doi:10.3788/gzxb20154407.0710002

基于频谱融合技术的光学衍射成像彩色图像加密系统

李婧[1],吕晓东[2],马毛粉[2],秦怡[2]
(1 南阳师范学院 数学与统计学院,河南 南阳 473061)
(2 南阳师范学院 物理与电子工程学院,河南 南阳 473061)

摘 要:提出了一种基于光学衍射成像原理的彩色图像加密方法.首先把彩色图像分成红、绿、蓝三基色分量,并将三基色灰度图像分别作离散余弦变换,得到对应的离散余弦变换谱.保留离散余弦变换谱的主要数据,并用空间复用的方法把这三个主要数据融合于一个实值图像之中,该图像即为复合频谱.再将此复合频谱送入光学衍射成像系统中加密,得到单幅密文.解密过程为加密过程的逆过程,即首先由单幅密文恢复复合频谱,再由复合频谱分离出三基色图像的部分离散余弦变换谱,再对这些离散余弦变换谱做逆变换得到三基色图像.由于对复合频谱设置了一个特殊数据区,因此在利用相位恢复算法恢复复合频谱的过程中,这些特殊数据作为输入平面的部分振幅支撑,可以避免迭代过程的停滞问题并提高收敛速率,从而完全恢复复合频谱,进而恢复原始图像.本方法可以将一幅彩色图像加密成单幅具有噪声图样的强度密文,同时,解密恢复得到的原始彩色图像具有较高的像质.

关键词:信息光学;图像加密;光学衍射;频谱融合技术;彩色图像;离散余弦变换;相位恢复算法;衍射强度

中图分类号:TP751 **文献标识码**:A **文章编号**:1004-4213(2015)07-0710002-6

Optical Color Image Encryption in Diffraction Imaging Scheme Based on Spectrum Fusion

LI Jing[1], LÜ Xiao-dong[2], MA Mao-fen[2], QIN Yi[2]
(1 *School of mathematics and statistics, Nanyang Normal University, Nanyang, Henan* 473061, *China*)
(2 *College of School of mathematics and statistics, Nanyang Normal University, Nanyang, Henan* 473061, *China*)

Abstract: A method for color image encryption was proposed. For encryption, a color image is separated into three components which are red, green and blue. The three grey images are transformed with Discrete Cosine Transform (DCT). Then these DCT spectrums are partially retained and merged into a single real value matrix, namely the composite spectrum. Thereafter, the matrix is encrypted by the diffractive-imaging schemes. The decryption is the inverse of the encryption. Since a special domain has been set in the composite spectrum, the algorithm for retrieving the composite spectrum has overcome the stagnation problem and converges quickly. Computer simulations show that a color image can be successfully encrypted into a single noise-like intensity pattern, and the decrypted image can be obtained with high quality.

Key words: Information optics; Image encryption; Opticl diffraction; Spectrum fusion; Color image; Discrete Cosine Transform(DCT); Phase retrieval algorithm; Diffraction patterns

OCIS Codes:100.4998; 070.2025; 070.4560; 070.7345

基金项目:国家自然科学基金(No. U1404614)及南阳师范学院青年基金(No. QN2015013)资助

第一作者:李婧(1980—),女,讲师,硕士,主要研究方向为图像与信息安全. Email:644715359@qq.com
通讯作者:秦怡(1981—),男,讲师,硕士,主要研究方向为信息光学及图像处理. Email:641858757@qq.com

收稿日期:2015-01-21;**录用日期**:2015-03-08

0 引言

近年来，光学信息安全技术成为了信息光学的研究热点之一[1-13]. 与传统的信息安全技术相比，光学信息安全技术可以对二维数据进行并行高速加密与解密. 该领域的代表性成果是 Refregier 与 Javidi 提出的双随机相位编码系统(Double Random Phase Encoding System，DRPE)，该系统可将位于光学 4f 系统输入平面的原始图像加密为复平稳白噪声[14]. 由该系统衍生出来的菲涅尔域、分数傅里叶域双随机相位编码系统以及利用波长复用、距离复用技术的多图像加密系统也被广泛地研究[15-16]. DPRE 系统对盲反卷积攻击和暴力攻击具有稳健性[14]，然而，该系统的加密结果为复数，必须采用干涉的方法记录，而干涉系统对装置的稳定性要求极高，这成为了 DRPE 系统应用的重要障碍.

