文章编号:1001 - 2486(2005)06 - 0067 - 05

基于分数傅立叶变换的图像隐藏技术*

刘　莉,周　朴

(国防科技大学 光电科学与工程学院,湖南 长沙　410073)

摘　要:提出一种利用分数傅立叶变换实现图像隐藏的新方法。将多个不同图像的信息分别经不同阶的分数傅立叶变换后,记录在同一谱平面上,实现了图像的第一重隐藏。通过相位编码后,对谱平面进行另一次分数傅立叶变换,实现图像的第二重隐藏。在解密时,需要特定的分数阶及正确的解码相位才能再现不同的初始图像。提出的新方法用不同的分数阶实现多幅图频谱叠加的互不干扰,用相位编码使得两次的分数傅立叶变换互不干扰,随机设置多重密钥,且每重密钥都极其重要,使得破译的难度提高,因此图像加密的结果更加安全。

关键词:分数傅立叶变换;分数阶;图像隐藏

中图分类号:O438.1　　**文献标识码**:A

The Application of Fractional Fourier Transform in Hiding Images

LIU Li, ZHOU Pu

(College of Photoelectricity Science and Engineering, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: A new method of hiding images based on fractional Fourier transform (FRT) is presented. With this method, the FRT of several images with different fractional orders are recorded on one plate. And another fractional fourier transform accomplishes the hiding after adding the phase encoding. In order to reconstruct the encoded images, several FRT with certain orders and particular phase encoding are needed. That makes the encrypted images more difficult to decrypt even by an authorized person.

Key words: fractional Fourier transform (FRT); fractional order; hiding image

1993 年,Lohman 利用 Wigner 相空间旋转的概念定义了分数傅立叶变换,并给出了分数傅立叶变换的积分形式及基本性质[1]。由于分数傅立叶变换在保留傅立叶变换的原有性质和特点的基础上,又将其分数阶作为一个新的自由度,从而可获得许多新的应用。1995 年,Philippe Refregier and Bahram Javidi 提出了利用随机相位编码进行光学加密的理论[2]。由此,相位编码成为图像加密的关键因素,随之出现了双相位编码应用于光学加密[3]。在国内,基于分数傅立叶变换的光学图像隐藏多以光学实现的形式出现[4~9],随着分数傅立叶算法的不断改进以及计算机硬件、软件的更新换代,使得我们可以在计算机上将分数傅立叶变换的算法应用于图像信息的隐藏与再现。

1　利用分数傅立叶变换实现图像隐藏和再现

1.1　分数傅立叶变换的定义及与本算法相关的基本性质[10]

一维函数的分数傅立叶变换定义如下(将自变量改为二维矢量就可以直接推广到二维情况):

$$G(\zeta) = F_\alpha\{g(x)\} = \left\{\frac{\exp\left[-\mathrm{j}\left(\frac{\pi}{2}-\alpha\right)\right]}{2\pi\sin\alpha}\right\}^{1/2} \cdot \int_{-\infty}^{\infty} \exp\left[\frac{\mathrm{j}(\zeta^2+x^2)}{2\tan\alpha} - \frac{\mathrm{j}\zeta x}{\sin\alpha}\right] g(x)\,\mathrm{d}x \tag{1}$$

式中,$G(\zeta)$称为 $g(x)$的分数傅立叶谱,α 称为分数傅立叶变换的阶,可为任意实数,$F_{-\alpha}$ 是 F_α 的逆变换。当 $\alpha = \pi/2$ 和 $\alpha = -\pi/2$ 时,它转化为常规傅立叶变换,也就是说常规傅立叶变换是分数傅立叶

* 收稿日期:2005 - 09 - 30
基金项目:国家部委基金资助项目
作者简介:刘莉(1980—),女,博士生。

变换的特殊情况。

分数傅立叶变换是线性变换,即有

$$F_\alpha\{Ag(x)+Bh(x)\}=AF_\alpha\{g(x)\}+BF_\alpha\{h(x)\} \tag{2}$$

α 阶和 β 阶变换依次作用的结果相当于($\alpha+\beta$)阶的一次变换,即

$$F_\alpha\{F_\beta\{g(x)\}\}=F_\alpha F_\beta\{g(x)\}=F_{\alpha+\beta}\{g(x)\} \tag{3}$$

