一种基于随机相位板复用的光学多二值图像加密系统

秦 怡[1] 李 婧[2] 马毛粉[1] 吕晓东[1]

([1] 南阳师范学院物理与电子工程学院，河南 南阳 473061
[2] 南阳师范学院数学与统计学院，河南 南阳 473061)

摘要 利用随机相位板复用提出了一种基于干涉原理的光学多二值图像加密系统。该系统加密过程采用数字方法，解密过程既可以采用数字方法也可以采用光学方法。利用该方法可将多幅图像信息解析地隐藏于两个纯相位板中。解密时，通过分束镜将两个随机相位板的衍射场进行相干叠加形成干涉场，利用专用密钥对此干涉场进行调制，即可在输出平面上恢复出与该专用密钥对应的原始图像，此图像可以采用 CCD 等图像传感器件直接记录。该方法加密过程无需迭代，非常省时，且解密系统易于物理实现。利用相关系数评估了系统的加密容量，计算机模拟结果证实了该方法的有效性。

关键词 图像处理；多图像加密；干涉原理；随机相位板复用

中图分类号 TP751 **文献标识码** A **doi**：10.3788/AOS201434.0307001

System for Optical Multiple Binary Image Encryption by Random Phase Mask Multiplexing

Qin Yi[1] Li Jing[2] Ma Maofen[1] Lü Xiaodong[1]

([1] *College of Physics and Electronic Engineering, Nanyang Normal University, Nanyang, Henan* 473061, *China*
[2] *College of Mathematics and Statistics, Nanyang Normal University, Nanyang, Henan* 473061, *China*)

Abstract A system for interference-based optical multiple binary image encryption by random phase mask multiplexing is proposed. The encryption process is realized digitally and the decryption process can be completed optically or digitally. Multiple binary images can be analytically hidden into two phase only masks (POMs). For decryption, the diffraction filed of the two POMs are superposed by utilizing the beam splitters to form a complex field, then the complex field is further modulated by the private key, as a result of which the original plaintext assosicated with the private key is retrieved. The regenerated image can be directly recorded by CCD camera. The encryption algorithm for this new method is quite simple and does not need iterative encoding. In addition, the decryption system is easy to be realized physically. The multiplexing capacity is analyzed through the correlation coefficient. Computer simulation results confirm the validity of the proposal.

Key words image processing; multiple-image encryption; principle of interference; radom phase mask multiplexing

OCIS codes 070.4560; 070.1170 ; 090.2880

1 引 言

近年来，光学信息处理在信息安全领域内的应用引起了极大的兴趣与关注，成为目前信息光学的研究热点之一[1-10]。利用光学信息处理技术，可以实现对二维数据的高速并行加密及解密。光学信息安全领域内最著名的成果为 1995 年 Refregier 等[11]提出的双随机相位编码系统，在光学 4f 系统的输入平面以及频域平面分别放置一个随机相位板，可将任意一复数场加密为平稳白噪声。该系统提出不久即被推广至菲涅耳域[12]及分数傅里叶域[13]，同时，也被证实对多种密码学攻击具有脆弱性[14-15]，安全性不高。事实上，限制该系统应用的最重要的原因在于加密结果为复数场，这很难用目前的光学技术来实现，因为现有的空间光调制器无

收稿日期：2013-09-03；**收到修改稿日期**：2013-11-04

基金项目：国家自然科学基金项目(61306007)、河南省科技厅基础与前沿项目(132300410290)

作者简介：秦 怡(1981—)，男，硕士，讲师，主要从事光电信息处理方面的研究。E-mail：641858757@qq.com

法对光波的振幅和相位同时进行调制。于是，人们开始考虑将信息加密至两个或者多个纯相位板(POM)中[16-18]。其中，由 Zhang 等[18]提出的基于干涉原理的加密方法(IBOE)具有代表性，该系统解析地将一幅图像隐藏于两个 POM 之中，整个过程无需迭代，非常省时，同时，解密结构非常简单，易于光学实现，该系统已经被 Weng 等[19]使用实验间接证实。

