基于计算全息的双随机相位图像加密技术

席思星　孙　欣*　刘　兵　云茂金　孔伟金　张文飞　梁　健　田　巍

（青岛大学物理科学学院，山东 青岛 266071）

摘要　基于计算全息，结合 $4f$ 系统双随机相位图像加密技术，提出了一种图像加密以及传输的新方法。分析了计算全息(CGH)记录图像独具的扩频效应及特有的解密密钥，并实现了针对全息图不同的频谱单元及组合，采用原相位板、共轭板以及两者的有序组合作为解密密钥的计算机模拟，研究了其抗噪性能，新方法提高了图像加密的安全性。

关键词　图像处理；图像加密；计算全息；单元频谱；光学密钥；组合密钥

中图分类号　O438.1　　**文献标识码**　A　　**doi**：10.3788/LOP49.040902

New Image Encryption Technology of Image Based on Computer Generated Hologram

Xi Sixing　Sun Xin　Liu Bing　Yun Maojin　Kong Weijin　Zhang Wenfei　Liang Jian　Tian Wei

(*College of Physics Science*, *Qingdao University*, *Qingdao*, *Shandong* 266071, *China*)

Abstract　A new image encryption technology based on computer generated hologram (CGH) combined with the $4f$ system of double random phase image encryption technology is proposed. The unique spread spectrum characteristics of CGH recording encryption image is analyzed, achieving the computer simulation of using the original of phase plate, conjugate panels and the combination with them as the decryption keys of the different spectrum units or spectrum units combination. And the anti-noise ability of this image encryption method is also analyzed. This proposed method improves the security of image encryption.

Key words　image processing; image encryption; computer generated hologram; spectrum unit; optical keys; combined decryption keys

OCIS codes　090.1760; 090.1995; 010.1758

1　引　　言

近年来，随着信息技术的发展越来越快，涉及的领域越来越广，信息加密、防伪问题变得越来越重要。光学密钥这一信息隐藏技术随着相关技术的不断成熟倍受关注[1~6]。计算全息(CGH)加密术是一种虚拟光学技术[7]，它在计算机中利用全息的原理模拟实现全息过程，克服了光学全息加密解密过程中对实验设备的依赖，省略了曝光、显影等光化学处理过程，使得全息加密解密可以实现实时化，因此在机要文件的加密，贵重物品的保密方面得到广泛应用。目前，计算全息用于光学图像加密和隐藏的安全系统已开始引起学者们的关注[8,9]，而且这些方法显示出计算全息术特有的优势。

本文是基于计算全息结合 $4f$ 系统双随机相位加密技术的一种新的图像加密解密方法，以计算全息的形式记录加密图像，克服了传统方法加密图像不易存储和传输的问题，其频谱具有扩频效应，不同的频谱单元或组合需要组合的解密密钥，该方法与传统的双随机相位加密技术相比，继承了全息记录加密图像的优势，克服了实验中制作随机相位板共轭的困难和解密难以实现的问题，在抗噪性上与传统图像光学加密方法相似，在安全性[10]方面具有极大的优势。

收稿日期：2011-09-14；**收到修改稿日期**：2011-10-31；**网络出版日期**：2012-01-19

基金项目：国家自然科学基金(51072085,11104153)资助课题。

作者简介：席思星(1985—)，男，硕士，主要从事光信息处理方面的研究。E-mail：xisixing@126.com

* **通信联系人**。E-mail：qdwlxsx@163.com

2 图像的计算全息加密解密理论

2.1 图像的加密原理

图像加密的原理光路图是一个标准的 $4f$ 双随机相位加密光路,如图 1 所示。原始图像放在物平面 Σ 上,假设图像被垂直入射光照射,原始图像的分布 $\widetilde{E}(x_0,y_0)$。在物平面 Σ 上放置第一个白噪声随机相位板 $p_1=\exp[\mathrm{i}2\pi\boldsymbol{\alpha}(x,y)]$,在频谱面 Σ_0 上放置第二个白噪声随机相位板 $p_2=\exp[\mathrm{i}2\pi\boldsymbol{\beta}(\xi,\eta)]$,其中 $\boldsymbol{\alpha},\boldsymbol{\beta}$ 是 0 ~ 1 的随机矩阵,原始图像要经过两次傅里叶变换以及两个随机相位板的调制完成加密[2]。

