文章编号：1001-3806(2014)04-0515-07

随机偏振光学加密算法的加密及解密特性分析

林 超[1],沈学举[1*],杜 霜[2],郭耀阳[1],胡 申[1]
(1. 军械工程学院,石家庄 050003;2. 中国人民解放军 78336 部队,昆明 650211)

摘要：为了阐明随机偏振模板在光学加密系统中的作用,采用理论分析与数值模拟相结合的方法,进行了在双随机偏振光学加密系统中偏振模板的特性参量对系统加密效果及解密误差的影响的理论和仿真分析;对比了随机相位模板和随机偏振模板对光学加密系统加密效果及解密误差的不同影响。结果表明,加密方面,采用随机偏振模板或随机相位模板均能生成平稳白噪声分布的密文,但是偏振模板有两个构造参量,密钥空间更大;解密方面,系统对相位模板以及偏振模板中不同参量的解密敏感性有一定差异,随机偏振加密具有更高的应用灵活性。该结果对理解相位及偏振编码光学加密系统的本质属性及设计安全性更高的光学加密系统有一定的帮助。

关键词：信息光学;随机偏振加密;琼斯矢量;加密效果;解密误差
中图分类号：O438 **文献标志码**：A **doi**:10.7510/jgjs.issn.1001-3806.2014.04.016

Characteristic analysis of encryption and decryption in random polarization optical encryption algorithm

LIN Chao[1], *SHEN Xueju*[1], *DU Shuang*[2], *GUO Yaoyang*[1], *HU Shen*[1]
(1. Ordnance Engineering College, Shijiazhuang 050003, China; 2. Unit 78336, Chinese People's Liberation Army, Kunming 650211, China)

Abstract: To demonstrate the function of random polarization mask in an optical encryption system, the influence of parameters in random polarization mask on encryption effect and decryption error in double random polarization optical encoding system was analyzed by means of theoretical analysis and numerical simulation. The different effects of random phase encoding algorithm and random polarization encoding algorithm on encryption effect and decryption error were compared and presented. The results indicate that a satisfying white-noise liked encrypted image can be obtained when using random phase mask or random polarization mask. But a larger key space is observed with random polarization mask due to its two structured parameters. From decryption point of view, the key sensitivities are different among the different parameters in random polarization mask or random phase mask. The random polarization encoding algorithm has the favorable feasibility for practical application. The results are significant not only for the understanding on the intrinsic of random phase and polarization optical encoding system but also for the design of optical encryption system with high security level.

Key words: information optics; random polarization encryption; Jones vector; encryption effect; decryption error

引 言

光学信息安全技术是近些年信息安全领域发展起来的新兴技术之一,加密技术又是信息安全技术的核心。由于光波的固有属性,用光学硬件实现加密和解密具有处理速度快,加密自由度多等优势。在多种光学加密技术中,由 JAVIDI 等人提出的、并经研究人员深入分析和改进的双随机相位编码(double random phase encoding, DRPE)技术[1]是其中经典的技术之一。由于它能够把原始图像加密成平稳白噪声分布的密文,因而得到了广泛的关注和应用。

在双随机相位光学加密系统中,随机相位模板(random phase mask, RPM)起着关键作用,随机相位模板的特性参量对系统的加密效果有重要影响[2],事实上, RPM 是加密系统中的核心组件[3-6]。虽然随机相位模板像素数多,根据相位值量化等级

作者简介:林 超(1987-),男,博士研究生,主要从事光学信息安全及数字全息方面的研究。
*通讯联系人。E-mail: sxjpaper@163.com
收稿日期:2013-07-29;收到修改稿日期:2013-10-30

的不同,可以设计密钥空间巨大的光学加密系统,但是,研究表明,在采用随机相位作为密钥的加密系统中,由于相位值的周期性,系统的密钥空间和加密效果存在一定的制约关系,限制了光学加密系统安全性的进一步提高[7]。

除了采用相位作为密钥的光学加密系统之外,采用偏振状态作为密钥的光学加密系统也被提及。它充分利用了光波的矢量特性,将随机相位模板替换为随机偏振模板(random polarization mask, RPOLM),由于偏振模板的特性参量更多,从而扩大了系统的密钥空间[8-9]。在采用偏振状态作为密钥的光学加密系统中,双随机偏振编码(double random polarization encoding, DRPOLE)系统是其中比较经典的技术[10]。但是由于其较 DRPE 技术光学实现起来相对复杂,因而关注程度不高,在加密和解密方面的性质没有得到充分研究。

为了阐明随机偏振加密系统中偏振密钥的特性参量对系统加密和解密过程的影响,基于 DRPOLE 技术,分析了随机偏振模板特性参量对系统加密效果以及解密误差的影响,对比了随机偏振和随机相位加密算法的异同。仿真结果表明,采用随机偏振模板进行加密不仅能得到和随机相位加密系统统计特性相似的平稳白噪声分布的密文,而且由于其具有两个密钥构成参量,密钥空间更大。

