基于混沌序列和分数傅里叶变换的图像加密技术

王银花[1,2],柴晓冬[1],周成鹏[1],冯兆艳[1],左言胜[1]
(1.安徽大学 计算智能与信号处理教育部重点实验室,安徽 合肥 230039;
2.铜陵学院 电气工程系,安徽 铜陵 244000)

摘 要:采用混沌序列的特性和分数阶傅里叶变换,实现图像双重加密。由密钥生成实数值混沌序列,对数字图像进行空域置乱,然后进行分数傅里叶变换,实现图像的双重加密,只有同时清楚混沌序列和分数阶傅里叶变换阶数才可能对加密图像进行有效解密。计算机模拟表明该方法是有效的,具有很好的加密效果。

关键词:混沌序列;分数傅里叶变换;图像置乱;图像加密
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2006)09-0213-03

An Image Encryption Technology Based on Chaotic Sequences and Fractional Fourier Transform

WANG Yin-hua[1,2],CHAI Xiao-dong[1],ZHOU Cheng-peng[1],FENG Zhao-yan[1],ZUO Yan-sheng[1]
(1.Key Lab.of Intelligent Computing and Signal Processing,Anhui University,Hefei 230039,China;
2.Department of Electrical Engineering,Tongling College,Tongling 244000,China)

Abstract:Presents an image encryption technology based on chaotic sequences and fractional Fourier transform. At first, the real number value chaotic sequences are generated by using the key value, then encrypt the image combining the method of image scrambling in space. Combing it and fractional Fourier transform, multichannel image encryption is implemented. The experimental results show that the technology is valid and has good security.

Key words:chaotic sequences;fractional Fourier transform;image scrambling;image encryption

0 引 言

随着Internet技术与多媒体技术的飞速发展,多媒体通信逐渐成为人们进行信息交流的重要手段,许多重要信息要用数字图像形式进行传输。图像信息的安全与保密便成为人们关注的问题。

文献[1]利用分数阶傅里叶变换,对图像的 x,y 方向实施不同阶的分数傅里叶变换,得到加密图像。然而当 x,y 方向的逆变换级次分别与原变换级次都接近时,能看到原图像的部分信息。文献[2,3]提出对图像空间域置乱变换进行图像加密方法。

文中同时采用图像空间域置乱和频率域分数阶傅里叶变换,实现图像双重加密。只有同时清楚空间域置乱密码和分数阶傅里叶变换密码才可能对加密图像进行有效解密。

收稿日期:2006-03-02
基金项目:国家自然科学基金资助项目(60572129)
作者简介:王银花(1977-),女,安徽巢湖人,硕士研究生,主要从事图像加密与水印技术研究;柴晓冬,博士后,教授,主要从事信号处理、三维显示等领域的研究。

1 混沌序列和图像空间域置乱

1.1 混沌序列特性

混沌序列具有形式简单、对初始条件敏感、具有白噪声的统计特性等特性,可以应用于包括数字通信和多媒体数据安全等众多应用领域的噪声调制,因而能很好地应用于数字图像加密。非线性系统的动力学演化轨迹在一定的控制参数范围内会表现出混沌现象。文中利用混沌的性质设计一种二维置换网络,利用置换网络进行了数字图像加密。

Chebyshev映射是一类非常简单却被广泛研究的动力系统,k 阶Chebyshev映射定义如下:

$$x(n+1)=\cos(k\arccos(x(n))),\ -1\leqslant x(0)\leqslant 1 \quad (1)$$

由该映射产生的序列 $\{x(n)\}$ 在区间[-1,1]上遍历,具有 δ 函数的自相关性和零值互相关性。随着迭代次数的增加,初始相邻点将以指数分离,其混沌轨迹将均匀混合。这些混沌特性使得由Chebyshev映射适合于由密钥控制生成混沌序列,作为密码流用于图像加密的配对选择。

1.2 混沌二维置换网络的设计

密码学中,使用置换来进行数据变换,主要有两种作用:其一是对数据内容作不可预测的替换;其二是改变数

据在数据序列中的位置,即随机换位。对于第二种置换网络也称为置乱网络,文中采用了一种二维混沌置乱方法来应用于图像的加密。置换网络的目的是利用若干步骤的变换,打乱原来元素的位置,使原来有规则的元素分布在多次变换后显现无规则、接近随机的分布,从而起到信息保密的作用。这里将混沌序列引入密码置换网络,利用混沌映射产生序列的非线性以及其轨道点的遍历性,来产生置换网络的双射变换所需地址。

算法原理为:设二维数字图像的矩阵表示为 $\boldsymbol{A}=[a_{i,j}]M\times N$,其中 $a_{i,j}$ 代表图像第 i 行第 j 列像素的灰度值(或 RGB 分量值),对图像采用置换网络的置乱在本质上是原始图像与加密图像之间对应点处灰度值的移动。文中的基本思想是,对加密图像 $\boldsymbol{A}$ 进行行列置乱处理。置换阵列的行地址和列地址由混沌序列产生。

