文章编号：0258-7025(2009)Supplement 2-0312-06

基于计算全息和双随机相位的虚拟光学加密算法

潘 武 吴文雯 张雪莲

（重庆邮电大学光电工程学院，重庆 400065）

摘要 在计算全息和双随机相位编码技术的基础上，提出了一种虚拟光学加解密算法。该算法采用两路随机相位函数相同但是空间参数不同的双随机相位编码系统来实现。加密过程首先利用一路双随机相位编码系统对明文数据进行加密，将生成的加密数据作为物光信息，再与利用另一路双随机相位光学编码系统生成的参考光信息叠加，对生成的结果进行滤波后得到密文数据。解密过程首先恢复出参考光信息，然后计算出物光信息，利用双随机相位光学编码系统即可恢复出明文数据。理论分析部分证明了该算法的有效性。实验结果表明该算法具有很强的抗唯密文攻击和选择明文攻击的能力。

关键词 全息；虚拟光学；双随机相位；加密技术

中图分类号 O428.1 **文献标识码** A **doi**：10.3788/CJL200936s2.0312

Encryption Algorithm of Virtual Optical Based on Computer-Generated Hologram and Double Random Phase

Pan Wu Wu Wenwen Zhang Xuelian

(*College of Optoelectronic Engineering*, *Chongqing University of Posts and Telecommunications*, *Chongqing* 400065, *China*)

Abstract A new encryption algorithm of virtual optics is proposed based on computer-generated hologram and double random phase encoding system. The algorithm uses two-way double random phase encoding system which has same random phase masks but different parameters to achieve. In the encryption process, the plaintext is modulated by the first way double random phase encoding system, and its in-line hologram is superposed on a reference beam that generated by another double random phase encoding system, the ciphertext is the outcome of its filtering. The plaintext is recovered by calculations in reverse order of encryption process. Analysis proves that the virtual optics algorithm is valid. Computer simulation shows that the algorithm has a strong ability to resist the attacks of chosen-plaintext and ciphertext-only.

Key words holography; virtual optics; double random phase; encryption

1 引 言

密码学是信息安全技术的核心，其经过了几千年的演化与发展后，形成了丰富的内涵，并得到了广泛的应用。根据密码学的发展历程中表现出来的特征，密码主要表现出四种形式：艺术密码形式、古典密码形式、计算机密码形式以及非数学密码形式。最近发展起来的基于非数学密码形式的密码系统引起了人们极大的关注，目前主要有量子密码、混沌密码、光学密码等基于物理学原理的密码系统，以及基于生物学理论的生物密码体制。

基于信息光学的双随机相位光学加密技术，是 Javidi 等[1~4]于 20 世纪 90 年代初提出的一种新型物理密码技术。这种密码系统利用光学模式识别，特别是光学图像处理中的傅里叶变换实现对信息的加密。基于光学信息处理的加密系统中所用器件为光学元件，如透镜、相干光源等，不需要对数据进行复杂的算法和大量的二进制数据处理，与电子元件组成的加密系统相比，光学加密系统具有信息传输大，速度快等优点。

在双随机相位光学加密技术中，由于作为加密

基金项目：重庆市自然科学基金(CSTC2006BB2362)资助课题。

作者简介：潘 武(1966—)，男，教授，博士，主要从事光学信息处理及光码分多址技术等方面的研究。

E-mail：panwu@cqupt.edu.cn

系统的 $4f$ 光学系统对原件的空间排列精度要求非常高，尤其是在解密阶段，由于相位的随机性，当全部数据用于解密时，谱平面上相位板偏离匹配位置哪怕只有一个像素大小的距离，也不能获得解密图像，这样使得 $4f$ 光学系统成为一个具有优良密码特性的密码系统，同时也成为了光学图像加密技术走向实用化的一个瓶颈。彭翔等[5,6]提出了基于双随机相位编码系统的虚拟光学加密技术，使得光学信息安全技术与数字技术很好地结合起来，推动了光学信息安全技术的实用化。由于双随机相位编码光学加密技术是基于傅里叶变换的，本质上是一种线性变换，这就为其安全性留下了很大隐患。一些学者已经证明[7~10]，通过选择明文和密文的方法可以得到加密密钥。