因为变换关于 α 具有周期性,周期为 2π,所以

$$F_{2n\pi}\{g(x)\}=g(\zeta),\quad F_{(2n+1)\pi}\{g(x)\}=g(-\zeta),\quad F_{2n\pi+\alpha}\{g(x)\}=F_\alpha\{g(x)\}$$

α 和 P 的关系为 $\alpha=P\pi/2$,因此 α 阶广义傅立叶变换还可表为 $F^{(P)}\{g(x)\}$,其主值区间为 $\alpha\in(-\pi,\pi]$ 或 $P\in(-2,2]$。

例如,当 $P=P_1+P_2=0$ 时,$F^{(0)}\{g(x)\}=F_0\{g(x)\}=g(\zeta)$,即 0 阶分数傅立叶变换给出函数本身,也就是说对当对原像进行分数傅立叶分数阶 $P_2=-P_1$ 的逆变换时,再现原像;

当 $P=P_1+P_2=2$ 时,$F^{(2)}\{g(x)\}=F_\pi\{g(x)\}=g(-\zeta)$,即 π 阶分数傅立叶变换则给出它的倒像;

当 $P=P_1+P_2=4$ 时,$F^{(4)}\{g(x)\}=F_{2\pi}\{g(x)\}=g(\zeta)$,即经周期 2π 后又重现原像。

1.2 信息隐藏的图像处理流程

该方法把分数阶作为一个约束条件和保密的自由度,用不同的分数阶实现多幅图频谱叠加的互不干扰,把相位编码也作为加密的条件,使两次的分数傅立叶变换之间也不互相干扰。具体过程为:将多个不同图像的信息分别经不同阶的分数傅立叶变换后,记录在同一谱平面上,加入相位编码后,再进行下一次分数傅立叶变换,从而实现多幅图像的多重隐藏。在解密时,需要特定的分数阶及正确的解码相位才能再现不同的初始图像。信息隐藏的图像处理流程如图 1 所示。

设 A、B、C 为三幅待隐藏的图像,a、b、c 为解密得到的三幅图像,虽然解密图像含有噪声,但基本能看到图像的基本信息。

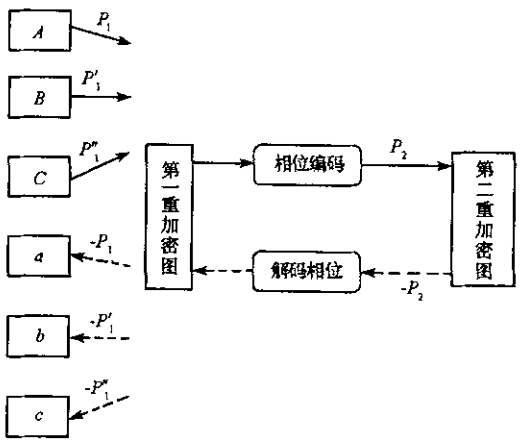


图 1 基于分数傅立叶变换的信息隐藏流程

Fig.1 The flow chart of hiding information based on fractional Fourier transform

1.3 图像隐藏过程

本文分以下两个步骤在频谱面隐藏图像信息。

1.3.1 第一重隐藏

以两幅图为例,设待加密的图像分别为 $f_1(x,y)$ 和 $f_2(x,y)$。对物函数 $f_1(x,y)$ 作分数阶为 P_1 的分数傅立叶变换,得到其分数傅立叶变换频谱 $F_1{}^{P_1}(U,V)$,或称 P_1 阶分数域谱。同样,对另一物函数 $f_2(x,y)$ 进行分数阶为 P'_1 的分数傅立叶变换,得到其分数域谱 $F_2{}^{P'_1}(U,V)$。之后将 $F_1{}^{P_1}(U,V)$ 和 $F_1{}^{P'_1}(U,V)$ 进行相干叠加,得到一个新的分数域谱 $F(U,V)$,其数学表达式为

$$F(U,V) = F_1^{P_1}(U,V) + F_1^{P'_1}(U,V) \tag{4}$$

1.3.2　**第二重隐藏**

加入相位编码 $M_1(U,V) = \exp[\mathrm{j}b(U,V)]$ 之后,再进行一次 P_2 阶分数傅立叶变换,其数学表达式为

$$F^{p_2}\{\exp[\mathrm{j}b(U,V)]F(U,V)\} \tag{5}$$

1.4　图像再现过程

图像再现过程即为加密过程的逆过程,亦分为两个步骤。

1.4.1　**第一重解密**

再现图像的分数傅立叶变换的分数阶必须与加密时的分数阶匹配,方可再现出原始的图像信息,这里最简单的情况为分数阶之和为 0 的情况。

为了恢复初始图像 $f(x,y)$,保密图像需要先进行级次为 $K_2 = -P_2$ 的分数傅立叶变换,然后用解码相位 $M_2 = \exp[-\mathrm{j}b(U,V)]$ 滤波,数学上可表示为

