doi:10.3788/gzxb20124103.0326

基于双随机相位编码的彩色图像加密技术

秦怡,郑长波

(南阳师范学院 物理与电子工程学院,河南 南阳 473061)

摘 要:为了实现仅用两个密钥对彩色图像进行加密,提出了一种基于光栅调制的彩色图像加密方法.该方法首先把彩色图像分成三基色分量:红,绿,兰.然后,把这三帧灰度图像分别用空间频率不同正弦振幅光栅调制,之后,再把调制结果进行叠加而形成一个实值目标图像,该目标图像包含了原始彩色图像的全部信息.对此目标图像进行双随机相位加密系统的加密,即实现了彩色图像的加密隐藏.由于正弦光栅的调制作用,R、G、B 灰度图像的频谱在实值目标图像的频谱中分离开来,通过选取合适的滤波窗口,就可以对他们的频谱分别提取并予以重建,并最终实现重构原始彩色图像.本文给出了理论分析和计算机模拟,实验结果证实了该方法的可行性.

关键词:图像加密;双随机相位编码;彩色图像;光栅调制

中图分类号:TP751 **文献标识码**:A **文章编号**:1004-4213(2012)03-0326-4

0 引言

随着信息技术的发展,图像已经成为信息表达的重要途径之一,因而图像的安全问题已成为信息安全的一个特别重要的研究领域.为保证图像的安全传送,在传送过程中要进行图像的加密和解密处理.目前已经有很多文献提出了针对图像的加密方法[1-8].其中 Refregier 和 Javidi 提出的双随机相位编码光学加密具代表性的成果[9-11],该系统在 4-f 系统的输入面和频谱面各放置一块随机相位板,先后对原始明文图像的空间信息和频谱信息做随机扰乱,从而使系统的输出信息的复振幅为平稳随机的白噪音,实现了加密的目的.在图像加密的研究对象中,彩色图像的加密具有重要的现实意义.由于彩色图像具有三个通道,通常无法将其作为一个整体进行处理,所以大多采用对彩色图像的三个通道分别加密的方法来实现.例如,文献[12-13]均是将彩色图像分解为 R、G、B 三个通道,分别采用波长复用无透镜菲涅尔全息法和分数傅里叶变换法对每一个通道分别进行双随机相位加密.这样不仅使得系统变得复杂,实现起来难度增大,而且在整个加密系统中,所必需的随机相位掩模的数量不再是 2 个,而变为 4 个或者更多,密钥数量的增多使得泄密的可能性增大.

本文提出了一种基于双随机相位编码系统的彩色图像加密的方法.对彩色图像的红、绿、蓝分量使用正弦光栅进行调制后再过叠加形成一个实值目标图像,之后再对该实值图像使用双随机相位编码系统进行加密.这样就实现了在密钥数量不变的情况下对彩色图像的加密过程,文中给出了理论分析及计算机模拟结果.

1 理论分析

1.1 双随机相位编码光学加密系统

双随机相位编码光学加密系统利用标准 4-f 系统来实现,如图 1 所示.$f(x,y)$是要被加密的图像,加密时,首先将输入信号 $f(x,y)$在空域乘以随机相位函数 $\exp[\mathrm{i}2\pi n(x,y)]$,之后经过傅里叶变换,在

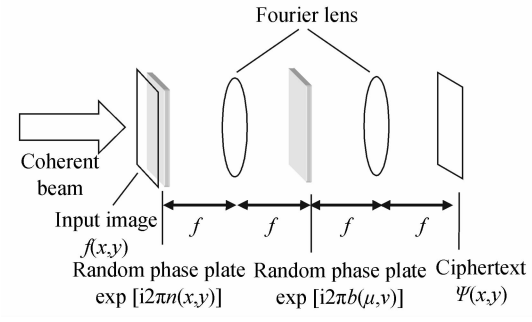

图 1 双随机相位加密系统示意图

Fig. 1 Schematic of double random phase encoding optical encryption system

频域被随机相位函数 $\exp[\mathrm{i}2\pi b(\mu,\nu)]$滤波,再经傅里叶逆变换,在输出面上得到密文 $\psi(x,y)$.整个加密过程可用公式表示为