为了解决这个问题，Chen 等人提出了光学衍射成像加密系统[17-19]. 此类系统通过对光学衍射成像系统的结构进行改造，通过改变系统的各种参数(照明波长、随机相位板位置)获取多幅衍射图像(密文)，进而利用相位恢复算法还原原始图像. 由于将衍射强度作为密文，避免了使用干涉装置，因而对系统稳定性的要求大大地降低. 此外，由于密文只保留了复数场的强度信息，破坏了系统的线性，安全性也较 DRPE 系统进一步增强. 为了能够高质量地恢复出原始图像，这些方法必须记录三幅以上的衍射强度图像作为密文，使传输较为不便. 更重要的是，为了记录三幅以上的衍射强度，加密过程需要移动光学元件[17-18]或者改变照明方式[19]，这极大地增加了加密过程实施的难度. 为了提高此类系统的效率，本课题组提出了从单幅衍射图像中恢复原始图像的新算法[20-21]，但是这些算法需要向原始图像添加冗余数据，或者在恢复明文的过程中需要大量的迭代运算，收敛速度较慢.

本文中将频谱融合技术与光学衍射加密相结合，提出一种彩色图像加密方法. 该方法可将一副彩色图像隐藏于单幅强度图像之中，在光学衍射图像加密系统中实现彩色图像的加密，与文献[17-19]的方法相比，提高了系统的加密容量. 此外，由于在光学衍射结构的输入平面引入了特殊的振幅限制，本方法完成解密过程所需要的迭代次数明显降低，极大地节省了解密时间.

1 理论分析

1.1 加密原理

本方法的基本思路为，在离散余弦变换(Discrete CosineTransform，DCT)域内，将原始彩色图像的R、G、B分量的频谱通过空间复用技术融合，得到一个大小与原始图像相同的正实值目标图像. 然后将此目标图像利用光学衍射加密系统加密，得到单幅衍射图像(密文).

设 $f_R(p,q)$，$f_G(p,q)$，$f_B(p,q)$分别是被加密彩色图像的 R、G、B 分量，为了实现加密目标，首先要把这三个分量的信息集中存储于单个实矩阵之中. 这里采用 DCT 域的频谱融合技术来实现[22]，其基本原理如下：首先，分别对 $f_R(p,q)$，$f_G(p,q)$，$f_B(p,q)$做离散 DCT 变换，得到相应的 DCT 频谱矩阵. 然后将每个频谱均乘以一个滤波器，以保留左上角 1/4 的频谱数据，而舍弃剩余 3/4 的数据，即把这些数据置零. 这样就得到了三个片段频谱数据. 然后将这三个片段频谱数据分别在原矩阵中移位，使之分别占据左上角、左下角以及右下角的位置. 再将移位后的频谱叠加，就得到了包含原始图像信息的复合频谱. 这个过程可用图 1 来表示. 由图 1 可见，由于三个频谱在空间上互不重叠，因而不会造成信息的混叠. 此外，由 DCT 变换的特性可知，矩阵经 DCT 变换之后的频谱能量主要集中于左上角，因此这些片段频谱数据已经保留了原始图像的大部分信息[22]. 需要说明的是，复合频谱右上角的数据全部为零，是一个特殊的数据区域，将此数据记作 SD(x,y)，并将其作为密钥保存. 显然，由于 SD(x,y)与三个片段频谱数据不相关，可以作为信息恢复密钥.

