分类号 0438.1　　学号 02072003
UDC　　密级

工学硕士学位论文

基于分数傅立叶变换的光学加密防伪技术

硕士生 姓名　刘　莉
学 科 专 业　光 学 工 程
研 究 方 向　光电对抗与光电信息处理
指 导 教 师　谭 吉 春　教 授

国防科学技术大学研究生院
二〇〇四年十一月

THE OPTICAL ENCRYPTION TECHNOLOGY BASED ON FRACTIONAL FOURIER TRANSFORM

A Dissertation Submitted for

MASTER'S DEGREE OF SCIENCE

by

LIULI

Under the Supervision of Professor

JICHUN TAN

GRADUATE SCHOOL OF NATIONAL UNIVERSITY

OF DEFENSE TECHNOLOGY

November 2004

独 创 性 声 明

本人声明所呈交的学位论文是我本人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表和撰写过的研究成果，也不包含为获得国防科学技术大学或其它教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

学位论文题目：基于分数傅立叶变换的光学加密防伪技术

学位论文作者签名：刘莉　　日期：2004 年 12月 1 日

学位论文版权使用授权书

本人完全了解国防科学技术大学有关保留、使用学位论文的规定。本人授权国防科学技术大学可以保留并向国家有关部门或机构送交论文的复印件和电子文档，允许论文被查阅和借阅；可以将学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。

（保密学位论文在解密后适用本授权书。）

学位论文题目：基于分数傅立叶变换的光学加密防伪技术

学位论文作者签名：刘莉　　日期：2004 年 12月 1 日

作者指导教师签名：谭吉春　　日期：2004 年 12 月 1 日

目 录

图表目录

摘　要

光学信息处理具有容量大、速度快、并行性及装置简单等优点，并且信息可以被隐藏在诸如相位或空间频率等多种参数中，因此利用光学信息处理对光学图像进行安全加密是一种行之有效的方法。

本文将傅立叶变换系统扩展到分数傅立叶变换系统，提出一种利用分数傅立叶变换实现多幅图像多重加密隐藏的方法。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。本文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。最后，用计算机模拟实验进行了验证。

本文提出的基于分数傅立叶变换结合相位编码的技术，可实现多幅图像的多重隐藏，在防伪及安全认证方面具有应用前景。

关键词：光学图像加密　分数傅立叶变换　随机相位编码　信息安全　防伪

ABSTRACT

Optical information processing(OIP) combines the characteristic of having large-capability, high-speed, parallelism and configuration. The most important thing is that the information can be hided in many parameter such as phase、spatial frequency. So it is an effective method of optical image security.

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. However, with the additional degrees of freedom provided by the fractional Fourier transform, the numbers of security keys can be increased. That makes the encrypted images more difficult to be decrypted even by an authorized person. The validity and feasibility of this method is proved though computer simulation.

The research product has wide application and prospect in optical encryption and security verification.

Key words: Optical image encryption; fractional Fourier transform (FRT); Random phase encryption technique; information security; anti-counterfeiting.

第一章 绪论

本文研究基于分数傅立叶变换结合相位编码原理，实现多幅图像、多重隐藏的光学加密技术，探索这种新技术在防伪及安全认证方面的应用。

§1.1 研究背景和意义

1.1.1 光学加密技术的研究背景

自水印和凹板印刷问世以来，防伪、加密以及检验领域的发展经历了很长时间。最早的防伪对象是货币，采用的方法如暗线、水印、光照引起的内容改变等。70年代末80年代初，国际上出现了用于商品的激光全息防伪技术，而且迅速发展和普及。这种防伪技术成本继续下降，每张防伪用的小全息图只有几分钱。但由于图像的可见性和图像处理技术的发展，这种全息图很容易通过照相或CCD相机摄取，并重新产生全息图[1]，因此信用卡、护照、纸币及商标的伪造已变得越发容易，这给一些银行、企业及消费者带来了很大的经济损失。

从90年代初期开始，发达国家便非常重视防伪技术的开发利用以保护本国知识产权和高附加值产品，在短短几年里，光学加密防伪技术迅猛发展。国际光学工程学会(SPIE)已连续多年举办光学防伪技术座谈会，美国国家基金会(NSF)、美国国防部高级研究计划局(DARPA)和美国空军(USAF)也多次联合举行专题研讨会，讨论光学在安全、加密和防伪中的作用，向政府和财团对这一领域的投资提供指导。

1.1.2 光学技术在信息安全中应用

近几年来利用光学信息处理进行图像加密(Optical Image Encryption)越来越引起人们的关注。光学技术与传统的计算机和电子系统相比，提供了两个固有的优点:(1)光学系统具有“本征”的并行数据处理能力，也就是信息的快速变换能力；(2)信息可以被隐藏在多种参数中，诸如相位或空间频率，也就是光学系统有优良的编码容量。鉴于上述原因，光学信息处理应用于信息安全得到了广泛的研究和应用。

§1.2 光学图像加密技术的研究现状与发展趋势

据文献报道，国内外已发展和研究成功多种新型光学加密技术，并投入使用[2-6]。其中，加密码全息标识比较成熟，它指的是在原有全息标识图像版面上的某个部分或整个版面置

人密码,密码以一些特殊函数的变换谱或光学现象为物理模型,最后以光学图案形式显现出来。给全息图置入密码,即使是同行也难以伪造,从而极大地增强了全息标识的抗伪造性能。主要有:计算全息加密、菲涅尔加密点阵全息、散斑全息加密防伪、幻纹(莫尔条纹)全息加密防伪以及最近几年才出现的分数傅立叶变换全息加密防伪等。

以下侧重分析与本文相关的分数傅立叶变换加密和随机相位加密技术的发展动态。

1.2.1 分数傅立叶加密原理及其应用

郭永康等[6-9]人提出利用光波经分数傅立叶变换后在分数域上的场分布与分数级有关的性质,可以记录一种既包含物体信息又包含有系统参量信息的分数傅立叶变换全息图。分数傅立叶变换全息图(Fractional Fourier Transform Hologram,简称 FRTH)是利用物光波经分数傅立叶变换后的光波与参考光波干涉所形成的干涉图样,即分数傅立叶变换全息图记录的是物光波经特定阶分数傅立叶变换的波前。因此,FRTH 既记录有物光波的信息,又记录有分数傅立叶变换系统的信息。为了利用 FRTH 再现原物体的像,用原参考光照明全息图后,还须使全息图再现的波前再经过一个与原记录系统的变换阶相匹配的另一分数傅立叶变换系统后才能成像。

本文第三章中将借鉴上述理论,用计算机软件实现了多幅图像的加密和解密。

1.2.2 随机相位加密原理及其应用

1 随机相位加密技术

自从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以来[10],关于这个领域的研究已经得到越来越多人的重视,目前有很多用于光学图像加密的方法[10-21],其中双相位编码技术应用的最为广泛。其原理是利用两个独立的随机相位掩模分别对原始图像在空间域和频域进行加密,将原始图像编码为复振幅稳定的白噪声,如果不知道两个相位密钥就不能恢复出原始图像。用普通光照、目视等方法均无法识别原图像。制作起来略为复杂,但防伪和隐藏效果非常之好。相对加密而言,解密方法比较简便。可以采用光学方法快速预解密,如发现可疑之处再用计算机精确解密。如果不知道两个相位密匙,不可能恢复出原始图像。该方法保密性好,非委托方和制作方无法伪造。因此成为目前研究热点,应用前景看好。

2 基于分数傅立叶变换结合随机相位的加密技术

Gopinathan Unnikrishnan 等[18-21]人利用分数傅立叶变换对双相位编码技术加以改进,提出基于分数傅立叶变换的双随机相位加密技术。由于光学系统的自由度的增多,使图像加密的密钥由原来的两重增加到四重,即增加了分数级次。这无疑增加了图像解密的复杂性,

从而提高了系统的保密性能。

本文第四章提出一种基于分数傅立叶变换结合相位编码的新方法，它不仅增加了加密的重数，提高了安全性，而且扩大了加密的范围，即实现了多幅图像的多重加密隐藏。

§1.3 本文的研究内容

图像加密技术是本研究领域的前沿课题之一。本文借鉴国内、外先进成果，利用相关学科的最新成就，从理论、计算和实验观察等方面入手，对多图多重加密技术进行了比较系统的研究。主要研究内容及解决的问题如下：

（1）利用分数傅立叶全息实现多图的光学加密隐藏，并用计算机模拟进行了验证。

（2）提出了基于分数傅立叶变换结合随机相位编码的多图多重光学加密隐藏理论，用计算机进行了验证，并进行了噪声分析。

本论文共分六章，其中，第二章简述分数傅立叶变换及随机相位编码相关理论；第三章论述基于分数傅立叶变换的多幅图的光学加密技术；第四章提出了基于分数傅立叶变换结合随机相位编码的多重加密技术；第五章对本文进行了总结。

第二章 相关基本理论简述

§2.1 分数傅立叶变换概述

2.1.1 分数傅立叶变换

分数傅立叶变换(Fractional Fourier Transform，简称 FRT)是将信号由空域或时域变换到分数傅立叶域的一种方法，它实际上是一系列的傅立叶变换，是傅立叶变换的全族。它在保留傅立叶变换的原有性质和特点的基础上，又增加了傅立叶变换所没有的新性质和特点，将其分数阶作为一个新的自由度，藉之可以从一个全新的角度去认识光的传播、成像和信息处理，从而可获得许多新的应用。

1 分数傅立叶变换(FRT)的数学描述[23]

在实验中需要对二维的光学图像进行处理，设$g(x, y)$为待处理的原始图像，它的分数傅立叶变换的定义为

$$G(u,v)=F_{\alpha}\{g(x,y)\}=\{\frac{\exp\{-j[\frac{\pi}{2}-\alpha]\}}{2\pi\sin\alpha}\}^{1/2}\cdot\int_{-\infty}^{\infty}\exp[\frac{j(u^2+v^2+x^2+y^2)}{2\tan\alpha}-\frac{jux+jvy}{\sin\alpha}]g(x,y)dxdy \tag{2.1}$$

式中 x, y 为空间域坐标，u、v为频率域坐标，$G(u,v)$称为$g(x,y)$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。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$F^{(P)}\{g(x)\}$。分数阶不仅可以是分数，还可以是整数甚至是复数，因此称此变换为广义傅立叶变换更为合适，但习惯上我们还是称之为分数傅立叶变换。

为阐明基本概念，我们仅讨论一维函数的分数傅立叶变换，有关的定义和性质可以直接推广到二维的情况。

以$-\alpha$代替上式中的α得到

$$F_{-\alpha}\{g(x)\}=\{\frac{\exp\{j[\frac{\pi}{2}-\alpha]\}}{2\pi\sin\alpha}\}^{1/2}\cdot\int_{-\infty}^{\infty}\exp[\frac{-j(u^2+x^2)}{2\tan\alpha}+\frac{jux}{\sin\alpha}]g(x)dx \tag{2.2}$$

在得出上式时用到了$-1=\exp(j\pi)$。$F_{-\alpha}\{\}$是$F_{\alpha}\{\}$的逆变换。

当$\alpha=\pi/2$和$\alpha=-\pi/2$时,式(2.1)转化为常规傅立叶变换，也就是说常规傅里叶变换是分数傅立叶变换的特殊情况。

$$F_{\pi/2}\{g(x)\}=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}g(x)\exp(-jux)dx \tag{2.3}$$

$$F_{-\pi/2}\{g(x)\}=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}g(x)\exp(jux)dx \tag{2.4}$$

这是常规傅立叶变换的另一种形式。

2 分数傅立叶变换的基本性质

从分数傅立叶变换的定义可以推出它的性质:

（1）线性性

几个函数线性叠加的分数傅立叶变换等于这几个函数同阶次的分数傅立叶变换的线性叠加,

$$F^{P}\{Ag(x)+Bh(x)\}=AF^{P}\{g(x)\}+BF^{P}\{h(x)\} \tag{2.5}$$

其中A,B是任意复常数.