本文在虚拟光学加密理论框架下，提出一种新的加密算法，该算法结合双随机相位加密技术和计算全息技术实现对信息的加密。在加密过程中，分别通过双随机相位加密系统产生物光波和参考光波，然后通过计算全息技术实现对明文信息的二次调制加密。该算法无需改变 $4f$ 系统的结构，实现非常简单，并且通过线性系统的叠加运算能够达到非常好的非线性效果。

2　加密/解密算法

2.1　双随机相位光学编码系统

虚拟光学加密系统的核心是双随机相位编码系统。G. H. Situ 等[11,12]在 Javidi 等提出的双随机相位编码系统的基础上描述了一种更简单、紧凑和方便的光学装置，即基于菲涅耳衍射域的双随机相位编码系统，这种光学装置的最大特点是不需要光学透镜。图 1 是该系统的光学装置示意图。

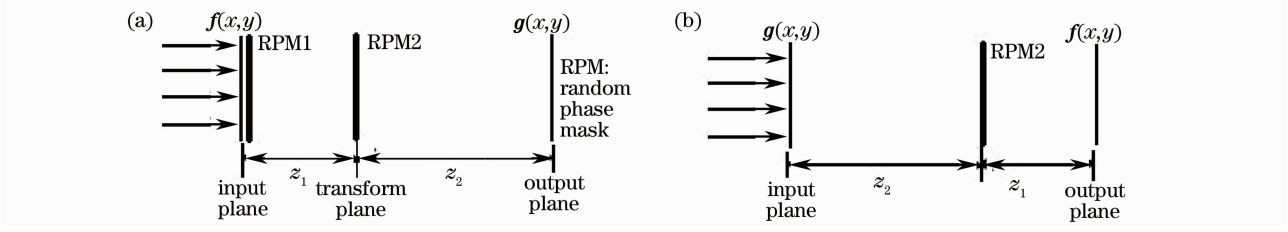

图 1　菲涅耳域的双随机相位编码系统示意图。(a) 编码系统；(b) 解码系统

Fig. 1　Double random phase encoding in the Fresnel domain. (a) Coding system; (b) decoding system

假设相位型随机相位板 RPM1 和 RPM2 的复振幅分别为 $\exp[\mathrm{i}2\pi\boldsymbol{p}(x,y)]$ 和 $\exp[\mathrm{i}2\pi\boldsymbol{q}(x,y)]$，其中 $\boldsymbol{p}(x,y)$ 和 $\boldsymbol{q}(x,y)$ 是两个分布在 $[0,1]$ 之间的独立白噪声矩阵。明文数据用 $\boldsymbol{f}(x,y)$ 来表示，激光波长用 λ 表示。照射到 RPM2 前面的物光波复振幅为

$$\boldsymbol{u}_2(x_2,y_2)=c_1\boldsymbol{p}(x_2,y_2)\iint\boldsymbol{f}(x_1,y_1)\boldsymbol{p}(x_1,y_1)\exp\left[-\frac{\mathrm{i}2\pi}{\lambda z_1}(x_1x_2+y_1y_2)\right]\mathrm{d}x_1\mathrm{d}y_1,\tag{1}$$

式中 $c_1=\exp(\mathrm{i}kz_1)/(\mathrm{i}\lambda z_1)$，$\boldsymbol{p}(x,y)=\exp[\mathrm{i}k(x^2+y^2)/(2z_1)]$，波矢 $k=2\pi/\lambda$。经相位板 RPM2 衍射到输出平面的复振幅为

$$\boldsymbol{g}(x,y)=c_2\boldsymbol{p}(x,y)\iint\boldsymbol{u}(x_2,y_2)\boldsymbol{p}(x_2,y_2)\exp\left[-\frac{\mathrm{i}2\pi}{\lambda z_2}(xx_2+yy_2)\right]\mathrm{d}x_2\mathrm{d}y_2,\tag{2}$$

式中 $c_2=\exp(\mathrm{i}kz_2)/(\mathrm{i}\lambda z_2)$。

为方便，用 L 表示菲涅耳衍射过程。则(1)，(2)式可以合并为

$$\boldsymbol{g}(x,y)=L\{L[\boldsymbol{f}(x,y);\boldsymbol{p}(x,y)z_1,\lambda];\boldsymbol{q}(x,y),z_2,\lambda\},\tag{3}$$

