双随机相位图像加密的实值编码研究*

李 榕 李 萍
(华南师范大学物理与电信工程学院,广州 510631)

摘 要 提出了一种基于双随机相位的图像实值编码方法,该方法可应用于光学图像加密. 要编码的纯相位图像分别在空间域和频域加入随机相位掩膜,其中在频域将编码范围扩大 4 倍,经过光学系统的变换,将生成的图像取实部作为编码图像. 实值编码的图像利用与编码过程类似的方法进行解码,可以准确地重建原图像. 该编译码方法简单,编码图像是一个近似随机噪声的实值图像,便于数字图像的传输与输出.

关键词 光学加密;图像;双随机相位编码;实值编码
中图分类号 TN911 **文献标识码** A

0 引言

在日常工作和生活中,数字图像通信和存储中信息安全的地位越来越重要,如护照、信用卡、身份证的防伪,条码、生物识别图像和一些重要文件的网络传输等都涉及到图像加密. 光学信息处理技术由于具有高速的并行处理能力,以及信息可以隐藏在相位、波长、空间频率和偏振等光学变量之中的特点,所以它在信息加密方面的应用引起了国内外许多学者的研究兴趣[1~4,9]. 在图像加密的研究上,最具代表性的是 B. Javidi 等人提出的双随机相位编码技术[5],分别在空域和频域用两个随机相位掩膜对原图像编码. 编码图像是复振幅白噪声. 但是用该编码方法编码出的图像是一个复值图像,在某些应用场合,如传输或输出时只能取其部分信息,这样通过部分信息重构的原图像会严重失真. 文献[6,7]分别提出了一种单随机相位的实值编码和解码方法,编码图像是实值. 然而从图像加密的安全性考虑,它不如双随机相位编码方法好. 本文通过对双随机相位编码方法分析研究,提出了一种双随机相位实值编码解码方法,编码图像是一个实值图像,解码后可以完全重构原图像. 该方法可应用于数字图像通信和存储中的加密.

1 双随机相位实值编码及解码方法

1.1 双随机相位编码的基本方法

编码和译码的过程如图 1. 其中图 1(a)是编码过程.

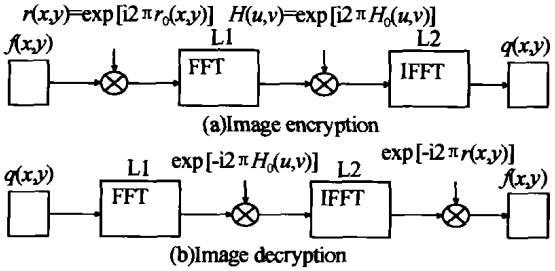


图 1 双随机相位编码的原理方框

Fig. 1 Block diagram of the double random phase encryption

原图像 $f_0(x,y)$是一个灰度图像,$f_0(x,y)$的取值范围在[0,1]之间. 首先将其转换为纯相位图像 $f(x,y)=\exp[\mathrm{i}2\pi f_0(x,y)]$,编码键 $r(x,y)$和 $H(u,v)$分别是空间域和频域的随机纯相位掩膜,$r(x,y)=\exp[\mathrm{i}2\pi r_0(x,y)]$,$H(u,v)=\exp[\mathrm{i}2\pi H_0(u,v)]$,其中 $r_0(x,y)$和 $H_0(u,v)$的取值范围都是[0,1].

$$g(x,y)=f(x,y)\,r(x,y)=\exp[\mathrm{i}2\pi f_0(x,y)]\cdot\exp[\mathrm{i}2\pi r_0(x,y)] \tag{1}$$

$$G(u,v)=\mathrm{FFT}[g(x,y)]=\mathrm{FFT}[f(x,y)\,r(x,y)] \tag{2}$$

$$Q(u,v)=G(u,v)H(u,v) \tag{3}$$

$$q(x,y)=\mathrm{IFFT}[Q(u,v)]=\mathrm{IFFT}[G(u,v)H(u,v)] \tag{4}$$

如果将式(4)的结果作为编码图像,则解码的过程如图1(b). 在频域加入解码随机相位掩膜 $H^*(u,v)$,* 号表示复数的共轭,即 $H^*(u,v)$是编码键 $H(u,v)$的共轭复数,在空间域加入解码随机相位掩膜 $r^*(x,y)$,$r^*(x,y)$是编码键 $r(x,y)$的共轭复数.

