第 57 卷 第 11 期 2008 年 11 月
1000-3290/2008/57(11)/6955-07

物 理 学 报
ACTA PHYSICA SINICA

Vol.57,No.11,November,2008

基于离散四元数傅里叶变换的双随机相位加密技术*

盖 琦 王明伟 李智磊 翟宏琛†

(南开大学现代光学研究所,天津 300071)

(2008 年 4 月 20 日收到;2008 年 5 月 13 日收到修改稿)

应用光学图像加密的思想,将离散四元数傅里叶变换(DQFT)与双随机相位加密技术相结合,提出了一种应用于彩色图像的双随机相位加密新技术. 基于 DQFT 的双随机相位加密技术可将彩色图像作为一个整体进行加密,从而在保持了系统的保密性能的同时,有效地降低了复杂性. 阐述了加密和解密的原理,并通过实验对其鲁棒性进行了验证.

关键词:四元数,离散四元数傅里叶变换(DQFT),双随机相位加密

PACC:4230V,4230K

1. 引 言

随着信息技术的发展,图像已经成为信息表达的一种重要方式,人们对图像信息安全的要求也越来越高,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—9]. 其中采用双随机相位加密技术[4—7]实现图像的加密是采用光学方法对图像进行处理,此技术保密性很好,已取得了很大的成功. 其基本思想是利用两个独立的随机相位掩模将图像加密为稳定的白噪声,在不知道密钥的情况下,几乎不可能恢复出原来的图像. 双随机相位加密技术在处理灰度图像时简单易行,但是在处理彩色图像时,由于彩色图像具有三个通道,通常的处理方法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[8]将彩色图像分解为 R,G,B 三个通道,采用波长复用无透镜菲涅尔全息的方法对每一个通道分别进行双随机相位加密;文献[9]将彩色文字图像分解为 R,G,B 三个通道,采用分数傅里叶变换双随机相位加密技术,对每一个通道分别进行加密. 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 6 个及更多,密钥数量的增多使得密钥在保存和发布时泄密的可能性增大,不利于密钥的保存和发布.

近年来 Sangwine 和 Ell 等人提出了将离散四元数傅里叶变换(DQFT)应用到多通道数字媒体如彩色图像的处理中[10—18]. 基于 DQFT 的彩色图像处理技术对彩色图像的运算是多通道整体进行[11,13],而不是单个通道分别进行的,所以在运算空间以及保留彩色图像各通道之间的相互关系上具有很大的优势[11,13]. 这种良好的性质已被应用于各种彩色图像处理技术中,如彩色图像的边缘检测[16,17]、彩色图像的滤波[18]以及彩色图像的水印技术[14]等.

我们将 DQFT 与双随机相位加密方法相结合,提出了一种应用于彩色图像的离散四元数双随机相位加密的新技术. 该技术将待加密彩色图像表示为一离散四元数矩阵,由于四元数与普通复数结构相似,也可以用模和相位表示,所以我们应用光学图像双随机相位加密技术的思想,将离散四元数在傅里叶变换前后均进行基于光学原理的双随机相位加密,即在空间域和频率域各乘以一个四元数随机相位掩模函数,实现对彩色图像的加密. 与前面提到的彩色图像加密方法相比,由于我们只在一个通道上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 2 个,

* 国家自然科学基金(批准号:60577017,60777007)资助的课题.

† 通讯联系人. E-mail:zhai@nankai.edu.cn

从而在密钥的保存与发布上具有很大优势. 通过理论分析及计算机实验验证,此技术对彩色图像的高斯噪声及椒盐噪声具有较好的鲁棒性,为彩色图像的加密提供了一种新方法.

2. 彩色图像的 DQFT

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.