基金项目:南阳师范学院青年基金(No. QN2012004)资助

第一作者:秦怡(1981—),男,讲师,硕士,主要研究方向为光电信息处理. Email: 641858757@qq.com

收稿日期:2011-10-11;**修回日期**:2011-11-07

$$\psi(x,y)=FT^{-1}\{FT(f(x,y)\exp[\mathrm{i}2\pi n(x,y)])\cdot \exp[\mathrm{i}2\pi b(\mu,\nu)]\} \quad (1)$$

式中，$n(x,y)$和 $b(x,y)$ 是均匀分布在[0,1]上的独立白噪音矩阵. FT 与 FT^{-1}分别表示傅里叶变换与傅里叶逆变换. 可以证明，加密后的密文 $\psi(x,y)$为平稳随机白噪音. 解密时，将密文 $\psi(x,y)$置于标准 4-f 系统的输入平面，经傅里叶变换后，在频谱平面上用解密密钥 $\exp[-\mathrm{i}2\pi b(\mu,\nu)]$滤波，再经傅里叶逆变换和 $\exp[-\mathrm{i}2\pi n(x,y)]$调制，即可恢复出 $f(x,y)$. 如果在输出面用 CCD 探测并记录 $f(x,y)$，因图像 $f(x,y)$为正实函数，CCD 可以将相位因子 $\exp[\mathrm{i}2\pi n(x,y)]$滤掉，这样在解密过程中可以不利用 $\exp[-\mathrm{i}2\pi n(x,y)]$进行调制，只需恢复出 $f(x,y)\exp[\mathrm{i}2\pi n(x,y)]$即可.

1.2　彩色图像的单矩阵存储及加密

彩色图像由三个独立分量组成，如在 RGB 空间，由 R、G、B 三个分量组成，在 HIS 空间由 H、I、S 三个分量组成等等，下面以 RGB 空间为例进行讨论. 对于 R、G、B 三基色分量，每一个均为灰度矩阵，如果能够在单个矩阵中同时存储这三个灰度矩阵，就实现了在单个矩阵中存储彩色图像的目的. 再使用双随机相位编码加密系统对这个矩阵加密，即实现了彩色图像的加密. 为了在单个矩阵中同时存储这三个矩阵，提出采用以下的方法. 设 $f_R(x,y)$，$f_G(x,y)$，$f_B(x,y)$分别是被加密彩色图像的 R、G、B 分量. 首先构造三个二维正弦振幅光栅 $G_1(x)$，$G_2(x)$，$G_3(x)$.

$$G_1(x)=m_0+m\cos 2\pi\mu_1 x \quad (2)$$

$$G_2(x)=m_0+m\cos 2\pi\mu_2 x \quad (3)$$

$$G_3(x)=m_0+m\cos 2\pi\mu_3 x \quad (4)$$

式中，m_0，m 为常量，μ_1，μ_2，μ_3 为光栅的空间频率. 然后用这三个空间频率不同的光栅对三个基色分量进行调制，即令

$$g_1(x,y)=f_R(x,y)G_1(x) \quad (5)$$

$$g_2(x,y)=f_G(x,y)G_2(x) \quad (6)$$

$$g_3(x,y)=f_B(x,y)G_3(x) \quad (7)$$

最后. 将以上三个分量进行叠加，得到

$$g(x,y)=g_1(x,y)+g_2(x,y)+g_3(x,y) \quad (8)$$

显然，实矩阵 $g(x,y)$里面包含了图像 $f(x,y)$的三基色矩阵的信息，对矩阵 $g(x,y)$使用双随机相位编码加密系统进行加密，就实现了对彩色图像的加密过程. 这里的问题是，能否从 $g(x,y)$中把 $f_R(x,y)$，$f_G(x,y)$，$f_B(x,y)$重新提取出来？答案是肯定的.

