科学通报 2008 年 第 53 卷 第 11 期: 1241 ~ 1245
论 文
《中国科学》杂志社
SCIENCE IN CHINA PRESS

物光和参考光双加密的数字全息系统

朱一超, 张家森*, 龚旗煌

北京大学物理学院现代光学研究所, 北京 100871
* 联系人, E-mail: jszhang@pku.edu.cn

2008-02-08 收稿, 2008-05-14 接受
国家自然科学基金资助项目(批准号: 10434020, 10521002)

摘要 实现了物光和参考光双加密的数字全息加密方法, 并从理论模拟和实验上分别验证了该方案, 其安全性远高于仅加密一束光时的情况. 使用双随机相位加密法加密了原始图像, 并使用随机相位片编码了参考光. 加密后的图像由 CCD 接收后再使用计算机处理. 此外, 在实验上检测了该系统的信噪比和容错性, 并计算得到系统的密钥长度高达 6.3×10^{14}.

关键词
光加密
数字全息系统
双随机相位加密
随机相位编码

光学加密由于其高速数据处理、传输和高安全性等优点, 受到了人们的广泛关注 [1~12]. 随着计算机性能和电子图像获取设备的发展, 数字全息系统由于其具有和现有电脑技术良好的兼容性 [13,14], 成为光加密的一个重要的应用领域. 此外, 数字全息技术可以通过图像处理方法降低系统的噪音, 并可以通过数学方法从多个不同角度重现原始图像.

数字全息系统中, 常见的加密方法包括物光加密和参考光加密. 常见的物光加密方法有双随机相位加密法 [3,9]和全相位加密法 [4,11], 而参考光加密则通常使用随机相位编码 [2,8]. 在需要解密时, 通常使用相移法, 包括四步、三步或二步相移 [7~9,11,15~19]. 系统的误码率会随着相移步数的增加而下降. 所以, 为了提高解密图像的质量, 需要使用更多步的相移来提取更多的图片进行计算, 这样无形中增大了系统的复杂性. 此外, 相移法还有其他限制, 如需要精确地调整相移的间隔等.

本文中, 我们设计了一个物光和参考光同时加密的数字全息系统方案, 并从理论和实验上分别进行了验证. 本系统不需要使用相移法进行解密. 原始图像被分别置于输入平面和傅里叶面上的随机相位片加密, 同时参考光被另一块随机相位片加密. 加密后的图像由 CCD 接收后保存在计算机中以便进一步处理. 系统拥有两个密钥, 物光光束上的傅里叶随机相位片和参考光光束上的随机相位片. 任何一个密钥错误, 都将导致解密失败. 此外, 我们也检测了该系统的信噪比和容错性, 并计算了密钥长度.

1 实验系统

实验光路如图 1 所示. 一束由 1064 nm 的连续倍频 Nd:YVO_4 激光器输出的平面波光束经扩束为 13 mm 后, 被分光镜 BS1 分为两束: 一束信号光和一束参考光. 在物光光束上, 原始图像和一块随机相位片 RPM1 置于透镜 L1 的前焦面上. 第二块随机相位片 RPM2 置于傅里叶面上, 并被由 L2 和 L3 组成的 4F 系统成像到 CCD 上. 在参考光光束上放置另一个由 L4 和 L5 组成的 4F 系统, 以保持系统的空间关联性. L1 至 L5 五个透镜的焦距分别为 15, 12, 12, 25 和 25 cm. 在参考光光束上, RPM3 置于 CCD 约 8 cm 远处.

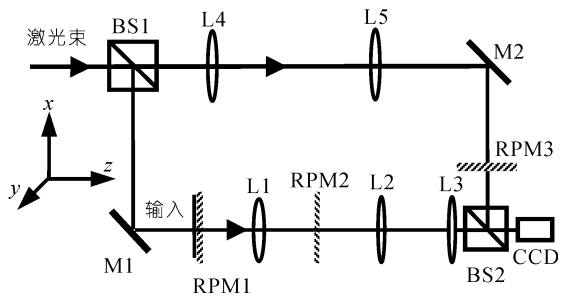

图 1 物光和参考光双加密系统的光路图
M, 反射镜; BS, 分光镜; RPM, 随机相位片; L, 透镜

三块随机相位片均为自制的经 HF 酸腐蚀的玻璃片.

