单通道彩色图像加密技术研究

强俊杰,姚丽莉,冯少彤,袁操今,聂守平

(南京师范大学江苏省光电技术重点实验室,江苏 南京 210023)

[摘要] 研究了一种基于双随机相位编码的单通道彩色图像加密算法.在该算法中,采用正弦光栅对彩色图像进行预处理,使得彩色图像可以单通道加密.两个随机相位掩膜函数构成了对预处理图像加密的双相位(即密钥),保证了彩色图像单通道加密的安全性.由于解密图像的画质不是很好,故采用零级融合的方法加以改善.同时,针对加密图像作了剪切攻击模拟实验.模拟实验结果证实了该算法的有效性.

[关键词] 正弦光栅,双随机相位加密,零级融合,剪切攻击

[中图分类号]TP391.9 [文献标志码]A [文章编号]1672-1292(2015)04-0041-06

Research on Single Channel Color Image Encryption Technology

Qiang Junjie, Yao Lili, Feng Shaotong, Yuan Caojin, Nie Shouping

(Key Laboratory for Opto-Electronic Technology of Jiangsu Province, Nanjing Normal University, Nanjing 210023, China)

Abstract: The paper studies a single channel based on double random phase encoding color image encryption algorithm. In this algorithm, the sinusoidal grating is adopted to preprocess color image, and the color image can be encrypted in the single channel. Two random phase mask function together constitute the double phase of preprocessing image encryption, which guarantees the safety of the single channel color image encryption. As the decrypted image quality is not very good, the zero level fusion method can be improved. At the same time, the shear attack simulation experiment on encryption image is conducted. Simulation results confirm the effectiveness of the algorithm.

Key words: sine grating, double random phase encryption, zero level fusion, shear attack

随着信息技术的发展,图像已成为人们进行信息交流的一种重要方式.与此同时,人们对于图像信息安全的要求也越来越高.为保证图像的安全传输,在传输过程中需对图像信息进行必要的加密及解密处理.目前针对图像信息加密的方法众多[1-7],其中双随机相位加密技术[1-6]采用的是光学方法对图像的空域和频域同时进行加密,其基本思想是采用两个互相独立的随机相位模板将图像加密成平稳的白噪声,在不知道空域和频域密钥的情况下不可能恢复出原始图像.同时,该方法具有高保密性、光学并行加密等优点,应用十分广泛.因此,双随机相位加密已逐步成为光学加密的基础.

近年来光学加密技术越来越受到人们的关注,文献[8]采用变形分数傅里叶变换替换傅里叶变换的方法,提高了图像的保密性能;文献[9]基于光全息图强脆弱性的特性提出了混合图像加密算法,将Arnold置乱、基于Twister的灰度置乱与光全息图加密相结合,提高了图像的强脆弱性;文献[10]则采用了非对称光学加密方法实现了图像的加密,提高了图像的保密性能.文献[8,10]均涉及到双随机相位加密,但其加密对象均为灰度图像.

目前图像加密算法多数是对灰度图像的加密,而对彩色图像的加密通常采用三通道分别加密的方法[11].对三通道分别进行加密,不仅使得系统变得复杂,也增大了实现难度,且在整个加密系统中,由于每个通道加密一次均需要2个随机相位掩膜函数(密钥),此类加密意味着需要6个甚至更多的密钥,不利于

收稿日期:2015-06-26.

基金项目:国家自然科学基金(61377003、61275133)、南京师范大学高层次人才科研启动项目(184080H20162)、南京师范大学青年领军人才培养项目(184080H20178).

通讯联系人:聂守平,博士,教授,研究方向:光电图像处理. E-mail:nieshouping@njnu.edu.cn

密钥的保存及发布.

本文研究了一种单通道彩色图像加密算法,其基本思路是利用不同频率的正弦光栅对彩色图像的三基色分量分别进行调制,将调制后的3幅灰度图像叠加成一幅灰度图像.在此基础上,利用双随机相位加密方法对预处理灰度图像进行加密.为了重构解密图像,可选择合适尺寸的滤波窗口提取相应的频谱,并与零级低频信息进行融合重构出解密图像.