作者首先介绍了双随机偏振加密算法,结合 2 维码的特点,数值模拟了其加密和解密过程。然后,通过对偏振模板结构参量的理论分析和数值模拟,研究了偏振加密系统的加密效果和解密时对密钥的敏感性。其结论对于设计高安全性的光学加密系统具有一定意义。

1 双随机偏振加密理论基础

图 1 为双随机偏振加密技术的原理图。为简单起见,用 2 维离散二值数据来展示系统的加解密过程。输入平面原始偏振态分布用两个正交的线性偏振光在空间的分布来表示,这种偏振状态可以通过

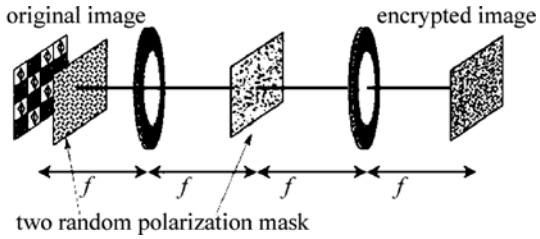

Fig. 1 Schematic diagram for double random polarization encoding system

使用一个线偏器转换成强度分布。输入平面和傅里叶平面上有两个随机偏振调制模板,对原始图像中各像素点处的偏振态进行调制[10]。

琼斯矢量 $\boldsymbol{d}_{jk}$ 表示原始图像分布中任一点 (j,k) 处的偏振态,琼斯矩阵 $\boldsymbol{M}_{jk}$ 表示输入平面调制模板上任一点 (j,k) 处的偏振态,而 $\boldsymbol{N}_{lm}$ 则表示傅里叶平面调制模板上任一点 (l,m) 处的偏振态。假设每个像素点的偏振态有两个参量:双折射材料的主轴方向和两个主轴之间的相位差。在这种情况下有:

$$\boldsymbol{M}_{jk} = \boldsymbol{R}(\theta_{jk})\begin{bmatrix} \exp\left(\frac{-\mathrm{i}\Delta_{jk}}{2}\right) & 0 \\ 0 & \exp\left(\frac{\mathrm{i}\Delta_{jk}}{2}\right) \end{bmatrix}\boldsymbol{R}(-\theta_{jk}) \tag{1}$$

$$\boldsymbol{N}_{lm} = \boldsymbol{R}(\theta_{lm})\begin{bmatrix} \exp\left(\frac{-\mathrm{i}\Delta_{lm}}{2}\right) & 0 \\ 0 & \exp\left(\frac{\mathrm{i}\Delta_{lm}}{2}\right) \end{bmatrix}\boldsymbol{R}(-\theta_{lm}) \tag{2}$$

$$\boldsymbol{R}(\alpha) = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \tag{3}$$

式中,Δ_{jk} 和 Δ_{lm} 表示快轴和慢轴之间的相位差,θ_{jk} 和 θ_{lm} 表示快轴相对于水平方向的方位角。Δ_{jk} 和 Δ_{lm} 随机分布在区间 $[0,2\pi]$ 内,θ_{jk} 和 θ_{lm} 随机分布在区间 $[0,\pi]$ 内。每个像素点处双折射液晶分子的主轴旋转可通过结合两个 $\lambda/4$ 波片和纯相位液晶空间光调制器(spatial light modulator, SLM)来实现,其中旋转角度取决于可以由电压控制的 SLM 的延迟[11]。输入平面上经过编码的偏振状态 $\boldsymbol{p}_{jk}$ 可表示为:

$$\boldsymbol{p}_{jk} = \boldsymbol{M}_{jk}\boldsymbol{d}_{jk} \tag{4}$$

用二值数据来模拟加密和解密过程。假设灰度值为 1 和 0 的原始二值数据分别用两个线性极化的偏振态表示:

$$\boldsymbol{d}_0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{5}$$

$$\boldsymbol{d}_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{6}$$

经过傅里叶变换,然后由傅里叶平面上的偏振调制模板进行调制。再经过一次傅里叶逆变换,加密后的偏振态分布可表示为:

$$\boldsymbol{e}_{jk} = \mathscr{F}_{jk}^{-1}[\boldsymbol{N}_{lm}\mathscr{F}_{lm}(\boldsymbol{p}_{jk})] \tag{7}$$

式中,$\mathscr{F}$ 表示傅里叶变换,$\mathscr{F}^{-1}$ 表示逆傅里叶变换。

解密时要用到 $\boldsymbol{M}_{jk}$,$\boldsymbol{N}_{lm}$的逆 $\boldsymbol{M}_{jk}^{-1}$,$\boldsymbol{N}_{lm}^{-1}$,解密过程为:

$$\boldsymbol{r}_{jk} = \boldsymbol{M}_{jk}^{-1}\mathscr{F}^{-1}[\boldsymbol{N}_{lm}^{-1}\mathscr{F}(\boldsymbol{e}_{jk})] = \boldsymbol{d}_{jk} \tag{8}$$

式中,$\boldsymbol{M}_{jk}^{-1}=\boldsymbol{M}_{jk}^{*}$,$\boldsymbol{N}_{lm}^{-1}=\boldsymbol{N}_{lm}^{*}$,$*$ 表示复共轭。