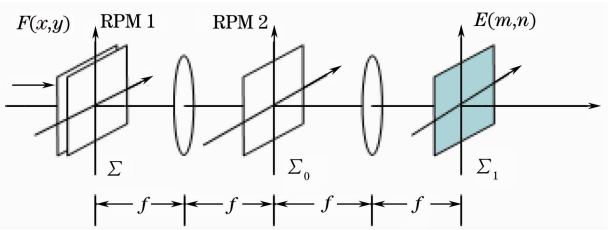

图 1 双随机相位加密光路

Fig. 1 Encryption optical path of double random phase

基于 Matlab 完成图象信息的傅里叶变换以及两个随机相位板对数字图像的调制加密作用,采用快速傅里叶变换算法(FFT),则频谱面 Σ_0 上的光场分布 $\widetilde{E}_0(\xi,\eta)$ 即为加密图像信息 $\widetilde{F}(x,y)\exp(\mathrm{i}2\pi\boldsymbol{\alpha})$ 的快速傅里叶变换,而输出平面 Σ_1 上的光场分布 $\widetilde{E}(x_1,y_1)$ 则是加密频谱信息 $\widetilde{E}_0(\xi,\eta)\exp(\mathrm{i}2\pi\boldsymbol{\beta})$ 的快速傅里叶变换;并且以离散抽样的数字图像矩阵与随机相位矩阵的点乘积计算相位板的调制作用。经过两次变换及调制后,原始图像即转化为一随时间统计无关的高斯白噪声。

2.2 图像的解密原理

由于光路的可逆性,解密为加密的逆过程,解密光路如图 2 所示。加密图像经过两个相位板 RPM3(RPM′2),RPM4(RPM′1)的调制解密,以及两次傅里叶变换得到原图像。

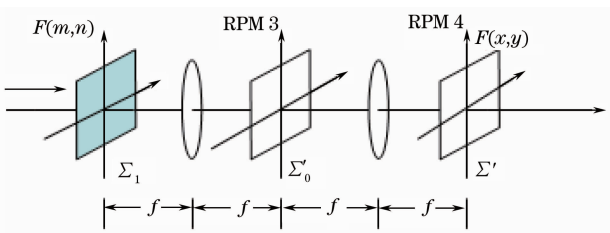

图 2 解密光路图

Fig. 2 Decryption light path of vertical light incident

3 计算全息记录加密图像的设计制作

3.1 计算像面全息加密图的记录

实验用蝴蝶图像如图 3(a)所示[像素为 128 pixel×128 pixel]作为待加密图象,采用图 1 的加密光路,利用罗曼Ⅲ型编码方法对平面 Σ_1 上的输出图像制作像面计算全息图,假设参考光为单位振幅的单色垂直入射光,在制作计算全息图过程中采用一些特殊处理[11]。

通过上述编码制作完成的计算全息加密图像如图 3(c)所示[像素为(128×9) pixel×(128×9) pixel],图 3(b)是传统双随机相位加密技术得到的加密图像,通过比较可见两者有着明显的区别,图 3(c)表示计算全息图是一幅隐藏了原图像尺度大小信息的加密图像。