$$H^*(u,v)=\exp[-\mathrm{i}2\pi H_0(u,v)]$$

$$r^*(x,y)=\exp[-\mathrm{i}2\pi r(x,y)]$$

$$\mathrm{FFT}[q(x,y)]=\mathrm{FFT}[\mathrm{IFFT}[Q(u,v)]]=Q(u,v)=G(u,v)H(u,v) \tag{5}$$

$$Q(u,v)H^*(u,v)=G(u,v)H(u,v)H^*(u,v)=G(u,v) \tag{6}$$

*广东省自然科学基金(021089)、广东省教育厅自然科学研究项目(Z02020)资助
Tel:020-85214399 Email:lirong@scnu.edu.cn
收稿日期:2004-09-17

$$g(x,y)=\mathrm{IFFT}[G(u,v)] \tag{7}$$

$$g(x,y)\,r^*(x,y)=f(x,y)\,r(x,y)\,r^*(x,y)=f(x,y) \tag{8}$$

由式(8)可以看出解码图像与原图像完全相同

1.2　双随机相位实值编码方法

在一些应用场合，特别是光电混合系统中，要将编码图像传输或输出，往往要求编码图像是一个实值的图像，但是如果简单地将式(4)$q(x,y)$的实部或虚部作为编码图像，用上述方法解码解出的原图像严重失真．若取$q(x,y)$的实部作为编码图像

$$\mathrm{Re}[q(x,y)]=\mathrm{Re}[\mathrm{IFFT}[Q(u,v)]]=\mathrm{Re}[\mathrm{IFFT}[G(u,v)H(u,v)]] \tag{9}$$

根据二维傅里叶变换实部与虚部的性质[8]

$$\mathrm{FFT}[\mathrm{Re}[q(x,y)]]=[Q(u,v)+Q^*(-u,-v)]/2 \tag{10}$$

所以在频域解码得到

$$\mathrm{FFT}[\mathrm{Re}[q(x,y)]]H^*(u,v)=[Q(u,v)+Q^*(-u,-v)]H^*(u,v)/2=[G(u,v)H(u,v)\cdot H^*(u,v)+G^*(-u,-v)H^*(-u,-v)\,H^*(u,v)]/2=[G(u,v)+G^*(-u,-v)H^*(-u,-v)\cdot H^*(u,v)]/2 \tag{11}$$

再在空间域解码得到

$$\mathrm{IFFT}[[G(u,v)+G^*(-u,-v)H^*(-u,-v)\cdot H^*(u,v)]/2]r^*(x,y)=g(x,y)r^*(x,y)/2+\mathrm{IFFT}[G^*(-u,-v)H^*(-u,-v)H^*(u,v)]\cdot r^*(x,y)/2=f(x,y)r(x,y)r^*(x,y)/2+\mathrm{IFFT}[G^*(-u,-v)H^*(-u,-v)\,H^*(u,v)]\cdot r^*(x,y)/2=f(x,y)/2+\mathrm{IFFT}[G^*(-u,-v)\cdot H^*(-u,-v)\,H^*(u,v)]r^*(x,y)/2 \tag{12}$$

从解码的结果来看，式(12)中的$G^*(-u,-v)H^*(-u,-v)$是$G(u,v)H(u,v)$的反向共轭图像，与原图像没有函数关系，所以解出的图像严重失真．

如果扩大编码范围，可以减少反向共轭图像对原图像的影响[6]．为此，在频域将图像编码范围扩大为原来的四倍，用$G'(u,v)$表示，$G(u,v)$只占$G'(u,v)$的四分之一，$G'(u,v)$用矩阵表示为

$$G'(u,v)=\begin{bmatrix}G(u,v) & Z\\ Z & Z\end{bmatrix} \tag{13}$$

Z表示与原图像大小相同的全0矩阵，频域编码得到

$$\mathrm{IFFT}[G'(u,v)H(u,v)]=q(x,y) \tag{14}$$

取$q(x,y)$的实部作为编码图像，解码过程如下经过频域解码得到

$$\mathrm{FFT}[\mathrm{Re}[q(x,y)]]H^*(u,v)=[Q(u,v)+Q^*(-u,-v)]/2H^*(u,v)=[G'(u,v)H(u,v)\cdot H^*(u,v)+G'^*(-u,-v)H^*(-u,-v)\;H^*(u,v)]/2=[G'(u,v)+G'^*(-u,-v)H^*(-u,-v)\cdot H^*(u,v)]/2 \tag{15}$$