2 随机偏振和随机相位加密算法加密效果的理论分析

$$\boldsymbol{M}_{jk} = \begin{bmatrix}\cos\theta_{jk} & -\sin\theta_{jk}\\ \sin\theta_{jk} & \cos\theta_{jk}\end{bmatrix}\begin{bmatrix}\exp\left(\frac{-\mathrm{i}\Delta_{jk}}{2}\right) & 0\\ 0 & \exp\left(\frac{\mathrm{i}\Delta_{jk}}{2}\right)\end{bmatrix}\begin{bmatrix}\cos\theta_{jk} & \sin\theta_{jk}\\ -\sin\theta_{jk} & \cos\theta_{jk}\end{bmatrix} =$$

$$\begin{bmatrix}\cos^2\theta_{jk}\exp\left(\frac{-\mathrm{i}\Delta_{jk}}{2}\right)+\sin^2\theta_{jk}\exp\left(\frac{\mathrm{i}\Delta_{jk}}{2}\right) & \cos\theta_{jk}\sin\theta_{jk}\exp\left(\frac{-\mathrm{i}\Delta_{jk}}{2}\right)-\sin\theta_{jk}\cos\theta_{jk}\exp\left(\frac{\mathrm{i}\Delta_{jk}}{2}\right)\\ \cos\theta_{jk}\sin\theta_{jk}\exp\left(\frac{-\mathrm{i}\Delta_{jk}}{2}\right)-\sin\theta_{jk}\cos\theta_{jk}\exp\left(\frac{\mathrm{i}\Delta_{jk}}{2}\right) & \sin^2\theta_{jk}\exp\left(\frac{-\mathrm{i}\Delta_{jk}}{2}\right)+\cos^2\theta_{jk}\exp\left(\frac{\mathrm{i}\Delta_{jk}}{2}\right)\end{bmatrix} \tag{9}$$

分两种情况进行分析。第 1 种情况,当 $\boldsymbol{d}_0=\begin{bmatrix}1\\0\end{bmatrix}$时,将(9)式代入(4)式,可以得到:

$$\boldsymbol{p}_{jk} = \begin{bmatrix}\cos^2\theta_{jk}\exp\left(\frac{-\mathrm{i}\Delta_{jk}}{2}\right)+\sin^2\theta_{jk}\exp\left(\frac{\mathrm{i}\Delta_{jk}}{2}\right)\\ \cos\theta_{jk}\sin\theta_{jk}\exp\left(\frac{-\mathrm{i}\Delta_{jk}}{2}\right)-\sin\theta_{jk}\cos\theta_{jk}\exp\left(\frac{\mathrm{i}\Delta_{jk}}{2}\right)\end{bmatrix} = \begin{bmatrix}\cos\left(\frac{\Delta_{jk}}{2}\right)-\mathrm{i}\sin\left(\frac{\Delta_{jk}}{2}\right)\cos(2\theta_{jk})\\ -\mathrm{i}\sin\left(\frac{\Delta_{jk}}{2}\right)\sin(2\theta_{jk})\end{bmatrix} \tag{10}$$

第 2 种情况,当 $\boldsymbol{d}_1=\begin{bmatrix}0\\1\end{bmatrix}$时,将(9)式代入(4)式,可以得到:

$$\boldsymbol{p}_{jk} = \begin{bmatrix}\cos\theta_{jk}\sin\theta_{jk}\exp\left(\frac{-\mathrm{i}\Delta_{jk}}{2}\right)-\sin\theta_{jk}\cos\theta_{jk}\exp\left(\frac{\mathrm{i}\Delta_{jk}}{2}\right)\\ \sin^2\theta_{jk}\exp\left(\frac{-\mathrm{i}\Delta_{jk}}{2}\right)+\cos^2\theta_{jk}\exp\left(\frac{\mathrm{i}\Delta_{jk}}{2}\right)\end{bmatrix} = \begin{bmatrix}-\mathrm{i}\sin\left(\frac{\Delta_{jk}}{2}\right)\sin(2\theta_{jk})\\ \cos\left(\frac{\Delta_{jk}}{2}\right)+\mathrm{i}\sin\left(\frac{\Delta_{jk}}{2}\right)\cos(2\theta_{jk})\end{bmatrix} \tag{11}$$

则输入平面上偏振态分布在 x 和 y 方向上的分量分别为:

$$\boldsymbol{p}_1 = \begin{cases}\cos\left(\frac{\Delta_{jk}}{2}\right)-\mathrm{i}\sin\left(\frac{\Delta_{jk}}{2}\right)\cos(2\theta_{jk}), & \left(\boldsymbol{d}_0=\begin{bmatrix}1\\0\end{bmatrix}\right),\\ -\mathrm{i}\sin\left(\frac{\Delta_{jk}}{2}\right)\sin(2\theta_{jk}), & \left(\boldsymbol{d}_1=\begin{bmatrix}0\\1\end{bmatrix}\right)\end{cases} \tag{12}$$