在加密过程中, 我们假设 $o(x, y)$, $f(x, y)$和 $M(\xi, \eta)$ 分别代表待加密的二维二进制图像, 输入随机相位片和傅里叶随机相位片, 其中(x, y)为空间坐标, (ξ, η)为傅里叶平面坐标. 我们使用双随机相位加密法加密原始图像, 其密钥为傅里叶随机相位片 RPM2. 这样, 傅里叶面上的加密图像可表达为

$$S(\xi,\eta)=\left[O(\xi,\eta)\otimes F(\xi,\eta)\right]M(\xi,\eta), \quad (1)$$

其中 $O(\xi, \eta)$和 $F(\xi, \eta)$分别为 $o(x, y)$和 $f(x, y)$的傅里叶变换, ⊗表示卷积. 此波前进一步传输后, 与参考光 $H(\xi, \eta)$相干, 则 CCD 上接收到的全息图可表示为

$$I_E(\xi,\eta)=\left|S(\xi,\eta)\right|^2+\left|H(\xi,\eta)\right|^2 +S(\xi,\eta)H^*(\xi,\eta)+S^*(\xi,\eta)H(\xi,\eta). \quad (2)$$

在需要解密时, 我们需要首先移去输入图像和透镜 L1, 以便记录密钥的全息图. 当使用密钥 $M'(\xi, \eta)$和 $H'(\xi, \eta)$进行解密时, CCD 上接收到的信息可以表示为

$$I_M(\xi,\eta)=\left|M'(\xi,\eta)\right|^2+\left|H'(\xi,\eta)\right|^2 +M'(\xi,\eta)H'^*(\xi,\eta)+M'^*(\xi,\eta)H'(\xi,\eta). \quad (3)$$

上述(2)和(3)式中的前两项均为常数, 可以很方便地移去. 当参考光稍微倾斜时(本实验中约为 1°), 我们可以通过傅里叶变换提取出(2)式中的第4项和(3)式中的第 3 项 [3]. 这样, 通过把提取出来的两项相乘, 再进行傅里叶逆变换, 我们就可以得到解密的图像

$$\begin{aligned} o'(x,y)&=FT^{-1}\left\{\left[S(\xi,\eta)H^*(\xi,\eta)\right]\right.\\ &\quad\left.\times\left[M'^*(\xi,\eta)H'(\xi,\eta)\right]\right\}\\ &=FT^{-1}\left\{\left[O(\xi,\eta)\otimes F(\xi,\eta)\right]\left[M(\xi,\eta)\right.\right.\\ &\quad\left.\left.\times M'^*(\xi,\eta)\right]\cdot\left[H^*(\xi,\eta)H'(\xi,\eta)\right]\right\}, \end{aligned} \quad (4)$$

其中 $FT^{-1}[\ ]$表示傅里叶逆变换. 仅当解密时的 $M'(\xi, \eta)$和 $H'(\xi, \eta)$与加密时完全相同, 则(4)式的后 4 项 $M(\xi, \eta)M'^*(\xi, \eta)H^*(\xi, \eta)H'(\xi, \eta)=|M(\xi, \eta)|^2|H(\xi, \eta)|^2$ 是一个常数, 可以略去, 则(4)式可以简化为

$$\begin{aligned} o'(x,y)&\propto FT^{-1}\left[O(\xi,\eta)\otimes F(\xi,\eta)\right]\\ &=o(x,y)f(x,y). \end{aligned} \quad (5)$$

由于原始图像 $o(x, y)$是一个实函数, $f(x, y)$只是个相位函数, 故 $o'(x, y)$的强度信息就直接给出了原始图像.

为了量化实验结果, 我们也引入信噪比(SNR):

$$\mathrm{SNR}=\frac{\sum_{x,y}\left[E(x,y)\right]^2}{\sum_{x,y}\left[E(x,y)-D(x,y)\right]^2}, \quad (6)$$

其中$E(x, y)$为待加密的二进制图形, $E(x, y)$为解密得到的二进制图像 [20].