式中 $\boldsymbol{g}(x,y)$ 即为明文数据 $\boldsymbol{f}(x,y)$ 通过双随机相位加密系统后得到的密文数据。

通过以下步骤可以通过接收到的密文数据恢复出明文数据

1)　将密文数据 $\boldsymbol{g}^*(x,y)$ 做距离为 z_2 的逆菲涅耳衍射；

2)　得出的复振幅乘以 $\exp[-\mathrm{i}2\pi\boldsymbol{q}(x,y)]$；

3)　做另一个距离为 z_1 的逆菲涅耳衍射；

4)　取出场复振幅的振幅，即为解密后的明文数据 $\boldsymbol{f}^*(x,y)$。

从双随机相位编码系统的数据恢复过程可以看到，如果直接将实数型数据放置于 RPM1 之前进行

编码，在解码时 RPM1 并不起作用，为了加强系统安全性，在编码之前首先将明文数据 $\boldsymbol{f}(x,y)$ 编码为相位型数据 $\boldsymbol{f}'(x,y)$。

$$\boldsymbol{f}'(x,y)=\exp\left\{\mathrm{i}2\pi\frac{\boldsymbol{f}(x,y)}{\max[|\boldsymbol{f}(x,y)|]}\right\},\quad(4)$$

$\max[|\boldsymbol{f}(x,y)|]$ 为 $\boldsymbol{f}(x,y)$ 取正后的最大值，这样就必须使用 RPM1 才能正确解码。

2.2 加密和解密算法设计

本文设计的加密和解密算法采用两路单色平面波照射的双随机相位编码光学系统来实现，分别将两路光学系统称为物光光路和参考光路，两路光学系统采用相同的随机相位板，但两路光学系统的空间参数不同，其加密算法框图如图 2 所示。

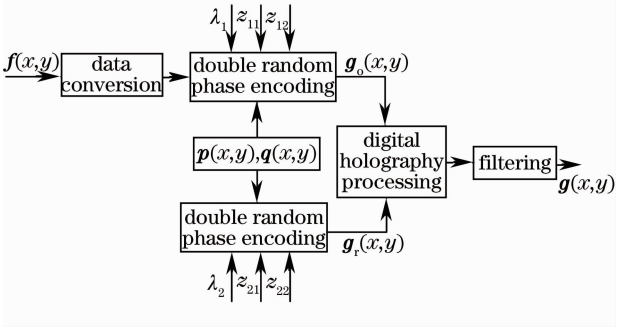

图 2 加密算法流程图

Fig. 2 Flowchart of encryption algorithm

具体的加密过程如下：

1) 将明文数据 $\boldsymbol{f}(x,y)$ 根据(4)式转换成相位型数据 $\boldsymbol{f}'(x,y)$；

2) 在[0,1]之间选择均匀、随机分布的 $M\times N$ 相位阵列 $\boldsymbol{p}(x,y)$ 和 $\boldsymbol{q}(x,y)$ 作为双随机相位光学加密系统的第一块和第二块相位模板的值；

3) 将 $\boldsymbol{f}'(x,y)$ 通过第一路双随机相位光学编码系统进行编码，根据(3)式得到物光波复振幅

$$\boldsymbol{g}_{\mathrm{o}}(x,y)=L\{L[1;\boldsymbol{p}'(x,y),z_{11},\lambda_1];\boldsymbol{q}(x,y),z_{12},\lambda_1\}=a_{\mathrm{o}}(x,y)\exp[\mathrm{i}\varphi_{\mathrm{o}}(x,y)],\quad(5)$$

式中 $\boldsymbol{p}'(x,y)=\boldsymbol{f}''(x,y)+\boldsymbol{p}(x,y)$，$\boldsymbol{f}''(x,y)$ 为 $\boldsymbol{f}'(x,y)$ 的相位，λ_1 为入射光波长，z_{11}，z_{22} 分别为入射光经过第一块相位板和第二块相位板的衍射距离，$a_{\mathrm{o}}(x,y)$ 和 $\varphi_{\mathrm{o}}(x,y)$ 分别为 $\boldsymbol{g}_{\mathrm{o}}(x,y)$ 的振幅和相位；