为了阐明随机相位函数和随机偏振函数对明文信息的噪声化程度,首先从理论上分析单随机相位和单随机偏振加密算法的扩散特性,即用 $2f$ 系统替代 $4f$ 系统进行分析,进而可以得出两种随机函数对加密效果的影响。

在单随机偏振加密算法中,将(3)式代入(1)式进行展开,可得到:

$$\boldsymbol{p}_2 = \begin{cases}-\mathrm{i}\sin\left(\frac{\Delta_{jk}}{2}\right)\sin(2\theta_{jk}), & \left(\boldsymbol{d}_0=\begin{bmatrix}1\\0\end{bmatrix}\right),\\ \cos\left(\frac{\Delta_{jk}}{2}\right)+\mathrm{i}\sin\left(\frac{\Delta_{jk}}{2}\right)\cos(2\theta_{jk}), & \left(\boldsymbol{d}_1=\begin{bmatrix}0\\1\end{bmatrix}\right)\end{cases} \tag{13}$$

而单随机相位加密算法中,输入平面复振幅分布为:

$$\boldsymbol{p}_3 = \mathscr{F}(x,y)\cdot\boldsymbol{N}(x,y) = \mathscr{F}(x,y)\cdot\exp[\mathrm{i}n(x,y)] \tag{14}$$

式中,$n(x,y)$和 Δ_{jk}为均匀分布在[0,2π]内的随机数,且二者的分布相互独立。θ_{jk}为均匀分布在[0,π]内的随机数。从两种加密算法输入平面复振幅分布的相位值范围以及相位分布出发,通过分析其傅里叶变换谱的振幅分布对比两种算法对明文的扩散能力。仿真结果如图 2 ~ 图 4 所示。为了对比,任选一个随机相位函数 $\boldsymbol{p}_4=-\mathrm{i}\sin(\Delta_{jk}/2)\times\sin(2\theta_{jk})$,做相同的操作,结果如图 5 所示。

首先对比 $\boldsymbol{p}_1$,$\boldsymbol{p}_2$,$\boldsymbol{p}_3$ 和 $\boldsymbol{p}_4$ 的相位分布直方图可以发现,$\boldsymbol{p}_1$,$\boldsymbol{p}_2$ 和 $\boldsymbol{p}_3$ 的相位基本上较均匀地分布在[0,2π]之间,虽然具体某一相位值所占的像素数比例不同,但均满足相位相差 π 时对应直方图柱形的高度相同,即相位差为 π 的两个相位值所占据的像素个数相同。根据相位模板参量对明文信息扩散效果的分析[12],满足这一条件的随机相位模板对明文信息扩散效果较好。而 $\boldsymbol{p}_4$ 的相位分布不满足这一分布规律,因而扩散效果较差。再对比对应的 2 维和 3 维傅里叶变换谱振幅分布图可以发现 $\boldsymbol{p}_1$,$\boldsymbol{p}_2$ 和 $\boldsymbol{p}_3$ 的分布图能量分布比较均匀,没有明显

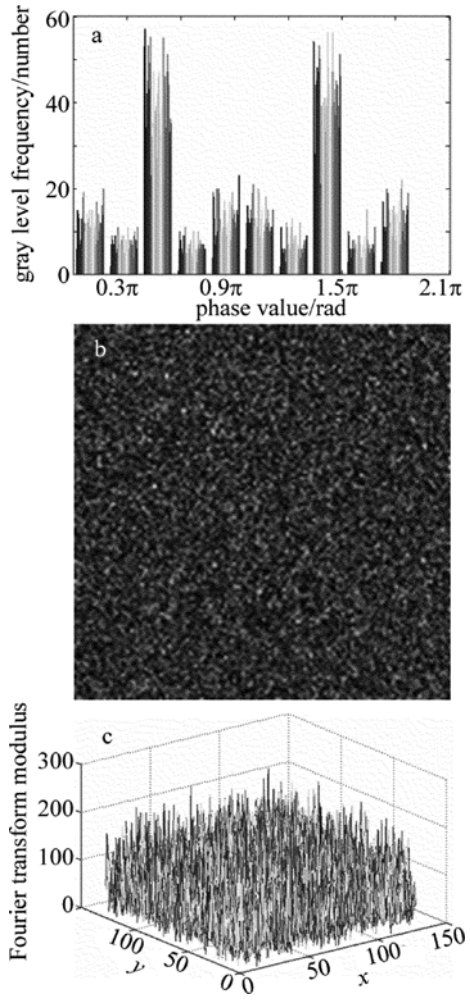

Fig. 2 Phase and Fourier transform spectrum amplitude distribution diagrams for $\boldsymbol{p}_1$

a—phase distribution histogram for $\boldsymbol{p}_1$ b—2-D amplitude distribution of Fourier transform spectrum for $\boldsymbol{p}_1$ c—3-D amplitude distribution of Fourier transform spectrum for $\boldsymbol{p}_1$