对于一个大小为 $(X\times Y)$ 的彩色图像 $I(x,y)$, x 和 y 分别表示像素所在矩阵的行和列的位置,$x\in[0,X-1]$, $y\in[0,Y-1]$,令四元数的 3 个虚部分量分别代表红(R)、绿(G)、蓝(B) 3 个基色分量,实部为 0,则彩色图像 $I(x,y)$ 可表示为[14,15]

$$I(x,y)=R(x,y)\,i+G(x,y)\,j+B(x,y)\,k. \tag{1}$$

而对于任何一个四元数 $f=f_r+f_ii+f_jj+f_kk$, 都可以用模和相位的形式表示为[15] $f=|f|\mathrm{e}^{\mu\phi}$,由此可见,一幅彩色图像可以表示为一个四元数矩阵,并与普通复数一样,具有模和相位. 为分析方便,将图像采用下式表示为

$$f(x,y)=f_r(x,y)+f_i(x,y)\,i+f_j(x,y)\,j+f_k(x,y)\,k, \tag{2}$$

对于彩色图像,$f_r(x,y)=0$. $f(x,y)$ 的离散傅里叶变换可定义为[13—15]

$$F(u,v)=\frac{1}{\sqrt{XY}}\sum_{x=0}^{X-1}\sum_{y=0}^{Y-1}\mathrm{e}^{-\mu 2\pi\left(\frac{xu}{X}+\frac{yv}{Y}\right)}f(x,y). \tag{3}$$

对应的逆变换定义为[13—15]

$$f(x,y)=\frac{1}{\sqrt{XY}}\sum_{u=0}^{X-1}\sum_{v=0}^{Y-1}\mathrm{e}^{\mu 2\pi\left(\frac{xu}{X}+\frac{yv}{Y}\right)}F(u,v), \tag{4}$$

式中的 μ 是一个单位纯四元数,即 μ 的实部为 0,模为 1,且 $\mu^2=-1$. 由上面的公式可看出,选取不同的 μ,所得结果也就不同. 参数 μ 可表示为[13—15]

$$\mu=\mu_i i+\mu_j j+\mu_k k. \tag{5}$$

这里我们把 $f(x,y)$ 称为空间域,$F(u,v)$ 称为频率域,所以 $F(u,v)$ 可看作是彩色图像的频谱. $F(u,v)$ 也是一四元数,可表示为

$$F(u,v)=F_r(u,v)+F_i(u,v)\,i+F_j(u,v)\,j+F_k(u,v)\,k. \tag{6}$$

3. 基于 DQFT 的双随机相位加密技术

对于一幅待加密的彩色图像,我们可以按照(2)式先将其表示成四元数矩阵的形式,并记为 $f(x,y)$. 设 $n(x,y)$, $b(u,v)$ 分别代表两个独立的在 $[0,1]$ 上均匀分布的随机矩阵. 加密过程可以分为以下四步:

1) 将待加密彩色图像 $f(x,y)$ 乘以一随机相位掩模函数 $\mathrm{e}^{\mu_A 2\pi n(x,y)}$ 后得 $g(x,y)$,

$$g(x,y)=f(x,y)\cdot\mathrm{e}^{\mu_A 2\pi n(x,y)}.$$

2) 将 $g(x,y)$ 用参数 μ_1 作 DQFT 变换,得到频谱,记为 $G(u,v)$.

3) 将 $G(u,v)$ 乘以另一随机相位掩模函数 $\mathrm{e}^{\mu_B 2\pi b(u,v)}$,得 $H(u,v)$,

$$H(u,v)=G(u,v)\cdot\mathrm{e}^{\mu_B 2\pi b(u,v)}.$$

4) 将 $H(u,v)$ 用参数 μ_2 作 DQFT 逆变换,得 $h(x,y)$, $h(x,y)$ 即为加密后的图像.

加密过程的数学表达式如下:

$$h(x,y)=\mathrm{DQFT}^{-1}\{\mathrm{DQFT}[f(x,y)\cdot\mathrm{e}^{\mu_A 2\pi n(x,y)}]\cdot\mathrm{e}^{\mu_B 2\pi b(u,v)}\},$$

其中,参数 μ_1,μ_2,μ_A,μ_B 均为单位纯四元数, $n(x,y)$, $b(u,v)$, μ_1,μ_2,μ_A,μ_B 作为解密的密钥.

加密过程的原理框图如图 1 所示.