1　基本原理

设 $f_r(x,y)$ 、$f_g(x,y)$ 、$f_b(x,y)$ 为彩色图像的三基色分量,以红色分量为例,构造正弦光栅 $g_1(x)$:

$$g_1(x)=m_0+m_1\cos 2\pi\omega_1 x\ , \tag{1}$$

式中, m_0 、m_1 为常量, ω_1 为正弦光栅的空间频率.正弦光栅 $g_1(x)$ 对红色分量 $f_r(x,y)$ 的调制可以表示为:

$$G_1(x,y)=f_r(x,y)g_1(x)\ . \tag{2}$$

同样,可以构造正弦光栅 $g_2(y)$ 、$g_3(y)$:

$$g_2(y)=m_0+m_1\cos 2\pi\omega_2 y\ , \tag{3}$$

$$g_3(y)=m_0+m_1\cos 2\pi\omega_3 y\ . \tag{4}$$

正弦光栅方向以及空间频率的不同,是为了避免频谱信息的交叠.正弦光栅对绿色分量及蓝色分量的调制可以表示为:

$$G_2(x,y)=f_g(x,y)g_2(y)\ , \tag{5}$$

$$G_3(x,y)=f_b(x,y)g_3(y)\ . \tag{6}$$

将三基色分量的调制结果 $G_1(x,y)$ 、$G_2(x,y)$ 、$G_3(x,y)$ 进行叠加得到预处理灰度图像,即待加密图像 $G(x,y)$:

$$G(x,y)=G_1(x,y)+G_2(x,y)+G_3(x,y)\ . \tag{7}$$

这样即可将彩色图像的3个分量融合为一幅灰度图像.以下将利用双随机相位加密方法对待加密图像 $G(x,y)$ 进行加密.如图1(a)所示,首先将待加密图像在空域内乘以随机相位掩膜函数 $e^{i2\pi n(x,y)}$,经傅里叶变换后,利用随机相位掩膜函数 $e^{i2\pi b(\mu,v)}$ 滤波得到的结果再经傅里叶逆变换,最终在输出平面上得到加密图像 $\Psi(x,y)$.其中,随机相位模板的作用是将待加密图像 $G(x,y)$ 加密成一幅平稳分布的白噪声图像 $\Psi(x,y)$,且随机相位模板自身作为加密系统的密钥.该过程可以表示为:

$$\Psi(x,y)=\mathrm{FT}^{-1}\left\{\mathrm{FT}(G(x,y)\cdot e^{i2\pi n(x,y)})\cdot e^{i2\pi b(\mu,v)}\right\}\ , \tag{8}$$

式中,FT表示傅里叶变换,FT^{-1} 表示傅里叶逆变换; $\boldsymbol{n}(x,y)$ 、$\boldsymbol{b}(\mu,v)$ 是均匀分布在 [0,1] 上的白噪声矩阵; $G(x,y)$ 为待加密图像, $\Psi(x,y)$ 为加密后的图像.

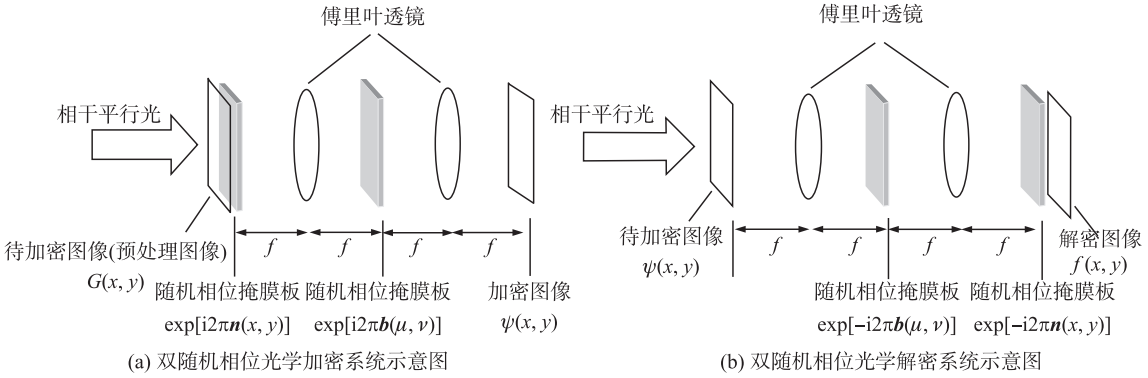


图1　双随机相位光学加密及解密系统示意图

Fig.1　Schematic diagram of double random phase optical encryption and decryption system

图1(b)所示为双随机相位解密系统示意图.解密过程的数学表达式可表示为:

$$f'(x,y)=\mathrm{FT}^{-1}\left\{\mathrm{FT}(\Psi(x,y))\cdot e^{-i2\pi b(\mu,v)}\right\}\cdot e^{-i2\pi n(x,y)}\ . \tag{9}$$

不难发现,图像解密过程的实质是加密的逆过程,解密过程分为4个步骤:首先对待解密图像进行傅

里叶变换,将傅里叶变换后的结果利用加密系统频谱密钥的复共轭 $e^{-i2\pi b(\mu,\upsilon)}$ 进行调制,将调制后的结果经傅里叶逆变换,采用加密系统空域密钥的复共轭 $e^{-i2\pi n(x,y)}$ 来调制上述结果,最后在输出平面上即可得到解密图像 $f'(x,y)$.