（2）连续性

对于P_1、P_2阶分数傅立叶变换，有

$$F^{AP_1+BP_2}g(x)=F^{AP_1}F^{BP_2}g(x)=F^{AP_1}F^{BP_2}g(x) \tag{2.6}$$

（3）指数可加性和交换性

级联的数学分数傅立叶变换可以改变其先后次序，并有可加性和交换性，有

$$F^{P_1}\{F^{P_2}\{g(x)\}\}=F^{P_2}\{F^{P_1}\{g(x)\}\}=F^{P_1+P_2}\{g(x)\} \tag{2.7}$$

（4）可逆性

对一个函数进行P阶分数傅立叶变换后，接着进行一P阶的分数傅立叶变换，则可得到原函数:

$$F^{P}\{F^{-P}\{g(x)\}\}=F^{0}\{g(x)\}=g(x) \tag{2.8}$$

（5）周期性

因为变换关于α具有周期性，周期为2π，其主值区间为$\alpha\in(-\pi,\pi]$,所以

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

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 $F^{(P)}\{g(x)\}$，周期为 4，其主值区间为 $P\in(-2,2]$。

3 分数傅立叶变换概念在图像隐藏中的应用

式(2.1)所定义的变换当 α =0 时没有意义，因而 F_0 必须另行定义。现在来计算当 $\alpha \to 0$ 时的分数傅立叶变换。由于 $\alpha \sim 0$ 时，$\sin\alpha \sim \alpha$，$\tan\alpha \sim \alpha$，于是

$$F_{\alpha\to 0}\{g(x)\} = \lim_{\alpha\to\infty}\{\frac{\exp\{-j[\frac{\pi}{2}-\alpha]\}}{2\pi\alpha}\}^{1/2}\cdot\int_{-\infty}^{\infty}\exp[\frac{j(u^2+x^2)}{2\alpha}-\frac{jux}{\alpha}]g(x)dx$$

$$=\int_{-\infty}^{\infty}g(x)\delta(x-\xi)dx = g(u) \tag{2.9}$$

其中用到极限意义下的 δ 函数的定义

$$\lim_{\alpha\to\infty}\frac{\exp[-x^2/j\varepsilon]}{\sqrt{j\pi\varepsilon}} = \delta(x) \tag{2.10}$$

因此我们可以通过极限过程来定义 F_0，即

$$F_0\{g(x)\} = g(u) \tag{2.11}$$

用类似的方法还可以定义 F_π，即

$$F_\pi\{g(x)\} = g(-u) \tag{2.12}$$

以上两式表明：0 阶分数傅立叶变换给出输入图像本身，π 阶分数傅立叶变换则给出输入图像的倒像。

图 2.1 为 α 及 P 的周期性示意图，其中 $\alpha = \pi/2$ 或 $P = 1$ 表示常规傅立叶变换，$\alpha = -\pi/2$ 或 $P = -1$ 则表示常规的傅立叶逆变换。

当 $P = P_1 + P_2 = 0$ 时，$F^{(0)}\{g(x)\} = F_0\{g(x)\} = g(u)$，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，$F^{(2)}\{g(x)\} = F_\pi\{g(x)\} = g(-u)$，即 π 阶分数傅立叶变换则给出它的倒像；当 $P_1 = 1$，$P_2 = 1$ 时，表示两次傅立叶变换，得到输入图像的倒像，可以用 4f 系统实现，它们都是分数傅立叶变换的特例。

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

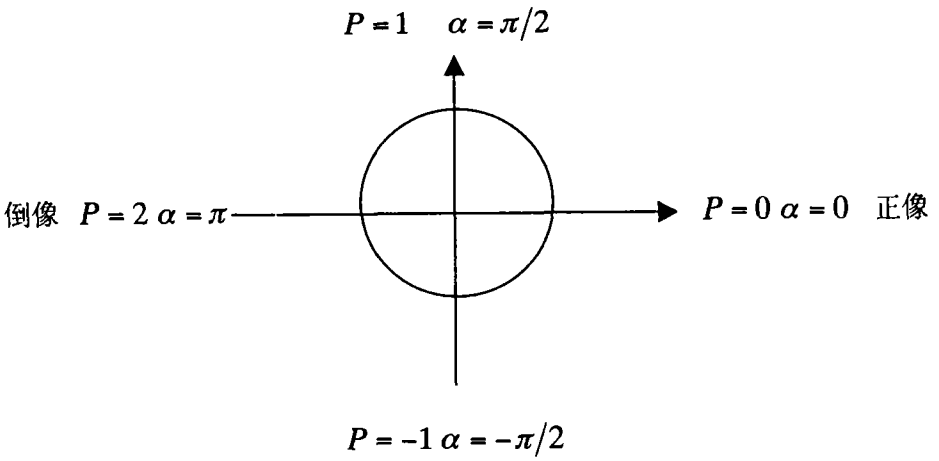


图 2.1 分数傅立叶变换的周期性示意图

4 分数傅立叶变换的光路实现

Lohmann 等人提出用透镜系统可实现分数傅立叶变换，其基本原理与用透镜实现傅立叶变换一样，利用了菲涅尔衍射原理[22]。透镜系统实现分数傅立叶变换有两类基本的光学单元，即 Lohmann I 型单透镜系统和 Lohmann II 型双透镜系统。

对 Lohmann I 型分数傅立叶变换系统，输入面和输出面距透镜的距离相等，均为z，透镜的焦距为f，当z和f满足下列条件时，输出面上函数为输入面上函数的 P 阶分数傅立叶变换：

$$z=\tilde{f}\tan(P\pi/4) \tag{2.13}$$

$$\tilde{f}=f\sin\alpha=f\sin(P\pi/2) \tag{2.14}$$

P为分数傅立叶变换的阶数，(2.14)式中$\tilde{f}$称为标准焦距，对系统来讲，仅当标准焦距相等时才有可加性，即

$$F^{P_1}F^{P_2}[g_0(x_0)]=F^{P_1+P_2}[g_0(x_0)] \tag{2.15}$$

当变换系统确定时，标准焦距取某一常数，P或α可取两个值

$$\alpha_1=\alpha\ (P_1=P=2\alpha/\pi) \tag{2.16}$$

$$或\alpha_1=\pi-\alpha\ (P_2=2-P) \tag{2.17}$$

由此导出两个不同的 d

$$d_1 = f(1-\cos\alpha) = f(1-\cos\frac{P\pi}{2}) \tag{2.18}$$

以及

$$d_2 = f(1+\cos\alpha) = f(1+\cos\frac{P\pi}{2}) \tag{2.19}$$

我们以透镜焦距相等的两个 Lohmann I 型单透镜系统的组合为例，说明本文所用到的分数傅立叶变换迭加性的光学实现，组合系统如图 2.2 所示[25]。

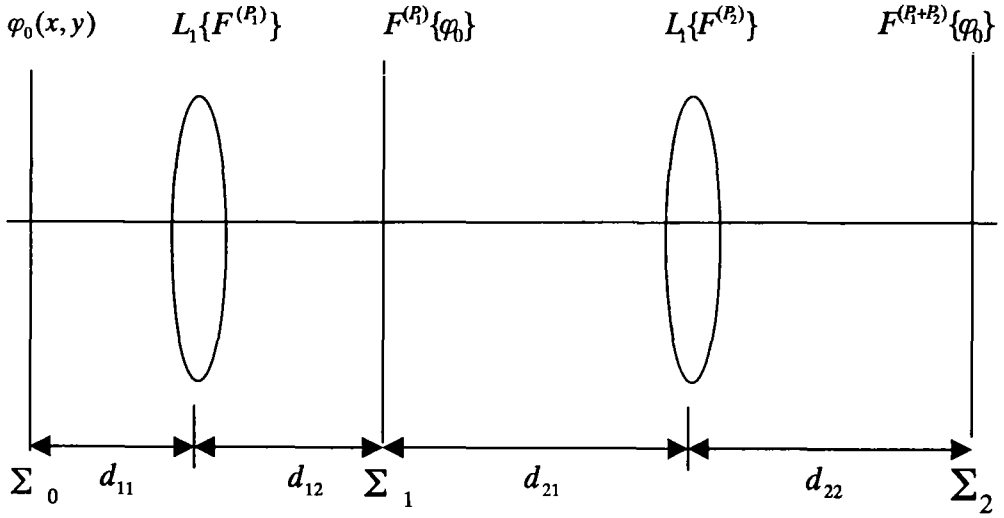


图 2.2 两个相同透镜组成的分数傅立叶变换系统

该系统由两个焦距均为 f 的透镜单元构成，它们的规格：

第一个光学单元（Σ_0—Σ_1）：

$$d_{11} = d_{12} = d_1 = f(1-\cos\alpha) = f(1-\cos\frac{P\pi}{2}) \tag{2.20}$$

第二个光学单元（Σ_1—Σ_2）：

$$d_{21} = d_{22} = d_2 = f(1+\cos\alpha) = f(1+\cos\frac{P\pi}{2}) \tag{2.21}$$

两个透镜的间距为 $d_{12} + d_{21} = d_1 + d_2 = 2f$ (2.22)

它们共同的标准焦距为 $\tilde{f} = f\sin\alpha_i = f\sin(\frac{P_i\pi}{2})$

设在 Σ_0 平面输入图像 $\varphi_0(x,y)$，则在单色光的照射下，第一个光学单元对 φ_0 进行阶为 P_1 的分数傅立叶变换，$\varphi_1 = F^{(P_1)}\{\varphi_0\}$；第二个光学单元再对其进行阶数为 P_2 的分数傅立叶变换，$\varphi_2 = F^{(P_2)}\{\varphi_2\}$，最后在输出平面 Σ_2 上得到输出图像 $\varphi_2(x,y)$，且有

$$\varphi_2 = F^{P_2}F^{P_1}\{\varphi_0(x,y)\} = F^{(P_1+P_2)}\{\varphi_0(x,y)\} = F^{(2)}\{\varphi_0(x,y)\} = \varphi_0(-x,-y) \tag{2.23}$$