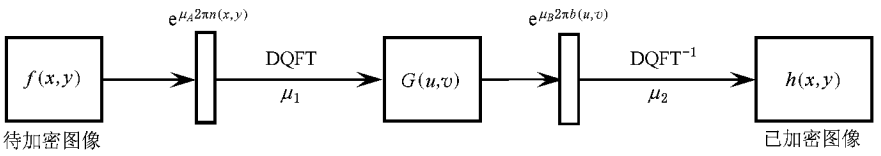

图 1 加密过程框图

解密过程是加密过程的逆过程,可由以下四步完成:

1)以密钥 μ_2 为变换参数,将 $h(x,y)$ 作 DQFT 变换得 $H(u,v)$.

2)根据密钥 μ_B, $b(u,v)$ 解出 $G(u,v)$,

$$G(u,v)=H(u,v)\cdot\mathrm{e}^{-\mu_B 2\pi b(u,v)}.$$

3)以密钥 μ_1 为变换参数，将 $G(u,v)$ 作 DQFT 逆变换，得 $g(x,y)$.

4)根据密钥 μ_A，$n(x,y)$ 解出 $f(x,y)$，

$$f(x,y) = g(x,y) \cdot \mathrm{e}^{-\mu_A 2\pi n(x,y)}.$$

解密过程的原理框图如图 2 所示.

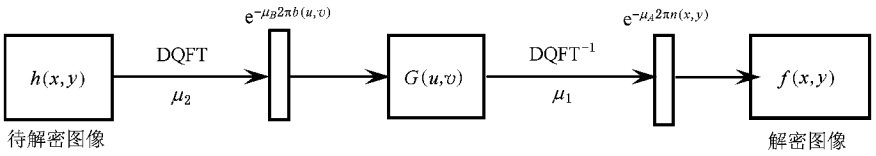

图 2　解密过程框图

解密过程的数学表达式如下：

$$f(x,y) = \mathrm{DQFT}^{-1}\{[\mathrm{DQFT}[h(x,y)]] \cdot \mathrm{e}^{-\mu_B 2\pi b(u,v)}\} \cdot \mathrm{e}^{-\mu_A 2\pi n(x,y)}.$$

4. 分　　析

本加密系统中所需的随机相位掩模数量为 2，攻击者在不知道这两个随机相位掩模的信息时，无法破解此系统. 本方法在保证安全性的基础上，减少了密钥的数量. 具体分析如下：在密钥存储问题上，如果是用计算机实现，则密钥占据存储介质的空间大小是主要因素. 本文方法中，密钥 μ_A，μ_B，μ_1，μ_2 对图像加密的作用要远远小于随机相位掩模 $n(x,y)$ 和 $b(u,v)$，而且其复杂度与占用空间也远小于随机相位掩模，可以忽略，所以这里主要讨论随机相位掩模的数量. 现有的对彩色图像进行双随机相位加密的方法中，通常需要的随机相位掩模数量至少为 6 个[9]，即每个通道在空间域和变换域各需要一个随机相位掩模. 也有方法[8]将紧贴彩色图像三通道的 3 个空间域的随机相位掩模合而为一，即一共至少需要 4 个随机相位掩模. 为分析方便，我们在此定义一个系统的必要随机相位掩模数量的概念. 所谓必要随机相位掩模数量是指一个随机相位加密系统在攻击者不知道密钥的情况下无法破解所需要的最少的随机相位掩模数量. 按照这个定义，文献[4]中针对灰度图像的单通道双随机相位加密系统的必要随机相位掩模数量为 2，而文献[8,9]中的两种方案，由于把彩色图像分为三个通道进行处理，其必要随机相位掩模数量分别是 4 和 6. 当用少于必要随机相位掩模数量的随机相位进行加密，或因为泄漏等原因使得攻击者未知的随机相位掩模数量小于必要随机相位掩模数量时，攻击者可以恢复部分原始图像，甚至可能获得关于原始图像的重要信息[8,9]，从而导致泄密. 从这个意义上说，本方法所需要的随机相位掩模数量减少为 2 个，在保证安全性的基础上减少了密钥的数量，有利于密钥的保存与发布.

5. 实验结果

我们选取了 50 幅不同内容、不同格式的彩色图像进行了多次实验，结果表明，与选取图像的特点无关，使用正确的密钥均可准确地恢复原始图像，而用随机的密钥无法恢复原始图像.