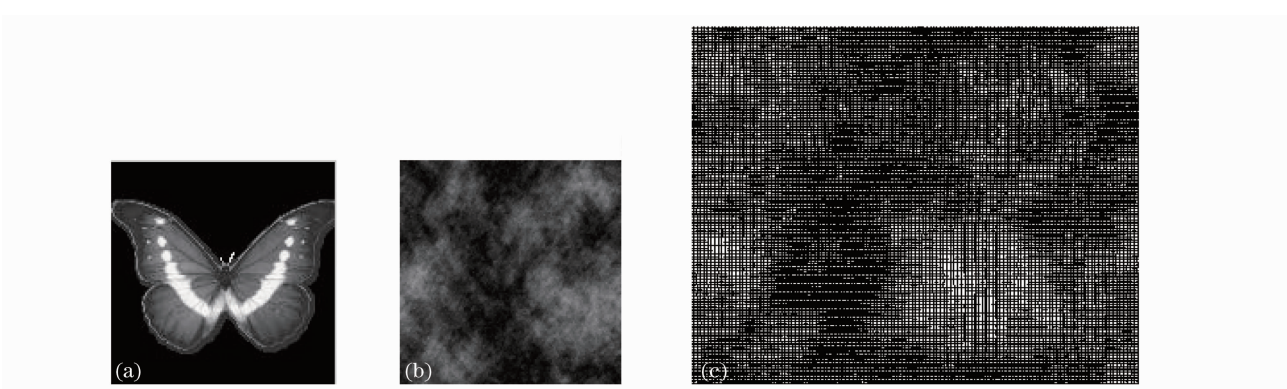

图 3 (a) 原始图像;(b) 传统方法加密图像;(c)计算全息法加密图像

Fig. 3 (a) Original image figure; (b) encryption image of traditional methods; (c) encryption image of calculation holographic method

3.2 计算全息加密图像的扩频效应分析

实验发现计算全息记录方法使得加密图像的频谱被扩大,对计算全息加密图像[图 3(c)]进行傅里叶变换得到其频谱,图 4(a)是传统双随机相位加密技术得到的加密图像的频谱。对比两个频谱图可见,传统方

法加密图像的频谱是一个频谱点，而计算全息加密图频谱是 $M\times N$ 个单元频谱的组合，如图 4(b)所示，由此可得用罗曼编码制得的计算全息图具有扩频特性。对比可发现：

1) 由于计算全息编码参数的未知性，使得计算全息本身具有加密性能，是一幅肉眼不容易识别的图像。

2) 基于计算全息采用了罗曼Ⅲ型迂回相位这一特殊的编码方式，其频谱是一个与编码参数有关的频谱单元的组合，每个频谱单元相当于一个加密图像频谱，且每一个频谱单元包含有原加密图像的完整频谱信息，只是边缘的频谱单元噪声相对较大。其中一些频谱单元是原加密图像的频谱的共轭[图 4(b)中(0，－1)频谱单元]，一些频谱单元是原加密图像的频谱[图 4(b)中(0，＋1)频谱单元]，而中间频谱单元是两者的叠加[图 4(b)中(0，0)频谱单元]。通过图 4(a)和图 4(b)的对比可见计算全息加密图像的扩频特性。

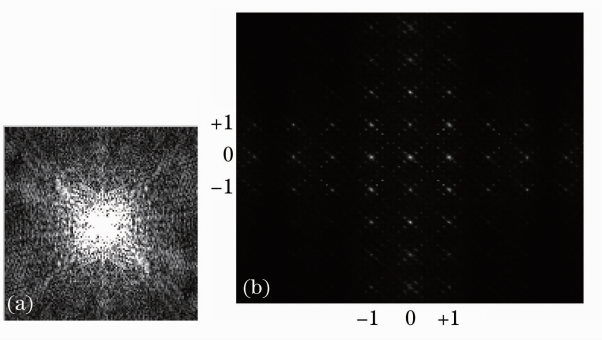

图 4 (a)传统方法加密图像的频谱；(b)计算全息法加密图像的频谱

Fig. 4 (a) Spectrum of image encryption using the traditional method; (b) spectrum of encrypted image using calculation holographic method