即当$P=P_1+P_2=2$时，最后的再现光场是相应的物光场的坐标反演，在输出面上将获得与输入图像等大而倒立的像。

此分数傅立叶变换系统可应用于光学图像加密，当初始图像经过第一个光学单元后，在Σ_1面上将得到它的P_1阶分数谱，由于分数谱上已看不到原始图像，因此可视为一种加密图，如果我们要进行解密，则只要对此分数谱再进行分数阶为$2-P_1$的分数傅立叶变换即可。

当$P=1$时，我们得到$4f$系统，其区别在于，在上述系统中，谱平面Σ_1上呈现输入信号的分数傅立叶谱。而在$4f$系统中，谱平面上呈现了输入信号的傅立叶谱。

§2.2 随机相位加密技术

在利用随机相位掩模实现光学防伪的方法基础上，P.Refregier和B.Javidi等[10]人提出采用双随机相位加密技术来实现防伪和信息隐藏。

该技术采用如图1所示的4f系统来实现：

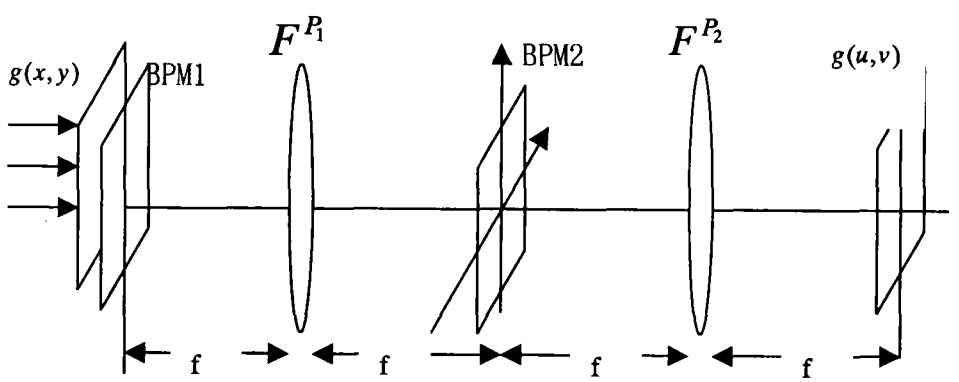


图2.3 双随机相位编码加密光学实现示意图

具体原理如下：

设$g(x,y)$表示待加密的图像，$\exp[jn(x,y)]$和$\exp[jb(u,v)]$表示两个独立的，同时均匀分布在$[0,2\pi]$上的随机函数。它们分别应用在空间域和频率域中，x,y为空间域坐标，u、v为频率域坐标。

加密时，输入的原始图像$g(x,y)$首先被随机相位函数$\exp[jn(x,y)]$所调制，完成空间域的加密。然后对调制后的函数进行傅里叶变换，在频谱面上用另一个随机相位函数

$\exp[jb(u,v)]$对其滤波，最后的加密图像变为：

$$e(x,y)=\{g(x,y)\exp[jn(x,y)]\}*h(x,y) \tag{2.24}$$

式中*表示卷积运算，$h(x,y)$为$\exp[jb(u,v)]$的逆傅立叶变换，即

$h(x,y)=F^{-1}\{\exp[jb(u,v)]\}=\exp[-jb(u,v)]$。

这样，两个相位函数$\exp[jn(x,y)]$和$\exp[jb(u,v)]$使输入的原始图像$g(x,y)$转变成为稳定的白噪声$e(x,y)$，从而完成了加密。

为了对图像解密，将加密图像$e(x,y)$用相位函数$\exp[-jb(u,v)]$滤波，该函数就是解密的密钥。因为：

$$\exp[-jb(u,v)]\cdot\exp[jb(u,v)]=\exp\{j[-b(u,v)+b(u,v)]\}=1 \tag{2.25}$$

所以解密后的函数变为：$g(x,y)\exp[jn(x,y)]$。

如果$g(x,y)$是正的实函数，则用强度探测器(如CCD)探测时，相位项$\exp[jn(x,y)]$消失，由此就完成了对加密图像的解密。

第三章 基于分数傅立叶变换的多图加密技术

经纯粹的光学系统加密的图像数据是复数形式的，必须以全息方式存储到高密度记录介质中，才能获得高质量的恢复图像。基于分数傅立叶变换理论并以分数阶这一重要参量为纽带，将分数傅立叶变换与光全息术相结合，从而产生了分数傅立叶变换加密全息图。

§3.1 多图加密的光路实现

3.1.1 加密光路

基于分数傅立叶变换的多图加密光路如图 3.1 所示。

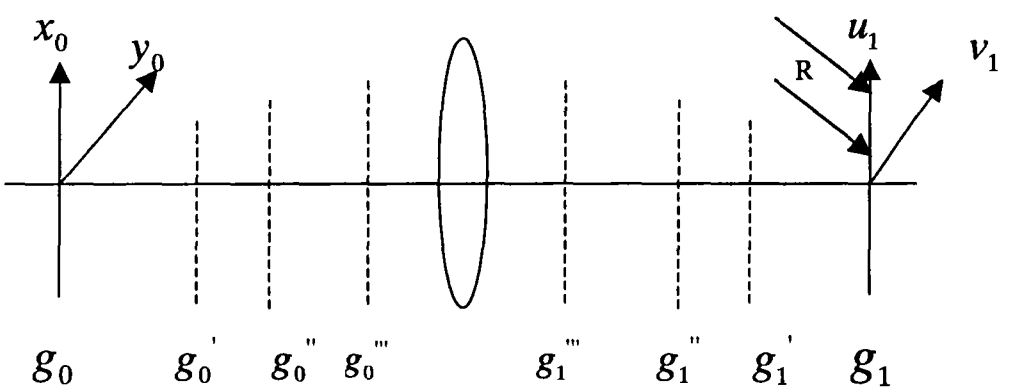


图 3.1 多图加密光路示意图

根据文献[7]，设多个物体(或将一个物体分割为几个部分)分别处在不同的位置上，即物函数分别为 $g_0(x_0,y_0,z_0)$，$g_0'(x_0+a_0,y_0+b_0,z_0')$，$g_0''(x_0-a_0,y_0-b_0,z_0'')$，$g_0'''(x_0,y_0,z_0''')$，……对应于各个物函数的 P_1，P_1'，P_1''，P_1'''，……阶分数傅立叶变换分别为 $g_1(u_1,v_1,z_0)$，$g_1'(u_1+a_1,v_1+b_1,z_0')$，$g_1''(u_1-a_1,v_1-b_1,z_0'')$，$g_1'''(u_1,v_1,z_1''')$，……。其中 a_0，b_0，a_1，b_1 均为常数。引入参考光 R 分别和各个物体的分数傅立叶变换光场干涉，经过多次曝光后，在同一块感光板 H_1 上记录了多个物体不同阶的分数傅立叶变换全息图。

3.1.2 再现光路

基于分数傅立叶变换的多图解密光路如图 3.2 所示。

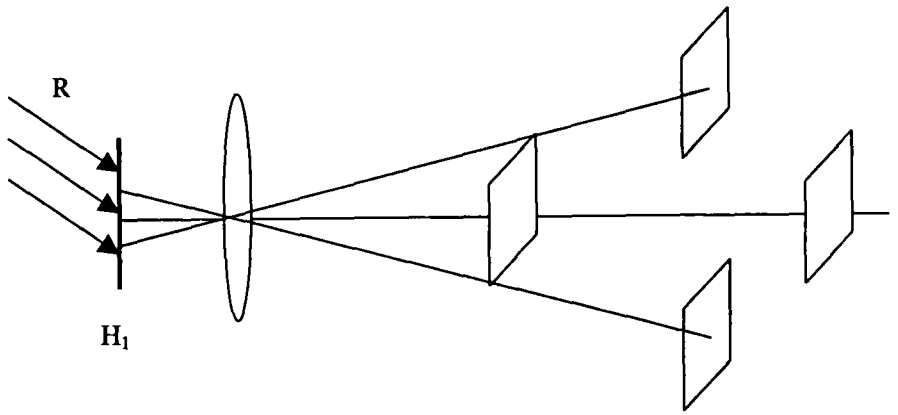


图 3.2 多图解密光路示意图

根据文献[7]，用原参考光 R 照明全息图 H_1，将再现出物光波 $g_0(x_0,y_0,z_0)$，$g_0'(x_0+a_0, y_0+b_0,z_0')$ $g_0'(x_0+a_0,y_0+b_0,z_0')$，$g_0''(x_0-a_0,y_0-b_0,z_0'')$，$g_0'''(x_0,y_0,z_0''')$，……分别经 P_1，P_1'，P_1''，P_1'''，……阶分数傅立叶变换后的光场。然后对分数傅立叶变换全息图再现的各个光场实行逆变换，或前后移动透镜 L 实行与原变换阶 P_1，P_1'，P_1''，P_1'''，……相匹配的 P_2，P_2'，P_2''，P_2'''，……阶变换，(如 $P_1+P_2=2$，$P_1'+P_2'=2$，$P_1''+P_2''=2$，$P_1'''+P_2'''=2$，……)，则在不同输出面的不同位置上可分别得到像 g_2，g_2'，g_2''，g_2'''，……。

§3.2 多图加密原理

3.2.1 加密原理

其基本原理是，用全息的方法在分数傅立叶变换域上的同一块感光板上记录多个不同物体物光波的不同阶的分数傅立叶变换频谱分布。由于分数傅立叶变换的频谱中已不见远原始图像的分布，故可认为我们已对原来的多幅图像进行了初步的加密。为分析简单起见，本章以两幅图的分数傅立叶变换加密为例说明多图加密与再现的原理[9]。

图 3.3 中，$g_0(x_0)$ 与 $g_0'(x_0)$ 是 2 个不同的物函数，$g_1(u_1)$ 与 $g_1'(u_1')$ 分别对应于 $g_0(x_0)$ 与 $g_0'(x_0)$ 的 P_1 与 P_1' 阶分数傅立叶变换，即：

$$g_1(u_1)=F^{P_1}[g_0(x_0)]=\int_{-\infty}^{\infty}B_{P_1}(x_0,u_1)g_0(x_0)dx_0 \tag{3.1}$$

$$g_1'(u_1')=F^{P_1'}[g_0'(x_0)]=\int_{-\infty}^{\infty}B_{P_1'}(x_0,u_1')g_0'(x_0)dx_0 \tag{3.2}$$