作为示例，图 3 给出了对 512 × 512 的彩色 lena 图像的实验结果. 其中，(a)图为原始图像；(b)，(c)，(d)，(e)分别为加密后图像的实部和三个虚部；(f)为采用正确的密钥还原后的图像(其峰值信噪比 PSNR = 305.69)；(g)为采用随机的密钥 $n(x,y)$ 和 $b(u,v)$ 还原后的图像.

由实验结果可看出，用正确的密钥可以准确恢复原始图像，而用随机的密钥无法恢复原始图像.

图 4 给出了另外三幅 512 × 512 的彩色图像(peppers，airplane，mandrill)的实验结果. 其中，(a)，(c)，(e)分别为原始图像，(b)，(d)，(f)为对应的解密后的图像，并给出了各自的峰值信噪比.

鲁棒性测试：高斯噪声和椒盐噪声是传输过程中经常会遇到的干扰，为了测试本方法对这两种噪声的鲁棒性，我们对选取的 50 幅图像进行了多次实验，对加密后的不同图像分别加入不同系数的高斯噪声及椒盐噪声，观察还原后所得图像的峰值信噪比(PSNR). 表 1 中列出了 lena，peppers，airplane，mandrill 四幅图像经加噪还原后所得图像的 PSNR，其中，高斯噪声的平均值为 0，方差为加入系数；椒盐噪声的系数表示噪声密度.