若忽略图像的第一行与第一列，则

$$G'(-u,-v)=\begin{bmatrix}Z & Z\\ Z & G^T(u,v)\end{bmatrix} \tag{16}$$

$G^T(u,v)$是$G(u,v)$的反向图像，由于$G'(-u,-v)$矩阵的左上四分之一是0矩阵，如果频域解码后只取左上四分之一作为频域解码结果，则式(15)第二项对解码结果没有影响，而第一项的左上四分之一恰好是$G(u,v)/2$．再按照式(7)、(8)的方法在空间域解码，可以准确地解出原图像$f(x,y)$．

2　仿真实验

将1．2节的实值编码解码方法进行计算机仿真实验．原图像$f_0(x,y)$是64×64象素的panda图像，图2所示是保持原编码范围的实值编码及解码方法仿真结果．其中图2(a)是原图像$f_0(x,y)$，图2(b)、2(c)分别是空间域的纯相位掩膜$r(x,y)$的实部和虚部，图2(d)、2(e)分别是频域的纯相位掩膜$H(u,v)$的实部和虚部，图2(f)、2(g)分别是编码图像$q(x,y)$的实部和虚部．如果将$q(x,y)$的实部作为编码结果，则解码图像$f(x,y)$的实部和虚部如图2(h)、2(i)，取其相位得到图2(j)的解码图像．比较图2(a)与图2(j)，可以看出解码图像严重失真．

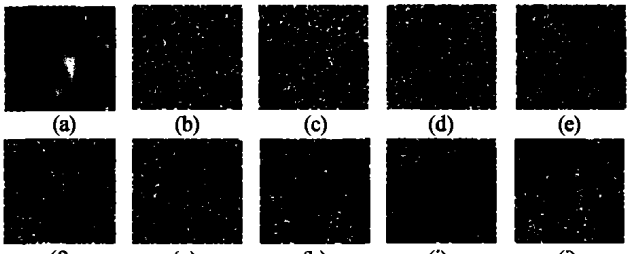


图2　未扩大频域图像的双随机相位实值编译码方法

Fig. 2　The double random phase real-value encryption and decryption without Fourier space image enlarged

图3所示是扩大编码范围的实值编码及解码算法的仿真结果．图3(a)是原图$f_0(x,y)$，图3(b)、3(c)分别是空间域的纯相位掩膜$r(x,y)$的实部和虚部，图3(d)、3(e)分别是频域的纯相位掩膜$H(u,v)$的实部和虚部，图3(f)、3(g)分别是在频域扩大4倍的图像$G'(u,v)$的实部和虚部，图3(h)、3(i)分别是编码图像$q(x,y)$的实部和虚部．如果将$q(x,y)$的实部作为编码结果，图3(j)、3(k)分别是频域解码图像的实部和虚部，只保留其左上四分之一的图像，再作空间域解码，图3(l)是解码图像．比较图3(a)的原图像与图3(l)的解码图像，可以看出解码图像可以准确地再现原图像．