式中，B_{P_1}，$B_{P_1'}$ 分别为相应的 FRT 的核函数。

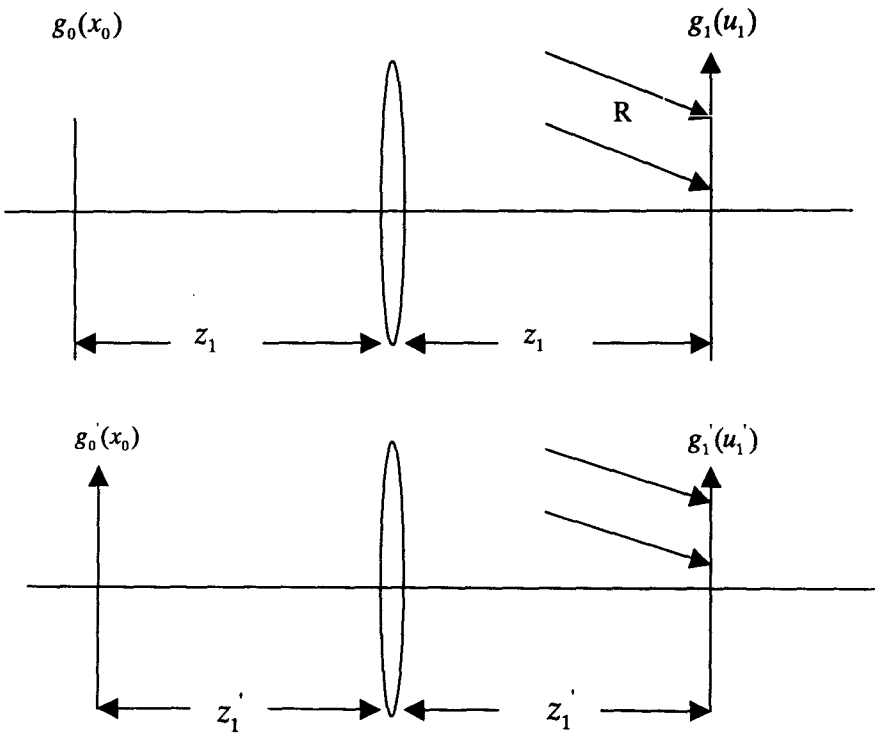


图 3.3 多图的分数傅立叶全息加密记录

两物函数的分数傅立叶变换频谱分别为

$$g_1(u_1)=\int_{-\infty}^{\infty} g_0(x_0)\exp\{i\pi(x_0^2+u_1^2)/\lambda f\sin(P_1\pi/2)\tan(P_1\pi/2)]\}\cdot \exp\{-i2\pi x_0u_1/[\lambda f\sin^2(P_1\pi/2)]\}dx_0 \tag{3.3}$$

$$g_1'(u_1')=\int_{-\infty}^{\infty} g_0'(x_0)\exp\{i\pi(x_0^2+u_1'^2)/\lambda f\sin(P_1'\pi/2)\tan(P_1'\pi/2)]\}\cdot \exp\{-i2\pi x_0u_1'/[\lambda f\sin^2(P_1'\pi/2)]\}dx_0 \tag{3.4}$$

式中，λ 是记录光波长。设 R 为记录时的参考光，两次曝光时间为 t_1 和 t_2，在线性记录条件下，全息图的振幅透射系数 τ_H 与曝光量成正比，即：

$$\tau_H \propto t_1|g_1(u_1)+R|^2+t_2|g_1'(u_1')+R|^2$$

$$=t_1(|g_1|^2+|R|^2)+t_1g_1^*R+t_1g_1R^*+t_2(|g_1'|^2+|R|^2)+t_2g_1'^*R+t_2g_1'R^* \tag{3.5}$$

3.2.2 再现原理

图 3.4 中，由原参考光 R 照明全息图，将再现出物光波 $g_0(x_0)$ 和 $g_0'(x_0)$ 分别经 P_1，P_1' 阶分数傅立叶变换后的光场。由(3.5)式得再现光波为：

$$i = t_1[|g_1(u_1)|^2 + |R|^2]R + t_1 g_1(u_1)^* R^2 + t_1 g_1(u_1)|R|^2$$
$$+t_2[|g_1'(u_1')|^2 + |R|^2]R + t_2 g_1'(u_1')^* R^2 + t_2 g_1'(u_1')|R|^2 \quad (3.6)$$

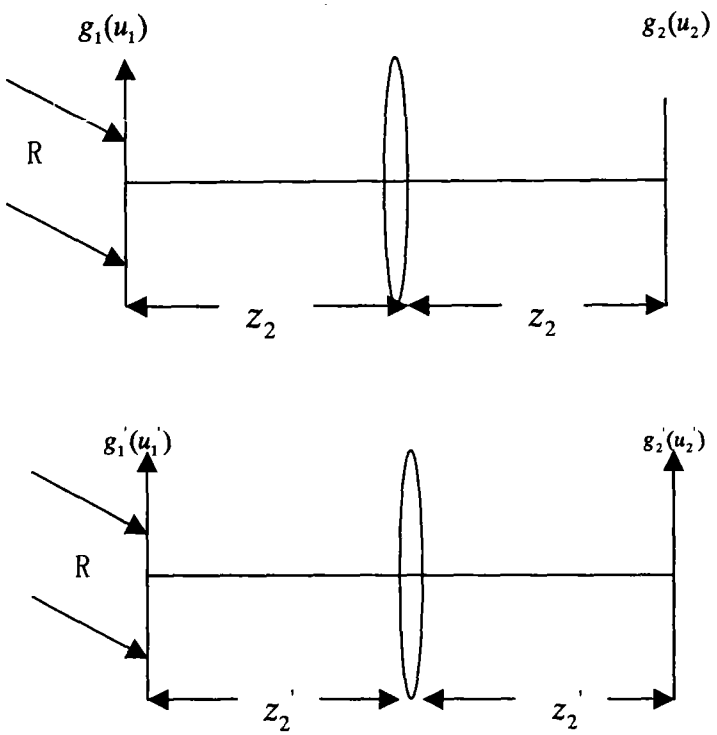


图 3.4 多图的分数傅立叶全息加密再现

(3.6)式中第一、四两项包含零级光和晕轮光；第二、五两项是共轭像项；第三、六两项是原始像项。单独考虑原始像项

$$t_1|R|^2 g_1(u_1) = t_1|R|^2 F^{P_1}[g_0(x_0)] \quad (3.7)$$

$$t_2|R|^2 g_1'(u_1') = t_2|R|^2 F^{P_1'}[g_0'(x_0)] \quad (3.8)$$

其复振幅为

$$A = t_1|R|^2 g_1(u_1) + t_2|R|^2 g_1'(u_1') \quad (3.9)$$

强度为：$I \propto AA^*$

要得到物体$g_0(x_0)$与$g_0'(x_0)$的像，需对全息图的再现光场实行与原变换阶P_1，P_1'相匹配的P_2，P_2'阶分数傅立叶变换。两原始像项再分别经P_2，P_2'阶分数傅立叶变换到达输出面u_2和u_2'，其光场分布为

$$g_2(u_2)=F^{P_2}\{t_1|R|^2F^{P_1}[g_0(x_0)]\}=t_1|R|^2F^{P_1+P_2}[g_0(x_0)] \tag{3.10}$$

$$g_2'(u_2')=F^{P_2'}\{t_2|R|^2F^{P_1'}[g_0'(x_0)]\}=t_2|R|^2F^{P_1'+P_2'}[g_0'(x_0)] \tag{3.11}$$

根据分数傅立叶变换的周期性，当$P_1+P_2=4$或$P_1'+P_2'=4$时，在输出面上将获得物体的等大而正立的像。特别是

当$P_1+P_2=2$时，$g_2(u_2)\propto F^2[g_0(x_0)]=g_0(-x_0)$

当$P_1'+P_2'=2$时，$g_2'(u_2')\propto F^2[g_0'(x_0)]=g_0'(-x_0)$

即最后的再现光场是相应的物光场的坐标反演。在2个不同输出面上将分别获得与原物等大而倒立的像。也就是说，利用 FRT 的周期性和再现像的位置与再现系统与分数阶有关的特性，可在不同位置再现出不同物的像，而其余信息则形成背景噪声。

由上面分析可知，分数傅立叶变换加密全息再现有以下特性：

多重分数傅立叶变换全息图不仅记录了多个不同物体的信息，而且还记录了相应多个系统的信息，如透镜的焦距 f，物体与透镜的距离z_1,z_2,z_3，……等，由它们所决定的分数阶可作为新的密钥。

普通的多重菲涅尔全息图是通过旋转全息干版来记录的，只能在一个位置观察其再现像，且两个再现像互相重迭干扰严重；而多重分数傅立叶变换全息图是基于分数傅立叶变换，通过改变分数阶来实现的，它具有更大的灵活性。

此外，多重分数傅立叶变换全息图的多个再现像一般在多个不同的位置（除非各种参数相同即加密和解密阶数相同，且物体与透镜的距离相同），再现像之间干扰很小：只需适当选取记录时物体与透镜远近不同的距离z_1，z_1'，z_1''，……便可使多个再现像之间的距离在很大范围内变化，即可远可近；再现时，如果在分数傅立叶变换加密全息图的后面放上一片 45° 的半透半反镜，则可在互成 90° 的两个平面上观察其相应的像，即两个再现的观察方向可发生改变。

如果多个物体$g_0(x_0)$，$g_0'(x_0)$，$g_0''(x_0)$，……分别处在物面多个不同位置（如上下或左右

错开),则再现时零级光产生的噪声对某一个再现像的影响可忽略,且可减少多个再现像的交叉影响,此时某一物体的再现像位置处的背景噪声将大为减少。

§3.3 计算机模拟实验与结果分析

3.3.1 计算机模拟

为了检验本文基于分数傅立叶变换的多图像隐藏的有效性，我们用 Matlab 语言编程对三幅不同的二值图进行了隐藏与再现的计算机模拟实验。

1 图像加密实验

图 3.5(1)、3.5(2)、3.5(3)为三幅待加密的二值图像，分别进行不同阶的分数傅立叶变换。对图 3.5(1)进行 $P_1=1.5$ 的分数傅立叶变换，对图 3.5(2)进行 $P_2=1.75$ 的分数傅立叶变换，对图 3.5(3)进行 $P_3=1$ 的分数傅立叶变换，得到各自的分数傅立叶变换频谱，如图 3.6(a)所示。为了增加对比度，将各分数傅立叶变换的频谱图进行了对数变换显示，如图 3.6(b)所示。