4 计算全息加密图像的解密及分析

4.1 计算全息加密图像单个单元频谱的实验研究

为了检验加密方法的实用性，进行了计算机模拟实验。模拟的过程涉及离散傅里叶变换和相位板“调制”效果。本文用光场的复振幅分布与计算机生成的随机矩阵的点乘积模拟相位板“调制”。由于计算全息的扩频特性，针对计算全息加密图像频谱的单元频谱、单元频谱的组合，利用 Matlab 7.1 对加密方法进行了实验模拟。

4.1.1 计算全息加密图像单频谱单元的加密解密实验

以计算全息图的频谱面 Σ'_0 上的频谱单元(0，＋1)作为传输的加密图像，进行模拟实验，结果如图 5 所示。图 5(a)是计算全息加密图像的(0，＋1)频谱单元图像，图 5(b)是解密过程中，解密频谱面上以 P_r 为解密密钥的解密结果(其中 P_r 为任意随机相位)，图 5(c)是解密频谱面上以原相位板 P_2 为解密密钥的解密结果，图 5(d)是解密频谱面上以原相位板的共轭 P_2^* 为解密密钥的解密结果。可得针对频谱单元为加密图像的解密，只有在解密频谱面上以原相位板的共轭 P_2^* 作为解密密钥才能正确解密。

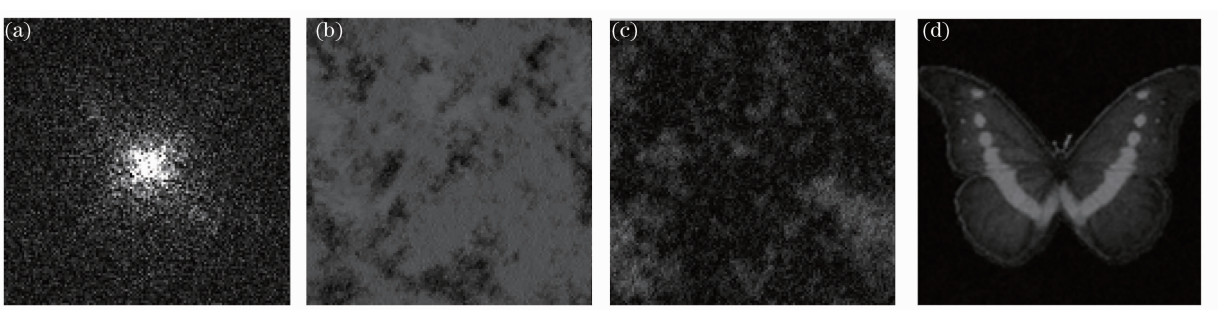

图 5 (a)＋1 级频谱单元；(b) $P_3=P_r$ 解密图像；(c) $P_3=P_2$ 解密图像；(d) $P_3=P_2^*$ 解密图像

Fig. 5 (a) (0，＋1) spectrum unit; (b) decrypted image figure by $P_3=P_r$; (c) decrypted image figure by $P_3=P_2$; (d) decrypted image by $P_3=P_2^*$

以计算全息图的频谱面 Σ'_0 上的频谱单元(0，－1)作为传输的加密图像，模拟结果如图 6 所示，可见只有在解密频谱面上以原相位板 P_2 作为解密密钥才能正确解密。

以计算全息图的频谱面 Σ'_0 上的中心频谱单元(0，0)作为传输的加密图像，模拟结果如图 7 所示，由于(0,0)级单元频谱是(0，＋1)和(0，－1)级单元频谱的叠加，所以以原相位板 P_2 及其共轭 P_2^* 都可以解密，但是会掺有一定的噪声。