为了从 $g(x,y)$还原出 $f_R(x,y)$，$f_G(x,y)$，$f_B(x,y)$，首先对 $g(x,y)$做二维傅里叶变换

$$G(\mu,\nu)=FT[g(x,y)]=m_0F_R(\mu,\nu)+mF_R(\mu+\mu_1,\nu)+mF_R(\mu-\mu_1,\nu)+m_0F_G(\mu,\nu)+mF_G(\mu+\mu_2,\nu)+mF_G(\mu-\mu_2,\nu)+m_0F_B(\mu,\nu)+mF_B(\mu+\mu_3,\nu)+mF_B(\mu-\mu_3,\nu) \quad (9)$$

式中，FT 表示傅里叶变换，$F_R(\mu,\nu)$，$F_G(\mu,\nu)$，$F_B(\mu,\nu)$分别表示 $f_R(x,y)$，$f_G(x,y)$，$f_B(x,y)$的傅里叶变换. 首先考察式(9)中用黑色下划线标出的这一项. 它表明，在 $g(x,y)$的频谱面 $G(\mu,\nu)$上，R 分量 $f_R(x,y)$的频谱形成了三个部分，这三个部分完全相同，但处于不同的位置. 其中，$t_0F_R(\mu,\nu)$的中心位于坐标原点(0,0)，$tF_R(\mu-\mu_1,\nu)$的中心位于$(\mu_1,0)$，$tF_R(\mu+\mu_1,\nu)$的中心位于$(-\mu_1,0)$. 显然，调制光栅的空间频率 μ_1 决定了这三者中心距离的远近. μ_1 越大，这三者互相距离越远，反之越近. 这个分析同样适用于另外两个分量. 这样，只要恰当的选取 μ_1，μ_2，μ_3，就可以实现三基色分量在 $g(x,y)$频谱面上的分离，进而通过选取相应的滤波窗口，经频域的滤波就可以把这三个分量再分别提取出来. 例如要提取 $f_R(x,y)$分量，那么可以选择在 $G(\mu,\nu)$中单独保留 $tF_R(\mu+\mu_1,\nu)$项，同样也可以选择单独保留 $tF_R(\mu-\mu_1,\nu)$项，然后再进行傅里叶逆变换，这样就再现出来了 $f_R(x,y)$. 但是无法单独保留 $t_0F_R(\mu,\nu)$这项，因为原点处的频谱是 $t_0F_R(\mu,\nu)$，$t_0F_G(\mu,\nu)$及 $t_0F_B(\mu,\nu)$的叠加，这三者无法实现空间上的分离.

这样就成功地把彩色图像的 R、G、B 数据矩阵存储到了同样大小的矩阵 $g(x,y)$里面，实现了在单个灰度矩阵中储存多维信息信息的目的. 之后再对实矩阵 $g(x,y)$进行双随机相位编码加密，也就实现了在单数据矩阵的彩色图像的加密隐藏.

2　实验结果

为了验证所提方法的有效性，在 PC 机上使用 MATLAB7.0 进行了实验. 被测试的图片为 peppers，大小为 512×512 pixel. 图 2 给出了采用正弦振幅光栅对原始彩色图像的 R、G、B 分量进行调制的过程. 图 2(a)、(b)、(c)分别为为原始图像的 R、G、B 分量，图 2(d)、(e)、(f)是用来对其进行调制的、空频率不同的正弦光栅 G_1、G_2、G_3. 其中 G_1 的空间频率最高，G_2 次之，G_3 的空间频率最低. 图 2(g)、(h)、(i)是图 2(a)、(b)、(c)分别被 G_1、G_2、G_3 所调制后的结果.

图 3(a)是图 2(g)、(h)、(i)叠加之后的结果，这个图像是实值目标图像，即第 2 部分讨论中所定义的 $g(x,y)$，它包含了原始彩色图像的全部信息，对其使用双随机相位编码系统进行加密，结果如图