$$F^{-P_2}\{F^{p_2}\{\exp[\mathrm{j}b(U,V)]F(U,V)\}\}\exp[-\mathrm{j}b(U,V)] = F(U,V) \tag{6}$$

1.4.2　**第二重解密**

作分数阶为 $K_1 = -P_1$ 的分数傅立叶变换,得到含有噪声 $F_2^{-P_1}[F_2^{P'_1}(U,V)]$ 的物函数 $f'_1(x,y)$,即:

$$f'_1(x,y) = F_1^{-P_1}[F_1^{P_1}(U,V)] + F_2^{-P_1}[F_2^{P'_1}(U,V)] = f_1(x,y) + F_2^{-P_1}[F_2^{P'_1}(U,V)] \tag{7}$$

作分数阶为 $K'_1 = -P'_1$ 的分数傅立叶变换,则得到含有噪声 $F_1^{-P'_1}[F_1^{P_1}(U,V)]$ 的物函数 $f'_2(x,y)$,即:

$$f'_2(x,y) = F_1^{-P'_1}[F_1^{P_1}(U,V)] + F_2^{-P'_1}[F_1^{P'_1}(U,V)] = F_1^{-P'_1}[F_1^{P_1}(U,V)] + f_2(x,y) \tag{8}$$

对多幅图进行加密隐藏,每幅解密图虽然都会受到由其它图引起的噪声干扰,但基本上可以看出图像的基本特征,由此达到了图像隐藏的目的。如果被加密隐藏的仅是幅单图,那么其解密图像就没有噪声干扰,重现像将是非常清晰的。

在这种方法中,将两个不同的图像分别经不同阶的分数傅立叶变换后,记录在同一谱平面上,它需要两个特定的分数傅立叶变换才能再现出所记录的原始图像信息,即再现像分别与隐藏图像时所选的分数傅立叶变换的阶数有关,即分数阶 P_1、P'_1、P_2 具有加密作用。此外,随机相位编码 $M_1(U,V)$ 也成为图像加密的重要参数。

2　计算机模拟

为了检验本文基于分数傅立叶变换的图像隐藏的有效性,我们用 Matlab 语言编程对两幅像元的灰度图进行了隐藏与再现的计算机模拟实验。

2.1　图像加密实验

图 2(a)、(b)为待隐藏的灰度图。先对图像 2(a)进行分数级次为 $P_1 = 0.1$ 的第一次分数傅立叶变换,对图像 2(b)进行分数级次为 $P'_1 = 0.6$ 的第一次分数傅立叶变换,并记录在同一谱平面上,再加入由计算机随机函数产生的随机相位编码 M_1,又经过 $P_2 = 0.2$ 的第二次分数傅立叶变换,完成二重加密图像如图 2(c)。


a.原始图像1


b.原始图像2


c.加密后的图像

图2 图像的加密

Fig.2 The original image and the encrypted image

2.2 解密及解密噪声

当分数阶匹配、解码相位正确时，可得到正确解密的图像，即当 M_2 正确，分数阶 $K_2 = -P_2 = -0.2$，$K_1 = -P_1 = -0.1$ 时，得出解密图像3(a)；当分数阶 $K_2 = -P_2 = -0.2$，$K'_1 = -P'_1 = -0.6$ 时，得出另一幅解密图像3(b)。