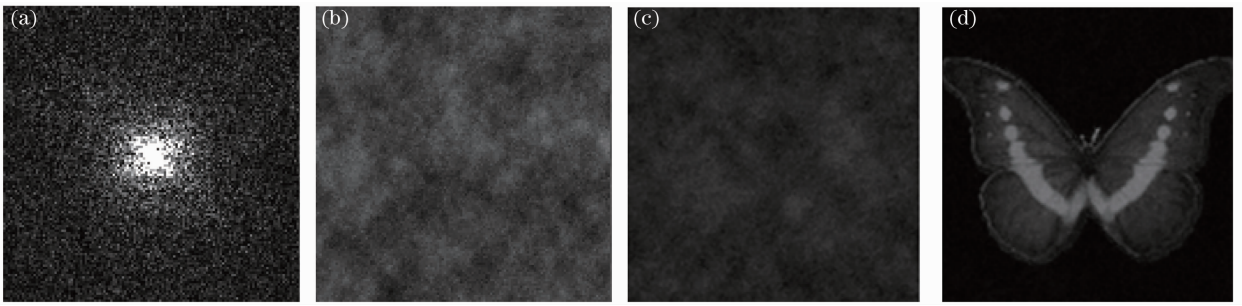

图 6 (a)－1 级频谱单元；(b) $P_3=P_2^*$ 解密图像；(c) $P_3=P_r$ 解密图像；(d) $P_3=P_2$ 解密图像

Fig. 6 (a) (0, −1) spectrum unit; (b) decrypted image figure by $P_3=P_2^*$; (c) decrypted image figure by $P_3=P_r$; (d) decrypted image by $P_3=P_2$

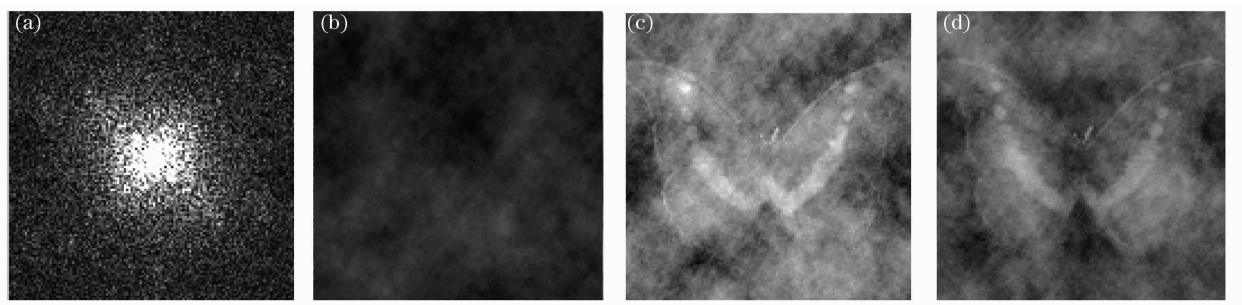

图 7 (a) 0 级频谱单元；(b) $P_3=P_r$ 解密图像；(c) $P_3=P_2^*$ 解密图像；(d) $P_3=P_2$ 解密图像

Fig. 7 (a) (0, 0) spectrum unit; (b) decrypted image figure by $P_3=P_r$; (c) decrypted image figure by $P_3=P_2^*$; (d) decrypted image by $P_3=P_2$

实验结果表明，单频谱单元作为加密图像，该方法与传统的双随机相位加密技术相同，一个单元频谱需要正确的解密密钥，加密性能与传统的双随机相位加密技术相同，但是不同的单元频谱又需匹配两种解密密钥，对图像加密的安全性有一定提高。

4.1.2 单个单元频谱解密的抗噪性能分析

通过计算恢复图像相对于原始图像的平均方差，分析该加密方法的抗噪性能。针对单个频谱单元解密，一个像素数为 $N\times N$ 的二维图像的归一化能量定义为

$$|s|^2=\frac{1}{N\times N}\sum_{i=1}^{N}\sum_{j=1}^{N}|s(i,j)|^2. \tag{1}$$

根据这一归一化的能量值，计算恢复图像对于原始图像的平均方差，令 o 表示原始图像，r 表示解密后的恢复图像，其平均方差可表示为

$$E_{MS}=|r-o|^2=\frac{1}{N\times N}\sum_{i=1}^{N}\sum_{j=1}^{N}|r(i,j)-o(i,j)|^2. \tag{2}$$