2 理论模拟

我们使用 Matlab 仿真模拟了整个系统的运行以检验其可行性. 原始图像是一个 400×400 像素的二进制图像, 如图 2(a)所示. 三块随机相位片的强度为均匀分布, 相位为[0,1]之间的随机分布. 使用上述方法得到的加密和解密的图像如图2(c)和(b)所示, 可见加密和解密过程均十分成功. 图2(d)和(e)分别是使用错误的密钥 RPM2 或 RPM3 时, 得到的解密结果, 很显然, 无法从中分辨出原始信息.

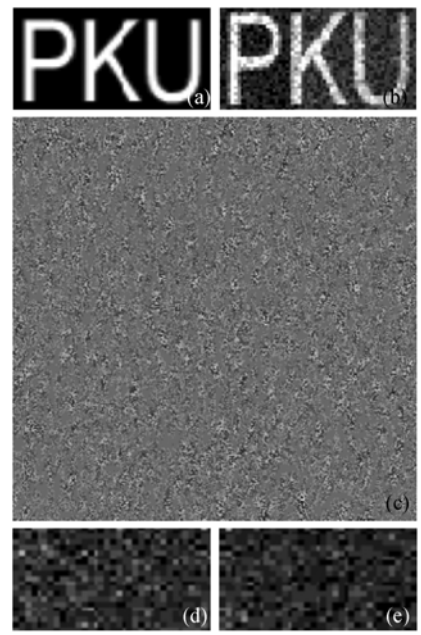

图 2 理论模拟的加密和解密结果

(a) 原始图像; (b) 加密图像; (c) 正确解密的图像; (d) RPM2 错误的解密图像; (e) RPM3 错误的解密图像

此外我们在解密时, 分别把 RPM2 和 RPM3 在垂直于光轴的平面内沿横向或纵向平移一个像素, 进行解密. 图 3(a)和(b)分别是把 RPM2 沿 x 方向或 y 方向平移一个像素后, 得到的解密图像. 类似地, 把 RPM3 沿 y 方向或 z 方向平移一个像素后, 得到的解密图像如图 3(c)和(d)所示. 在上述 4 种情况下, 均无法正确解密. 如果把两个密钥沿光轴方向平移, 则将

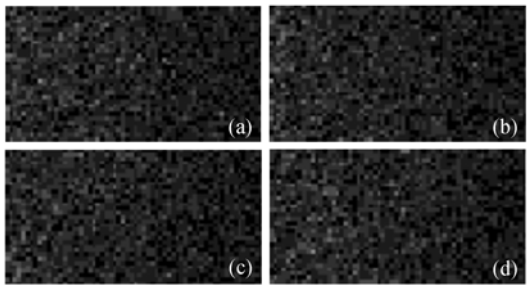

图 3　密钥在垂直于光轴平面平移一个像素后的解密图像

(a) RPM2 沿 *x* 方向; (b) RPM2 沿 *y* 方向; (c) RPM3 沿 *y* 方向; (d) RPM3 沿 *z* 方向

导致加密在 Fresnel 域中进行，这大大增加了计算的复杂性，所以为简单起见，我们不计算这维密钥的容错性．这样，我们可以确定，这两个密钥对于解密都十分重要，任何一个密钥错误，都会导致无法正确解密．

3　结果与分析

我们也在实验上验证了本系统．图 4(a)是仅加载了 RPM1 而没有 RPM2 时的原始图像经成像到 CCD 上得到的，为增强视觉效果，图像的对比度已经过调整．图像中有一定噪音，可能是由于 RPM1 具有一定厚度而导致的散射造成的．原始图像经过三块随机相位片加密后，得到的一个类似白噪声的图像如图 4(e)所示．傅里叶随机相位片 RPM2 和参考光随机相位片 RPM3 的全息图见图 4(f)和(g)．使用与加密时完全相同的密钥解密得到的图像如图 4(b)所示，可见图像被成功地解密了．图 4(c)和(d)分别是使用错误的 RPM2 或 RPM3 解密得到的图像，无法分辨任何原始图像的信息．解密得到的图像质量有一定下降，这可能是由于晶体和 CCD 的尺寸有限，其他光学元件的带宽较低，导致整个系统的带宽受限造成的．我们知道，随机相位函数具有很大的空间带宽，在光学系统中，为无损地传输一个信号，需要保证这个信号的空间带宽不超过整个光学系统的空间带宽．所以，如果使用面积更大的 CCD 接收，可以在一定程度上缓解这个空间带宽问题．