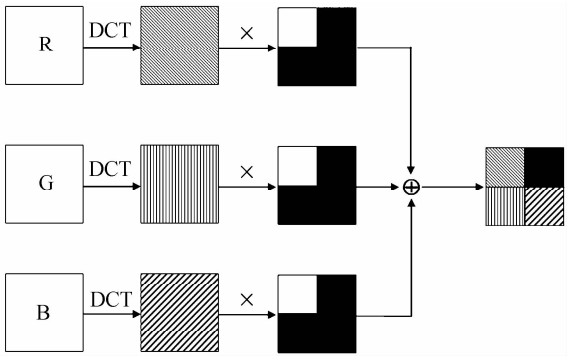

图 1 基于 DCT 变换的频谱融合过程

Fig. 1 The process of spectrum fusion based on DCT transform

在得到复合频谱之后，将其置入光学衍射成像加密系统中进行加密，如图 2 所示. 其中 U 为待加密的明文，即复合频谱. M_1，M_2 是相位板，其相位均匀地分布在$[0,2\pi]$区间，且二者统计独立. 原始明文被波长为 λ 的单色平面光波所照射，首先被与之紧贴的随机相位板 M_1 调制，之后经过距离为 d_1 的衍射之后到 M_2 所在平面，再被 M_2 调制，之后衍射至输出平面，其强度被 CCD 记录，该衍射强度即作为密文保存. 方便起见，采用(x,y)，(η,ξ)，(μ,ν)分别表示 M_1，M_2 及 CCD 所在平面的坐标.

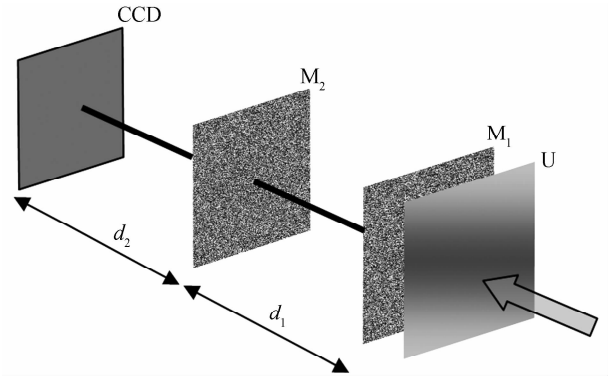

图 2 所提出的用于加密复合频谱的光学衍射加密结构

Fig. 2 The proposed schematic of optical setup for encrypting the composite spectrum

在图 2 所示结构中，根据菲涅耳近似，入射到随机相位板 M_2 的光波前可表示为[15]

$$U(\eta,\xi)=\frac{\exp(\mathrm{j}2\pi d_1/\lambda)}{\mathrm{j}\lambda d_1}\times\iint U(x,y)M_1(x,y)\cdot \exp[\mathrm{j}\pi[(x-\eta)^2+(y-\xi)^2]/\lambda d_1]\mathrm{d}x\mathrm{d}y \quad (1)$$

便于标记，将式(1)改写为

$$U(\eta,\xi)=\mathrm{FrT}_\lambda[U(x,y)M_1(x,y);d_1] \quad (2)$$

式中 FrT_λ 表示菲涅耳变换. 因此，输出平面 CCD 所获取的强度图像可以表示为

$$I(\mu,\nu)=|\mathrm{FrT}_\lambda\{\mathrm{FrT}_\lambda[U(x,y)M_1(x,y);d_1]M_2(\eta,\xi);d_2\}|^2 \quad (3)$$

$I(\mu,\nu)$作为密文保存.

1.2 解密过程

解密过程为加密过程的逆过程，首先从密文 $I(\mu,\nu)$中恢复出复合频谱. 本文提出的恢复复合频谱的算法如下：

首先，给欲恢复的复合频谱赋予一个随机实值矩阵 $T_n(x,y)$，$n=1$ 作为初始值，n 表示迭代次数. 在 CCD 平面得到的复振幅为

$$U_n(\mu,\nu)=\mathrm{FrT}\{\mathrm{FrT}[T_n(x,y)M_1(x,y);\lambda;d_1]M_2(\eta,\xi);\lambda;d_2\} \quad (4)$$