设用户密钥为 $x01,x02$。利用密钥值 $x01,x02$ 采用式(1)生成实数值混沌序 $x1k,x2k$,在该算法中不使用该序列的初始段部分,设起始位置分别为 $n1,n2$。然后由 $x1k$ 和 $x2k$ 分别生成二维置换阵列的行地址和列地址,这里采用两个 Chebyshev 映射产生的序列加 1 成为区间[0,2]间的数,然后乘以 $(M+1)/2$ 和 $(N+1)/2$ 取整来作为置换阵列的行地址和列地址。密钥为 $(x01,x02,n1,n2)$。

1.3 算法的安全性分析

关于密钥的安全性,该算法加密所用的密钥流发生器的密钥为 $(n1,n2,x01,x02)$,其中 $n1$ 和 $n2$ 的取值为正整数;初值 $x01$ 和 $x02$ 可在区间 $[-1,1]$ 取值,因此置乱算法拥有很大的密钥空间。由于混沌系统对初值的敏感依赖性,即使用很接近 $x01$ 或 $x02$ 的数作为初值,其映射轨迹也将因为指数分离而不能正确预测由密钥生成的序列。另外,Chebyshev 映射轨迹还具有零值互相关性,所以在统计意义上由迭代参数 $(n1,x01)$ 得不到另一迭代 $(n2,x02)$ 的信息,符合密钥的安全性要求。

2 数字图像的分数傅里叶变换

2.1 分数傅里叶变换的定义和性质

以一维为例讨论,设输入信号为 $f(x)$,则其 p 阶分数傅里叶变换定义为[4]:

$$f_p(x_p)=C_p\times\exp(j\pi\frac{x_p^2}{\tan\phi})\times\int_{-\infty}^{+\infty}f(x)\times\exp(-j\pi\cdot\frac{x^2}{\tan\phi})\times\exp(-2j\pi\frac{xx_p}{\sin\phi})\mathrm{d}x \tag{2}$$

其中常数

$$C_p=\frac{\exp\{-j[\pi\mathrm{sgn}(\sin\phi)/4-\phi/2]\}}{\sqrt{|\sin\phi|}} \tag{3}$$

$p(0<|p|<2)$ 为分数阶,$\phi=p\cdot\frac{\pi}{2}$。

特别的,当 $p=1$ 时,上式分数傅里叶变换即为普通傅里叶变换。

由此定义可得出分数傅里叶变换的两条重要性质[5]:

1) 可加性:$f_{p1}(f_{p2})=f_{p1+p2}$;

2) 周期性:当 $p1+p2=4n$ 时,$f_{p1+p2}=f$,其中 n 为整数。

2.2 分数傅里叶变换的数值计算

对分数傅里叶变换的定义(2)进行离散化处理,分数傅里叶变换的数值计算可通过下面几个步骤得到[6]:

(1) 初始化。

(2) 由采样定理对输入信号和啁啾信号进行离散化处理得到 $f(n);(-N/2<n<N/2)$,$\exp(i\pi n2\cot\phi)$,其中 N 为总采样数。

(3) 信号 $f(n)$ 乘以啁啾信号 $\exp(i\pi n2\cot\phi)$。

(4) 进行 FFT 运算。

(5) 进行尺度变换,系数为 $\csc\phi$。

(6) 再与同一啁啾信号相乘。

(7) 与常数位相因子相乘。

第(7)步可以略去而不会对理论分析造成影响,因为常数位相因子不改变分数傅里叶变换的分布,只是使位相增加了一个共同的移动。文中算法的结果很容易扩展到二维可分离变量情况。

2.3 数字图像的离散分数傅里叶变换

数字图像的离散分数傅里叶变换是二维的,变换过程可转换为两次一维离散分数傅里叶变换,转换步骤如下:

(1) 对数字图像的行向量进行一维离散分数傅里叶变换,变换阶数为 px,得到变换结果 F_1;

(2) 对 F_1 的列向量进行一维离散分数傅里叶变换,变换阶数为 py,得到变换结果 F_2;

(3) 对 F_2 进行转置,得到的结果就是二维离散分数傅里叶变换结果。

3 图像双重加密技术

图像双重加密即是结合使用图像区域置乱加密和分数傅里叶变换加密。将区域置乱记为 $J_C(\ )$,区域置乱的反变换记为 $J_{-C}(\ )$。设输入图像用 $f(x,y)$ 表示。

