文章编号:1002-2082(2007)03-0262-03

基于不对称非标准傅里叶变换的光学图像加密

邓晓鹏
(怀化学院 物理与电子信息科学系,湖南 怀化 418008)

摘 要:针对以往光学图像加密系统中输入面和频谱面对称性的缺点,在不增加系统元件的基础上,利用球面波照射不对称非标准傅里叶变换系统进行图像加密。通过把相位掩模置于该系统的傅里叶变换平面,利用不对称非标准傅里叶变换系统的输入面和频谱面的不对称性以及频谱面对于点光源相关参数的依赖性,克服了以前光学加密系统中输入面和频谱面的对称性所带来的安全隐患,并且获得了除相位掩模以外的另外四重密匙。理论分析和模拟实验表明:该方法不仅可行,而且多增加了几重密匙,增强了系统的安全性能。

关键词:光学图像加密;非标准傅里叶变换;球面波;相位掩模
中图分类号:TN911.73 **文献标志码**:A

Optical image encryption based on asymmetric abnormal Fourier transform

DENG Xiao-peng
(Department of Physical Electronics, University of huaihua, Huaihua 418008, China)

Abstract: To overcome the disadvantage of the symmetry of input and frequency planes in the previous optical image encoding systems, an improved encryption method is proposed. Instead of adding optical elements, the optical image encryption is realized by spherical wave illumination on asymmetric non-normal Fourier transform system and by placing the phase mask on the Fourier transform plane of the system. Due to the asymmetry of this system and the dependence of the Fourier spectrum plane on relevant parameters of the spotlight, it overcomes the hidden trouble resulting from the symmetry of the previous optical image encoding system and increases four fold security keys. Theoretic analysis and computer simulation indicate that this method is feasible and enhances the security greatly.

Key words: optical image encrypting; abnormal Fourier transform; spherical wave; phase mask

引 言

B. Javid 等人提出的双随机相位加密方法是:用2个独立的随机相位掩模对需要保护的图像分别在4f系统的空域和Fourier频域进行编码,使原始图像变成噪声,但是2块相位板分别位于2个特殊的平面内,因此相位板的纵向位置不能作为密钥[1]。虽然采用分数傅里叶变换系统可以使相位板的纵向位置随分数变换级数的变化而改变,但是分数傅里叶变换系统中输入与输出平面相对透镜是对称的,因此只要知道了输入平面就知道了输出平面,也就知道了相位板的纵向位置。这在一定程度上降低了系统的安全性能[2-5]。针对这一点,在不增

收稿日期:2006-08-24; 修回日期:2006-10-31
作者简介:邓晓鹏(1972—),男,苗族,湖南沅陵人,讲师,主要从事光电图像处理研究。E-mail:dxpzqh@tom.com

加系统元件的基础上,提出用球面波照射透镜,把相位板置于点光源的像平面,即在系统的傅里叶变换平面上进行加密。由于点光源照射傅里叶变换系统的输入面和频谱面不对称,而且它的频谱面位置依赖于点光源的相关参数,所以,当把相位掩模置于它的频谱面上时,相位掩模的纵向位置以及透镜的焦距也成为密匙,这就大大增强了系统的安全性能。

1 基本原理

基于不对称非标准傅里叶变换加密系统原理设计的加密系统如图1所示。

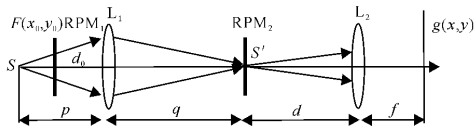


图1 加密系统

Fig. 1 Optical set-up for encryption

图1左半部分是一个点光源照射的傅里叶变换系统。其中,S 和 S' 互为像共轭关系,即 $\frac{1}{p}+\frac{1}{q}=\frac{1}{f}$。该系统的频谱面位于 S' 所处的平面上,其位置不是固定的,随透镜的焦距 f 和点光源与透镜的距离 p 的变化而变化[6]。如果把相位掩模置于该系统的频谱面上,则相位掩模的纵向位置以及透镜的焦距也将成为密匙。图1右半部分是1个非标准傅里叶变换系统,它的输出面位于第2透镜的后焦面上,输入面(S' 所处平面)与第2个透镜的距离 d 可以自由变化,这样 d 也可作为密匙控制相位掩模的位置。设整个系统输入面(S 所处平面)的坐标为 (x_0,y_0),S' 所处平面的坐标为 (ξ,η),输出面的坐标为 (x,y)。RPM$_1$ 和 RPM$_2$ 分别为独立的随机相位函数 $\exp[\mathrm{j}n(x_0,y_0)]$ 和 $\exp[\mathrm{j}b(\xi,\eta)]$。系统加密时,待加密图像 $f(x_0,y_0)$ 与 $\exp[\mathrm{j}n(x_0,y_0)]$ 相乘完成空域编码,然后经第1个透镜 L$_1$ 作傅里叶变换,可得傅里叶频谱面上的光场分布[6]:

$$U(\xi,\eta)=c\exp\left[\mathrm{i}\pi m\lambda\frac{f-d_0}{f^2}(\xi^2+\eta^2)\right]\times F\{f(x_0,y_0)\}*F\{\exp[\mathrm{j}n(x_0,y_0)]\} \tag{1}$$

式中:$m=fq-d_0q+d_0f$;$\xi=\frac{f}{m\lambda}x_0$、$\eta=\frac{f}{m\lambda}y_0$。$U(\xi,\eta)$ 与第2块相位掩模 $\exp[\mathrm{j}b(\xi,\eta)]$ 相乘完成频域编码,再经过第2个透镜 L$_2$ 做傅里叶变换,最后可得输出平面上的光场分布[6]:

$$g(x,y)=c\exp[\mathrm{i}\pi\lambda(f-d)(x^2+y^2)]\times F\{U(\xi,\eta)\}\cdot F\{\exp[\mathrm{j}b(\xi,\eta)]\} \tag{2}$$

式中:$x=\frac{\xi}{\lambda f}=\frac{1}{\lambda f}\frac{f}{m\lambda}x_0=\frac{x_0}{m\lambda^2}$;$y=\frac{\eta}{\lambda f}=\frac{1}{\lambda f}\frac{f}{m\lambda}y_0=\frac{y_0}{m\lambda^2}$。显然(2)式是一个随机白噪声,可作为最后的加密图像。

解密时,(2)式不是 $U(\xi,\eta)$ 与 $\exp[\mathrm{j}b(\xi,\eta)]$ 乘积的严格傅里叶变换,存在着相位弯曲,所以对(2)式进行标准的逆傅里叶变换就不可能得到 $U(\xi,\eta)$ 与 $\exp[\mathrm{j}b(\xi,\eta)]$ 的乘积。根据光路的可逆性,我们可得到 $U(\xi,\eta)$ 与 $\exp[\mathrm{j}b(\xi,\eta)]$ 乘积的共轭。只要把 $g(x,y)^*$ 置于图1的右端输入,就可在距离透镜 d 处,S' 所处的平面上得到 $U(\xi,\eta)$ 与 $\exp[\mathrm{j}b(\xi,\eta)]$ 乘积的共轭,然后与 $\exp[\mathrm{j}b(\xi,\eta)]$ 相乘进行频域解码。同理,可以在原加密系统的输入面上得到 $f(x_0,y_0)$ 与 $\exp[\mathrm{j}n(x_0,y_0)]$ 乘积的共轭。如果 $f(x_0,y_0)$ 是正的实函数,则可用CCD接收解密图像。

2 安全性能分析

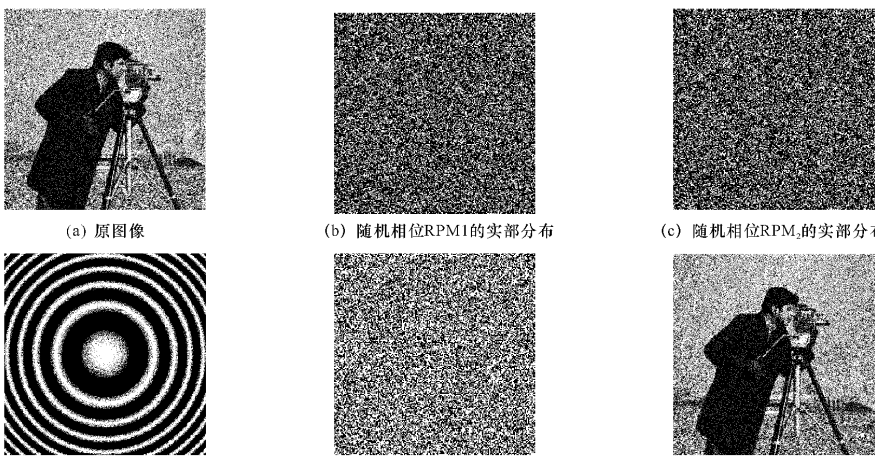
从上面的加、解密过程可以看出,采用不对称非标准傅里叶变换系统进行傅里叶变换时,傅里叶变换式前有一个相位因子,使光场产生了相位弯曲,因此解密时,系统不可能像 $4f$ 系统那样进行2次简单的逆傅里叶变换,必须利用加密图像的共轭 $g(x,y)^*$ 从原加密系统的输出端输入,在原加密系统的输入端接收解密图像。系统的有关参数 d_0、d、p(或 q)和 f 在解密时必须已知,否则就解不出原图像。具体分析如下。