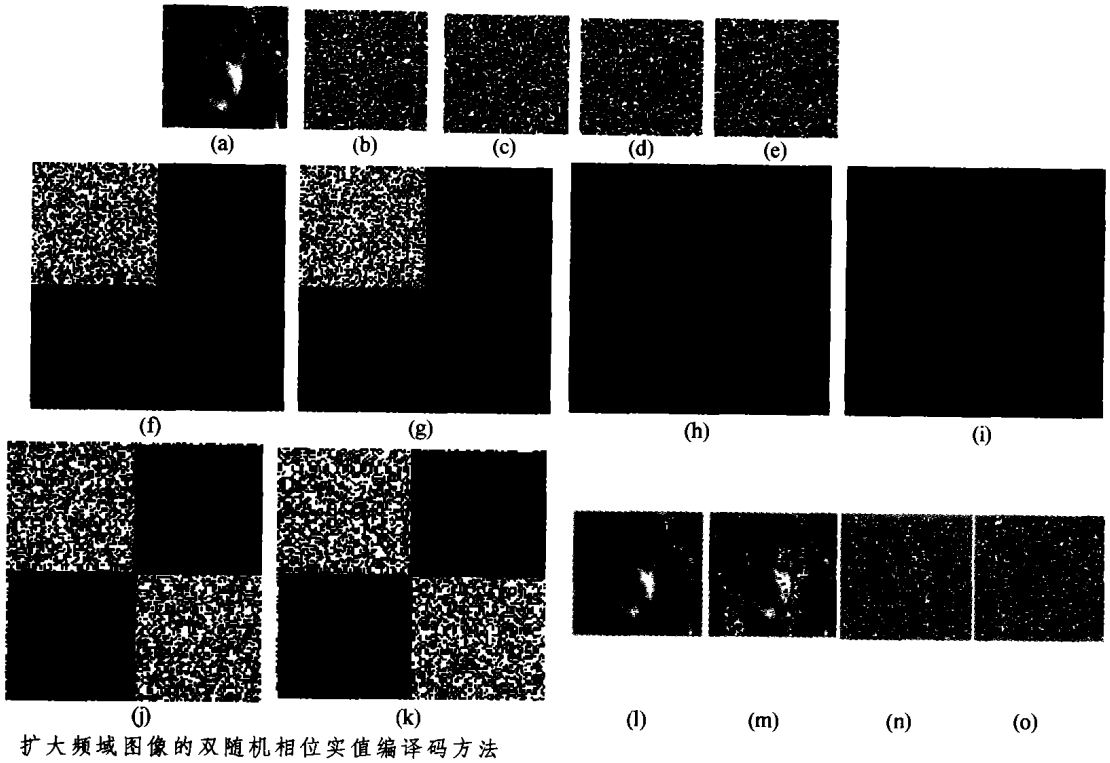


图 3 扩大频域图像的双随机相位实值编译码方法

Fig. 3 The double random phase real-value encryption and decryption method with Fourier space image enlarged

图 3(n)、3(o)分别是错误的时域解码键和错误的频域解码键时的解码图像，由此可以看出，对于未授权者如果没有两个解码键的信息，是无法解出原图像的，必须掌握两个正确的解码键才可以解出正确的图像．

在编码图像中加入高斯白噪声，仍然可以再现原图像．图 3(m)是实值编码加入均值为 0、方差为 0.01 时的解码图像．

3 结论

本文针对数字图像的光学加密问题，提出了一种基于双随机相位的实值编码解码方法，并进行了仿真实验．结果表明，该方法可以得到实值的编码图像，便于数字图像的传输与输出，解码图像失真小，能够准确地再现原图像，可用于护照、信用卡、身份证的防伪，条码、生物识别图像和一些重要文件的网络传输等方面的图像加密．

参考文献

1 Towghi N, Javidi B, Luo Z. Fully phase encrypted image processor. *J Opt Soc Am A*, 1999, **16**(8): 1915～1927

2 Mogensen P C, Glückstad J. Phase-only optical encryption. *Opt Lett*, 2000, **25**(8): 566～568

3 Chang H T. Image encryption using separable amplitude-based virtual image and iteratively retrieved phase information. *Opt Eng*, 2001, **40**(10): 2165～2171

4 Matoba O, Javidi B. Secure holographic memory by double-random polarization encryption. *Appl Opt*, 2004, **43**(14): 2915～2919

5 Refregier P, Javidi B. Optical image encryption based on input plane and fourier plane random encoding. *Opt Lett*, 1995, **20**(7): 767～769

6 李榕，李萍．基于随机相位实值编码的光学图像加密．光子学报，2004，**33**(5)：605～608
Li R, Li P. *Acta Photonica Sinica*, 2004, **33**(5): 605～608

7 Ohtsubo J, Fujimoto A. Pratical image encryption and decryption by phase-coding technique for optical security systems. *Appl Opt*, 2002, **41**(23): 4848～4855

8 Dudgeon D E, Mersereau M, 著．多维数字信号处理．北京：科学出版社，1991. 52～53
Dudgeon D E, Mersereau R M. Multidimensional Digital Signal Processing. Beijing: Science Press, 1991. 52～52

9 于力，朱邦和，刘树田．用于光学图像加密的分数傅里叶变换双相位编码．光子学报，2001，**30**(7)：904～907
Yu L, Zhu B H, Liu S T. *Acta Photonica Sinica*, 2001, **30**(7): 904～907