4) 通过第二路双随机相位光学编码系统编码得到参考光波复振幅

$$\boldsymbol{g}_{\mathrm{r}}(x,y)=L\{L[1;\boldsymbol{p}(x,y),z_{21},\lambda_2];\boldsymbol{q}(x,y),z_{22},\lambda_2\}=a_{\mathrm{r}}(x,y)\exp[\mathrm{i}\varphi_{\mathrm{r}}(x,y)],\quad(6)$$

式中 λ_2 为入射光波长，z_{21}，z_{22} 分别为入射光经过第一块相位板和第二块相位板的衍射距离，$a_{\mathrm{r}}(x,y)$ 和 $\varphi_{\mathrm{r}}(x,y)$ 分别为 $\boldsymbol{g}_{\mathrm{r}}(x,y)$ 的振幅和相位；

5) 将物光波和参考光波经过数字全息处理后得到全息图的光强分布为

$$\begin{aligned}\boldsymbol{u}(x,y)&=|\boldsymbol{g}_{\mathrm{o}}(x,y)+\boldsymbol{g}_{\mathrm{r}}(x,y)|^2=\\&|\boldsymbol{g}_{\mathrm{o}}(x,y)|^2+|\boldsymbol{g}_{\mathrm{r}}(x,y)|^2+\boldsymbol{g}_{\mathrm{o}}(x,y)\boldsymbol{g}_{\mathrm{r}}^*(x,y)+\boldsymbol{g}_{\mathrm{o}}^*(x,y)\boldsymbol{g}_{\mathrm{r}}(x,y);\end{aligned}\quad(7)$$

6) 对(7)式进行傅里叶变换可得

$$U(\boldsymbol{f}_x,\boldsymbol{f}_y)=A_0(\boldsymbol{f}_x,\boldsymbol{f}_y)+A_1(\boldsymbol{f}_x,\boldsymbol{f}_y-\boldsymbol{f}_0)+A_2(\boldsymbol{f}_x,\boldsymbol{f}_y+\boldsymbol{f}_0).\quad(8)$$

式中 $A_0(\boldsymbol{f}_x,\boldsymbol{f}_y)=\mathscr{F}[|\boldsymbol{g}_{\mathrm{o}}(x,y)|^2+|\boldsymbol{g}_{\mathrm{r}}(x,y)|^2]$，$A_1(\boldsymbol{f}_x,\boldsymbol{f}_y-\boldsymbol{f}_0)=\mathscr{F}[|\boldsymbol{g}_{\mathrm{o}}(x,y)\boldsymbol{g}_{\mathrm{r}}^*(x,y)]$，$A_2(\boldsymbol{f}_x,\boldsymbol{f}_y+\boldsymbol{f}_0)=\mathscr{F}[|\boldsymbol{g}_{\mathrm{o}}^*(x,y)\boldsymbol{g}_{\mathrm{r}}(x,y)]$，

对于限带的物光波，上面三项在频谱面上是彼此分离的，则可以将 $A_1(\boldsymbol{f}_x,\boldsymbol{f}_y+\boldsymbol{f}_0)$ 分离出来，如图 3 所示；

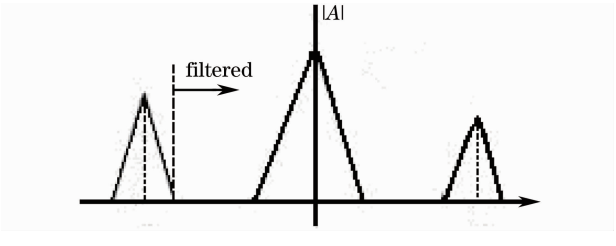

图 3 全息图频谱

Fig. 3 Frequency spectrum for hologram

7) 对滤波后的结果做逆傅里叶变换得到加密后的密文

$$\boldsymbol{g}(x,y)=\boldsymbol{g}_{\mathrm{o}}(x,y)\boldsymbol{g}_{\mathrm{r}}^*(x,y)=a_{\mathrm{o}}(x,y)a_{\mathrm{r}}(x,y)\exp\{\mathrm{i}[\varphi_{\mathrm{o}}(x,y)-\varphi_{\mathrm{r}}(x,y)]\}.\quad(9)$$