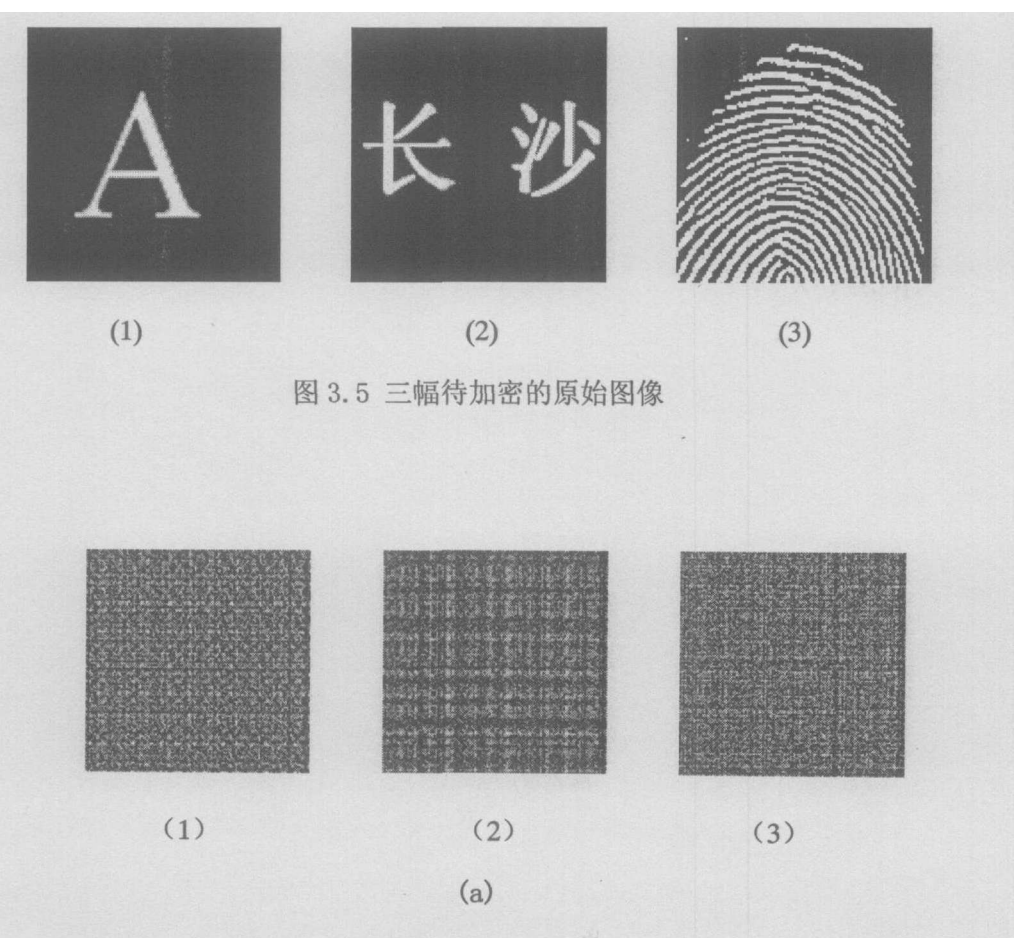
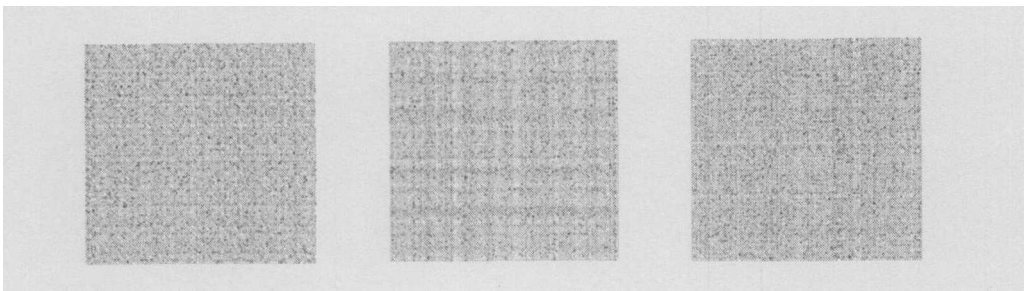


图 3.5 三幅待加密的原始图像



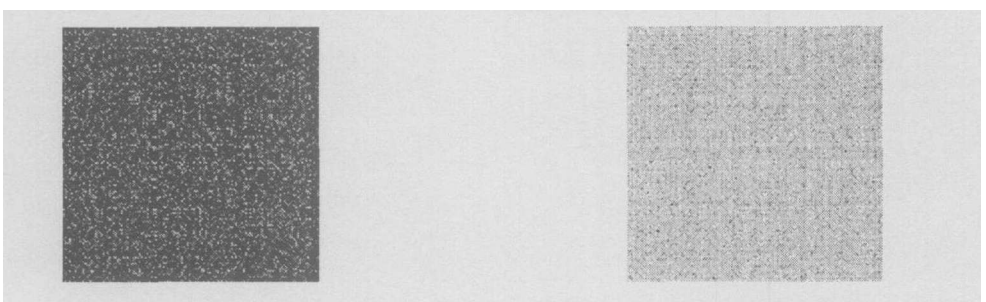
（1）　　（2）　　（3）

(b)

图 3.6 三幅图各自的分数谱示意图

a---各自分数谱平面的直接显示图；　**b---**对数变换后各自的分数谱平面显示图

将三幅频谱叠加在同一平面内，如图 3.7(a)所示，这时已看不到任何的原始信息，由此我们认为已完成三幅图的隐藏。图 3.7(b)为加密图的对数变换显示。



(a)　　**(b)**

图 3.7 三幅图的谱平面叠加图

a---谱平面叠加图的直接显示图；　b---对数变换后的谱平面叠加图

2 解密及解密噪声

对频谱图进行与加密分数阶匹配的变换，可得到解密的图像。即对叠加频谱分别进行 $K_1 = -P_1 = - = 1.5$，$K_2 = -P_2 = -1.75$，$K_3 = -P_3 = -1$的分数傅立叶逆变换时，可由频谱叠加图分别得到各自的解密图，见图 3.8(1)、图 3.8(2)、图 3.8(3)。各解密图上，其他的两个图像已成为模糊的背景噪声，无法辨认。

(1) (2) (3)

图 3.8 正确解密的图像

3.2.2 防伪特性分析

由于多图的分数傅立叶变换全息加密图不仅记录了多个不同物体的信息(或分别记录了一个物体的不同部分的信息),而且还分别记录了相应的多个变换系统的信息,如每个系统透镜的焦距 f,物体与透镜的距离 $z_1, z_2, z_3, \cdots\cdots$。因此在记录多图的分数傅立叶变换加密全息图时,可分别对每个物体进行尺度编码,为了读出经编码的多个物体的信息,每个物体再现像所对应的分数傅立叶变换系统的分数阶必须与其相应记录系统的分数阶匹配,我们可依据能否在多个特定的分数傅立叶变换系统的输出面分别再现出所有被记录物体清晰的像,来判断全息图的真伪。

利用分数傅立叶变换多图加密全息图再现条件的特殊性,可以制成一种光学安全认证系统,使其与普通多次曝光(傅立叶变换)全息图或单图分数傅立叶变换加密全息图相比具有更高的安全认证可靠性与防伪力度,能广泛用于钞票、证件、商标的制作中。

第四章 基于分数傅立叶变换结合相位编码的多图多重加密技术

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[10]。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。

本章提出一种基于分数傅立叶变换结合相位编码的新方法，对多幅图像进行多重隐藏。它利用分数阶扩展了加密的范围，即实现了多图的加密隐藏，同时结合相位编码增加了加密的重数，实现了多重隐藏，即增加了密钥，从而具有极高的安全性。

§4.1 多图多重加密的光路实现

4.1.1 加密光路

基于分数傅立叶变换的多图多重加密光路，如图 4.1 所示。

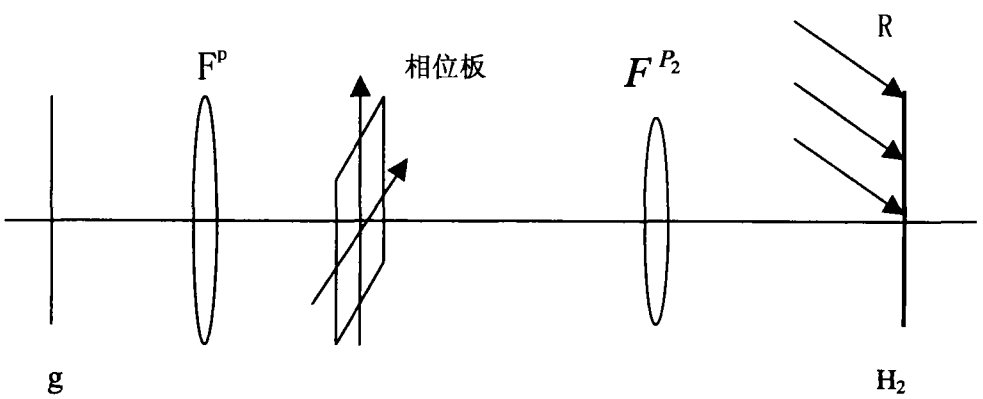


图 4.1 多图多重加密光路示意图

物光波 g 代表$g_0(x_0,y_0,z_0)$，$g_0'(x_0+a_0,y_0+b_0,z_0')$，$g_0''(x_0-a_0,y_0-b_0,z_0'')$，$g_0'''(x_0,y_0,z_0''')$……分别经 P(代表$P_1$，$P_1'$，$P_1''$，$P_1'''$，……)阶分数傅立叶变换后的频谱面上紧贴一随机相位掩模，则得到经相位调制的频谱图，再经P_2阶分数傅立叶变换，引入参考光 R 分别和此分数傅立叶变换光场干涉，经多次曝光后，则在感光板H_2上记录了多个物体的第二重分数傅立叶变换加密全息图。

4.1.2 再现光路

基于分数傅立叶变换的多图多重解密光路如图 4.2 所示。

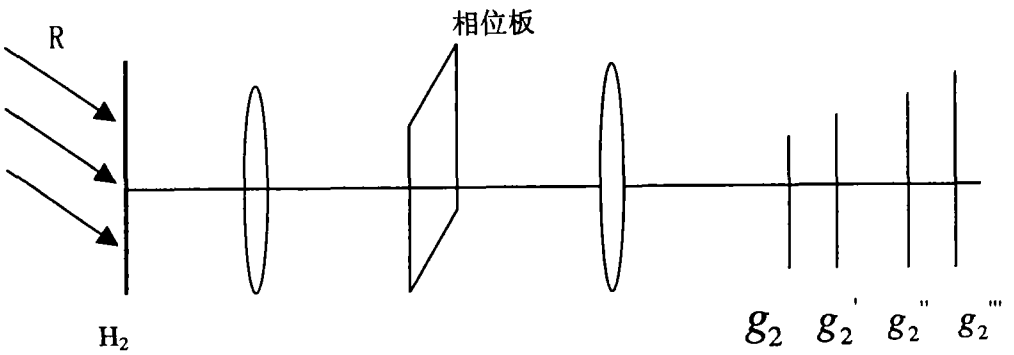


图 4.2 多图多重解密光路示意图

用原参考光R照明全息图 H_2,将再现出分别经P_2阶分数傅立叶变换后的第二重加密频谱图，然后对此频谱图进行与原变换阶数P_2相匹配的分数傅立叶变换，再经过反相位掩模，得到了第一重加密频谱图，即将再现出物光波$g_0(x_0,y_0,z_0)$，$g_0'(x_0+a_0,y_0+b_0,z_0')$，$g_0''(x_0-a_0,y_0-b_0,z_0'')$，$g_0'''(x_0,y_0,z_0''')$……分别经$P_1$，$P_1'$，$P_1''$，$P_1'''$，……阶分数傅立叶变换后的频谱叠加图。然后与上一章相同，对其实行逆变换,或前后移动透镜L实行与原变换阶数P_1，P_1'，P_1''，P_1''',……相匹配的P_2，P_2'，P_2''，P_2''',……阶变换,(如$P_1+P_2=2$，$P_1'+P_2'=2$ $P_1''+P_2''=2$，$P_1'''+P_2'''=2$，……),则在不同输出面的不同位置上可分别得到像g_2，g_2'，g_2''，g_2''',……。

§4.2 多图多重加密原理

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。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。信息隐藏的图像处理流程如图 4.3 所示。