Research on the Image Security in Double Random Phase Real-value Encryption

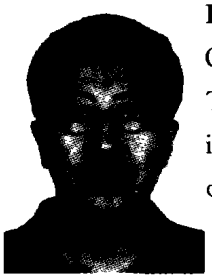
Li Rong, Li Ping

South China Normal University, Department of Physics, Guangzhou 510631

Received date: 2004-09-17

Abstract The double random phase real-value encryption and decryption method is proposed for the optical image security system. A phase-only image to be encrypted together with a random phase mask in space plane is Fourier transformed . Then it attached anther random phase mask in Fourier plane is enlarged and reverse-Fourier transformed . Real part of the result is used as an encrypted image. The decryption of the real-value encrypted image can be carried out in the same means with encryption. That gives the exact original image. The method of encryption and decryption is simply performed and encrypted image is real-valued, so it is convenient for output.

Keywords Optical security; Image; Double random phase; Real-value encryption



Li Rong received the M. S. degree from Northwestern Polytechnical University , Xi′an, China in 1989. He is now an associate professor in the School of Physics and Telecommunications Engineering, South China Normal University, China . His research interests include optical information processing, signal and image processing , communication systems.

(上接 960 页)

2 Howland D. A model for hospital system planning. in: Krewernas G, Morlat G, eds. Actes de la 3eme Conference International de Recherche Operationells, Oslo, 1963. Paris: Dunod, 1964. 203～212

●专利文献　专利申请者. 题名. 其他责任者(供选择). 附注项 (供选择). 专利国别, 专利文献种类, 专利号. 日期　**示例**

1 曾德超. 常速高速通用优化犁. 中国专利, 85203720, 1. 1986-11-13

2 Fleming G L, Martin R T. Ger Par. US patent, C08g, 139291. 1972-02-07

●学位论文　作者. 论文题目[学位论文]. 地名: 授予单位, 年. 起止页码

●译著　作者. 书名. 译者(译). 出版地, 年. 起止页码

3.9 照片及英文简介　来稿需提供第一作者的照片(可用数码照)和不多于 100 个实词的英文简历(包括出生年月、出生地、职称、职务、熟悉的学科和课题)

4 **投稿要求**　1)2005 年 1 月 1 日起实行网上投稿, 网址: www. photon. ac. cn; 2)文章最后一页请注明以下内容: 创新点说明 100～300 字; 推荐同行审稿专家 2～4 位(给出他们从事研究的学科和课题不超过 3 个, 通讯地址和 E-mail).

5 **稿件审理程序**

5.1 收到电子投稿后, 对初审通过的稿件, 将收稿回执(含审理费收取通知)、稿件状态查询帐号、密码、作者承诺书发邮件给作者. 收到稿件审理费后, 分送两位同行专家评审. 自审理费收到之日起 3 个月内未收到本刊审稿意见和通知, 作者可自行改投它刊, 但需告知编辑部.

5.2 本刊将对下列稿件作自动退稿处理: a. 收稿回执发出 2 个月而投稿手续仍办理不全的稿件; b. 修改意见发出 2 个月仍未修回的稿件; c. 版面费通知发出 1 个月而汇款未到的稿件.

6 **作者承诺书**　作者承诺书在收稿后发邮件给作者, 请全体作者签名并附单位盖章后寄回编辑部.

7 **收费标准**　每篇文章收稿件审理费 100 元; 文章 4 页以内收版面费 800 元; 超过 4 页的部分, 每页加收 200 元. 文章出版后为每篇文章作者免费提供 1 份正刊、10 份单行本, 并酌付稿酬.

8 **注意事项**

1)本刊反对一稿两投. 在投本刊前后投他刊、或在内刊登载等, 务必来函说明. 2)本刊已入编《中国学术期刊(光盘版)》、"中国期刊网"、"万方数据(ChinaInfo)系统科技期刊群"、"维普数据库"和"中国光学期刊网", 向本刊投稿并录用的文章, 将一律由编辑部统一纳入中国期刊网、万方数据(ChinaInfo)系统、维普数据库和中国光学期刊网, 进入因特网提供信息服务. 对版权有特殊要求者, 请事先声明. 3)本刊所付稿酬包含刊物内容上网服务及收录光盘版报酬, 不再另付.