的能量集中点,扩散效果比较好。而 $\boldsymbol{p}_4$ 的 2 维分布图中可以观察到中心突出的亮点,3 维分布图中可以观察到明显的尖峰,即不能将中心点处得能量均匀地扩散到整个傅里叶频谱面,扩散效果较差[7]。

由于双随机偏振和双随机相位加密算法在频域的随机模板和空域随机模板具有相同的结构和分布特性,因此对单随机模板的分析可以得出两种加密算法噪声化原始图像的性能。对比图 2、图 3 和图 4,由光学分组密码系统主要引入扩散操作的性质,扩散效果越好,加密效果就越好,因此双随机偏振加密算法和双随机相位加密算法的加密效果均较好。

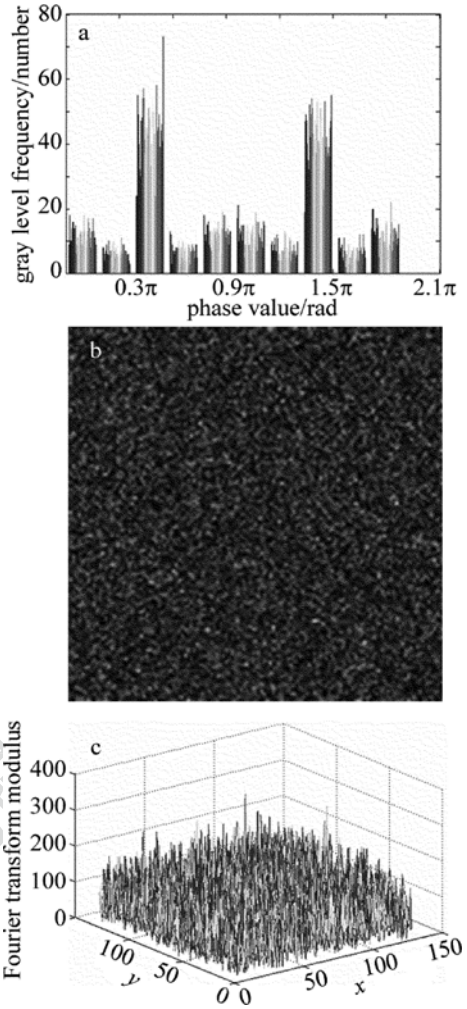

Fig. 3 Phase and Fourier transform spectrum amplitude distribution diagrams for $\boldsymbol{p}_2$

a—phase distribution histogram for $\boldsymbol{p}_2$ b—2-D amplitude distribution of Fourier transform spectrum for $\boldsymbol{p}_2$ c—3-D amplitude distribution of Fourier transform spectrum for $\boldsymbol{p}_2$

3 仿真结果

3.1 双随机偏振加密结果

数值模拟过程中选用的原始图像是一个经过二值化处理的 2 维码。之所以选用 2 维码图像,是因为它信息密度较高,且具有很强的纠错功能。2 维码不仅可以表示多种语言,而且可以表示文字、图像等数据类型,在现实生活中有着广泛运用,因此选用 2 维码图像有着很强的实用背景[12]。

首先运用双随机偏振加密技术对像素大小为 128 × 128 的 2 维码原始图像进行加密,再将得到的图像进行解密,得到的加密和解密图像如图 6 所示。

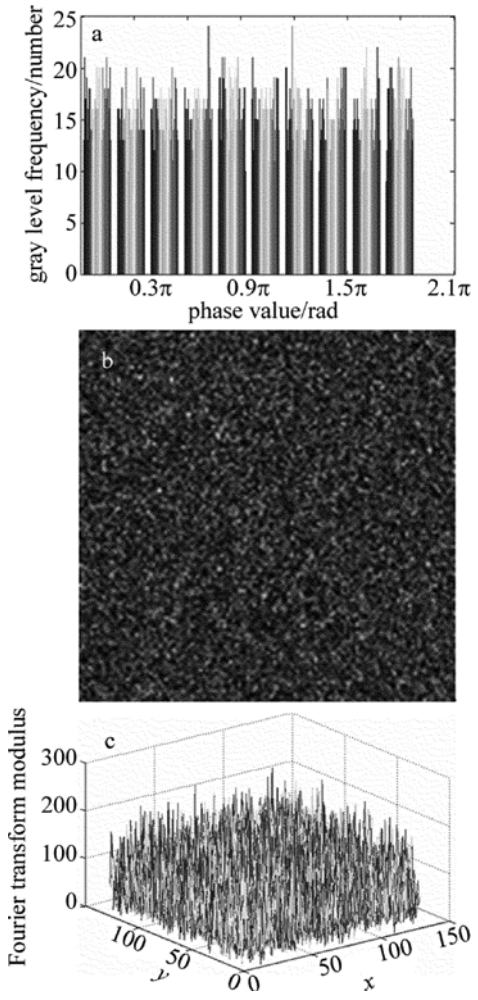

Fig. 4 Phase and Fourier transform spectrum amplitude distribution diagrams for $\boldsymbol{p}_3$

a—phase distribution histogram for $\boldsymbol{p}_3$ b—2-D amplitude distribution of Fourier transform spectrum for $\boldsymbol{p}_3$ c—3-D amplitude distribution of Fourier transform spectrum for $\boldsymbol{p}_3$