之后，利用以 CCD 先前记录的密文(即 $I(\eta,\xi)$)作为振幅支撑替代 $U_n(\mu,\nu)$的实部构造一个新函数，即

$$\overline{U_n(\mu,\nu)}=I(\mu,\nu)^{1/2}U_n(\mu,\nu)/|U_n(\mu,\nu)| \quad (5)$$

之后，将$\overline{U_n(\mu,\nu)}$逆衍射至输入平面，此时得到输入平面的振幅可表示为

$$\overline{T_n(x,y)}=|\mathrm{FrT}\{\mathrm{FrT}[\overline{U_n(\mu,\nu)};\lambda;-d_2]M_2^*(\eta,\xi);\lambda;-d_1\}|^2 \quad (6)$$

这里 $*$ 为复共轭，$\|$ 表示取模运算. 然后利用加密时保存的 $\mathrm{SD}(x,y)$作为输入平面的振幅支撑，与$\overline{T_n(x,y)}$相结合(对应位置的元素直接相乘)来形成一个对输入图像的新的估计 $T_{n+1}(x,y)$，此过程可表示为

$$T_{n+1}(x,y)=\mathrm{SD}[(x,y)]\overline{T_n(x,y)} \quad (7)$$

式(4)～(7)即描述了一次完整的迭代过程，该迭代过程一直持续，直至迭代收敛. 通过评估 $T_{n+1}(x,y)$与 $T_n(x,y)$之间的均方误差来决定迭代是否继续，该误差可表述为

$$\mathrm{Error}=\sum[|T_n(x,y)|-|T_{n+1}(x,y)|]^2 \quad (8)$$

如果 Error 不小于预先设定的阈值，则将 $T_{n+1}(x,y)$代入式(4)中进行下一次迭代. 否则，就将 $T_{n+1}(x,y)$作为解密图像(复合频谱).

在得到复合频谱之后，就可以从其中分别提取出来 R、G、B 的部分 DCT 频谱，再对这些频谱进行 DCT 逆变换，就可以恢复出来 $f_R(p,q)$，$f_G(p,q)$，$f_B(p,q)$. 此外，我们引入相关系数来客观地评价解密结果的质量. 以原始复合频谱和解密出来的复合频谱为例，二者之间的相关系数(Correlation Coefficient，CC)被定义为

$$\mathrm{CC}=\frac{E\{[U-E(U)][|T_{n+1}|-E(|T_{n+1}|)]\}}{\sqrt{E\{[U-E(U)]^2\}E\{[|T_{n+1}|-E(|T_{n+1}|)]^2\}}} \quad (9)$$

这里 $E[]$表示数学期望，此处为了简单起见省略了坐标.

2 计算机仿真实验

为了验证所提方法的有效性，在 PC 机上使用 MATLAB2011a 进行了实验. 模拟中，照明所用光波波长 $\lambda=632.8$ mm，轴向距离取值为 $d_1=d_2=50$ mm. 迭代过程中用来判断迭代次数的阈值为 Error=0.0001. 被测试的图片为 Lena，在图 3(a) 中给出，其大小为 512×512 像素. 图 3(b)，(c)，(d)分别为原始图像的 R，G，B分量，图3(e)，(f)，(g)分别为这些分量对应的

