DFRFT，其中 x 和 y 方向的变换阶数由两个混沌序列控制，其算法主要细节为：

(1)将原图像 I 按一定规格大小(本文取4×4)划分成不重叠的子块 I_k，则 $I=\bigcup I_k$，且 $I_i \bigcap I_j=\Phi(i\neq j)$；

(2)根据混沌映射，产生用于控制 x,y 方向分数傅里叶变换阶数控制序列 $Px=\{px_1,px_2,\cdots\}$，$Py=\{py_1,py_2,\cdots\}$，它们分别由(6)和(7)产生：

$$px_{k+1}=\mu \cdot px_k \cdot (1-px_k) \tag{6}$$

$$py_{k+1}=\mu \cdot py_k \cdot (1-py_k) \tag{7}$$

(3)对各子块进行二维DFRFT，变换后的子块为 I'_k，即 $I'_k=DFRFT_{px_k,py_k}(I_k)$。

步骤2 混沌置乱。对步骤1的结果进行混沌置乱，从而实施双重加密，其算法主要细节为：

(1) 将变换后的各子块 I'_k 重新组合成二维矩阵 M，并将其按行先序转换为一维序列 W，W 的长度为 L；

(2)用Logistic映射产生一个与序列 W 等长的混沌序列 $H=\{h(i)|i=1,2,\cdots,L\}$，对此混沌序列排序，并得到一个新的序列 $H'=\{h(d(i))|i=1,2,\cdots,L\}$；

(3) 根据 H' 对序列 W 进行置乱，其置乱规则如下：

$$W'(i)=W(d(i)) \tag{8}$$

其中 $i=1,2,\cdots,L$。最后将置乱后的一维序列 W' 再转换为一个二维矩阵 N。

步骤3 RGB分量映射。由于上述算法的结果均为复数形式，为了能够应用于实际，将复数实部和虚部按规则映射到彩色图像的RGB分量中，其算法主要细节为：

设经变换并置乱后的矩阵 N 的复数数据为 $N_{(s,t)}=Re_{(s,t)}+i\times Im_{(s,t)}$，其中RGB分量的映射规则为：

(1)分量 R 用于存储实部数据，分离 G 用作存储虚部数据；而分量 B 用作控制标志，B 的每一个元素值都是一个控制字，Fr,Fi 分别是实部虚部的符号标志位，而 Mr,Mi 分别是实部虚部的缩小的倍数，如图1所示。

表1 控制字的定义

8	7	6	5	4	3	2	1
Fr		Mr		Fi		Mi	

(2)置符号标志位，若实部为正，则将 Fr 位置为0，否则置为1；同理，对 Fi 位也作类似的处理。接着判断实部绝对值是否小于255，若是，则把其绝对值直接存入 R 中相应位置，Mr 位置为0；否则，对实部绝对值进行缩小若干倍后的值存入 R 中相应位置，同时将倍数存入 Mr。对虚部也作类似的处理。

(3)重复第二步直到整个加密图像数据处理完，此时，R,G,B 三个矩阵的相同位置上的三个元素组合表示了原灰度图像加密后的数据，即生成了加密后的彩色图像。

接收方通过密钥按加密的逆过程即可解密原灰度图像。

4 算法性能分析

下面我们从三个方面对本算法的性能进行分析，并与文献[7]中的方法进行对比。

(1) 复杂性

本算法依次对原图像数据进行了二维离散分数阶傅里叶变换、混沌置乱和RGB分量映射。由于分数阶傅里叶变换是介于空域与频域之间的变换，故对其变换结果的混沌置乱将使原图像数据分别在空域和频域都得到充分的非线性扰乱。最后的RGB分量映射又使置乱后的数据再次分散到 R,G,B 分量上，因此与文献[7]相比，本算法比单纯的二次加密算法的安全性要好。

(2) 密钥空间

下面从密码学的角度来分析本算法密钥的密钥空间。设算法的密钥为 K，各映射相互独立，则由上文算法描述可知：

$$K=(x_1,\mu_1,x_2,\mu_2,x_3,\mu_3)^T \tag{9}$$

这里 $x_i\in(0,1)$，$\mu_i\in(3.5699,4]$，$(i=1,2,3)$。根据混沌信号对初值的极端敏感性和计算机双精度浮点数的精度(本文取8字节、15位有效数字进行分析)可得：

$$|\{x_i\}|\approx 1.0\times 10^{14} \quad i=1,2,3 \tag{10}$$

其中 $|\cdot|$ 表示势。

设尝试一次破解所需时间的数量级为秒[11]，则仅分析初值分量对密钥空间的影响可得穷举破解所需时间为：

$$\frac{(1.0\times 10^{14})^3}{3.15\times 10^7}=\frac{1.0\times 10^{42}}{3.15\times 10^7}\approx 3.17\times 10^{34}\text{年} \tag{11}$$