与理论模拟部分相似，我们也测量了密钥 RPM2 和 RPM3 的容错性．首先使用上述方法得到了加密图像的全息图．然后，我们分别把 RPM2 或 RPM3 沿 *x*, *y* 或 *z* 方向平移一定距离，再进行解密．图 5 和图 6 分别给出了把 RPM2 和 RPM3 分别沿三个方向平移后得到的解密图像．各图像相应的信噪比如表 1 所示．可见，随着密钥位移的增大，解密图像的信噪比逐渐下降．RPM2 和 RPM3 在垂直于光轴平面内的最大可移动范围约为 10 μm，沿光轴方向的最大可移动

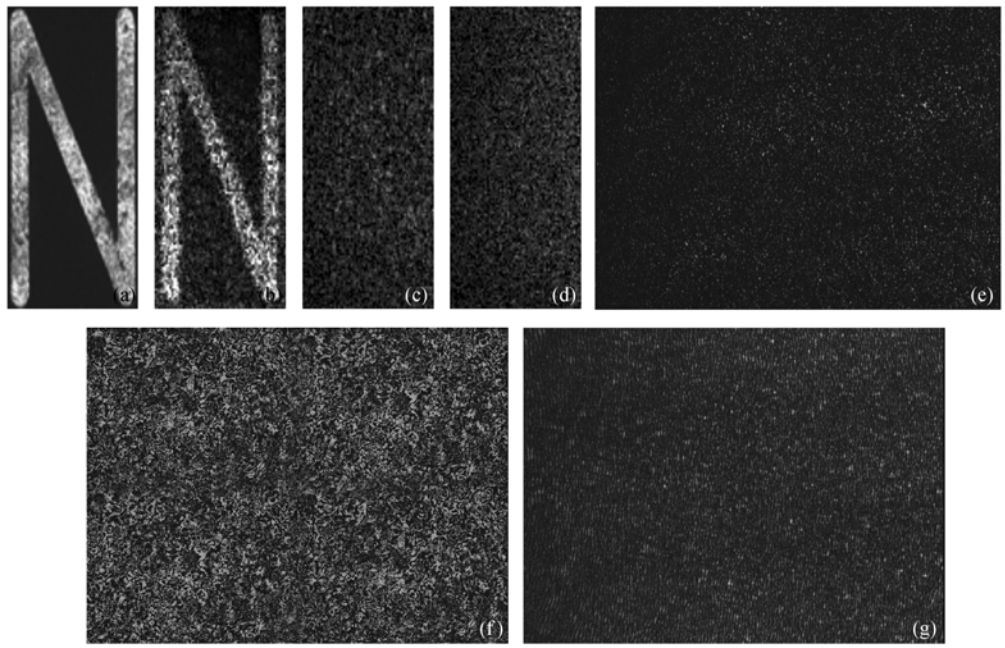

图 4　实验的加密和解密结果

(a) 原始图像; (b) 正确解密图像; (c) RPM2 错误时的解密图像; (d) RPM3 错误时的解密图像; (e) 加密图像; (f) RPM2 全息图; (g) RPM3 全息图