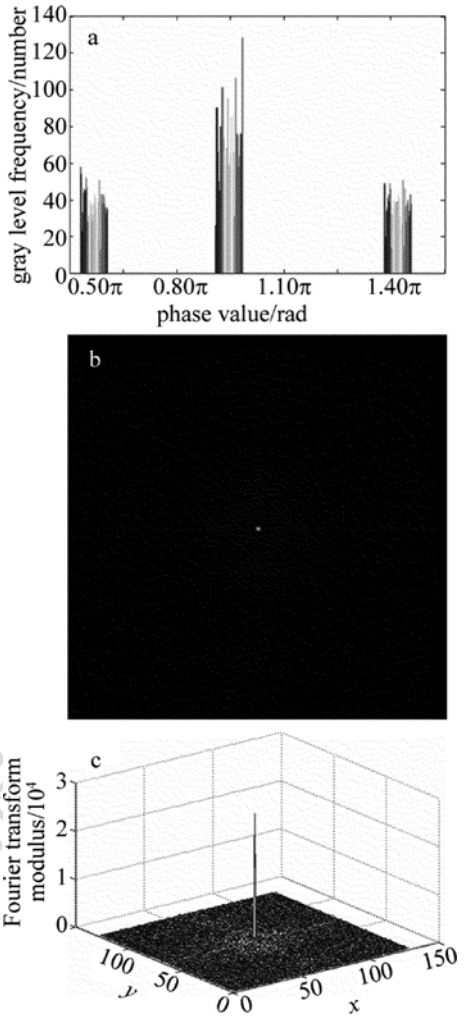

Fig. 5 Phase and Fourier transform spectrum amplitude distribution diagrams for $\boldsymbol{p}_4$

a—phase distribution histogram for $\boldsymbol{p}_4$ b—2-D amplitude distribution of Fourier transform spectrum for $\boldsymbol{p}_4$ c—3-D amplitude distribution of Fourier transform spectrum for $\boldsymbol{p}_4$

对比原始图像和加密图像,可以发现加密图像已经无法看出原始图像的任何信息,加密效果较好。而解密是加密的逆过程,对比解密后图像和原始图像,可以清楚地看到解密后图像能够近乎无损地还原原始图像的信息,解密效果较好。

3.2 双随机偏振和双随机相位的加密效果对比

选取同一个经过二值化处理的原始 2 维码,利用双随机相位加密技术进行加密,并对加密图像进行解密,可得到 1 组加密和解密图像如图 7 所示。

对比图 6 和图 7,人眼无法直观地辨别双随机偏振和双随机相位两种加密方法的加密效果差异,因此需要用一个参量来评价两者的加密效果,作者选用相关系数 C 来定量评价加密效果的好坏。所谓相关系数就是将加密图像或者解密图像与原始图像进行对比,显示出它们与原始图像的相似度。

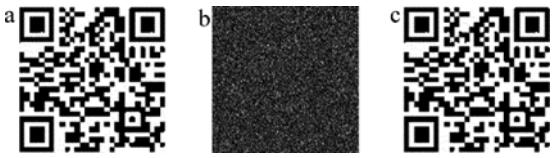

Fig. 6 Numerical simulation results of encryption and decryption with DRPOLE algorithm

a—original image b—encrypted image c—decrypted image

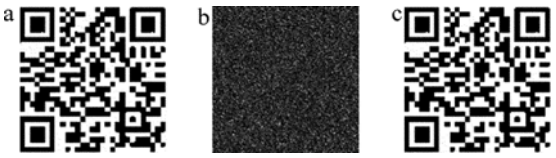

Fig. 7 Numerical simulation results of encryption and decryption with DRPE algorithm

a—original image b—encrypted image c—decrypted image

相关系数越小,两幅图像的相似度越小,加密效果越好。

由于随机相位模板和随机偏振模板中所含可变参量个数不同,即随机偏振模板中包含一个额外的随机旋转矩阵变量,在每次固定随机相位函数的前提下经过十余次的数值模拟得到了两种算法生成的加密图像和原始图像之间的相关系数变化规律,将这两组数据绘制成曲线如图 8 所示。

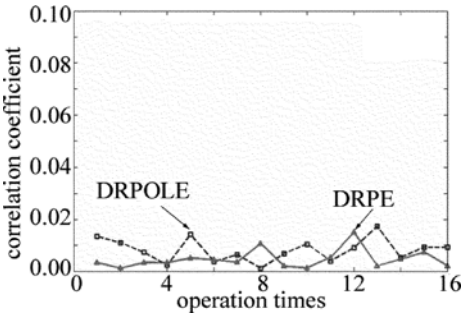

Fig. 8 Curve of correlation coefficients between encrypted image and original image with two kinds of encryption algorithms