故理论上本算法比文献[7]具有更大的密钥空间，其大小主要受双精度浮点数的位精度影响。

(3) 分布特性比较

下面分析加密前后的统计特征，由于分块变换，系数随序列变化，原图空域统计特性被充分掩盖，与简单对全图进行DFRFT相比，安全性更好。原图和彩色加密图亮度分量的直方图，如图2所示。

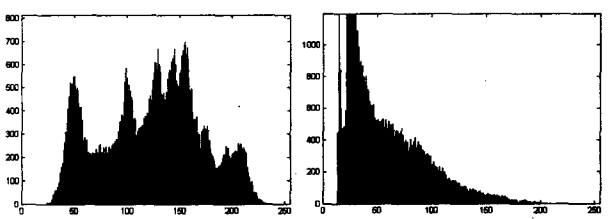


图2 Lenna原图和彩色加密图亮度的直方图

比较两幅直方图可知，图像经加密后，其灰度的真实分布已完全被掩盖，即恶意攻击者无法从直方图来推测图像的大体内容。

5 仿真与分析

本文采用标准测试灰度图像Lenna(256×256)作为仿真图像，对其进行4×4大小的不重叠分块操作，得到64×64个子块，在Matlab7.0平台上进行下列仿真：

(1) 对原图子块进行DFRFT仿真

在该过程中，用于控制 x,y 方向变换阶数的混沌序列的

(下转第274页)

级的软件可靠性参数的经验贝叶斯分布，一方面，有利于减少系统级的测试用例量，实现对一些高可靠性指标的验证；另一方面，在对先验分布的估计时，减小了冒进操作，有利于确保测评结果的可信性。

本文的工作，可以为多模块软件的测评实践提供理论支持。

参 考 文 献

[1] Lyu M R. Handbook of software reliability engineering. McGraw Hill and IEEE Society Press, 1996

[2] Lyu M R. Software reliability engineering: a roadma // Proceeding of 29th Int. conference on software engineering. Minneapolis, 2007: 153-170

[3] 陈火旺，王戟，董威. 高可信软件工程技术. 电子学报，2003，31(12A)：1933-1938

[4] 霍夫迈斯特，王千祥. 实用软件体系结构. 电子工业出版社，2004

[5] Leveson N G. Safetware, system safety and computers. Addison Wesley, 1995

[6] 覃志东，雷航，桑楠，等. 安全关键软件可靠性验证测试方法研究. 航空学报，2005，26(3)：334-339

[7] 覃志东，雷航，桑楠，等. 连续执行软件可靠性验证测试方法. 计算机科学，2005，32(6)：202-205

[8] Littlewood B. A reliability model for systems with Markov structure. Appl. Statist., 1975, 24 (2): 172-177

[9] Smidts C, Sova D. An architectural model for software reliability quantification: sources of data. Reliability Engineering and System Safety, 1999, 64(2): 279-290

[10] Gokhale S S, Trivedi K S. Analytical Models for Architecture-Based Software Reliability Prediction: A Unification Framework. IEEE Transactions on reliability, 2006, 55(4): 578-590

[11] Cheung L, Golubchik L, Medvidovic N, et al. Identifying and addressing uncertainty in architecture-level software reliability modeling // IEEE International parallel and distributed processing symposium. Miami, 2007: 1-6

[12] Jung Hua lo. Software reliability estimation for modular software systems and its applications // The 3rd international conference on information technology: research and education. Hsinchu, 2005: 312-316

[13] Siegrist K. Reliability of systems with Markov transfer of control. IEEE Transactions on software engineering, 1988, 14(7): 1049-1053

(上接第 240 页)