近年来，在关注光学加密系统性能的同时，人们也提出了不少方法来提高加密的效率，先后提出了一些多图像加密和隐藏技术[20-30]。例如，Liu 等[20]利用频谱移位并结合双随机相位编码实现了多图像加密，Zhe 等[25]在相移数字全息系统中利用随机相位匹配实现了多图像隐藏，Situ 等[26,29]利用波长复用技术，分别在菲涅耳域双随机相位编码系统以及光学联合相关变换结构中实现了多图像加密. 对于 IBOE 系统来说，已经由 Wang 等[31-32]分别在该系统上实现了双图像加密与多图像加密。但是，他们加密过程所采用的方法均为相位恢复中所使用的迭代算法，非常耗时，几乎抵消掉 IBOE 系统在节约时间方面的优越性。此外，Qin 等[33]也提出一种基于 IBOE 的新算法，但是算法中要求 POM 互相紧贴，这在物理上难以实现，且解密过程需要 CCD 进行轴向移动连续记录，因而使得系统空间成本较大。本文在 IBOE 系统引入一个作为密钥的相位板，利用所提出的复用方法成功地设计了一种无迭代过程的光学多二值图像加密系统。多幅图像被解析地隐藏于两个 POM 中，这两个 POM 作为密文保存。在解密过程中不仅需要密文，也需要一个与被加密图像对应的专用密钥，即第三个 POM。该方法加密原理非常简单，且加密过程无需迭代，因而与文献[31-32]所述方法相比，非常省时。同时，与文献[33]所述方法相比，不要求 POM 互相紧贴，解密过程也无需移动 CCD，因而易于光学实现，因而有望用于海量数据的加密及解密。此外，由于在系统中引入了第三个 POM，彻底消除了存在于 IBOE 系统的轮廓像问题，同时也极大地增加了系统的密钥空间，这表明本加密系统具有较高的安全性。

2　理论分析

2.1　加密算法

本方法加密过程采用数字方法实现，而解密过程既可以采用数字方法也可以采用光学方法来实现。为了便于说明系统的加密算法，图 1 给出了解密时所使用的光学结构。M1，M2 为纯相位板，BS 为分束镜，g 为中介函数，$\hat{f}_k$ 为解密所得第 k 幅复数图像。假定有 N 幅图像隐藏于纯相位板 M1 及 M2 中，并用 $f_k(x_o,y_o)$ 表示第 $k(k=1,\cdots,N)$ 幅原始图像，同时，用 P_k 表示与 $f_k(x_o,y_o)$ 相对应的密钥。解密过程可简述如下：随机相位板 M1，M2 被波长为 λ 的单色平面光波照射，均经过距离为 l 的菲涅耳衍射到达 S 平面。之后，此干涉场被随机相位板 P_k 进一步调制后，再经过距离为 d 的衍射到达输出平面 H，此时解密出来的即 $f_k(x_o,y_o)$，可以使用图像传感器(如 CCD 等)直接记录。可以看出，解密过程所涉及的光学器件非常少，容易利用光学方法实现。

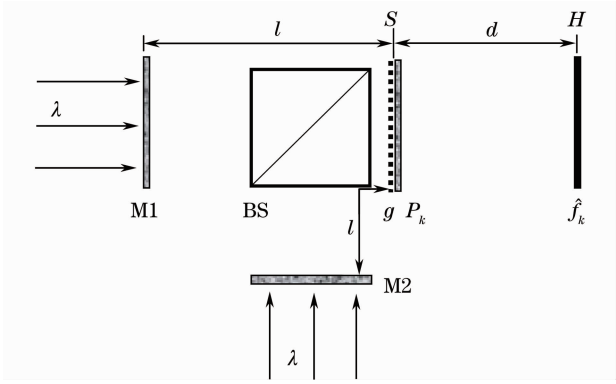

图 1　解密系统示意图

Fig. 1　Schematic of the optical decryption system

加密过程即把 N 幅图像隐藏于两个纯相位板 M1，M2 及相应的密钥 P_k 中。需要说明的是，$P_k(k=1,\cdots,N)$ 均为计算机产生的随机相位板，且彼此之间相互独立。对于第 k 幅待加密图像 $f_k(x_o,y_o)$，通过给其赋予一个随机相位而构成一个复函数

$$f'_k(x_o,y_o)=\sqrt{f_k(x_o,y_o)}\exp[\mathrm{i}2\pi\mathrm{rand}(x_o,y_o)], \tag{1}$$