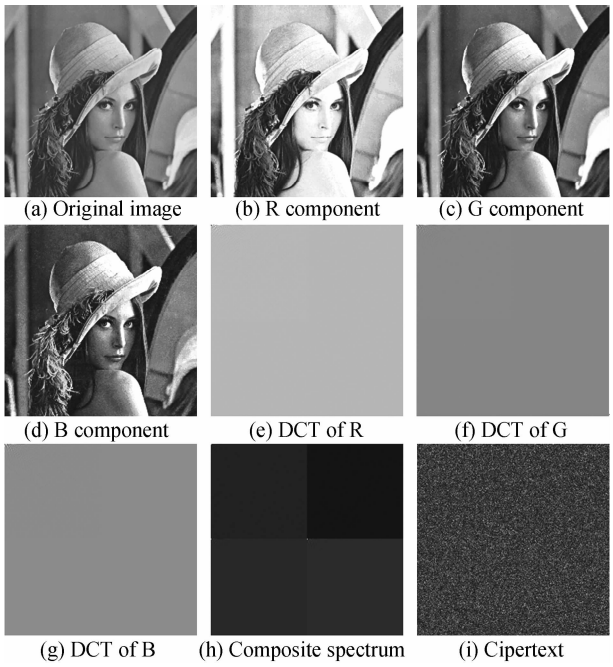

图 3 原始图像及加密结果

Fig. 3 The primary image and the encryption results

DCT 频谱.图 3(h)给出了图像的复合频谱,其右上角黑色区域即为数据为零的区域,即 SD(x,y),此区域在迭代过程中用作输入平面的振幅支撑.

利用本文所提出的算法对复合频谱(明文)进行恢复,相关系数与迭代次数的关系在图 4(a)中给出.可见,相关系数的收敛过程非常迅速,其在迭代 147 次后即达到 1,这说明复合频谱被准确地再现出来.在恢复出复合频谱之后,分别提取 R、G、B 三个灰度分量的 DCT 频谱,并作逆 DCT 变换,得到恢复出来的 R、G、B 分量灰度图,如图 4(c),(d),(e)所示,他们分别与原始图像的相关系数分别为 CC=0.9844,CC=0.9809,CC=0.9658.从图中可以看出,恢复出来的图像丢失了部分细节信息,这是因为在截取 DCT 频谱时候其高频分量被舍去.尽管如此,原始图像的大部分信息依然被恢复出来.图 4(f)是恢复出来的原始图像,可见其质量非常令人满意.

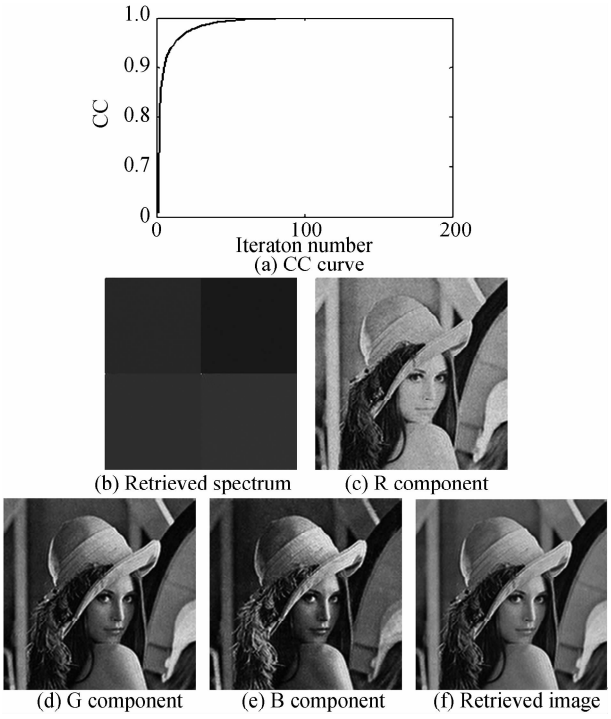

图 4 利用本文所提方法的解密结果

Fig. 4 The decryption results with the proposed method

作为对比,图 5 中给出了使用传统相位恢复算法时的解密结果[23].图 5(a)给出了相关系数与迭代次数的关系.可见,尽管在前 60 次迭代中上升非常迅速,但是迭代 360 次后相关系数就停滞在 CC=0.8 的平台上,迭代出现了停滞.对应于 CC=0.8 的时解密得到的复合频谱在图 5(b)中给出.从此复合频谱中提取 R、G、B 分量,如图 5(c),(d),(e)所示,其对应的相关系数分别为 CC=0.0511, CC=0.0762, CC=0.0727.可见,从这些图像中无法探知原始图像的任何信息.图 5(f)是恢复出来的原始图像.因此可知,在没有对输入平面采用振幅限制时,使用普通的相位恢复算法无法正确恢复原始图像.