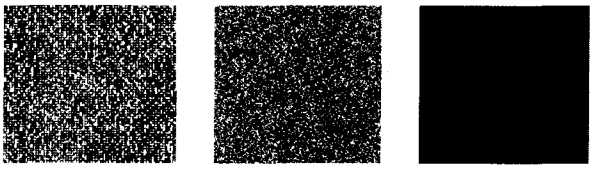
方程及参数我们选用 Logistic 映射来产生两个混沌序列，其仿真参数为 $(x_1, x_2, \mu_1, \mu_2) = (0.3, 0.6, 3.87, 3.95)$，各子块 DFRFT 的 x, y 方向阶数 px, py 由这两混沌序列确定。图 3(a)为分块 DFRFT 后的幅值图像。

(2) 对分块 DFRFT 后的图像进行混沌置乱仿真

再用 Logistic 映射产生一个混沌序列，其仿真参数为：$(x_3, \mu_3) = (0.32, 3.91)$，用来置乱分块 DFRFT 后的图像。图 3(b)为再进行混沌置乱后得到的双重加密图像。

(3) RGB 分量映射存储加密图像数据仿真

双重加密图像的复数数据经 RGB 分量映射存储为一幅混乱的图。此图即可用来传输至接收方。图 3(c)为存储成的加密图像。

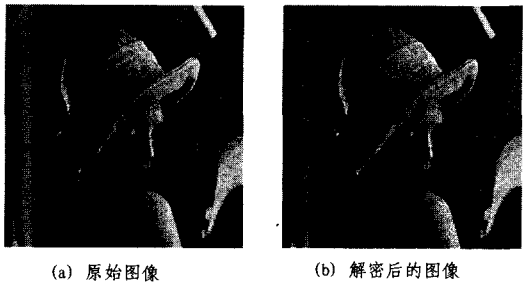


(a) DFRFT 后的幅值图　(b) 混沌置乱后　(c) RGB 分量映射后

(a)DFRFT 后的幅值图　(b)混沌置乱后　(c)RGB 分量映射后

图 3　仿真结果图

(4) 接收方解密出原图仿真



(a) 原始图像　(b) 解密后的图像

图 4　原始图像与解密后的图像

接收方对收到的混乱彩色图进行 RGB 分量逆映射即可得到双重加密图像的数据，然后对其用三个混沌序列的密钥解密得出原灰度图像。图 4(a)，4(b)分别为原始图像与解密后的图像。

结束语　本文利用混沌序列的特性，对灰度图像先进行分块 DFRFT，然后再混沌置乱，实现了图像的双重加密。进一步，为了实现图像的加密传输，故把加密图像数据映射到彩色位图的 R, G, B 分量中，形成一幅混乱的彩色图像，这样可用它来进行传输。计算机仿真结果表明，本算法实现容易，密钥空间大，安全性强，可应用于实际传输中，因而具有了较强的实用性。

参 考 文 献

[1] Nikolaids, Athanasios. Asymptotically optimal detection for additive water-marking in the DCT and DWT domains. IEEE Trans. on Image Processing, 2003, 12(5): 563-571

[2] Mendlovic D, Ozakatas H M. Fractional Fourier transforms and their optical implementation: I. J. Opt. Soc. Am., 1993, A10: 1875-1881

[3] Mendlovic D, Zalevsky Z, Dorsch R G, et al. New signal representation based on the frac-tional Fourier transform. J. Opt. Soc. Am., 1995, A12: 2424-2431

[4] 何俊发，李俊，王红霞，等. 不对称离散分数傅里叶变换实现数字图像的加密变换. 光学技术，2005，31(3)：410-412

[5] Ozaktas H M, Arikan O, Kutay M A, et al. Digital computation of the fractional Fourier transform. IEEE Trans. on Signal Processing, 1996, 44(9): 2141-2150

[6] Candan C, Kutay C A, Ozaktas H M. The discrete fractional Fourier transform. IEEE Trans. on Signal Processing, 2000, 48(5): 1329-1337

[7] 王银花，柴晓冬，周成鹏，等. 基于混沌序列和分数傅里叶变换的图像加密技术. 计算机技术与发展，2006，16(9)：213-215

[8] 于凤芹，姚旭辉，曹家麟. 分数阶傅里叶变换的若干问题. 江南大学学报，2002，1(4)：349-353

[9] 张峰. 基于分数阶 Fourier 变换的 chirp 类数字水印算法研究. 郑州大学硕士学位论文. 2006

[10] 陶然，齐林，王越. 分数阶 Fourier 变换的原理与应用. 北京：清华大学出版社，2004

[11] 张可，王典洪. 基于 Logistic 混沌序列的图像空域复合加密研究. 计算机与现代化，2005(1)：66-69