首先,对图像进行区域移位变换,得到:

$$J_C\{f(x,y)\} \tag{4}$$

接着,对变换过后的图像进行分数傅里叶变换,可以得到:

$$F(px,py)\{J_C\{f(x,y)\}\} \tag{5}$$

注:px,py 分别为 x,y 方向的分数傅里叶变换阶数。

这样,也就得到最后加密结果为:

$$g(x,y)=F(px,py)\{J_C\{f(x,y)\}\} \tag{6}$$

图像解密的过程也就是加密的反过程。只要对(6)式进行反变换就可以得到原来图像信息,可由下式表示:

$$f(x,y)=J_{-C}\{F(-px,-py)\{g(x,y)\}\} \tag{7}$$

(7)式即为解密输出图。像一次变换都包含 x 和 y 两个方向,即有 px,py 两个变换密钥。另外,双重加密也可以先进行分数傅里叶变换后再进行区域置乱加密,即最后的加密结果为:

$$g'(x,y)=J_C\{F(px,py)\{f'(x,y)\}\} \tag{8}$$

相应的解密过程为:

$$f'(x,y) = J_{-C}\{F(-px,-py)\{g'(x,y)\}\} \quad (9)$$

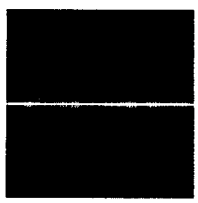
4　计算机模拟

(1)离散分数傅里叶变换实现数字图像的加密变换的计算机模拟。

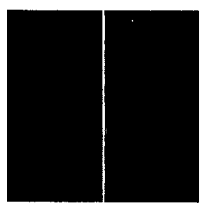
图 1 为 256 灰度级原始图像,256×256 像素。对其实施 $px = 0.1, py = 0.6$ 的不对称分数傅里叶变换。

图 1　原始图像

图 2 为实施不同级次逆变换对原图像进行解码所得结果。各解码参数 px, py 如各图所标示。



(a) px=-0.1, py=-1.6



(b) px=-1.1, py=-0.6

(c) px=-0.12, py=-0.62

(d) px=-0.1, py=-0.6

图 2　不同级次逆变换复原原图像

(2)结合混沌置乱和分数傅里叶变换的图像加密变换的计算机模拟。

图 3 是对图 1 原始图像先用混沌序列进行置乱,然后再进行分数傅里叶变换得到的加密图像。混沌密钥为 $(x01, x02, n1, n2) = (0.4, 0.6, 5, 10)$。分数傅里叶变换阶数密钥 $(px, py) = (0.1, 0.6)$。

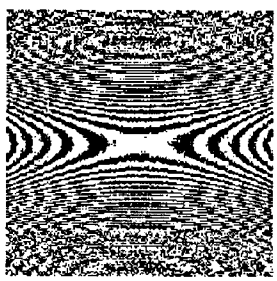
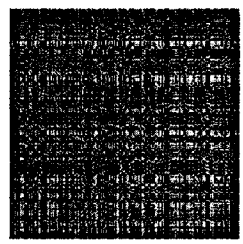


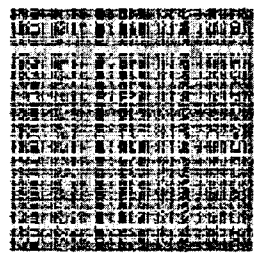
图 3　结合混沌置乱和分数傅里叶变换得到的加密图像

对加密后的图像进行解密,图 4 是密钥不正确时的解密图像,其中图 4(a) 是分数傅里叶变换密钥不正确,分数阶为 $(px = -0.12, py = -0.62)$,置乱反变换密钥正确得到的解密图像;图 4(b) 是分数傅里叶反变换密钥正确,置乱反变换密码不正确得到的解密图像,$(x01, x02, n1, n2) = (0.4001, 0.6001, 5, 10)$。

图 5 是密钥都正确时的解密图像。可见只有同时知道置乱密钥和分数傅里叶变换密钥时才能得到原始图像信息。



(a)置乱反变换密钥正确



(b)分数傅里叶反变换密钥正确

图 4　仅有一个密钥正确时解密后的图像

图 5　密钥都正确时解密后的图像

5　结　论

文中利用混沌序列的特性,对图像空域置乱,然后进行分数傅里叶变换,实现了图像双重加密。因为采用了在空间域与频域都进行变换的双重复合加密,所以就进一步强化了加密图像的安全性。计算机模拟结果表明,该方法有很好的加密/解密效果和安全性。

参考文献:

[1] 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[J].光学技术,2005,31(3):410-412.

[2] 徐耀群,刘　健,秦红磊.平面帐逢映射二进制混沌序列分析[J].哈尔滨商业大学学报(自然科学版),2003,19(1):47-48.

[3] 齐东旭,邹建成.一类新的置乱变换及其在图像信息隐蔽中的应用[J].中国科学(E辑),2000,30(5):440-447.

[4] Ozaktas H M, Mendlovic D. Fractional Fourier optics[J]. J Opt Soc Am,1995,10(12):2522-2531.

[5] McBride A C, Kerr F H. On Namiass's fractional Fourier transform[J]. J Appl Math,1987,15(39):1875-1881.

[6] 刘树田,孙凯霞,任宏武.分数傅立叶变换的数值模拟算法[J].计算物理,1997,14(6):760-764.