式中 rand 函数产生位于[0，1]之间的随机白噪声。之后，假设该复函数被一波长为 λ 的单色平面波所照射，并从如图 1 所示的输出平面 H 经菲涅耳逆衍射至平面 S，衍射距离为 d。平面 S 上所得到的衍射光场 $g'_k(x,y)$ 可用数学公式描述为

$$g'_k(x,y)=\mathrm{FrT}_\lambda[f'_k(x_o,y_o);-d], \tag{2}$$

式中 FrT_λ 表示关于 λ 的菲涅耳变换[8]。将 $g'_k(x,y)$ 乘以随机相位板 P_k 的共轭，得到

$$g_k(x,y)=g'_k(x,y)P_k^*(x,y). \tag{3}$$

把所得到的 $g_k(x,y)$ 进行叠加，得到一个中介函数

$$g(x,y)=\sum_{k=1}^{N}g_k(x,y). \tag{4}$$

该中介函数在图 1 所示的解密光路中用虚线表示，

用以说明加密过程。进一步将 $g(x,y)$ 隐藏于两纯相位板 M1 及 M2 中。由图 1 可知，$g(x,y)$ 可表示为二者衍射光场的叠加，即

$$g(x,y)=\exp(\mathrm{i}M_1)*h(x_m,y_m,l)+\exp(\mathrm{i}M_2)*h(x_m,y_m,l),\tag{5}$$

式中

$$h(x_m,y_m,l)=\frac{\exp(\mathrm{i}2\pi l/\lambda)}{\mathrm{i}\lambda l}\exp[\mathrm{i}\pi(x_m^2+y_m^2)/\lambda l].\tag{6}$$

表示菲涅耳衍射过程的单位冲击响应，* 表示卷积运算，l 表示相位板至 $g(x,y)$ 所在平面的距离，M_1，M_2 分别为 M1 和 M2 的相位。利用傅里叶变换理论，可将(5)式变形为

$$\exp(\mathrm{i}M_1)+\exp(\mathrm{i}M_2)=D,\tag{7}$$

式中 $D=\mathscr{F}^{-1}\{\mathscr{F}[g(x,y)]/\mathscr{F}[h(x_m,y_m,l)]\}$。这里 $\mathscr{F}$ 表示傅里叶变换，而 $\mathscr{F}^{-1}$ 表示逆傅里叶变换。因为 M1 及 M2 均为纯相位板，所以其模均为 1，因此有

$$[D-\exp(\mathrm{i}M_1)][D-\exp(\mathrm{i}M_1)]^*=1.\tag{8}$$

解得

$$M_1=\arg(D)-\arccos[\mathrm{abs}(D)/2].\tag{9}$$

代入(7)式可得

$$M_2=\arg[D-\exp(\mathrm{i}M_1)],\tag{10}$$

式中 arg 和 abs 分别表示取复数的辐角与模。这样，就把 $g(x,y)$ 隐藏于两个纯相位板 M1 及 M2 中。

2.2　解密过程

根据加密过程的原理，解密过程可以认为包含两个过程(见图 1)。第一个过程为由波长为 λ 的相干光分别照射 M1 及 M2，其衍射场在距离相位板 l 处叠加形成中介函数 $g(x,y)$。由于 M1 及 M2 是经解析所得，因而该过程是无损的，即由 M1 及 M2 可完全恢复出 $g(x,y)$。第二个过程为中介函数 $g(x,y)$ 被解密密钥 P_k 调制后，再经距离为 d 的衍射，在输出面上得到第 k 幅解密图像，这个过程可以表示为

$$\hat{f}_k(x_o,y_o)=\sum_{k=1}^{N}\mathrm{FrT}_\lambda[g_k(x,y)P_k^*(x,y)P_q(x,y);d]=f'_k(x_o,y_o)+n^k(x_o,y_o),\tag{11}$$

式中

$$n^k(x_o,y_o)=\sum_{q\neq k}^{N}n_q(x_o,y_o)=\sum_{q\neq k}^{N}\mathrm{FrT}_\lambda\{\mathrm{FrT}_\lambda[f'_q(x_o,y_o);-d]P_q^*(x,y)P_k(x,y);d\}.\tag{12}$$

由于中介函数 $g(x,y)$ 仅仅用于分析解密与加密过程，所以在图 1 中使用虚线表示。由(11)式可以看出，解密结果由两部分组成：一部分为 $f'_k(x_o,y_o)$，这正是加密时被加密的第 k 幅复数图像；第二部分为 $n^k(x_o,y_o)$，这是 $g(x,y)$ 中所包含的另外 $N-1$ 幅图像的信息经不正确的专用密钥解密所得到的结果。一般来说，只有 $n^k(x_o,y_o)$ 表现为白噪声图样时，$f'_k(x_o,y_o)$ 才可以被正确地恢复出来。