从上面的算法可以看出，明文数据经过一次双随机相位编码后的复振幅被参考光波调制，并且参考光波是通过双随机相位编码后所得，虽然是通过线性变换叠加产生的密文，但已经不是简单的数学变换，因此增加了系统的安全性，并且变换过程简单。

解密算法框图如图 4 所示。具体的解密过程为：

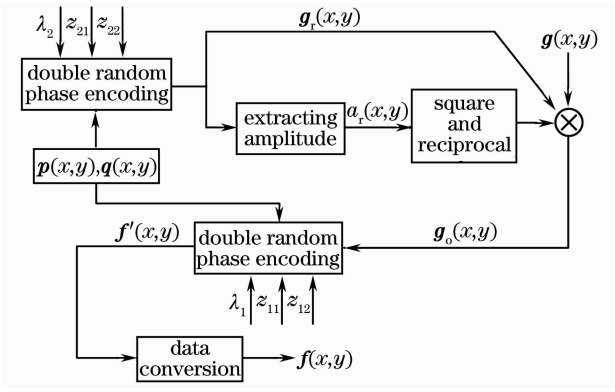

图 4　解密算法流程图

Fig. 4　Flowchart of decryption algorithm

1) 利用密钥恢复出参考光波的复振幅 $\boldsymbol{g}_{\mathrm{r}}(x,y)$；

2) 取 $\boldsymbol{g}_{\mathrm{r}}(x,y)$ 的振幅 $a_{\mathrm{r}}(x,y)$；

3) 利用得到的密文 $\boldsymbol{g}(x,y)$，$\boldsymbol{g}_{\mathrm{r}}(x,y)$ 和 $a_{\mathrm{r}}(x,y)$ 可以得到物光波的复振幅

$$\boldsymbol{g}_{\mathrm{o}}(x,y)=\frac{\boldsymbol{g}(x,y)\boldsymbol{g}_{\mathrm{r}}(x,y)}{a_{\mathrm{r}}^{2}(x,y)}; \tag{10}$$

4) 将 $\boldsymbol{g}_{\mathrm{o}}(x,y)$ 通过双随机相位解码系统解码，并将获得的相位型数据转换成实数型数据得到解密结果 $\boldsymbol{f}(x,y)$。

从上面的论述可以看出，本文所提出的算法是一种虚拟光学的加密技术，混淆和扩散技术得到充分的应用，密文数据中每个数据元均受到明文数据中所有数据元的影响。将明文数据通过二次加密的方式加密，明文、密文和密钥之间已经不是线性变换，在该算法中虽然两次加密过程都为线性运算，但却能够得到非常好的非线性效果。只有在相位模板排列和两路光学系统的空间参数正确，才能得到正确的解密结果。

3　对算法的攻击分析

3.1　唯密文攻击

唯密文攻击是指攻击者仅获得了一些密文，并且试图恢复尽可能多的明文，并进一步试图推算出加密消息的密钥。

在仅知道密文的情况下，攻击者试图通过穷举的密钥空间的办法来寻找会话密钥在计算上将是不可行的。在不考虑光学系统空间参数的情况下，假设 $N\times N$ 个元素的随机相位函数 $\boldsymbol{p}(x,y)$，$\boldsymbol{q}(x,y)$ 在[0,1]分别量化为 L_p，L_q 级，完全恢复出原始明文需要进行 $L_p^N\times L_q^N$ 次的运算。如果 $N=10$，$L_p=L_q=2$，对于一台运算速度为 10^{10} Hz 的计算机需要 1.7×10^{45} 年的时间，这样的破解是没有实际意义的。

3.2　已知明文攻击和选择明文攻击

已知明文攻击是指攻击者不仅掌握若干密文，还知道对应的明文本身。攻击者利用它来推出加密的密钥。选择明文攻击指攻击者不仅知道一些消息的密文以及与之对用的明文，而且可以选择被加密的明文，并试图推导出加密密钥，因为明文是经过选择的，所以提供了更多可破译信息，攻击力更强。