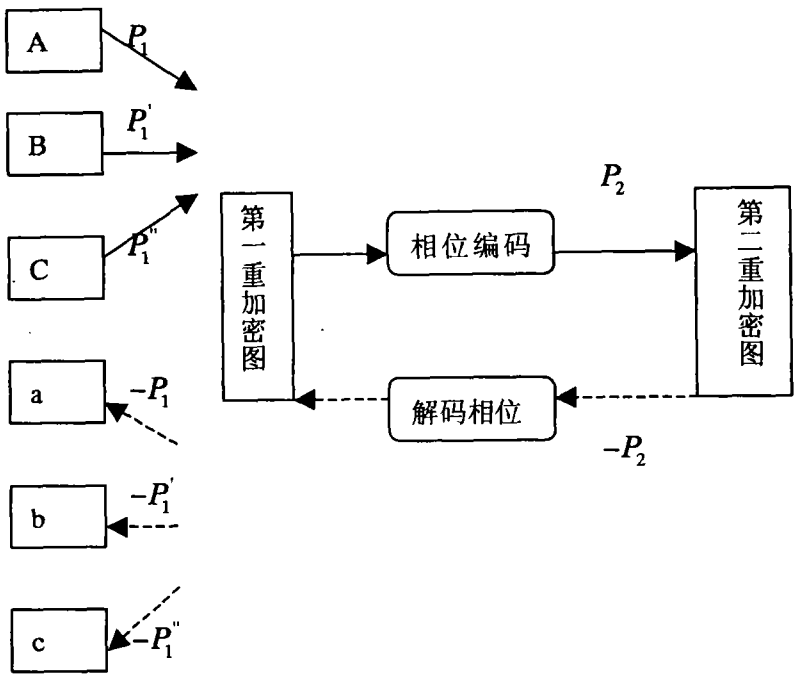


图 4.3 基于分数傅立叶变换的信息隐藏流程

A、B、C---三幅待隐藏的图像； a、b、c---解密得到的三幅图像

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。

为分析简单起见，我们以两幅图的分数傅立叶变换加密为例说明多图加密与再现的原理。

4.2.1 加密原理

本文分以下两个步骤在频谱面隐藏图像信息。

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 $F_2^{P_1'}(U,V)$ 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

$$F(U,V)=F_1^{P_1}(U,V)+F_2^{P_1'}(U,V) \tag{4.1}$$

2 第二重隐藏

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

$$F^{P_2}\{\exp[jb(U,V)]F(U,V)\} \tag{4.2}$$

4.2.2 解密原理

图像解密过程即为加密过程的逆过程，亦分为两个步骤。

1 第一重解密

再现图像的分数傅里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 $M_2=M_1^*=\exp[-jb(U,V)]$ 滤波，数学上可表示为

$$F^{-P_2}\{F^{P_2}\{\exp[jb(U,V)]F(U,V)\}\}\exp[-jb(U,V)]=F(U,V) \tag{4.3}$$

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：

$$f_1'(x,y)=F_1^{-P_1}[F_1^{P_1}(U,V)]+F_2^{-P_1}[F_c^{P_1'}(U,V)]=f_1(x,y)+F_2^{-P_1}[F_2^{P_1'}(U,V)] \tag{4.4}$$

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：

$$f_2'(x,y)=F_1^{-P_1'}[F_1^{P_1}(U,V)]+F_2^{-P_1'}[F_2^{P_1'}(U,V)]=F_1^{-P_1'}[F_1^{P_1}(U,V)]+f_2(x,y) \tag{4.5}$$

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的引起的噪声干扰，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。我们也可以通过减去经计算过的噪声值，而得到清晰的图像。

如果被加密隐藏的仅是幅单图，那么其正确解密图像就没有来自其它图的噪声干扰，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里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里叶变换的阶数有关，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。

4.2.3 相位板作用

图 4.4 为分数傅立叶变换结合随机相位编码加密方法的光学实现示意图，其中 Σ_0 为输入面，Σ_1 为第一重分数频谱面，Σ_2 为加密面。

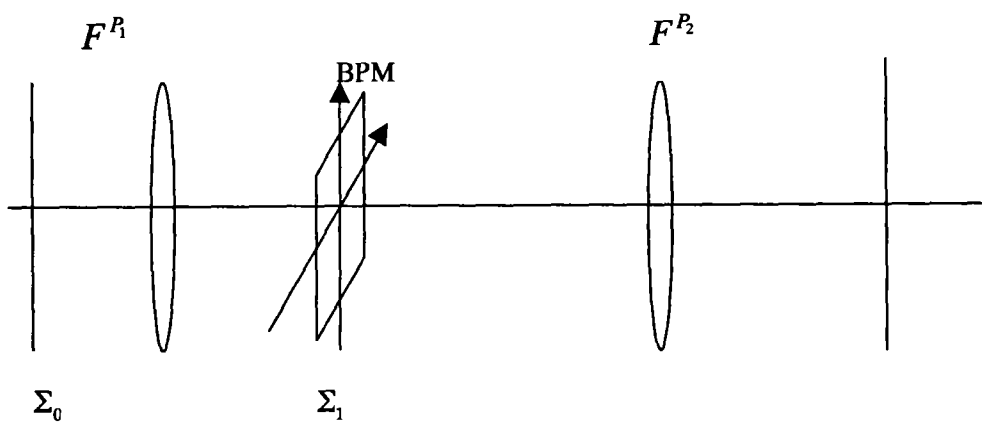


图 4.4 分数傅立叶变换结合随机相位编码加密方法的光学实现示意图

随机相位板（Random Phase Mask,简称 RPM）是一种全透明的塑料薄片，具有极高的分辨率，在数平方毫米的面积上分布着上百万个像素，各个像素的折射率或光学密度大小不一，像素的相位满足白噪声分布，能对入射光产生 0～2π 间的随机相位延迟。因此相位密钥的空间非常大，在不得知密钥相位分布的情况下，很难通过盲目反运算恢复加密图像，因而该算法具有较高的安全性。

由于分数傅立叶变换具有叠加性，所以在进行下一次分数傅立叶变换之前，先进行了相位编码。随机相位板置于第一重加密的谱平面 Σ_1 上，直接对分数傅立叶频谱进行位相变换，然后再进行第二次分数傅立叶变换加密。与 Philippe Refregier and Bahram Javidi[10]提出的双相位随机相位编码相比，本方法实现了多图加密，并且少用了一块相位板，因为当对物函数进行分数傅立叶变换后，其分数谱已是复振幅形式，具有了位相信息。

由于此加密系统对元件的空间排列精度要求非常高，尤其是在解密阶段，只有当解密密钥及其空间位置都匹配得非常准确时才能得到清晰的解密图像。由于相位的随机性，当全部数据用于解密时，谱平面上的 RPM 偏离匹配位置哪怕只有一个像素大小的距离，也不

能获得解密图像。

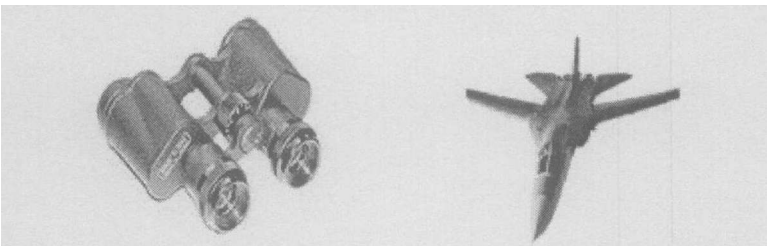
§4.3 计算机模拟实验与结果分析

4.3.1 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119×119像元的灰度图进行了隐藏与再现的计算机模拟实验。

1 图像加密实验

图 4.5(1)、4.5(2)为待隐藏的灰度图。先对图像 4.5(1)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 4.5(2)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 4.6。



(1) (2)

图 4.5 原始图像

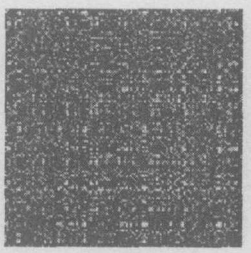
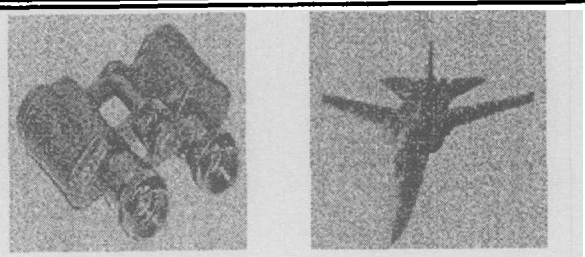


图 4.6 加密后的图像

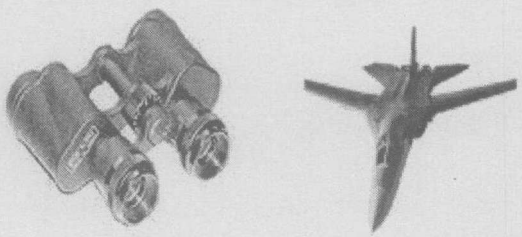
2 解密及解密噪声

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 4.7(1)；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 4.7(2)。他们都是含有噪声的解密图像，消噪后可得清晰的图像，如图 4.8(1), 4.8(2)



(1) (2)

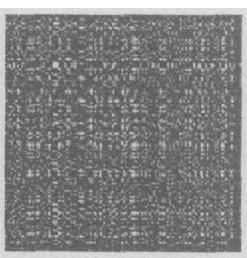
图 4.7 正确解密的图像



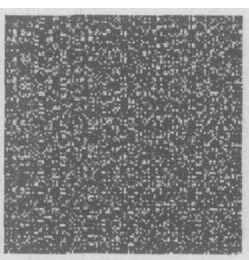
(1) (2)

图 4.8 消噪后的图像

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 4.9(1), 4.9(2)为与K_1, K_1'有 0.01 偏差, 其它密钥正确的解密结果；图 4.10(1)，4.10(2)为与K_2有 0.01 偏差, 其它密钥正确的解密结果；图 4.11(1), 4.11(2)为分数阶密钥正确，解码相位密钥错误时的解密结果。从图 4.9，4.10，4.11 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，都无法获得正确的解密结果，因而有着极强的安全性。

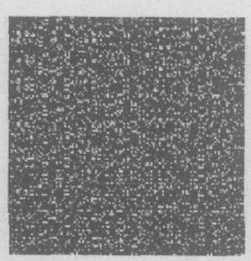


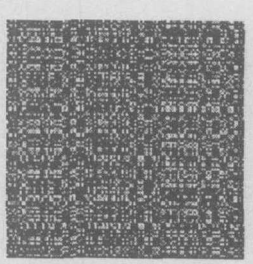
4.9(1) K_1错误，K_2、M_2正确



4.9(2) K_1'错误，K_2、M_2正确

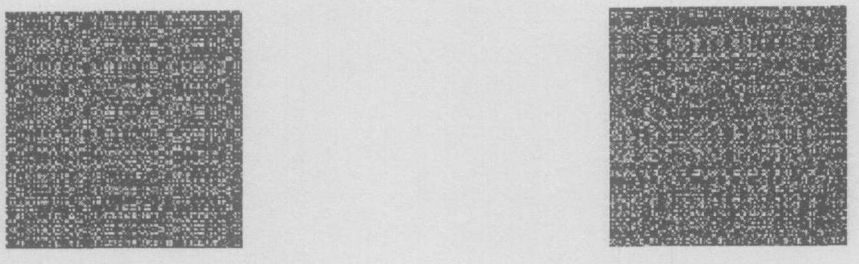
图 4.9 K_1或K_1'错误时的解密图像





4.10(1) K_2错误，K_1、M_2正确　　4.10(2) K_2错误，K_1'、M_2正确

图 4.10 K_2错误时的解密图像



4.11(1) M_2错误，K_1、K_2正确　　4.11(2) M_2错误,K_1'、K_2正确

图 4.11 M_2错误时的解密图像

各种情况下的解密结果可以用表 4.1 说明。

表 4.1 图像在分数阶密钥、解码相位密钥取不同值时的解密情况

	4.7(1)	4.9(1)	4.10(1)	4.11(1)	4.7(2)	4.9(2)	4.10(2)	4.11(2)
K_1	√	×	√	√				
K_1'					√	×	√	√
K_2	√	√	×	√	√	√	×	√
M_2	√	√	√	×	√	√	√	×