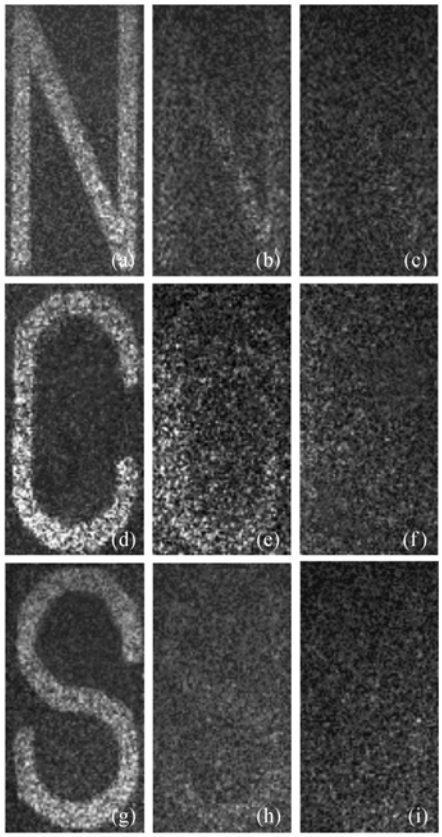

图 5 RPM2 沿各方向平移一定距离后的解密图像

沿 x 轴方向平移(a) 0 μm, (b) 5 μm, (c) 10 μm; 沿 y 轴方向平移(d) 0 μm, (e) 5 μm, (f) 10 μm; 沿 z 轴方向平移(g) 0 mm, (h) 1 mm, (i) 3 mm

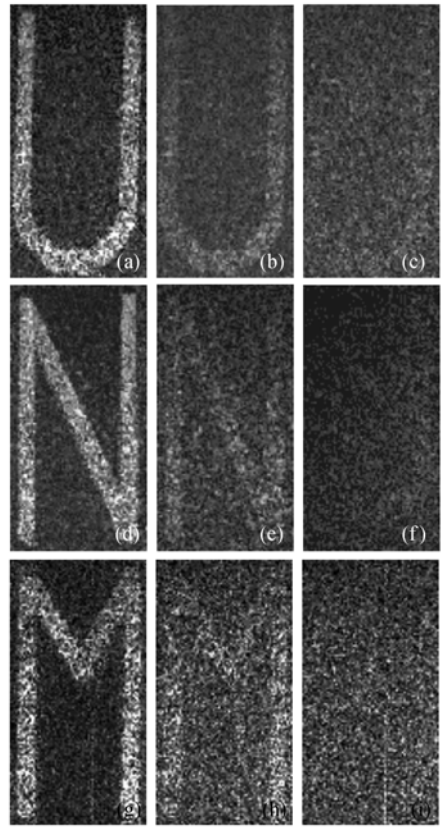

图 6 RPM3 沿各方向平移一定距离后的解密图像

沿 y 轴方向平移(a) 0 μm, (b) 5 μm, (c) 10 μm; 沿 z 轴方向平移(d) 0 μm, (e) 5 μm, (f) 10 μm; 沿 x 轴方向平移(g) 0 mm, (h) 1 mm, (i) 3 mm

表 1 RPM2 和 RPM3 沿不同方向平移不同距离时解密图像的信噪比

位移距离	RPM2			RPM3		
	x	y	z	x	y	z
0	6.74	5.76	6.41	3.84	6.6	5.2
5 μm	1.33	1.11			1.27	1.32
10 μm	1.04	1.02			1.01	0.98
1 mm			1.15	1.12		
3 mm			1.01	0.98		

范围约为 3 mm.

此外, 我们也计算了整个系统的密钥长度. 假设所使用的相位片均为 5 cm×5 cm, 则 RPM2 或 RPM3 在垂直于光轴的平面内移动, 均可提供的密钥长度为$[5\times10^{-2}/(10\times10^{-6})]^2 = 2.5\times10^7$, 即仅有物光和参考光中的一束加密可提供的密钥长度. 在我们的系统中, 物光和参考光同时加密, 而且两者互不干扰. 所以, 本系统的密钥长度为$(2.5\times10^7)^2 = 6.3\times10^{14}$, 可见我们的系统相对于物光或参考光单光束加密的系统有更高的安全性. 而且, 我们并没有考虑两个密钥沿光轴方向位移可能提供的密钥长度, 这是由于它们沿光轴方向位移的敏感度远小于垂直于光轴方向位移的敏感度. 此外, 我们也可以通过使用更大面积的随机相位片等方法获得更大的密钥长度.