本文所提出的加密算法采用数字计算全息技术[13~15]对通过双随机相位光学系统加密的数据进行第二次加密，使得明文、密文和密钥之间的关系变得更加复杂。两路双随机相位光学系统的密钥参数在数据处理过程中相互影响，很难单独分离、提取密钥，并且密钥和明文、密文之间不是简单的线性变换，相互之间存在较为复杂的制约关系，也使得本文提出的加密算法中明文、密文和密钥的关系成为需要进一步研究的内容。即使攻击者获得许多精心选择的明文-密钥对，他仍然无法成功分析对比推测出加密所用的密钥。

4　模拟实验

为了验证上述算法的效果，利用 Matlab 进行了计算机模拟实验。明文数据采用 256 pixel×256 pixel 和灰度阶数为 256 的 bmp 图像，如图 5 所示。两路光学系统采用振幅为 1 的单色平面波照明，物波光路的入射光波波长为 630 nm，第一块相位板与第二块相位板之间的距离为 1 m，第二块相位板与相平面之间的距离为 1.4 m，参考光路的入射光波波长为 850 nm，两相位板平面和图像平面采用同样的尺寸，第一块相位板与第二块相位板之间的距离为0.7 m，第二块相位板与相平面之间的距离为1.1 m。

为了评估图像解密效果，引入关系数 r 来评价解密结果的质量，定义为

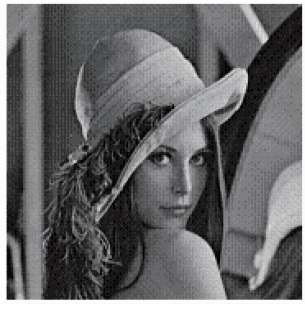

图 5　待加密的明文图像

Fig. 5　Target image to be encrypted

$$r=\frac{\sum_m\sum_n(f_{mn}-\bar{f})(\hat{c}_{mn}-\bar{\hat{c}})}{\sqrt{\left[\sum_m\sum_n(f_{mn}-\bar{f})^2\right]\left[\sum_m\sum_n(\hat{c}_{mn}-\bar{\hat{c}})^2\right]}},\tag{11}$$

式中 f 和 $\hat{c}$ 分别表示原始明文数据与解密后的明文数据。$\bar{f}$ 和 $\bar{\hat{c}}$ 表示原始明文数据和解密后的明文数据的平均值。相关系数越大，估计的解密密钥越逼近于真实的解密密钥，解密效果越好。

图 6(a)是使用正确的光学系统空间参数和相位板的解密结果，图 6(b)是使用错误的相位板和空间参数解密的结果，图 6(c)是在解密时恢复参考光波所使用的空间系统参数错误时得到的解密结果，图 6(d)是两路光学系统空间参数均错误时的解密结果。

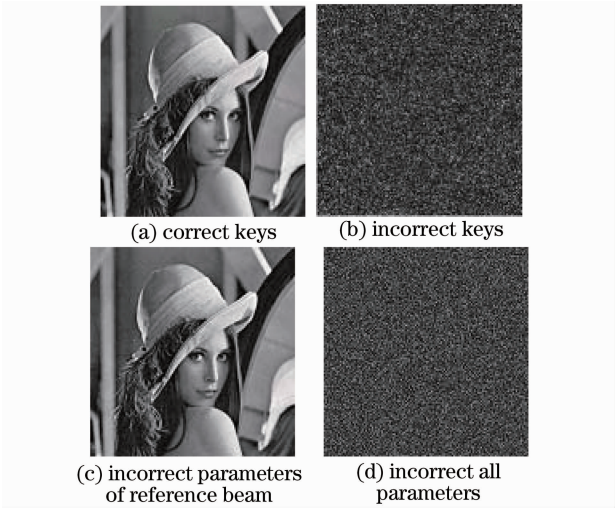

图 6 不同情况解密后的图象

Fig. 6 Decrypted image with different conditions

图 6 四种结果的相关系数分别为：1，0.0052，0.9994，0.0063。从相关系数可以看出，如果解密是相位板函数不正确，很难得到正确的解密结果。当只有参考光路的空间参数错误时，解密结果近似于完全解码，但是在解密相位板函数完全正确，两路光学系统参数同时错误时，解密结果却近似于暴力破解，说明提出的算法具有非常好的混淆和扩散性能。