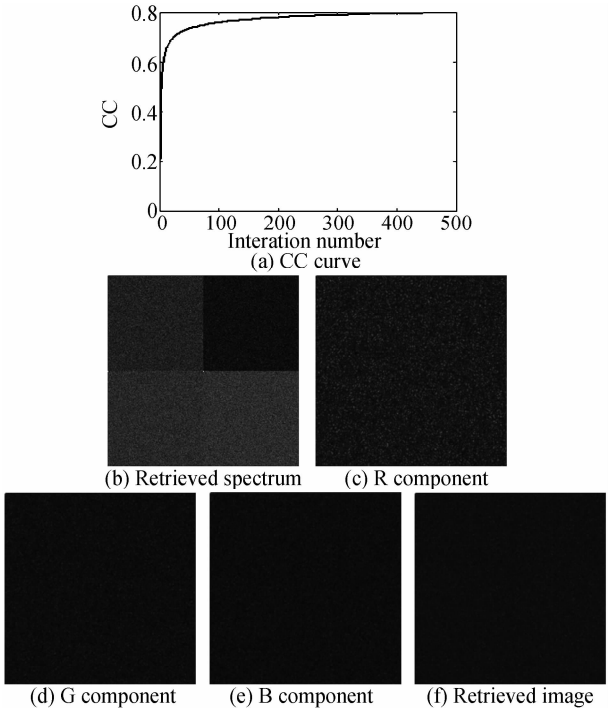

图 5 利用普通相位恢复算法的解密结果

Fig. 5 The decryption results with the traditional phase retrieval method

为了测试本方法的安全性,分别测试了解密结果对于密钥 M_1 和 M_2 的敏感性.图 6(a)~(c)给出了当 M_1 错误而其他参数正确的情况下的解密结果.图 6(a)为此时相关系数与迭代次数的关系,可见相关系数始终维持在一个较小范围之内.图 6(b)为迭代次数 500 次时解密得到的复合频谱,与原始复合频谱的相关系数为 CC=0.0035.图 6(c)为还原出来的原始图像,可见由其无法获知原始图像的任何信息.因此本方法对密钥 M_1 特别敏感,这证实了本方法具有较高的安全性.当 M_2 错误而其他参数正确情况下的解密结果与 M_1 类似,因此为了简明不再给出.在实际应用中,波长 λ 以及轴向距离 d_1, d_2 作为附加密钥可进一步加强系统的安全性,因此我们也研究了解密结果对于他们的敏感性.图 6(d),(e),(f)则给出了解密时轴向距离 d_1 与正确值相差 1mm 的解密结果,图 6(d)为此时相关系数与迭代次数的关系,图 6(e)为迭代次数 500 次时解密得到的复合频谱,与原始复合频谱的相关系数为CC=0.0006.图 6(f)为由图 6(e)还原出来的原始图像,可见由其无法获知原始图像的任何信息.由于对 d_2 存在偏差的情况下的仿真结果与 d_1 类似,因此这里不再给出.图 6(g),(h),(i)则给出了解密时其他参数正确情况下,所使用波长偏离正确波长(加密时所用波长)10 μm情况下的解密结果.其中图 6(g)为相关系数与迭代次数之间的关系,图 6(h)为迭代次数 500 次时解密得到的复合频谱,与原始复合频谱的相

关系数为CC=0.0032. 图 6(i)为由图 6(h)还原出来的原始图像. 由以上仿真结果可知，本方法对于附加密钥波长 λ 以及轴向距离 d_1，d_2 相当敏感，因此本系统具有较高的安全性.