将加密图像加入不同标准偏差的噪声，选取频谱单元(−1,0)解密，计算其恢复图像相对原始图像的平均方差值，同时计算传统双随机相位板加密方法的恢复图像与原始图像的平均方差值，获得不同标准偏差噪声下的两条曲线，如图 8 所示。

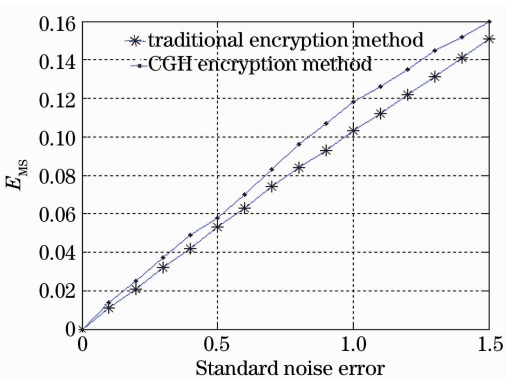

图 8 两种方法抗噪能力分析

Fig. 8 Two methods of antinoise ability analysis

比较两种方法的平均方差曲线可以发现，随着加入噪声标准偏差的增加，计算全息加密方法与传统加密方法的解密平均方差趋势相同，在噪声标准偏差较小时，计算全息加密方法并没有加大噪声，与传统双随机相位加密方法在抗噪性能方面相当，有较强的抗噪能力。

4.2 计算全息加密图像单元频谱组合的加密解密实验

针对计算全息加密图像的频谱面 Σ'_0 上的频谱单元,可以设计各种频谱单元的组合,作为传输的加密图像来提高图像加密的安全性,这里以三个单元频谱的组合为例,进行计算机模拟实验。图 9(a)是三个单元频谱组合的加密图像;图 9(b)是以正确密钥组合解密结果图像,其中解密频谱面上解密密钥为原相位板、0 相位板以及共轭相位板的排列组合;图 9(c)是解密频谱面上应用单一密钥(原相位板)解密结果图像;图 9(d)是解密频谱面上正确密钥的错误次序组合解密结果图像。可以看出只有正确密钥的有序组合方可解密,对图像加密的安全性是一个极大的提高。

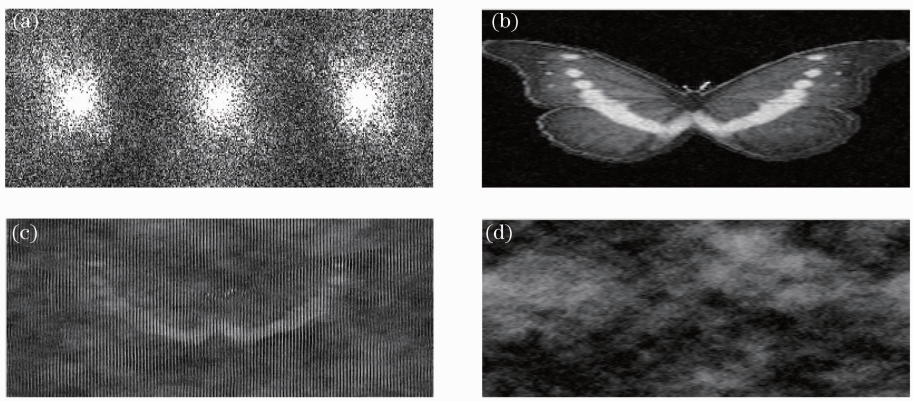

图 9 (a) 三频谱单元组合加密图像;(b) 正确密钥组合解密图像;(c) 单一密钥解密结果图像;(d) 密钥错误组合解密图像

Fig. 9 (a) Encryption image combined with three spectrum units; (b) decrypted image by correct key combination; (c) decrypted image by single key; (d) decrypted image by keys wrong combination