现在考察(12)式中每一项的统计特性。将(12)式中的各项重写为

$$n_q(x_o,y_o)=\mathrm{FrT}_\lambda\{\mathrm{FrT}_\lambda[f'_q(x_o,y_o);-d]P_q^*(x,y)P_k(x,y);d\}(q\neq k),\tag{13}$$

前面已经指出，N 个密钥 P_k 之间相互独立，那么 $P_q^*(x,y)P_k(x,y)(q\neq k)$ 依然为一随机相位分布。同时，联系(1)式，那么此时(13)式的物理含义为 $\sqrt{f_k(x_o,y_o)}$ 经历了菲涅耳域的双随机相位编码过程。Situ 等[13]已经证实，在这种情况下的编码结果 $n_q(x_o,y_o)$ 具有白噪声性质。因而作为各个白噪声项的简单叠加，$n^k(x_o,y_o)$ 同样具有白噪声特性。因此 $f'_k(x_o,y_o)$ 可以被正确地重建。这样，在输出平面用 CCD 记录得到的复数场 $f'_k(x_o,y_o)$ 的强度，就恢复出来了第 k 幅原始图像 $f_k(x_o,y_o)$。

3　计算机模拟

为了证实所提方法的有效性，在 PC 机上使用 Matlab R2011a 进行了模拟。对加密图像数为 $N=4$ 的情况进行测试，这 4 幅原始图像在图 2(a)～(d)中给出，图片大小均为 512 pixel×512 pixel，1 cm×1 cm。模拟中，所取距离参数分别为 $l=200$ mm，$d=100$ mm。照明所用光波波长 $\lambda=632.8$ nm。图 2(e)～(h)给出了与 4 幅原始图像对应的专用密钥，即 $P_k(k=1,2,3,4)$，这些专用密钥均使用 Matlab 的 rand 函数产生。随后，利用 2.1 节所提算法对 4 幅原始图像加密，所得到的密文，即随机相位板 M1 及 M2，如图 2(i)，(j)所示。

在解密参数正确的情况下得到的解密结果如图 3(a)～(d)所示。可以看出，尽管受到噪声影响，但是重建所得图像与原始图像具有较好的相似度，这表明原始结果被正确地解密出来。为了客观地评价这种相似程度，引入相关系数作为评价标准。

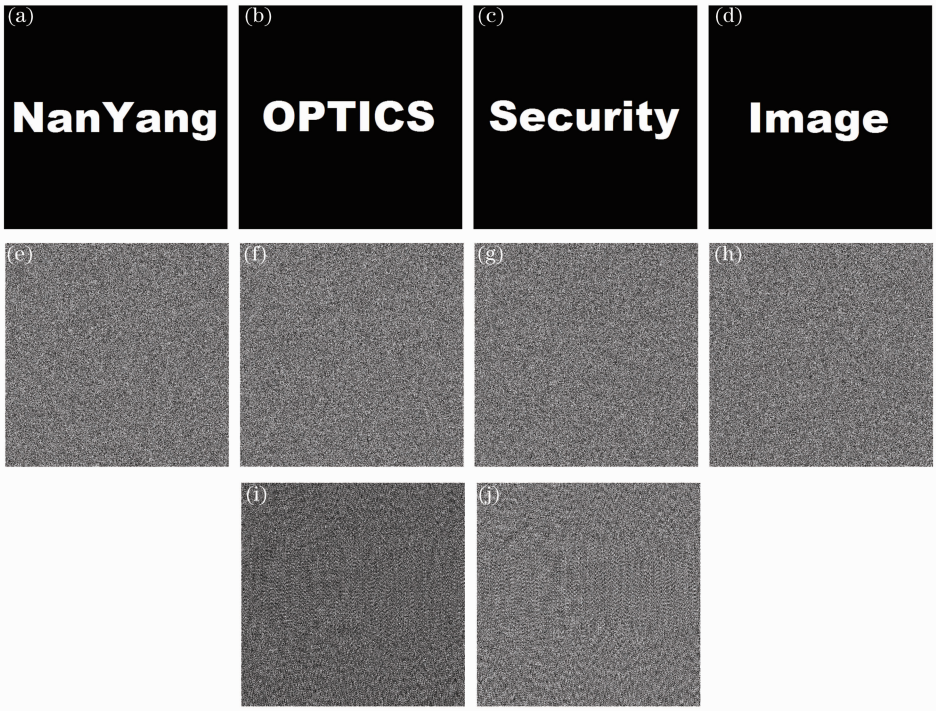

图 2　所提方法的加密结果。(a)～(d) 原始图像；(e)～(h)与原始图像对应的专用密钥；(i)，(j)相位板 M1 及 M2

Fig. 2　Encryption results of the proposal. (a)～(d) Original images; (e)～(h) private keys corresponding to original images; (i), (j) ciphertexts M1, M2