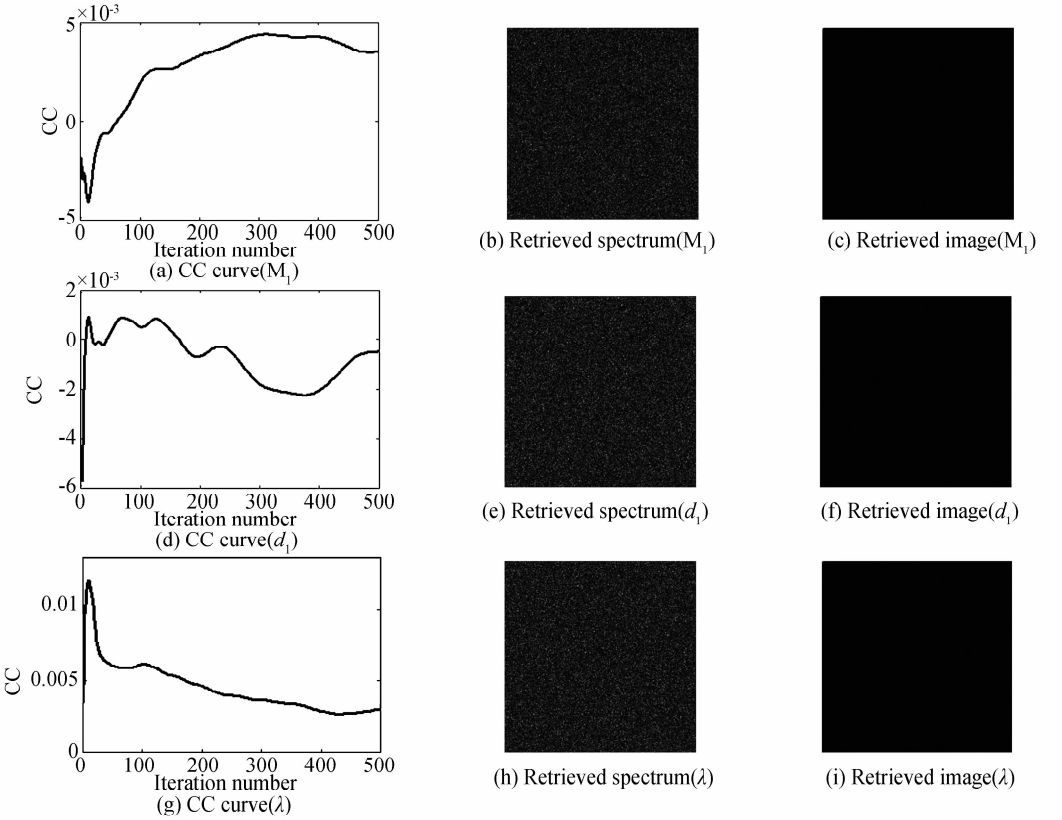

图 6　密钥错误时的解密结果

Fig. 6　The decryption results with wrong secret keys

3　结论

本文提出了一种基于频谱融合技术和光学衍射成像原理的彩色图像加密方法. 本方法首先通过将彩色图像分解为 R、G、B 分量，再对其进行 DCT 变换获取相应的频谱. 之后，通过频谱融合技术，保留着三个 DCT 频谱的主要成分，并将其储存于一个实值图像之中，此图像即为复合频谱. 利用光学衍射成像加密系统对复合频谱进行加密，可以利用相位恢复算法把复合频谱完全恢复出来，其原因在于已经在复合频谱中设置了一个特殊的数据区域. 此外，与先前的一些方法相比[17-19]，本文可将一幅彩色图像隐藏于单幅强度图像之中，极大地提高了加密效率. 计算机仿真结果证实了本方法的可行性和有效性.

参考文献

[1] ZHANG Da-kui, MA Li-hong, LIU Jian, *et al*. Amplitude image optical encryption based on two-step-only quadrature phase-shifting interferometry [J]. *Acta Photonica Sinica*, 2012, **41**(1):72-76.
曾大奎，马利红，刘健，等. 基于两步正交相移干涉的振幅图像光学加密技术[J]. 光子学报，2012，**41**(1)：72-76.