2 实验结果

为验证上述方法的可行性,图2给出了对512×512像素的彩色图像的实验结果.其中,图2(a)为原始图像;图2(b)为经过3个正弦光栅调制后的待加密图像,其包含原始彩色图像的所有信息,以确保彩色图像能够单通道表示;图2(c)为采用密钥 $\boldsymbol{n}(x,y)$ 和 $\boldsymbol{b}(\mu,\upsilon)$ 加密后得到的振幅图像.从实验结果可以看出,加密图像为广义平稳白噪声.

(a) 原彩色图像　(b) 正弦光栅调制图像　(c) 双随机相位加密图像

图2　彩色图像、预处理图像及加密图像

Fig.2　Color image, preprocessing image and encrypted image

经过双随机相位解密系统后的解密图像如图3(a)所示,对其进行傅里叶变换,即:

$$F(\mu,\upsilon)=\mathrm{FT}[f'(x,y)]=m_0F_r(\mu,\upsilon)+m_1F_r(\mu+\omega_1,\upsilon)+m_1F_r(\mu-\omega_1,\upsilon)+m_0F_g(\mu,\upsilon)+m_1F_g(\mu,\upsilon+\omega_2)+$$
$$m_1F_g(\mu,\upsilon-\omega_2)+m_0F_b(\mu,\upsilon)+m_1F_b(\mu,\upsilon+\omega_3)+m_1F_b(\mu,\upsilon-\omega_3)\,, \tag{10}$$

式中, $f'(x,y)$ 为解密图像; $F_r(\mu,\upsilon)$ 、$F_g(\mu,\upsilon)$ 、$F_b(\mu,\upsilon)$ 分别为对应于三基色分量 $f_r(x,y)$ 、$f_g(x,y)$ 、$f_b(x,y)$ 的傅里叶变换结果.图3(b)所示为 $F(\mu,\upsilon)$ 的分布图,可以看出,正弦光栅的空间频率 ω_1 、ω_2 和 ω_3 决定了三基色分量频谱的分布区域.图4所示的3幅图像分别为图3(b)中的各颜色分量经傅里叶逆变换得到的结果.

(a) 解密图像　(b) 解密图像的频谱图

图3　解密图像及其频谱图像

Fig.3　Decrypted image and spectrum image

将图4中的3个分量进行融合,结果如图5(a)所示.该彩色图像基本恢复了原彩色图像的颜色特征,但与原图相比,其对比度及亮度明显降低,为此将图5(a)由RGB色彩空间转换至HSI色彩空间[12],利用零级频谱解码图像(如图5(b)所示)来替换图5(a)的I分量,然后由HSI色彩空间转换回RGB色彩空间,即可重构出融合零级后的彩色图像,如图5(c)所示.

(a) 红色分量　　(b) 绿色分量　　(b) 蓝色分量

图4　三基色分量

Fig.4　Three primary color components

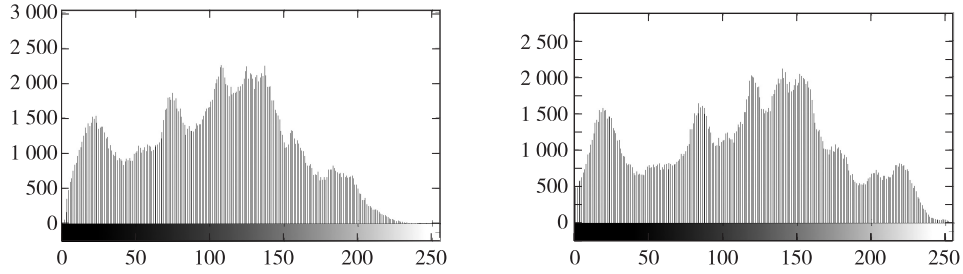
(a) 未经零级融合的图像　　(b) 零级频谱解码的图像　　(c) 融合零级后重构的图像

图5　未经零级融合图像、零级频谱图像、融合零级图像

Fig.5　Image of without the zero level fusion, zero order spectrum and with the zero level fusion

图6(a)、(b)分别给出了图5(a)及图5(c)的灰度直方图. 不难发现,图6(a)灰度范围比较狭窄,没有覆盖整个灰度范围[0,255],因此对比度不好. 而图6(b)的像素灰度范围覆盖了整个灰度范围[0,255]. 由此可见,采用HSI色度变换融合零级重构图像的方法可以提高图像的对比度,使图像具有较好的视觉效果. 此外,由于图6(a)的灰度值在255及其附近的点的数量明显少于图6(b),故图5(a)的亮度没有图5(c)高.

综上所述,采用HSI色度变换融合零级重构图像的方法不仅提高了图像的对比度,使图像更加清晰,而且提高了图像的整体亮度.