注：√---加密图像的正确解密；　×---加密图像的错误解密

4.3.2 加密技术的误差容限分析

任何光学系统及通讯传输系统都存在各种内在或外在的噪音，它们必将影响图像的加/解密过程和传输。为了克服或减小噪音的影响，有必要对上述过程中的噪音行为进行分析。

在这一部分里将讨论加密技术的误差容限特性。这里的误差包括加密解密过程中引入的各种噪声，丢失加密图像的部分数据，等等。

为了评估解密图像的质量，采用解密图像同原始图像的均方差来作为评估参数。均方差定义为：$MSE=\frac{1}{N^2}\sum_{x=1}^{N}\sum_{y=1}^{N}[|g'(x,y)|-g(x,y)]^2$，$N^2$是图像的像素总数，$|g'(x,y)|$是解密图像的强度，$g(x,y)$是原始图像。

加密技术得到的加密图像是具有复振幅的灰度图像，而在光信息处理系统中，处理二

值图像要比其它图像更方便快捷。本实验采用的经二值化处理后的两幅图像，如图 4.7 所示

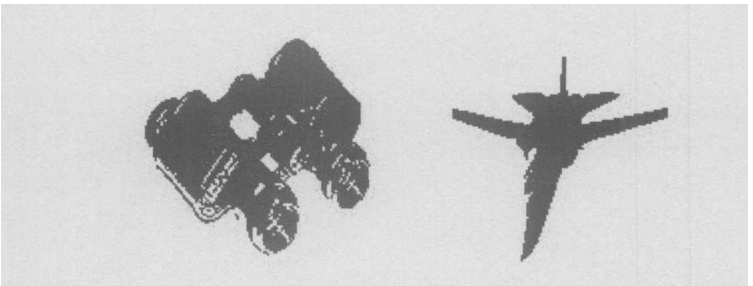


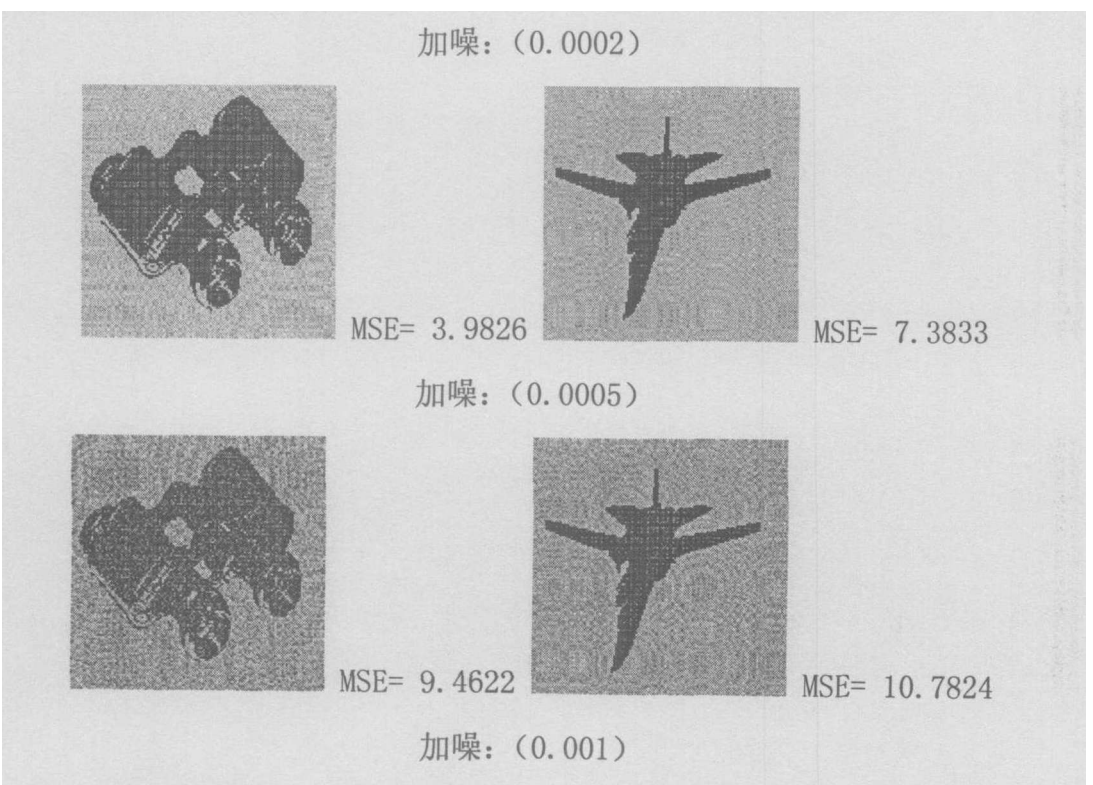
图 4.12 经二值化处理后的两幅图像

1 抗噪声性能的实验与分析

为了验证加密技术的抗噪声能力，我们将在“飞机”和“望远镜”的加密图像上分别添加了高斯白噪声（均匀性噪声）和乘积性噪声（非均匀噪声），得到解密结果。

（1）引入高斯白噪声的实验与分析

在“飞机”和“望远镜”的加密图像上分别添加了不同强度的高斯白噪声，解密结果如图 4.8 所示。



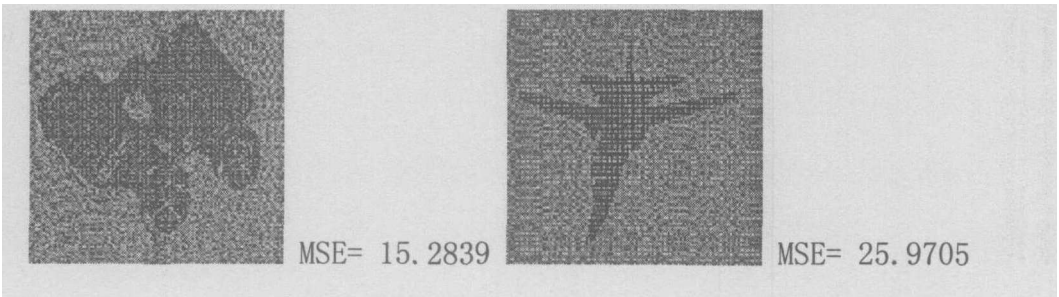


图 4.13 加入不同强度高斯白噪声的解密结果

(0.0005 等表示噪声强度与图像本身强度的比值)

(2) 引入乘积性噪声的实验与分析

在“飞机”和“望远镜”的加密图像上分别添加了不同强度的乘积性噪声，解密结果如图 4.9 所示。

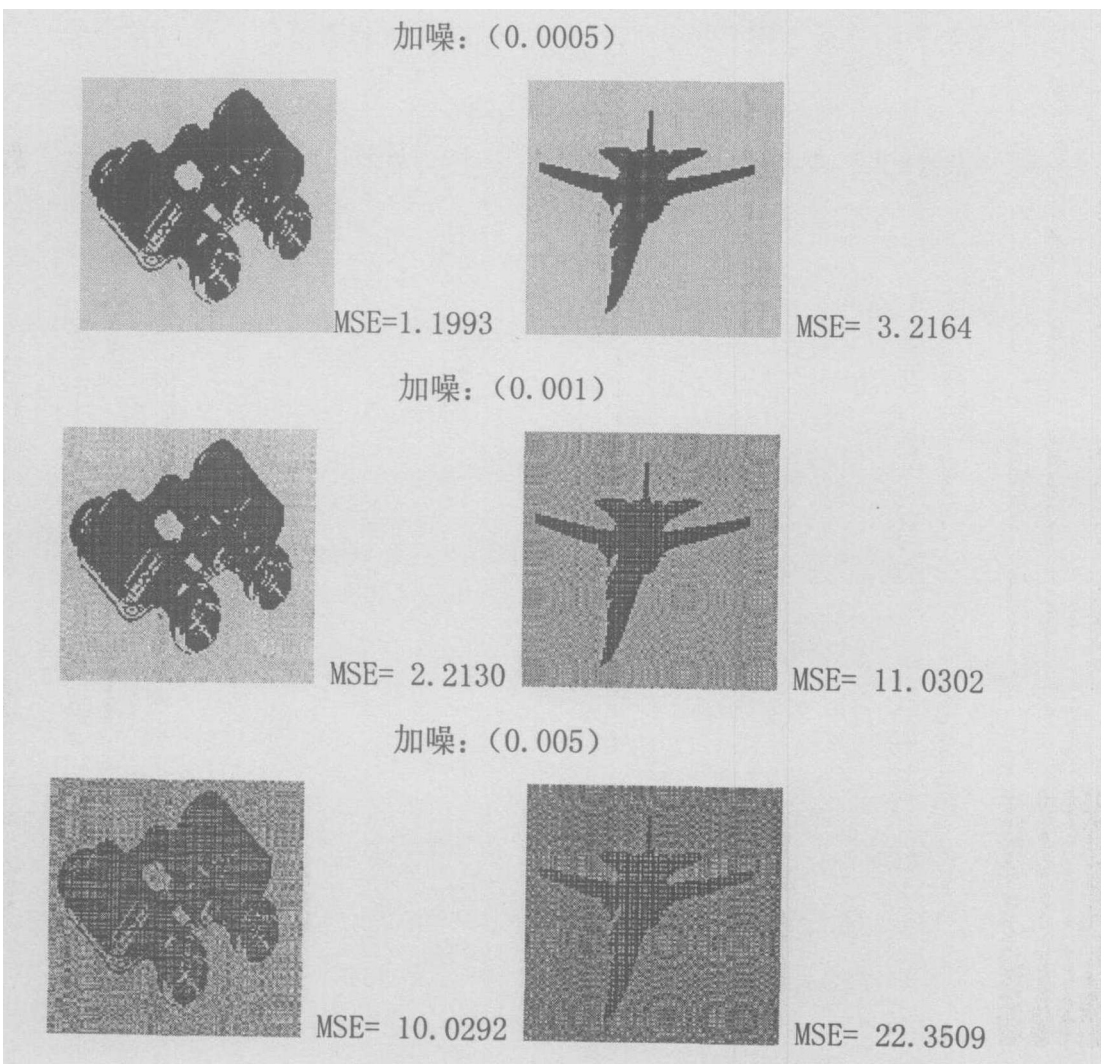


图 4.14 加入不同强度乘积性噪声的解密结果

(0.0005 等表示噪声强度与图像本身强度的比值)