图 5(a)，(b)，(c)，(d)分别为对加密图像 lena，

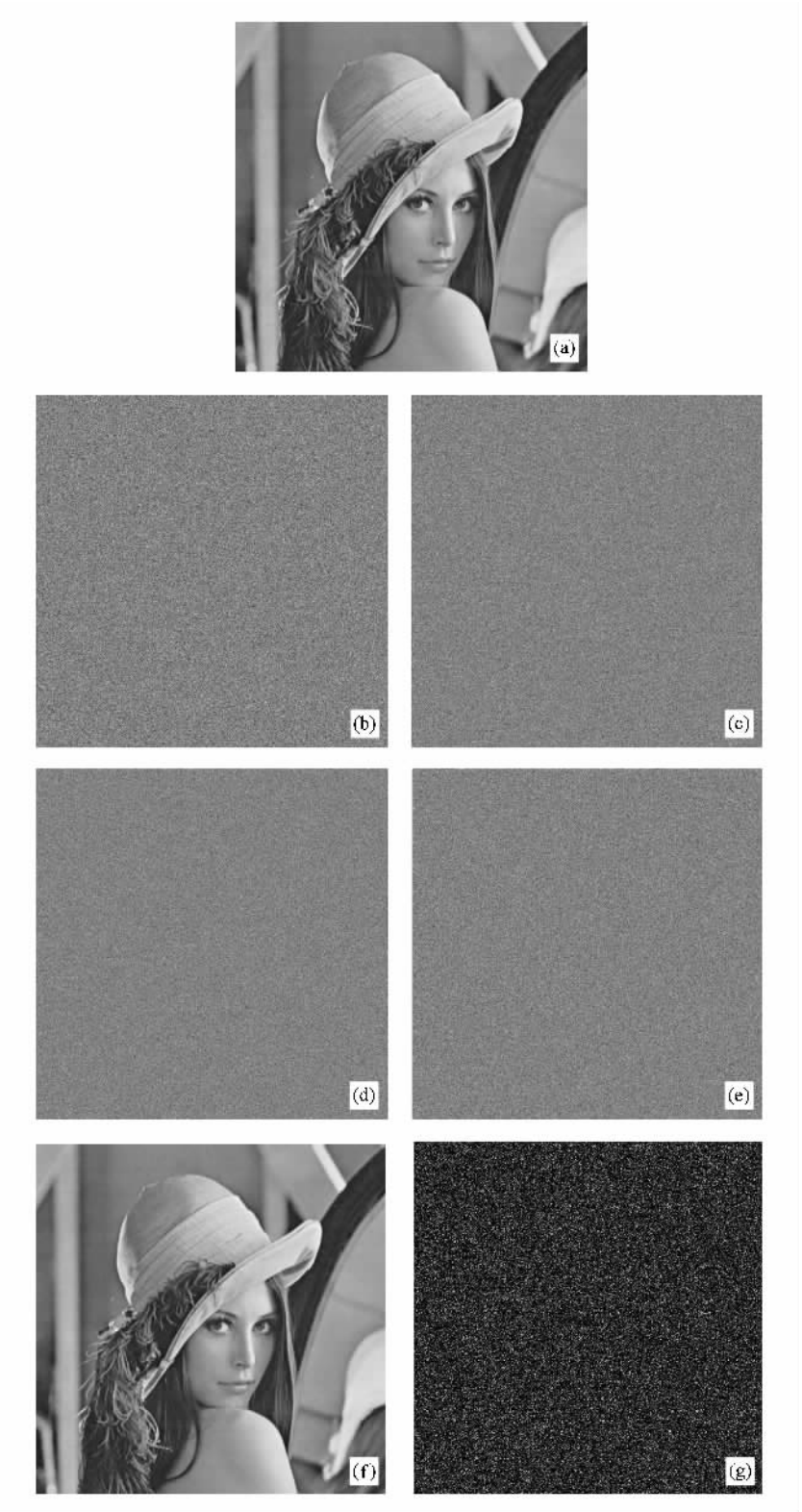

图 3 lena 图像加密及解密的实验结果 (a)为原始图像;(b),(c),(d),(e)分别为加密后图像的实部和三个虚部;(f)为采用正确的密钥还原后的图像(PSNR = 305.69);(g)为采用随机的密钥 $n(x,y)$和 $b(u,v)$还原后的图像

peppers,airplane,mandrill 同时加入高斯噪声(系数为 0.0005)及椒盐噪声(系数为 0.001)之后还原得到的图像. 由实验结果可以看出本加密方法对高斯噪声及椒盐噪声具有较好的鲁棒性.