在假设两路光学系统空间参数正确的情况下，利用文献[9]提供的方法做了选择明文攻击实验，图 7 为用选择明文攻击所得密钥解密的结果。

用选择明文攻击所得密钥解密的结果与原始明文之间的相关系数为 0.096，解密结果与原始明文相关系数很小，采用提出的加密算法的加密系统能非常好地抵御选择明文攻击。

图 7 用选择明文攻击所得密钥解密的结果

Fig. 7 Retrieved results with chosen-plain text attack

5 结 论

提出的虚拟光学加密算法建立在双随机相位光学编码技术的基础上，并利用数字全息技术为加密算法引入了非线性变换，明文和密钥的混淆与扩散得到充分实现，使得明文、密文和密钥之间函数依赖关系较为复杂，针对密文进行统计规律分析几乎不可能。理论分析证明了加密算法的可行性，实验证明了虚拟光学加密算法具有很强的抗暴力攻击、选择明文攻击的能力。通过正确相位函数和光学系统空间按参数都能正确解密，加密和解密过程简单、快速，易于用软件实现。

参 考 文 献

1 B. Javidi, J. L. Horner. Optical pattern recognition for validations and security verification [J]. *Opt. Eng.*, 1994, **33**(6): 1752～1760

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

3 B. Javidi, G. Zhang, J. Li. Experimental demonstration of the random phase encoding technique for image encryption and security verification[J]. *Opt. Eng.*, 1996, **35**(9): 2506～2518

4 B. Javidi, A. Sergent, G. Zhang *et al*.. Fault tolerance properties of a double phase encoding encryption technique[J]. *Opt. Eng.*, 1997, **36**(4): 992～1002

5 X. Peng, Z. Cai, T. Tan. Information encryption with virtual optics imaging system[J]. *Opt. Commun.*, 2002, **212**(4～6): 235～245

6 X. Peng, Z. Cai, T. Tan. Image encryption with virtual optics [C]. *SPIE*, 2002, **4929**: 96～104

7 Y. Frauel, A. Castro, T. J. Naughton. Security analysis of optical encryption[C]. *SPIE*, 2005, **5986**: 25～34

8 A. Carnicer, M. Montes-Usategui, S. Arcos *et al*.. Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys[J]. *Opt. Lett.*, 2005, **30**(13): 1644～1646

9 Wei Hengzheng, Peng Xiang, Zhang Peng *et al*.. Chosen-plaintext attack on double phase encoding encryption technique [J]. *Acta Optica Sinica*, 2007, **27**(5): 824～829
位恒政，彭 翔，张 鹏 等. 双随机相位加密系统的选择明文攻击[J]. 光学学报，2007，**27**(5)：824～829

10 Peng Xiang, Tang Hongqiao, Tian Jindong. 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唯密文攻击[J]. 物理学报, 2007, **56**(5): 2629～2636

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

12 G. H. Situ, J. J. Zhang. Multiple-image encryption by wavelength multiplexing [J]. *Opt. Lett.*, 2005, **30**(11): 1306～1308

13 Sun Liujie, Zhuang Songlin. Digital watermarking of encrypted in-line holography[J]. *Optics and Precision Engineering*, 2007, **15**(1): 131～137
孙刘杰,庄松林. 加密同轴全息数字水印[J]. 光学精密工程, 2007, **15**(1): 131～137

14 Zhong Liyun, Zhang Yimo, Lü Xiaoxu *et al*.. Analysis of some fundamental issue about digital hologram[J]. *Acta Optica Sinica*, 2004, **24**(4): 465～471
钟丽云,张以谟,吕晓旭 等. 数字全息中的一些基本问题分析[J]. 光学学报, 2004, **24**(4): 465～471

15 Wu Kenan, Hu Jiasheng, Lin Yong. A novel method of key design in optical encryption system based on JTC architecture[J]. *Optics and Precision Engineering*, 2007, **15**(4): 577～581
吴克难,胡家升,林　勇. 基于JTC的光学加密系统密钥设计新方法[J]. 光学精密工程, 2007, **15**(4): 577～581