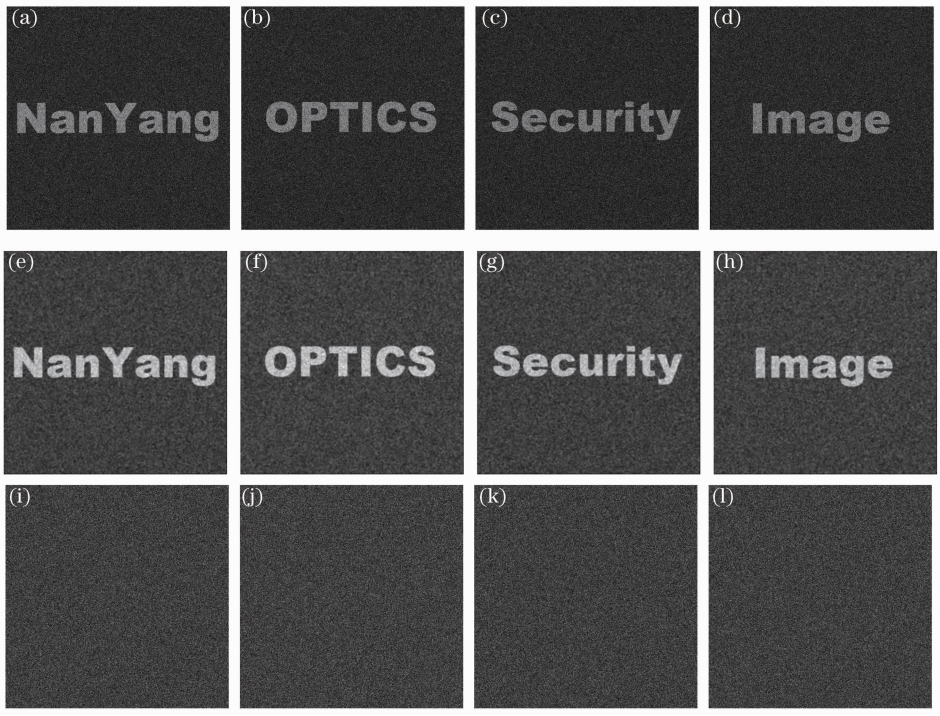

图 3　所提解密方法的解密结果。(a)～(d)直接解密结果；(e)～(h)用 4×4 的窗口进中值滤波；(i)～(l)使用错误密钥

Fig. 3　Decryption results by the proposal. (a)～(d) Directly decryption results; (e)～(h) with 4×4 window mediam filtering; (i)～(l) with wrong keys

原始图像 $f_k(x_o,y_o)$ 与恢复图像 $|\hat{f}_k(x_o,y_o)|$ 之间的相关系数被定义为

$$C_{\mathrm{C}}=\frac{E\{[f_k-E(f_k)][|\hat{f}_k|-E(|\hat{f}_k|)]\}}{\sqrt{E\{[f_k-E(f_k)]^2\}E\{[|\hat{f}_k|-E(|\hat{f}_k|)]^2\}}},\tag{14}$$

式中 E 表示求数学期望，为了简明起见省去了函数坐标。经计算可得以上 4 幅图像与原始图像之间的相关系数分别为 0.6609，0.6317，0.6245 和0.6018。

事实上，解密图像的质量可以通过简单的图像处理方法而得到进一步提高。正如(11)式所描述的，叠加于正确解密图像之上的噪声具有类似于白噪声的性质，而白噪声为典型的高频噪声。因而可以预期，对解密结果进行低通滤波操作可以对这些高频噪声进行有效抑制，进而提高解密图像与原始图像之间的相关系数。为此，对图 3(a)～(d)中的解密结果采用 4×4 的窗口进行中值滤波，得到的结果如图 3(e)～(h)中所示。可以看出，经过中值滤波后的图像质量得到明显提升，其对应的相关系数分别为 0.9206，0.9121，0.9082 和 08857。图 3(i)～(l)给出了在 M1 及 M2 正确，但专用密钥错误情况下的解密结果，可见解密结果为随机噪声，从中无法获取任何有关原始图像的相关信息，其对应的相关系数分别为-0.0031，-0.0014，-9.9397×10^{-4}和 0.0043。