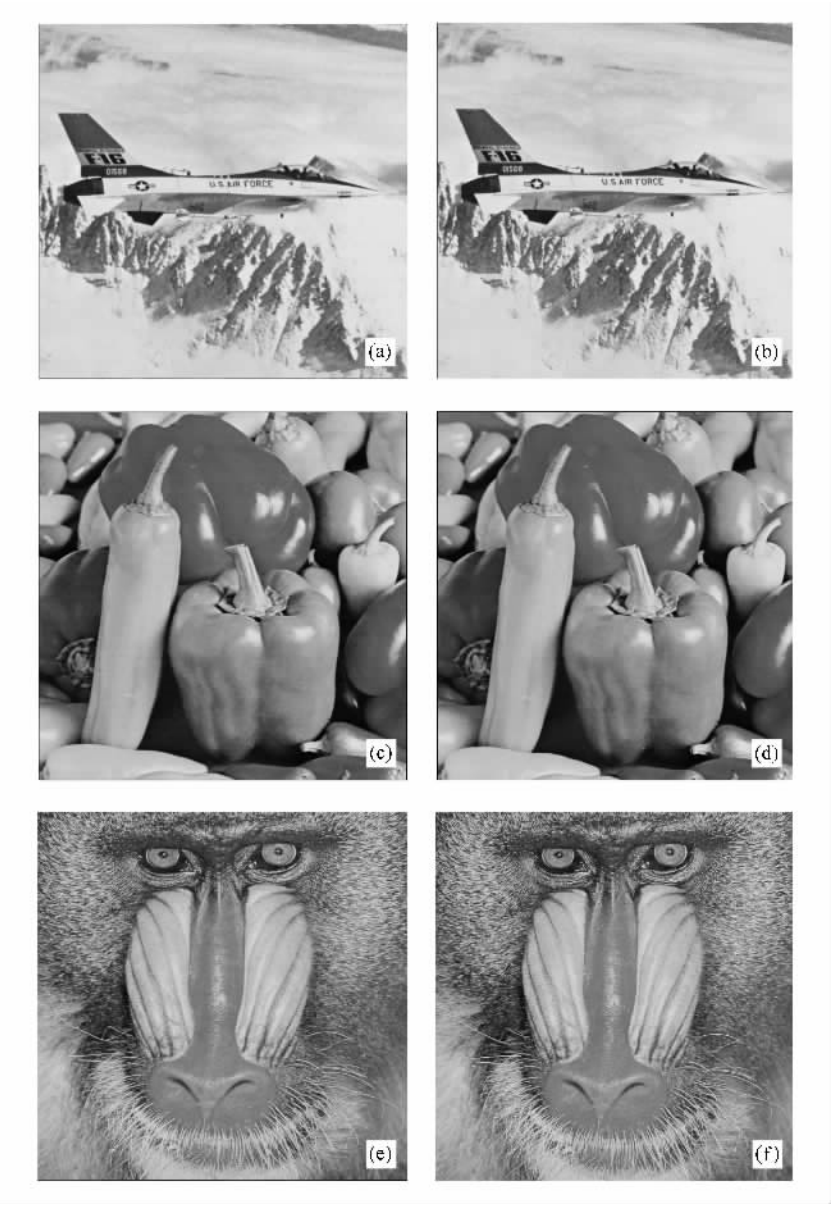

图 4　加密及解密的实验结果　(a),(c),(e)为原始图像；(b),(d),(f)为对应的解密后的图像((b),(d),(f)的 PSNR 分别为 303.29,306.76,305.87)

表 1　不同图像加入噪声后所得到的还原图像的峰值信噪比

噪声及加入系数	lena(PSNR)	peppers(PSNR)	airplane(PSNR)	mandrill(PSNR)
Gaussian 0.0001	31.70	32.79	28.47	30.78
Gaussian 0.0002	28.72	29.82	25.50	27.81
Gaussian 0.0005	24.82	25.94	21.62	23.93
Gaussian 0.001	21.92	23.03	18.73	21.06
salt & pepper 0.0005	24.75	25.73	22.05	24.12
salt & pepper 0.001	21.91	22.43	18.75	20.89
salt & pepper 0.002	18.78	19.32	15.84	17.99
salt & pepper 0.005	14.63	15.46	11.66	14.09
Gaussian 0.0002 + salt & pepper 0.0005	23.23	24.29	20.37	23.42
Gaussian 0.0005 + salt & pepper 0.001	20.31	21.03	16.85	19.95
Gaussian 0.001 + salt & pepper 0.002	17.08	17.71	13.78	16.85

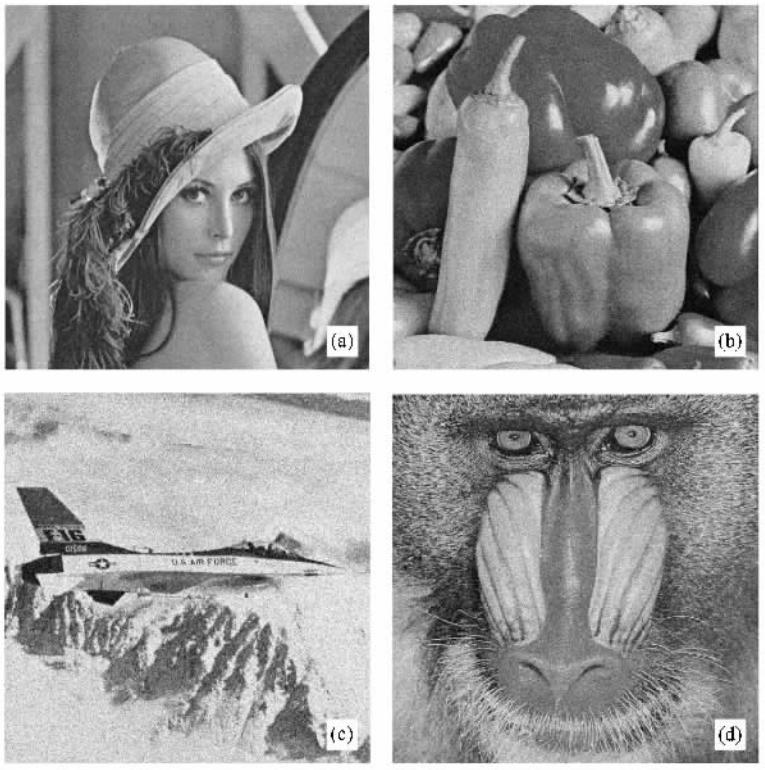

图 5 同时加入高斯噪声(系数为 0.0005)及椒盐噪声(系数为 0.001)之后还原得到的图像 (a) PSNR = 20.31;(b) PSNR = 21.03;(c) PSNR = 16.85;(d) PSNR = 19.95