由以上结果可以看出，加密时分别加入不同噪声后，仍可得到正确的解密图像。

2 丢失部分加密图像数据时的实验与分析

实验中,“飞机”和“望远镜”的加密图丢失 4 个像素时，其解密结果如下图所示。

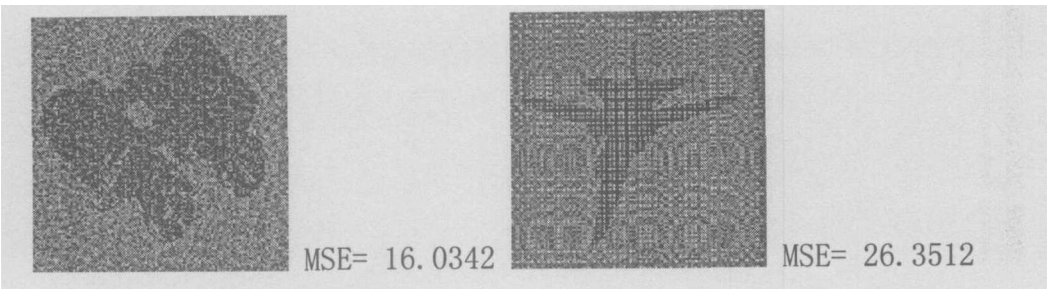


图 4.15 丢失 4 个像素的解密结果

从理论上来讲，加密图像具有复振幅，是包含了图像振幅与相位信息的全息图。从全息图的特点可知，由局部全息图就可以恢复原始图像。实验结果验证了这一点。

3 相位信息和振幅信息的加密作用。

具有复振幅的加密图像包含两部分信息:相位信息和振幅信息。采用图“飞机”和“望远镜”所示的图像进行了实验，分别由振幅信息和相位信息进行解密发现，相位信息和振幅信息缺一不可，少了任何一个都解不出来任何有用信息。

4.3.3 光学实现的三种建议方法

本文虽然完成了多幅图、多重加密解密的计算机模拟，得到了符合理论预测的结果，但这些数值模拟结果还需由光学实验进行验证。此技术的实现有三种建议方法：

1 制作全息胶片

由于经纯粹的光学系统加密的图像数据是复数形式的，必须以全息方式存储到高密度模拟型记录介质中，才能获得高质量的恢复图像。采用这种方式存储的信息，图像也必须用光学方法重建。

2 用空间光调制器代替相位板

如果同计算机、空间光调制器(Spatial Light Modulator)以及光信息处理系统结合起来，不仅可以实时加密和解密图像，而且可以更方便地变动使用中的密钥，从而更加易于实际应用。

3 数字全息技术

为了让光学加密技术更好的与目前的数字信号处理和通信系统相兼容，一个可行的方法是借助数字全息技术把光学模拟信号数字化，这可以在输出平面以干涉方法产生加密的全息信号，然后用 CCD 接收此加密信号来实现。经过 CCD 的光电转换，数字全息图像甚至可以通过通信链路传输，而在接收端可以通过数字方法或者光学方法恢复图像。

第五章 结束语

光学安全技术最初是将全息图粘贴在信用卡、商标、纸币上，人们可以直接通过眼睛观察，辨别真伪。但这种全息图由于图像的可见性和图像处理技术的发展，很容易通过照相或CCD相机从信用卡上摄取，并重新产生全息图，从而失去防伪或保密的安全性。

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的新方法，在解密时，我们可依据能否在多个特定的分数傅立叶变换系统的输出面分别再现出所有被记录物体清晰的像,来判断全息图的真伪。

§5.1 本文完成的主要工作

分数傅立叶变换的最重要参量是它的分数阶，利用分数阶扩展了加密的范围，即实现了多图的加密隐藏，同时结合相位编码增加了加密的重数，即实现了多重隐藏，增加了密钥，从而具有比常规加密更高的安全性能。分数傅立叶变换、随机相位编码理论等先进技术的综合构成了该项研究的核心。

本文用计算机软件实现了多幅图像的多重加密和解密，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，即分数阶次密钥 $K_1=-P_1$ 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。与单重加密相比，在又多了两重密钥的情况下，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。

本文还对加密图进行了抗噪声分析，实验结果表明，在加密图像上分别加入不同噪声后，当噪声强度较小时，直接可以得到令人满意的解密图像；在丢失部分加密图像的数据时，解密图像的清晰度和亮度有所降低，但在丢失数据较少的情况下，解密图像的质量还是不错的；单由振幅或相位信息根本无法正确解密，因此振幅和相位皆具有加密信息。

§5.2 本文研究结果的用途

本文除了作为理论研究外，它所发展的技术还有以下几种用途：

1 本方法对单幅图像的隐藏有着很好的解密效果，由于分数傅立叶变换中不同的阶数可对应不同的图像，所以也可用来隐藏多幅图像。虽其再现的所有解密像都含有噪声，但图像的基本特征已可见，不影响识别原物，由此可视为一种图像的加密存储方式。

2 对计算机文件进行加密，现有很多数字隐藏方法，如 Arnold 置换、序列迭代、数字水印技术等，这些基本上都是基于纯数学的算法理论，而本文提出了一种以光学原理为背景的算法理论。

3 本理论亦适用于网络图像加密传输技术，一幅加密图中可掩藏多幅图像，实现加密传输；同时，本方法具有较高的安全性，即使加密方法公开，如果不知道密钥，也很难再现。

本文取得了初步进展，但还有不足之处：我们仅对灰度图进行了基于分数傅立叶变换的隐藏和再现，对真彩色图像的处理还在继续研究、完善。

致　　谢

首先衷心感谢我的导师谭吉春教授。在我研究生学习期间，无论在学习上、思想上还是在生活上，导师都给予了无微不至的关怀和耐心细致的指导，并为我创造了一个良好的学习、讨论和研究的氛围和条件。尤其是在论文的选题、研究、撰写过程中导师倾注了大量的心血，提出了许多宝贵的意见和建议，令我受益匪浅。导师严谨的治学态度，一丝不苟的敬业精神，诲人不倦的高尚师德，为我树立了做人、做事的楷模，对我今后的人生之旅将产生深远的影响。

感谢光电科学与工程系的周朴、贾辉同学，他们帮助我借仪器、一起做实验，为我的论文提供参考意见。

感谢蒋治国、丁宁、梁晶、张徽强等实验室的全体同学，与你们共度的这段学习时光充实而快乐，是我一生中难忘的回忆。

感谢我的父母和家人，是你们多年来无私的关心、鼓励和支持，使我能够全身心地投入到工作和学习中。

最后，感谢所有给予我关心和帮助的朋友！

参考文献

[1] Thad G Walker,Holography without photography.Am Jphys, 67(9):783-785,1999

[2] 王永仲等，迂回相位编码的傅里叶变换计算全息图及其再现，红外技术 Vol.26 No.2,March,2004

[3] 张怡霄等，彩虹全息标识的计算全息加密，四川大学学报（自然科学板）Vol.37, No.1,February,2004

[4] 甑丽娟等，Moire 技术在防伪中的应用，应用激光 Yol.19 No.3,June,1999

[5] 黄义春等，散斑技术在防伪中的应用，激光与红外 Vol.29 No.3,June,1999

[6] 郭永康，黄奇忠，杜惊雷，分数傅立叶变换全息图及其在防伪中的应用，光学学报，Vol.19,No.6,June,1999

[7] 曾阳素等，多重分数傅立叶变换全息防伪术，中国激光，Vol.A29,No.8,August,2002

[8] 谢世伟等，分数傅立叶变换计算全息图，中国激光，Vol.30,No5,May,2003

[9] 曾阳素等，二次曝光分数傅立叶变换全息图，激光技术，Vol.26,No.1, February,2002

[10] Philippe Refregier and Bahram Javidi, Optical image encryption based on input plane and Fourier plane random encoding，Opt.lett, 20(7):767-769,1995

[11] Bahram Javidi and Takanori Nomura, Secure information by use of digital holography, Opt.Lett, 25(1)：28-30, 2000

[12] Xiaodi Tan, Osamu Matoba, Yoshiko Okada-Shudo, Masafumi Ide, Tsutomu Shimura, and Kazuo Kuroda, Secure Optical Memory System with Polarization Encryption, App.Opt, 40(14)：2310-2315, 2001

[13] Xiaodi Tan, Osamu Matoba, Tsutomu Shimura, Kazuo Kuroda, Bahram Javidi, Secure optical storage that use fully phase encryption, App.Opt, 39(35)：6689-6694, 2000

[14] J F Heanue, M C Bashaw, L Hesselink, Encrypted holographic data storage based on orthogonal-phase-code multiplexing App.Opt,34(26):6012-6015,1995

[15] Paul C. Mogensen, Jesper Glckstad, Phase-only optical encryption, Opt.Lett,25(8):566-568 ,2000

[16] Wei-Chia Su, Ching-Cherng Sun, Yu-Cheng Chen, Yueh Ouyang, Duplication of Phase Key for Random-Phase-Encrypted Volume Holograms, App. Opt. 43(8):1728-1733,2004

[17] Dong-Hoan Seo, Soo-Joong Kim, Interferometric phase-only optical encryption system that uses a reference wave, Opt.Lett, 28(5)：304-306, 2003

[18] Gopinathan Unnikrishnan, Joby Joseph, Kehar Singh, Optical encryption by double-random phase encoding in the fractional Fourier domain, Opt.Lett, 25(12)： 887-889, 2000

[19] G. Unnikrishnan, J. Joseph, K. Singh, Fractional Fourier Domain Encrypted Holographic Memory by Use of an Anamorphic Optical System App.Opt, 40(2)：299-306,2001

[20] B. Hennelly, J. T. Sheridan, Optical image encryption by random shifting in fractional Fourier domains , Opt. Lett, 28(4)：269-271,2003

[21] 于力等，用于光学图像加密的分数傅立叶变换双相位编码，光子学报，Vol.30,No.7,July,2001

[22]A.W.Lohmann,Image rotation Wigner rotation,and fractional Fourier transform,J.Opt.Soc. Am.(A),1993,10(10):2181-2186

[23] 虞祖良，金国藩，计算机制全息图，北京：清华大学出版社，1984 年 10 月第一版

[24] 苏显渝，李继陶，信息光学，科学出版社，1999 年第一版

[25] 宋菲君，S.Jutamulia，近代光学信息处理，北京大学出版社 1998 年 4 月第一版

[26] 竺子民, 光电图像处理, 华中科技大学出版社, 2000 年 9 月第一版

[27] Matlab6.0 高级应用-图形图像处理，清源计算机工作室，机械工业出版社 2001 年 5 月第一版

[28]刘莉，周朴，分数傅立叶变换在图像隐藏中的应用，（1）国防科技大学第四届研究生学术活动节，2004，10；（2）国防科技大学学报录用，待发表）