[2] JIA Li-juan, LIU Zheng-jun. Double image encryption algorithm based on random fractional Fourier transform[J]. *Acta Photonica Sinica*, 2009; **38**(4): 1020-1024.

[3] ZHOU Nan-run, WANG Yi-xian, GONG Li-hua, *et al*. Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform[J]. *Optics Communications*, 2011, **284**: 2789-2796.

[4] QIN Y, GONG Q. Interference-based multiple-image encryption with silhouette removal by position multiplexing [J]. *Applied Optics*, 2013,**52**(17):3987-92.

[5] QIN Yi, ZHENG Chang-bo. Color image encryption based on doublerandom phase encoding [J]. *Acta Photonica Sinica*, 2012, **41**(3):326-239.
秦怡，郑长波. 基于双随机相位编码的彩色图像加密技术[J]. 光子学报，2012，**41**(3)：326-239.

[6] WANG X, ZHAO D. A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms[J]. *Optics Communications*, 2012, **285**: 1078-1081.

[7] LIU W, LIU Z, LIU S. Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm[J], *Optics Letters*, 2013, **38**(10): 1651-1653.

[8] ALFALOU A, BROSSEAU C. Optical image compression and encryption methods [J]. *Advance in Optics and Photonics*, 2009, **1**(3):589-636.

[9] LIU S, GUO C, SHERIDAN J T. A review of optical image encryption techniques [J], *Optics and Laser Technology*, 2014, **57**:327-342.

[10] NOMURA T, JAVIDI B, Optical encryption using a joint transform correlator architecture[J], *Optical Engineering*, 2000, **39**(8): 2031-2035.

[11] ZHANG Y, WANG B. Optical image encryption based on interference[J]. *Optics Letters*, 2008, **33**(21):2443-2445.

[12] QIN W, PENG X. Asymmetric cryptosystem based on phase-truncated Fourier transforms[J]. *Optics Letters*, 2010, **35**(2): 118-120.

[13] HWANG H E, CHANG H T, LIE W N. Multiple-image encryption and multiplexing using a modi? ed Gerchberg - Saxton algorithm and phase modulation in Fresnel transform domain[J]. *Optics Letters*, 2009, **34**(24): 3917-3919.

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

[15] SI-TU Guo-hai, ZHANG Jing-juan. Double random-phase encoding in the Fresnel domain[J]. *Optics Letters*, 2004, **29**(14): 1584-1586

[16] UNNIKRISHNAN G, JOSEPH J, SINGH K. Optical encryption by double-random phase encoding in the fractional Fourier domain[J]. *Optics Letters*, 2000, **25**(12): 887-889.

[17] CHEN Wen, CHEN Xu-dong, SHEPPARD C J R. Optical image encryption based on diffractive imaging[J]. *Optics Letters*, 2010, **35**(22): 3817-3819.

[18] CHEN Wen, CHEN Xu-dong, SHEPPARD C J R. Optical double-image cryptography based on diffractive imaging with a laterally-translated phase grating[J]. *Applied Optics*, 2011, **50**(29): 5750-5757.

[19] CHEN Wen, CHEN Xu-dong, ANAND A, *et al*. Optical encryption using multiple intensity samplings in the axial domain[J]. *Journal of* the Optical *Society of America A*, 2013, **30**(5): 806-812.

[20] QIN Y, GONG Q, WANG Z. Simplified optical image encryption approach using single diffraction pattern in diffractive-imaging-based scheme[J]. *Optics Express*, 2014, **22**(18): 21790-21799.

[21] QIN Y, WANG Z, GONG Q. Diffractive-imaging-based optical image encryption with simplified decryption from single diffraction pattern[J]. *Applied Optics*, 2014, **53**(19): 4094-4099.

[22] ALFALOU A, BROSSEAU C, ABDALLAH N. Simultaneous compression and encryption of color video images[J], *Optics Communications*, 2015, **338**, 371-379.

[23] GERCHBERG R. A practical algorithm for the determination of phase from image and diffraction plane pictures[J]. *Optik*, 1972, **35**: 237-246.