实验结果表明针对计算全息加密图像的频谱面 Σ'_0 上的频谱单元组合,由于其组合次序、数量以及不同单元频谱的未知性,任意错误密钥完全不能解密。且知道正确密钥,密钥组合错误也完全不能解密,用单一密钥叠加解密得到的解密图像,伴有极大的噪声,几乎不能解密,对图像加密的安全性有极大的提高。

5 结 论

基于计算全息,提出了一种图像加密解密以及传输的新方法,以 $4f$ 系统双随机相位图像加密技术为基础,结合计算全息技术记录加密图像。由于计算全息本身具有加密作用和特有的扩频特性,以其频谱作为加密的传输图像,可以拆解不同的频谱单元或组合,因为需要原相位板或共轭相位板以及两者的有序组合作为解密密钥,这样可以提高图像加密以及传输的安全性。新方法实现了图像信息的快速加密、解密。该方法速度快 、精度高,并且有着极高的保密性能,可以广泛应用于防伪、图像保密传输、光学信息安全等领域。

参 考 文 献

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

2 B. Javidi, A. Sergent, G. Zhang *et al.*. Fault tolerance properties of a double phase encoding encryption technique [J]. *Opt. Engng.*, 1997, **36**(4): 992~998

3 B. Javidi. Optical spatial filtering for image encryption and security systems [C]. *SPIE*, 1997, **33**(86): 14~23

4 Wu Kenan, Hu Jiasheng, Wu Xu. Optical encryption for information security [J]. *Laser & Optoelectronics Progress*, 2008, **45**(7): 30~38

吴克难, 胡家升, 乌 旭. 信息安全中的光学加密技术 [J]. 激光与光电子学进展, 2008, **45**(7): 30~38

5 Zhu Zhuqing, Feng Shaotong, Nie Shouping *et al.*. Complex valued encrypted image hiding technology based on discrete cosine transform [J]. *Chinese J. Lasers*, 2009, **36**(1): 177~181

朱竹青, 冯少彤, 聂守平 等. 基于离散余弦变换的复值加密图像隐藏技术 [J]. 中国激光, 2009, **36**(1): 177~181

6 Zhang Qiuxia. Encryption technology for hologram of optical system [J]. *Information Technology*, 2010, (2): 33~35

张秋霞. 一类光学系统计算全息图像加密技术研究[J]. 信息技术, 2010, (2): 33～35

7 Su Xianyu. Communication Optics [M]. Beijing: Science Press, 1999. 87～92
苏显渝. 信息光学[M]. 北京: 科学出版社, 1999. 87～92

8 Yu Zuliang, Jin Guofan. Calculation Mechanism Hologram [M]. Beijing: Tsinghua University Press, 1984. 41～44
虞祖良, 金国藩. 计算机制全息图[M]. 北京:清华大学出版社, 1984. 41～44

9 B. Zhu, H. Zhao, S. Liu. Image encryption based on pure intensity random coding and digital holography technique [J]. *Optik*, 2003, **114**(2): 95～99

10 Zhang Jingjuan, Situ Guohai, Zhang Yan. Progress of optical security systems based on random phase encoding technology [J]. *J. Graduate School of the Chinese Academy of Science*, 2003, **20**(3): 265～270
张静娟, 司徒国海, 张 艳. 基于随机相位编码技术的光学安全系统的研究进展[J]. 中国科学院研究生院学报, 2003, **20**(3): 265～270

11 Sun Xin, Huang Yongfeng, Xi Sixing. True color holographic technology based on computer generated holography [J]. *Acta Optica Sinica*, 2009, **29**(2): 225～228
孙 欣, 黄永峰, 席思星. 基于计算全息的真彩色全息术[J]. 光学学报, 2009, **29**(2): 225～228