图 8 中,虚线 DRPOLE 表示双随机偏振加密的相关系数变化曲线,实线 DRPE 表示双随机相位加密的相关系数变化曲线。通过观察可以发现两条曲线虽然上下浮动,但是相差却不大,量级为 10^{-2},也就是说双随机偏振加密和双随机相位加密这两种加密算法的加密效果相差不大,这与第 2 节中的理论分析相吻合。

3.3 解密密钥错误对解密效果的影响对比

对于双随机偏振加密算法,它的加密和解密密钥中有两个变量:相位差 $\boldsymbol{\Delta}$、方位角 $\boldsymbol{\theta}$,为了研究解密密钥错误对解密效果的影响,分别对 $\boldsymbol{\Delta}$,$\boldsymbol{\theta}$ 以及 $\boldsymbol{\Delta}$ 和 $\boldsymbol{\theta}$ 进行扰动,使它们在解密矩阵中相同位置出现相同的错误百分比且相同的错误值的错误密钥。通过多次试验可以得到 3 组解密图像,如图 9 ~ 图 11 所示。

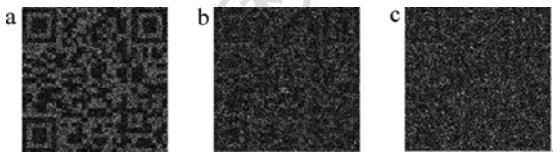

Fig. 9 Decrypted images when $\boldsymbol{\Delta}$ is wrong
a—error percentage is 39.06%, $C = 0.6467$ b—error percentage is 76.56%, $C = 0.3081$ c—error percentage is 95.38%, $C = 0.1899$

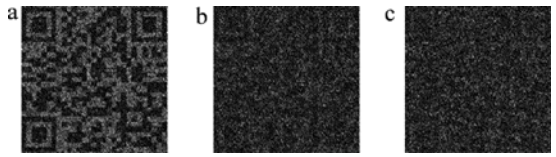

Fig. 10 Decrypted images when $\boldsymbol{\theta}$ is wrong
a—error percentage is 39.06%, $C = 0.7050$ b—error percentage is 87.89%, $C = 0.3156$ c—error percentage is 95.38%, $C = 0.2817$

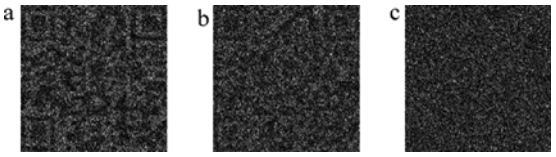

Fig. 11 Decrypted images when $\boldsymbol{\Delta}$ and $\boldsymbol{\theta}$ are both wrong
a—error percentage is 39.06%, $C = 0.4219$ b—error percentage is 48.35%, $C = 0.3099$ c—error percentage is 95.38%, $C = 0.0104$

双随机相位加密算法只有一个频域随机相位变量 $\boldsymbol{b}$ 作为密钥,而空域随机相位函数对实值原始图像的解密不起作用,因而对 $\boldsymbol{b}$ 进行改变,使之出现局部错误且错误的位置比例以及错误值和双随机偏振的情况相同,可得到 1 组解密图,如图 12 所示。

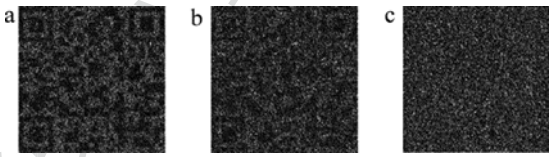

Fig. 12 Decrypted images when $\boldsymbol{b}$ is wrong
a—error percentage is 39.06%, $C = 0.4845$ b—error percentage is 55.08%, $C = 0.3082$ c—error percentage is 95.38%, $C = 0.0112$

观察解密图像可以发现,当相关系数在 0.3 以下的时候,解密图像基本分辨不出原始图像信息,这时的相关系数定义为解密阈值,即解密密钥错误比例超过阈值时,不能得到可分辨的解密图像。改变 $\boldsymbol{\Delta}$ 情况下的 C 阈值为 0.3081,此时的错误百分比为 76.56%;改变 $\boldsymbol{\theta}$ 情况下的 C 阈值为 0.3156,此时的错误百分比为 87.89%;改变 $\boldsymbol{\Delta}$ 和 $\boldsymbol{\theta}$ 情况下的 C 阈值为 0.3099,此时的错误百分比为 48.35%;改变 $\boldsymbol{b}$ 情况下的 C 阈值为 0.3082,此时的错误百分比 55.08%。对比这 4 种情况下的错误百分比,可以发现同时改变 $\boldsymbol{\Delta}$ 和 $\boldsymbol{\theta}$ 对解密效果影响最大,单独改变 $\boldsymbol{\theta}$ 对解密效果影响最小。

再将变量 $\boldsymbol{\Delta}$,$\boldsymbol{\theta}$,$\boldsymbol{b}$ 以及 $\boldsymbol{\Delta}$ 和 $\boldsymbol{\theta}$ 分别在相同位置取相同的错误百分比且相同的错误值,并算出相应的解密图像和原始图像之间的相关系数,可以得到 4 组相关系数数据,将这些数据绘制成曲线如图 13 所示。