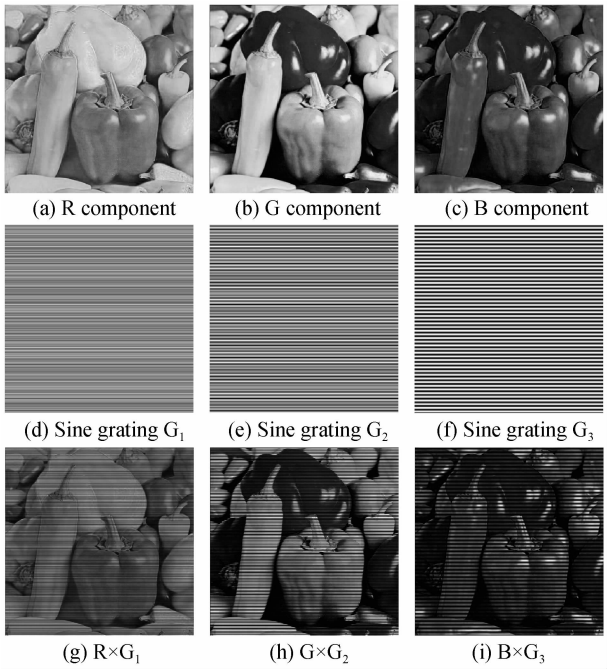

图 2 正弦光栅调制过程

Fig. 2 Process of modulation utilizing sine gratings

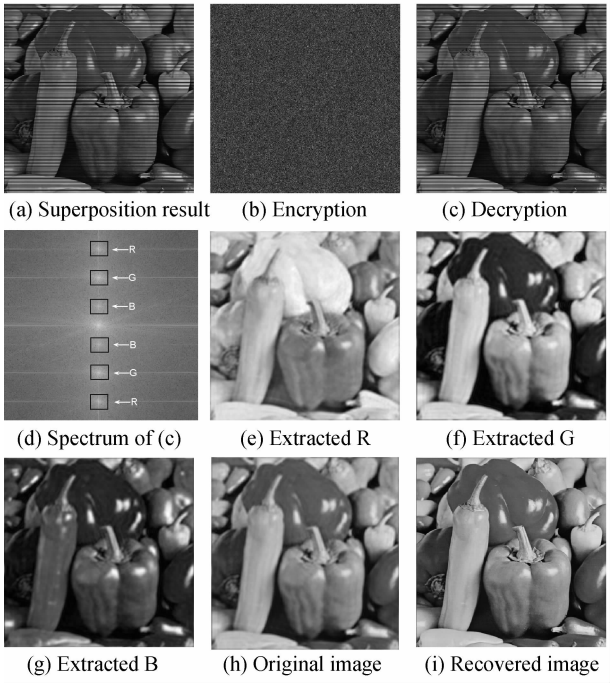

图 3 加密及解密过程

Fig. 3 Process of encryption and decryption

3(b)所示，至此就实现了对彩色图像的加密. 图 3(c)是使用正确的密钥对图 3(b)进行解密的结果，与图 3(a)相吻合. 图 3(d)为图 3(c)的傅里叶变换，即目标图像的频谱. 正如第 2 部分的分析，对于每一个分量，被正弦光栅调制后的频谱在 $g(x,y)$ 面上会形成三个与其原频谱完全相同的三个部分，其中一个在原点，另外两个对于原点呈对称分布. 由于对 R 分量采用空间频率最高的光栅进行调制，因此其另外两个频谱距离原点最远，在其频谱中心右边用字符‘R’标出. 同理，对 G，B 两个分量的频谱同采取的类似的标注.

图 3(e)、(f)、(g)是对图 3(d)采用相应的滤波窗口进行滤波，进而使用傅立叶逆变换而重建出来的原始图像的 R、G、B 分量. 滤波窗口在 3(d)中用黑色方框标识出来. 从提取的 R、G、B 分量可以看出，它们较原始图像显得模糊，这是由于滤波窗口的作用，一些高频成分被去除. 图 3(h)和图 3(i)分别是原始彩色图像和用提取出来的 R、G、B 分量重构的彩色图像. 从图中可以看出，除了损失一部分高频成分之外，重构图像和原始图像非常逼真.

从该方法的原理可以看出，其充分利用了图像频域的空间. 通过改变调制光栅的空间频率，可以方便地调整 R、G、B 分量频谱在目标图像频谱图中的位置，从而可以优化滤波窗口的选择来减少频谱的交叠，从而可以更加准确地恢复出 R、G、B 分量，也即更加准确地重建出原始彩色图像.

3 结论

本文提出了一种对彩色图像进行加密的方法，该方法采用光栅调制的方法把原彩色图像的 R、G、B 分量矩阵储存在一个实值矩阵之中，再对该实值矩阵使用双随机相位编码系统进行加密. 与通常的彩色图像加密方法相比，由于只需对实值目标图像进行双随机相位加密，因而降低了系统的复杂性，并且使系统必需的随机相位掩模数量减少为两个，使得加密过程变得更简单，更安全. 理论分析及计算机模拟结果证实了该方法的有效性.