(a) 图5(a)的灰度直方图　　(b) 图5(c)的灰度直方图

图6　零级频谱融合前后的灰度直方图

Fig.6　The gray histogram before and after fusion of zero order spectrum

此外,本文还针对加密图像作了剪切模拟实验. 图7给出了对加密图像作不同程度剪切后的实验结果,图8是经剪切攻击后恢复得到的解密图像.

(a) 剪切1/256　(b) 剪切1/64　(c) 剪切1/16

图7　不同程度的剪切攻击

Fig.7　Shear attack of different levels

(a) 剪切1/256解密图　(b) 剪切1/64解密图　(c) 剪切1/16解密图

图8　剪切攻击后的恢复图像

Fig.8　Image restoration after shear attack

表1为针对加密图像做剪切攻击实验,其实验数据如表1所示,重构的解密图像仍然具有较好的视觉效果.

表1　剪切攻击处理

Table 1　Treatment of shear attack

剪切攻击		$\frac{1}{256}$	$\frac{1}{64}$	$\frac{1}{16}$
评价标准	PSNR	71.210 4	70.969 3	68.742 4
	NC	0.922 03	0.921 85	0.888 27
	MSE	0.004 920 8	0.005 201 8	0.008 686 3

3　结论

本文研究了一种基于双随机相位的单通道彩色图像加密算法.该算法的核心是采用正弦光栅将彩色图像三基色分量进行调制,使得彩色图像能够单通道加密.加密过程中,不需分别对三基色分量进行加密.加密所需的密钥数量由原先的6个缩减为2个,这样既能提高加密效率,又降低了系统的复杂性.采用零级融合的方法提高了未经零级融合的图像的对比度及亮度.此外,该算法对剪切攻击具有较好的鲁棒性.理论分析及MATLAB仿真结果证实了该算法的有效性.

[参考文献](References)

[1] 刘福明,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):2 462-2 465.
LIU F M,ZHAI H C,YANG X P. Kinoform-based iterative random phase encryption[J]. Acta physics sinica,2003,52(10):2 462-2 465.(in Chinese)

[2] 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):2 629-2 635.
PENG X,TANG H Q,TIAN J D. Ciphertext-only attack on double random phase encoding optical encryption system[J]. Acta

physics sinica,2007,56(5):2 629-2 635.(in Chinese)

[3] 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.
SUN M,SU X Y. Technology of double random phase encode data hidden in RGB images[J]. Acta photonica sinica,2008,37(2):320-324.(in Chinese)

[4] 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):6 955-6 961.
GAI Q,WANG M W,LI Z L,et al. Doubled random phase encryption based on discrete quaternion Fourier transforms[J]. Acta photonica sinica,2008,57(11):6 955-6 961.(in Chinese)

[5] 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):2 114-2 117.
SHEN L N,LI J,CHANG H S. Image encryption based on joint transform correlator and phase-shifting digital holography[J]. Acta photonica sinica,2008,37(10):2 114-2 117.(in Chinese)

[6] KISHK S,JAVIDI B. Information hiding technique with double phase encoding[J]. Applied optics,2002,41(26):5 462-5 470.

[7] 邓晓鹏.基于公钥密钥分配体制的光学加密系统[J].光子学报,2010,39(7):1 263-1 267.
DENG X P. Optical encryption based on public key distribution system[J]. Acta photonica sinica,2010,39(7):1 263-1 267.(in Chinese)

[8] 王红霞,赵玮,刘长文,等.基于变形分数傅里叶变换的六重密钥图像加密[J].光子学报,2007,36(4):759-762.
WANG H X,ZHAO W,LIU C W,et al. Six security key for image encryption based on anamorphic fractional Fourier transform[J]. Acta photonica sinica,2007,36(4):759-762.(in Chinese)

[9] 张煜东,吴乐南,王水花.一种基于光全息的图像混合加密算法[J].计算机工程与应用,2011,47(20):201-205.
ZHANG Y D,WU L N,WANG S H. Hybrid image encryption method based on hologram[J]. Computer engineering and applications,2011,47(20):201-205.(in Chinese)

[10] 陈翼翔,汪小刚.基于双随机相位编码的非线性双图像加密方法[J].光学学报,2014,34(7):0710001-1-5.
CHEN Y X,WANG X G. Nonlinear double images encryption based on double random phase encoding[J]. Aata optica sinica,2014,34(7):0710001-1-5.(in Chinese)

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

[12] GONZALEZ R C,WOODS R E. 数字图像处理[M].阮秋琦,阮宇智,译.2版.北京:电子工业出版社,2007:235.
GONZALEZ R C,WOODS R E. Digital image processing[M]. RUAN Q Q,RUAN Y Z,translated. 2nd ed. Beijing:Publishing House of Electronics Industry,2007:235.(in Chinese)

[责任编辑:严海琳]