6. 结 论

我们将 DQFT 与双随机相位加密方法相结合,提出了一种应用于彩色图像的离散四元数双随机相位加密的新技术. 通过理论分析及数字模拟实验验证可以看出,运用此技术可使加密后的彩色图像对高斯噪声及椒盐噪声具有较好的鲁棒性. 此外,由于在该技术中使用了 DQFT 对彩色图像进行表述,与常规的彩色图像加密技术相比,可以使系统的必要随机相位掩模数量相应变少,因而在密钥的保存与发布方面具有很大优势.

采用双随机相位加密技术实现对图像的加密可基于光学方法实现,而且光学方法在处理信息方面具有高速并行的特点,因此利用光学方法来实现图像的加密具有一定的优势. 本文介绍的方法原则上也可以采用光学系统实现,采用光学系统实现对彩色图像加密的实验结果将另文报道.

[1] Lukac R, Plataniotis K N 2004 *Electron. Lett.* **40** 529

[2] Sawda R El, Alfalou A, Hamam H 2007 *Future Generation Communication and Networking* **2** 594

[3] Nien H H, Huang C K, Changchien S K *et al* 2007 *Chaos, Solitons and Fractals* **32** 1070

[4] Refregier P, Javidi B 1995 *Opt. Lett.* **20** 767

[5] Unnikrishnan G, Joseph J, Singh K 2000 *Opt. Lett.* **25** 887

[6] Liu F M, Zhai H C, Yang X P 2003 *Acta. Phys. Sin.* **52** 2462 (in Chinese) [刘福民、翟宏琛、杨晓苹 2003 物理学报 **52** 2462]

[7] Yang X P, Zhai H C 2005 *Acta. Phys. Sin.* **54** 1578 (in Chinese) [杨晓苹、翟宏琛 2005 物理学报 **54** 1578]

[8] Chen L F, Zhao D M 2006 *Opt. Exp.* **14** 8552

[9] Joshi M, Chandrashakher, Singh K 2007 *Opt. Commun.* **279** 35

[10] Sangwine S J 1996 *Electron. Lett.* **32** 1979

[11] Sangwine S J 1997 *In Proceedings 6th International Conference on Image Processing and its Applications* **2** 790

[12] Ell T A, Sangwine S J 2000 *in Proc. IEEE Int. Conf. Image Processing, Vancouver, BC, Canada* II 792

[13] Sangwine S J, Ell T A 2001 *in Proc. IEEE Int. Conf. Image Processing, Thessaloniki, Greece* I 37

[14] Bas P, Le Bihan N, Chassery J M 2003 *ICASSP* (Hong-Kong) 521

[15] Ell T A, Sangwine S J 2007 *IEEE Transactions on Image Processing* **16** 22
[16] Sangwine S J 1998 *Electronic Letters* **34** 969
[17] Evans C J, Sangwine S J, Ell T A 2000 *Proceedings of the tenth European Signal Processing Conference* (EUSIPCO) I 107
[18] Sangwine S J, Ell T A 2000 *IEE Proceedings-Vision, Image and Signal Processing* **147** 89

Doubled random-phase encryption based on discrete quaternion fourier-transforms *

Gai Qi　Wang Ming-Wei　Li Zhi-Lei　Zhai Hong-Chen†
(*Institute of Modern Optics, Nankai University, Tianjin* 300071, *China*)
(Received 20 April 2008; revised manuscript received 13 May 2008)

Abstract

In this paper, a new method for color-image encryption using discrete quaternion fourier-transforms (DQFT) combined with doubled random-phase encryption as used in the optical implementation is proposed, by which color images can be processed as a whole, rather than as separated color components in three channels, so that the complexity of the encryption system can be effectively reduced without any reduction in its security. The principle of both encryption and decryption is detailed and the robustness of the system has been examined experimentally.

Keywords: quaternion, discrete quaternion fourier-transforms (DQFT), doubled random-phase encryption
PACC: 4230V, 4230K

* Project supported by the National Natural Science Foundation of China (Grant Nos. 60577017, 60777007).
† Corresponding author. E-mail: zhai@nankai.edu.cn