根据菲涅耳衍射原理可知,如果解密相位掩模位置与透镜 L$_2$ 的距离不等于 d,则得不到 $U(\xi,\eta)$ 与 $\exp[\mathrm{j}b(\xi,\eta)]$ 乘积的共轭。同理,如果解密时 d_0 和 q 的大小与加密时不一致,将不能恢复原图像。另外,从(2)式可知,要想用1个对称的标准傅里叶变换系统获得 $U(\xi,\eta)$ 与 $\exp[\mathrm{j}b(\xi,\eta)]$ 的乘积,就必须设法抵消相位因子 $\exp[\mathrm{i}\pi\lambda(f-d)(x^2+y^2)]$。由于透镜的透过率函数 $\exp[\pm\pi\mathrm{i}(x^2+y^2)/\lambda f]$ 与该相位因子具有相同的形式,因此比较2式可知,若用1个透镜抵消此相位弯曲,那么这个透镜的焦距必须与 $1/\lambda^2(f-d)$ 相等;如果 f 和 d 未知,则不能抵消这个弯曲。因此,只能利用光路的可逆性解密和加密图像。由以上分析可知,采用该系统进行图像加密比 $4f$ 系

统多出几重钥匙,大大提高了系统的安全性能。

3 计算机模拟与分析

为了验证该方法的可行性,我们利用灰度图像进行计算机仿真实验,并验证在已知解密相位掩模而不知系统相关参数的情况下不可能解密出原图像。仿真时,采用波长为600 nm的发散球面波来照射不对称非标准傅里叶变换系统,取球面波的半径p为30 cm(或q为60 cm),透镜焦距f为20 cm,d_0为10 cm,d为15 cm,图像的像素为256×256。图2是对灰度图像进行加密和解密所得的仿真结果。图3是在已知解密相位掩模而不知系统相关参数的情况下,对灰度图像进行盲解密所得到的图像。

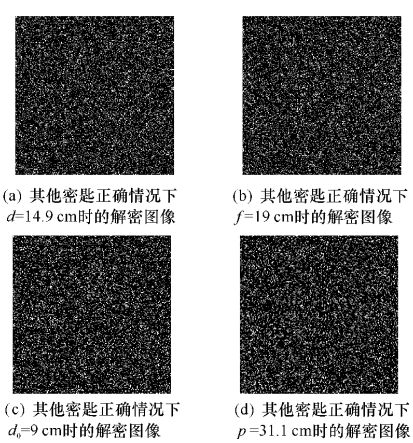


(a) 原图像 (b) 随机相位RPM1的实部分布 (c) 随机相位RPM$_2$的实部分布

(d) 球面波的实部分布 (e) 加密图像 (f) 正确密匙的解密图像

图2 仿真结果

Fig. 2 Simulation result



(a) 其他密匙正确情况下d=14.9 cm时的解密图像 (b) 其他密匙正确情况下f=19 cm时的解密图像

(c) 其他密匙正确情况下d_0=9 cm时的解密图像 (d) 其他密匙正确情况下p=31.1 cm时的解密图像

图3 盲解密图像

Fig. 3 Decrypted image with right phase mask but without any system related parameter

4 结论

从上述理论分析和模拟实验可以看出:在$4f$系统的基础上不增加系统元件,利用球面波照射不对称非标准傅里叶变换系统进行图像加密是完全可行的。由于采用不对称非标准傅里叶变换系统进行图像加密和解密,所以系统中每个透镜的输入面和输出面不象$4f$系统和分数傅里叶变换系统那样与透镜对称,并且系统的参数可以变化。因此,利用该系统加、解密时,除了与$4f$系统具有相同加密效果外,还成功地克服了$4f$系统中相位掩模的纵向位置不能作为密匙的缺点,系统具有不对称性。这些特点大大增强了系统的安全性能。

参考文献:

[1] REFREGIER P, JAVIDI B. Optical image encryption based on input plane and Fourier plane random encoding[J]. Opt. Lett., 1995, 20(7): 767-769.

[2] UNNIKRISHNAN G, JOSEPH J, SINGH K. Optical encryption by double-random phase encoding in the fractional Fourier domain[J]. Opt. Lett., 2000, 25(12): 887-889.

(下转第268页)