根据图 13 中的曲线趋势可以看出,在相同条件下,双随机偏振加密系统中同时改变 $\boldsymbol{\Delta}$ 和 $\boldsymbol{\theta}$ 的情况下解密图像和原始图像的相关系数最小,也就是对解密效果的影响最显著,双随机相位加密中改变

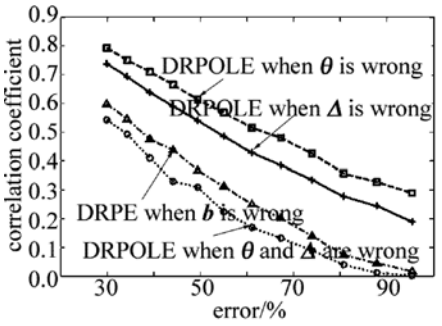

Fig. 13 Curve of correlation coefficients when different kinds of keys are wrong

b 对解密效果的影响仅次于改变 Δ 和 θ，改变 Δ 对解密效果的影响又次于改变 ***b***，而改变 θ 对解密效果的影响最小。

通过对比可知，双随机偏振加密算法对解密密钥中相位差或主轴方位角错误的敏感度较双随机相位加密算法对相位密钥错误的敏感度要低，而偏振加密算法对整体解密密钥的敏感度比相位加密算法的相位密钥要高[13]。

总之，由于随机偏振加密算法的偏振密钥有两个参量可以进行控制，因而其密钥空间势必较随机相位加密算法中的纯相位密钥空间要大，在两者的加密效果相差不大的前提下，可以充分利用随机偏振加密算法对解密密钥敏感度的差异，并结合 2 维码技术的特点设计出同时满足高解密密钥敏感性和高解密容错能力的实用的光学加密系统。

4 结 论

通过理论分析与数值模拟相结合的方式，深入研究了采用随机偏振模板作为密钥和采用随机相位模板作为密钥的情况下，系统的加密和解密特性的异同。通过分析可知，由于随机偏振模板和随机相位模板相位值分布满足特定规律，其对明文信息的扩散能力基本相同，采用两种类型的密钥进行加密时的加密效果相似。随机偏振模板含有两个结构参量，能为光学加密系统提供更大的密钥空间，安全性更高。从解密的角度考虑，随机偏振加密系统对偏振模板的两个参量的解密敏感性和双随机相位加密系统对相位密钥的敏感性存在显著差异，对纯相位密钥的敏感性高于对主轴方位角和正交方向相位差的敏感性，但是，当偏振模板中两个参量均错误时，系统对偏振密钥的敏感性最高。这说明，随机偏振加密系统比随机相位加密系统安全性更高。

参 考 文 献

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

[2] LIN Ch, SHEN X J, YANG Sh X. Simulation analysis of implementing random phase mask with spatial light modulator [J]. Laser Technology, 2013, 37(3): 365-370(in Chinese).

[3] JAVIDI B, HOMER J L. Optical pattern recognition for validation and security verification [J]. Optical Engineering, 1994, 33(6): 1752-1756.

[4] ZHANG J J, SITU G H, ZHANG Y. Progress of optical security systems based on random-phase encoding technology [J]. Journal of the Graduate School of the Chinese Academy of Sciences, 2003, 20(3): 265-272 (in Chinese).

[5] STEPHEN P, GAJDA R, SZNPLIK T. Distributed kinoforms in optical security applications [J]. Optical Engineering, 1996, 35(9): 2453-2458.

[6] JAVIDI B, SERGENT A. Fully phase encoded key and biometrics for security verification [J]. Optical Engineering, 1997, 36(3): 935-942.

[7] LIN Ch, SHEN X J, LI Z Y. Cryptographic analysis on the key space of optical phase encryption algorithm based on the design of discrete random phase mask [J]. Optics and Laser Technology, 2013, 49: 108-117.

[8] CHENG Ch J, CHEN M L. Polarization encoding for optical encryption using twisted nematic liquid crystal spatial light modulators[J]. Optics Communications, 2004, 237(1): 45-52.

[9] UNNIKRISHNAN G, NAUGHTON T, SHERIDAN J. Polarization encoding and multiplexing of two-dimensional signals: application to image encryption[J]. Applied Optics, 2006, 45(22): 5693-5700.

[10] MATOBA O, JAVIDI B. Secure holographic memory by double-random polarization encryption[J]. Applied Optics, 2004, 43(14): 2915-2919.

[11] ERIKSEN R, MOGENSEN P, GLUKSTAD J. Elliptical polarisation encoding in two dimensions using phase-only spatial light modulators[J]. Optics Communications, 2001, 187(1): 325-336.

[12] BARRERA J, MIRA A, TORROBA R. Optical encryption and QR codes: secure and noise-free information retrieval[J]. Optics Express, 2013, 21(5): 5373-5378.

[13] XIAO Y L, LIU Q, YUAN Sh, *et al*. Study about decryption based on optical image encryption system in the Fresnel domain [J]. Laser Technology, 2009, 33(4): 433-436 (in Chinese).