4 结论

我们从理论和实验上分别实现了在数字全息系统中物光和参考光同时加密的方案, 其安全性远高于仅加密一束光时的情况. 我们使用双随机相位加密法加密了原始图像, 并使用随机相位片编码了参考光. 加密后的图像由 CCD 接收后再使用计算机处理. 系统拥有两个密钥, 物光光束上的傅里叶随机相位片和参考光光束上的随机相位片. 理论计算和实验均证实, 无论任何一个密钥错误, 都将导致解密失败. 实验结果显示, 该系统具有良好的信噪比和容错

性，其密钥长度高达 6.3×10^{14}. 我们的系统提供了一个可同时加密物光和参考光，并具有较高安全性的数字全息系统方案，特别适合于下一代 Internet 传输等应用.

参考文献

1 Réfrégier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding. Opt Lett, 1995, 20(7): 767—768

2 Tajahuerce E, Javidi B. Encrypting three-dimensional information with digital holography. Appl Opt, 2000, 39(35): 6595—6601[doi]

3 Javidi B, Nomura T. Securing information by use of digital holography. Opt Lett, 2000, 25(1): 28—30 [doi]

4 Nishchal N K, Joseph J, Singh K. Fully phase encryption using digital holography. Opt Eng, 2004, 43(12): 2959—2966 [doi]

5 Zhu B H, Liu S T, Ran Q W. Optical image encryption based on multifractional Fourier transforms. Opt Lett, 2000, 25(16): 1159—1161 [doi]

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

7 Liu S T, Mi Q L, Zhu B H. Optical image encryption with multistage and multichannel fractional Fourier-domain filtering. Opt Lett, 2001, 26(16): 1242—1244[doi]

8 Tajahuerce E, Matoba O, Verrall S C, et al. Optoelectronic information encryption with phase-shifting interferometry. Appl Opt, 2000, 39(14): 2313—2320 [doi]

9 Meng X F, Cai L Z, Xu X F, et al. Two-step phase-shifting interferometry in image encryption. Opt Lett, 2006, 31(10): 1414—1416[doi]

10 Peng X, Zhang P, Wei H Z. Known-plaintext attack on optical encryption based on double random phase keys. Opt Lett, 2006, 31(8): 1044—1046[doi]

11 He M Z, Cai L Z, Liu Q, et al. Phase-only encryption and watermarking based on phase-shifting interferometry. Appl Opt, 2005, 44(13): 2600—2606 [doi]

12 Situ G H, Zhang J J. A lensless optical security system based on computer-generated phase only masks. Opt Comm, 2004, 232(1-6): 115—122[doi]

13 Grilli S, Ferraro P, Nicola S D, et al. Whole optical wavefields reconstruction by digital holography. Opt Express, 2001, 9(6): 294—302

14 Schnars U, Kreis T M, Juptner W P O. Digital recording and numerical reconstruction of holograms: Reduction of the spatial frequency spectrum. Opt Eng, 1996, 35(4): 977—982 [doi]

15 Yamaguchi I, Zhang T. Phase-shifting digital holography. Opt Lett, 1997, 22(16): 1268—1270 [doi]

16 Zhang T, Yamaguchi I. Three-dimensional microscopy with phase-shifting digital holography. Opt Lett, 1998, 23(15): 1221—1223[doi]

17 Cai L Z, Liu Q, Yang X L. Phase-shift extraction and wave-front reconstruction in phase-shifting interferometry with arbitrary phase steps. Opt Lett, 2003, 28(19): 1808—1810 [doi]

18 Lai S C, King B, Neifeld M A. Wave front reconstruction by means of phase-shifting digital in-line holography. Opt Comm, 2000, 173(1): 155—160 [doi]

19 Cai L Z, Liu Q, Yang X L. Generalized phase-shifting interferometry with arbitrary unknown phase steps for diffraction objects. Opt Lett, 2004, 29(2): 183—185 [doi]

20 Nomura T, Javidi B. Optical encryption system with a binary key code. Appl Opt, 2000, 39(26): 4783—4787[doi]