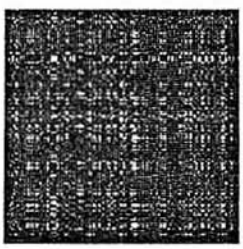

a.解密图像1

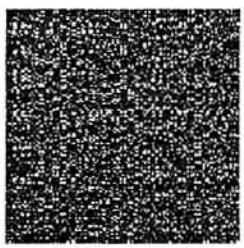

b.解密图像2

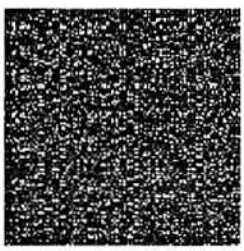
图3 图像的正确解密

Fig.3 Decrypted image with the right keys

在分数阶密钥 K_1 或 K'_1、K_2、解码相位密钥 M_2 中，只要有一个错误，就无法获得正确的解密图像。图4(a)，(a′)为与 K_1，K'_1 有0.01偏差，其它密钥正确的解密结果；图4(b)，(b′)为与 K_2 有0.01偏差，其它密钥正确的解密结果；图4(c)，(c′)为分数阶密钥正确，解码相位密钥错误时的解密结果。从图4可以看出，在这三重密钥中，即使密钥参数与正确密钥参数之间仅有一个小小的偏差，也无法获得正确的解密结果，因而有着极强的安全性。

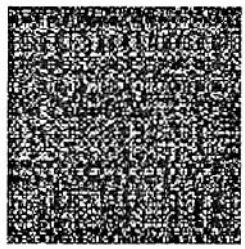

a. K_1 错误，K_2、M_2 正确


a′. K'_1 错误，K_2、M_2 正确


b. K_2 错误，K_1、M_2 正确


b′. K_2 错误，K'_1、M_2 正确

c. M_2 错误,K_1、K_2 正确



c′. M_2 错误,K'_1、K_2 正确

图 4　错误解密的结果

Fig.4　Decrypted image with a wrong key

各种情况下的解密结果可以用表 1 说明。

表 1　图像在分数阶密钥、解码相位密钥取不同值时的解密情况

Tab.1　The different Decrypted images with different keys

	3(a)	4(a)	4(b)	4(c)	3(b)	4(a′)	4(b′)	4(c′)
K_1	√	×	√	√				
K'_1					√	×	√	√
K_2	√	√	×	√	√	√	×	√
M_2	√	√	√	×	√	√	√	×

3　结束语

本文以分数傅立叶变换的理论为基础,提出了基于分数傅立叶变换结合相位编码对多幅图像进行多重加密解密的方法,并用计算机模拟的方法进行了验证。

研究结果表明,采用分数傅立叶变换同时配合相位编码的图像隐藏,具有多重密钥,即分数级次密钥 $K_1 = -P_1$ 或 $K_1 = -P'_1$、$K_2 = -P_2$ 和解码相位密钥 M_2。虽然分数阶密钥具有周期性,其主值区间为(-2,2],但由于密钥的精密性,即使是很小的偏差都无法正确解密。在又多了两重密钥并添加了相位密钥的情况下,这无疑将使图像加密的结果更加安全,就算了解此加密原理,破译的概率也很小。

本文仅对灰度图像进行了处理,对真彩色图像亦可作类似处理。虽然取得了初步进展,但还有不足之处:文中所采用的方法对图像的恢复不可避免地存在噪声,但图像的基本特征已可见,不影响识别原物,若要得到更加清晰的图像,则需对恢复的图像进行去噪处理,如何获得较满意的去噪图像,尚在进一步的研究当中。

参 考 文 献:

[1] Lohmann A W. Image Rotation, Wingner Rotation, and the Fractional Fourier Transform[J]. Opt.Soc.Am.(A),1993,10(10):2181 - 2186.

[2] Refregier P,Javidi B. Optical Image Encryption Based on Input Plane and Fourier Plane Random Encoding[J]. Opt.Lett.,1995,20(7):767 - 769.

[3] Unnikrishnan G,Singh K. Double Random Fractional Fourier-domain Encoding for Optical Security[J].Opt. Eng.,2000,39(11):2835 - 3859.

[4] 谢世伟,等.分数傅立叶变换计算全息图[J].中国激光,2003,30(5).

[5] 曾阳素,等.双重分数傅立叶变换计算全息[J].光学学报,2003,23(2).

[6] 曾阳素,等.二次曝光分数傅立叶变换全息图[J].激光技术,2002,26(1).

[7] 曾阳素,等.多重分数傅立叶变换全息防伪术[J].中国激光,2002,A29(8).

[8] 于力,朱邦和,刘树田.用于光学图像加密的分数傅立叶变换双相位编码[J].光子学报,2001,30(7).

[9] 虞祖良,金国藩.计算机制全息图[M].北京:清华大学出版社,1984.

[10] 宋菲君,Jutamulia S.近代光学信息处理[M].北京:北京大学出版社,1998.