参考文献

[1] SHEN Li-na, LI Jun, CHANG Hong-sen. Image encryption based on joint transform correlator and phase-shifting digital holography[J]. *Acta Photonica Sinica*, 2008, **37**(10): 2114-2117.
沈丽娜，李军，常鸿森. 基于联合变换相关及相移干涉的图像加密[J]. 光子学报，2008，**37**(10)：2114-2117.

[2] SUN Min, SU Xian-yu. Technology of double random phase encode data hidden in RGB images[J]. *Acta Photonica Sinica*, 2008, **37**(2): 320-324.
孙敏，苏显渝. 基于 RGB 传输的双随机相位加密隐藏技术[J]. 光子学报，2008，**37**(2)：320-324.

[3] DENG Xiao-peng. Optical encryption based on public key distribution system[J]. *Acta Photonica Sinica*, 2010, **39**(7): 1263-1267.
邓晓鹏. 基于公匙密匙分配体制的光学加密系统[J]. 光子学报，2010，**39**(7)：1263-1267.

[4] GAI Qi, WANG Ming-wei, LI Zhi-lei, *et al*. Doubled random phase encryption based on discrete quaternion Fourier transforms[J]. *Acta Physica Sinica*, 2008, **57**(11): 6955-6961.
盖琦，王明伟，李智磊，等. 基于离散四元数傅里叶变换的双随机相位加密技术[J]. 物理学报，2008，**57**(11)：6955-6961.

[5] LIU Fu-min, ZHAI Hong-chen, YANG Xiao-ping. Kinoform-based iterative random phase encryption[J]. *Acta Physica Sinica*, 2003, **52**(10): 2462-2465.

刘福民，翟宏琛，杨晓苹. 基于相息图迭代的随机相位加密[J]. 物理学报，2003，**52**(10)：2462-2465.

[6] KISHK S，JAVIDI B. Information hiding technique with double phase encoding[J]. *Applied Optics*，2002，**41**(26)：5462-5470.

[7] SI-TU Guo-hai，ZHANG Jing-juan. Multiple-image encryption by wavelength multiplexing[J]. *Optics Letters*，2005，**30**(11)：1306-1308.

[8] HE M Z，CAI L Z，LIU Q，*et al*. Multiple image encryption and watermarking by random phase matching[J]. *Optics Communications*，2005，**247**：29-37.

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

[10] PENG Xiang，TANG hong-qiao，TIAN Jin-dong. Ciphertext-only attack on double random phase encoding optical encryption system[J]. *Acta Physica Sinica*，2007，**56**(5)：2629-2635.
彭翔，汤红乔，田劲东. 双随机相位编码光学加密系统的唯密文攻击[J]. 物理学报，2007，**56**(5)：2629-2635.

[11] PENG Xiang，ZHANG Peng，WEI Heng-zheng，*et al*. Known-plaintext attack on optical encryption based on double random phase keys[J]. *Optics Letters*，2006，**31**(8)：1044-1046.

[12] CHEN Lin-fei，ZHAO Dao-mu. Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms[J]. *Optics Express*，2006，**14**(19)：8552-8559.

[13] JOSHI M，SHAKHER C，SINGH K. Color image encryption and decryption using fractional Fourier transform[J]. *Optics Communications*，2007，**279**(1)：35-42.

Color Image Encryption Based on Double Random Phase Encoding

QIN Yi，ZHENG Chang-bo

(*College of Physics and Electronic Engineering*，*Nanyang Normal University*，*Nanyang*，*Henan* 473061，*China*)

Abstract：For the purpose of color image encryption using two keys，a method based on grating modulation is proposed. First of all，a color image is separated into three components：red，green，and blue. The three grey images are multiplied by sine gratings with different spatial frequencies，and a superposition of the modulated results is introduced. Thus a real-valued target image that contains the whole information of the color image is obtained. Then the target image is encrypted using double phase encoding system，which means the original color image is encrypted. Due to the introduction of the sine gratings，the R，G，B frames are able to be spatially separated，so the color map can be reconstructed and the original color image can be recovered. Both theoretical analysis and simulations are proposed，and the validity of this method is verified by experimental results.

Key words：Image encryption；Double random phase encoding；Color image；Grating modulation