此外，由 Zhang 等提出的 IBOE 系统存在一个重要的安全漏洞，当攻击者仅获取两个相位板的其中任何一个时，在附加参数正确的情况下，就可通过解密系统得到原始图像的轮廓，而这个轮廓又提供了原始图像的足够信息，即所谓的轮廓像问题。对于本文提出的系统来说，由于作为密钥的第三个相位板的引入，轮廓像问题被完全消除。以图 2(a)中的待加密图像为例，在图 4 中给出了解密时其他参数正确的情况下，分别单独使用 M1、M2、专用密钥 P_1 这三种情况下的解密结果。可见，单独使用这三个相位板中的任何一个，均无法得到与原始图像相关的任何信息，这说明本系统成功的消除了轮廓像问题。同时，与 Zhang 等提出的 IBOE 系统相比，由于专用密钥的引入，使得解密每幅原始图像时均需要用到三个 POM。而由于轮廓像问题的影响，解密 IBOE 系统仅需要知道两个 POM 之一即可。假设 POM 的规格均为 512×512×8 bit，那么 IBOE 系统的密钥空间为 $2^{512\times512\times8\times1}$，而本文方法的密钥空间则为 $2^{512\times512\times8\times3}$，可见相比于 IBOE，本方法极大地扩展了系统的密钥空间，因而提高了系统的安全性。

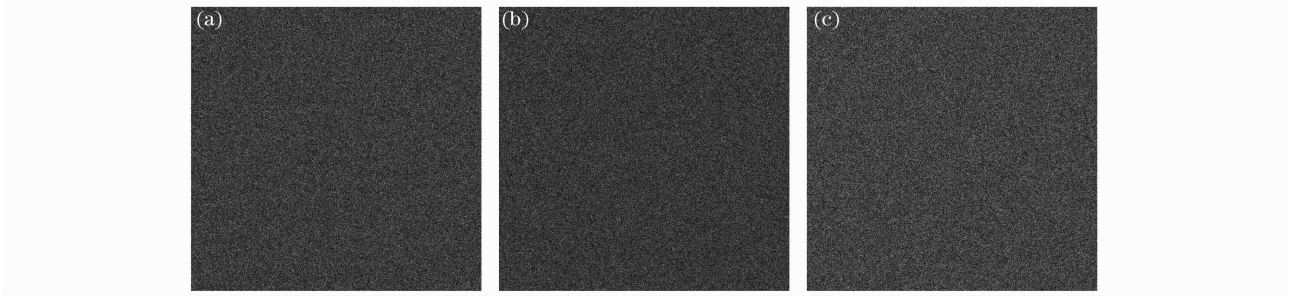

图 4　分别单独使用 (a) M1 (b) M2 和(c)专用密钥 P_1 的情况下的解密结果

Fig. 4　Decrypted images obtained by using only the POM (a) M1, (b) M2 and (c) private key P_1

对于多图像加密系统来说，加密容量是描述该系统性能的一个重要参数。由(12)式可以看出，随着系统加密图像个数的增多，叠加于正确解密图像之上的噪声强度越来越大，直至将正确的解密图像淹没。此时，即使解密参数正确，也不能正确地恢复与之对应的原始图像。因此，有必要确定该系统最多能加密的图像个数 $N_{\max}$，即系统的加密容量。在确定 $N_{\max}$的过程中，同样采用相关系数作为标准进行衡量。简单起见，在此次模拟中所加密的 N 幅图像均为图 2(a)所示图像，加密所采用的距离参数同样为 $l=200$ mm，$d=100$ mm。图 5(a)为加密图像数 $N=10$ 的解密结果。可以看出，图像的质量相比于 $N=4$ 时已经大大降低，其对应的相关系数为 0.3881。对该解密结果同样采用 4×4 的窗口进行中值滤波，得到的结果如图 5(b)所示出。此时对应的相关系数为 0.7807，可见，经中值滤波后的图像质量提升较大。

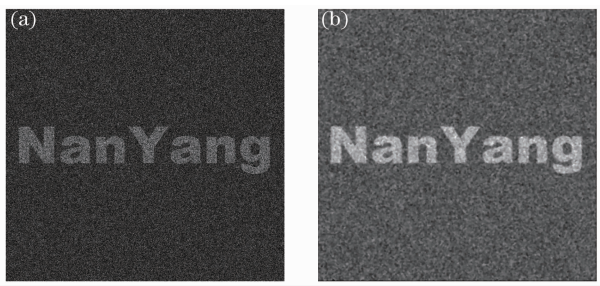

图 5　$N=10$ 时的解密结果。(a)直接解密结果；(b)中值滤波后结果

Fig. 5　Decryption results when $N=10$. (a) Directly decrypted result; (b) decrypted result with median filtering

图 6 中给出了相关系数与加密图像个数 N 之间的关系，其中圆形符号表示的为直接解密图像与原始图像之间的相关系数，正如所分析的，随着加密图像个数 N 的增大，相关系数迅速降低。如果将 $C_C=0.8$ 作为标准来评价原始图像是否被正确重建，那么该系统的加密容量仅为 $N_{max}=2$，不能满足实际应用的需要。但是，在对解密结果进行中值滤波之后，图像的质量得到较大提升，图 5 中倒三角形符号表示经中值滤波之后的解密图像与原始图像之间的相关系数。系统的加密容量提高到了 $N_{max}=9$，可满足实际应用。

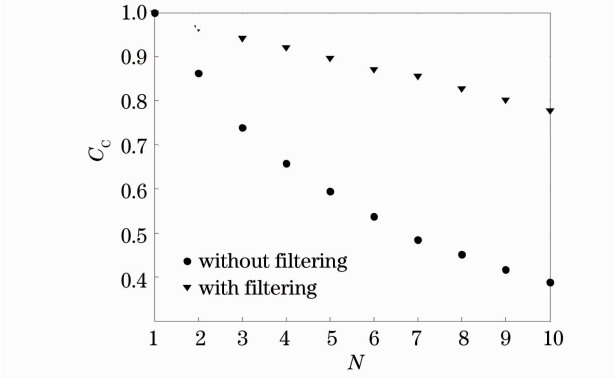

图 6　相关系数与 N 之间的关系

Fig. 6　Behavior of C_C versus N

4　结　论

提出了一种光学多二值图像加密与解密系统。该方法可将多幅图像解析地隐藏于两个纯相位板中，整个加密过程使用数字方法实现，且无需迭代过程，与一些类似方法相比较，该系统加密过程非常省时。解密过程既可以用数字方法也可以用光学方法实现，且所使用的解密光学结构非常简单，既节约了空间又增加了解密的快捷性。同时，该系统彻底消除了先前提出的基于干涉原理光学加密系统中的轮廓像问题。此外，如果将 $C_C=0.8$ 作为评价原始图像是否被正确重建的标准，在对解密结果进行中值滤波后，本系统的加密容量达到了 $N_{max}=9$，有望用于海量数据的高速加密及解密。

参　考　文　献

1 Nanrun Zhou, Yixian Wang, Lihua Gong. Novel optical image encryption scheme based on fractional Mellin transform [J]. Opt Commun, 2011, 284(13): 3234－3242.

2 Wan Qin, Xiang Peng. Asymmetric cryptosystem based on phase-truncated Fourier transforms [J]. Opt Lett, 2010, 35(2): 118－120.

3 Peter Tsang, K W-K Cheung, T-C Poon. Fast numerical generation and hybrid encryption of a computer-generated Fresnel holographic video sequence [J]. Chin Opt Lett, 2013, 11(2): 020901.

4 Xiaogang Wang, Daomu Zhao. Simultaneous nonlinear encryption of grayscale and color images based on phase-truncated fractional Fourier transform and optical superposition principle [J]. Appl Opt, 2013, 52(25): 6170－6178.

5 Qin Yi, Gong Qiong, Li Genquan, *et al*.. An optical encryption method with silhouette removal [J]. Chinese J Lasers, 2012, 39(12): 1209001.
秦　怡，巩　琼，李根全，等. 一种无轮廓像干扰光学加密系统[J]. 中国激光，2012，39(12)：1209001.

6 Qin Yi, Lü Xiaodong, Gong Qiong, *et al*.. Additional keys rotation multiplexing encryption using joint translation correlator [J]. Acta Optica Sinica, 2013, 33(3): 0307002.
秦　怡，吕晓东，巩　琼，等. 利用附加密钥旋转在光学联合相关结构中实现多二值图像加密[J]. 光学学报，2013，33(3)：0307002.

7 Nanrun Zhou, Yixian Wang, Lihua Gong, *et al*.. Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform [J]. Opt Commun, 2011, 284(12): 2789－2796.

8 Xiaogang Wang, Daomu Zhao. Security enhancement of a phase-truncation based image encryption algorithm [J]. Appl Opt, 2011, 50(36): 6645－6651.

9 Yan Zhang, Bo Wang. Optical image encryption based on interference [J]. Opt Lett, 2008, 33(21): 2443－2445.

10 Yujing Han, Yunhai Zhang. Optical image encryption based on two beams′ interference [J]. Opt Commun, 2010, 283(9): 1690－1692.

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

12 G Unnikrishnan, J Joseph, K Singh. Optical encryption by double-random phase encoding in the fractional Fourier domain [J]. Opt Lett, 2000, 25(12): 887－889.

13 G Situ, J Zhang. Double random-phase encoding in the Fresnel domain [J]. Opt Lett, 2004, 29(14): 1584－1586.

14 X Peng, P Zhang, H Wei, *et al*.. Known-plaintext attack on optical encryption based on double random phase keys [J]. Opt Lett, 2006, 31(8): 1044－1046.

15 X Peng, H Q Tang, J D Tian. Ciphertext only attack on double random phase encoding optical encryption system [J]. Acta Physica Sinica, 2007, 56(5): 2629－2636.
彭　翔，汤红乔，田劲东. 双随机相位编码光学加密系统的准密文攻击[J]. 物理学报，2007，56(5)：2629－2636.

16 H T Chang, W C Lu, C J Kuo. Multiple-phase retrieval for optical security systems by use of random-phase encoding [J]. Appl Opt, 2002, 41(23): 4825－4834.

17 Y Li, K Kreske, J Rosen. Security and encryption optical systems based on a correlator with significant output images [J]. Appl Opt, 2000, 39(29): 5295－5301.

18 Y Zhang, B Wang. Optical image encryption based on interference [J]. Opt Lett, 2008, 33(21): 2443－2445.

19 D Weng, N Zhu, Y Wang, *et al*.. Experimental verification of optical image encryption based on interference [J]. Opt Commun, 2011, 284(10): 2485－2487.

20 Z Liu, Y Zhang, H Zhao, *et al*.. Optical multi-image encryption based on frequency shift [J]. Optik, 2011, 122(11): 1010－1013.

21 Z Liu, Y Zhang, S Li, *et al*.. Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains [J]. Opt & Laser Technol, 2013, 47: 152－158.

22 Lihua Gong, Xingbin Liu, Fen Zheng, *et al*.. Flexible multiple-image encryption algorithm based on log-polar transform and

double random phase encoding technique [J]. J Modern Opt, 2013, 60(13): 1074－1082.

23 Ping Ping, Feng Xu, Zhijian Wang. Color image encryption based on two-dimensional cellylar automata [J]. Int J Mod Phys C, 2013, 24(10): 1350071.

24 Xiaogang Wang, Daomu Zhao. Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain [J]. Opt Commun, 2011, 284(1): 148－152.

25 M Zhe, L Z Cai, Q Liu, *et al*.. Multiple image encryption and watermarking by random phase matching [J]. Opt Commun, 2005, 247(1): 29－37.

26 Guohai Situ, Jingjuan Zhang. Multiple-image encryption by wavelength multiplexing [J]. Opt Lett, 2005, 30(11): 1306－1308.

27 Yongliang Xiao, Xianyu Su, Sikun Li, *et al*.. Key rotation multiplexing for multiple-image optical encryption in the Fresnel domain [J]. Opt & Laser Technol, 2011, 43(4): 889－894.

28 G Situ, J Zhang. Position multiplexing for multiple-image encryption [J]. J Opt A: Pure Appl Opt, 2006, 8(5): 391－397.

29 D Amaya, M Tebaldi, R Torroba, *et al*.. Wavelength multiplexing encryption using joint transform correlator architecture [J]. Appl Opt, 2009, 48(11): 2099－2104.

30 H Hwang, H T Chang, W Lie. Multiple-image encryption and multiplexing using a modified Gerchberg-Saxton algorithm and phase modulation in Fresnel-transform domain [J]. Opt Lett, 2009, 34(24): 3917－3919.

31 B Wang, Y Zhang. Double images hiding based on optical interference [J]. Opt Commun, 2009, 282(17): 3439－3443.

32 W Chen, X Chen. Optical multiple-image encryption based on multi-plane phase retrieval and interference [J]. J Opt, 2011, 13(11): 115401.

33 Yi Qin, Qiong Gong. Interference-based multiple-image encryption with silhouette removal by position multiplexing [J]. Appl Opt, 2013, 52(17): 3987－3992.

栏目编辑：李志兰