第 27 卷 第 3 期
2000 年 3 月

中 国 激 光
CHINESE JOURNAL OF LASERS

Vol. A27, No. 3
March, 2000

光学图像相位加密中旋转不变性的实现及环形相位解密*

张培琨[1,2] 李育林[1] 刘家英[2] 刘继芳[1] 忽满利[1] 乔学光[1]

([1] 中国科学院西安光机所光学室 西安 710068; [2] 西安应用光学研究所 西安 710065)

提要 计算机模拟研究了光学图像频域相位加密和解密过程,用混沌序列构造相位值并采用环形相位分布,不仅可以压缩密匙的数据量方便保存和传输,而且使加密图像具有中心旋转不变性从而避免解密中对加密图像方向自由度的要求,同时能使解密过程具有一定高低通滤波作用实现滤除噪声或边缘增强。在此加密方法中,解密的关键是加密图像频域中低频分量的解调,高频分量对解密质量和解密图像信噪比虽有影响但比低频分量的影响作用小。

关键词 光学图像,环形相位列阵,加密和解密

当前光学图像处理技术已被用于加密领域,随着计算机的日新月异以及 CCD 技术、图像处理方面的软硬件、激光打印机和扫描仪的飞速发展,使文字和图像以及货币愈来愈容易被复制。尽管现在普遍采用全息防伪技术,但由于全息照片可用一般照相技术再加上数字合成技术进行伪造,实际上并未真正起到防伪的目的。为此,B. Javidi 等提出了一种防伪编码新概念[1],即采用相位来调制要加密的对象使之成为复相位振幅图像,与采用的纯相位列阵密匙一样,是不能用强度探测器如 CCD 相机、复印机或显微镜等进行拷贝和分析,也就难以非法复制。

自 B. Javidi 等提出光学图像相位加密理论之后,对图像在其频域内进行纯相位调制就引起人们广泛注意[2~4]。借助于纯相位空间调制器和计算机能够使这种编码既安全可靠又便于识别。但对于密匙相位列阵而言,若其为随机相位列阵,虽然它不易被复制但却不便于合法用户用计算机重构解密相位。此时必须使用事先做好的解密相位掩模板,如此就给密匙保存和传输造成困难。若其为规律性相位列阵则虽使合法用户重构密匙有规律可依,却也给非法破译提供了方便。为了克服上述两者各自的不足,我们考虑一个混沌状态下的序列,它即具有类似随机信号那样的随机性,又由于它是由确定性系统产生的,故只要知道相应的系统初始参数就能完全重构该序列。以此序列构造密匙就能使合法用户根据初始参数用计算机重构密匙来解密。因此我们认为用确定性系统的混沌序列来构造二维相位列阵最适合实际中的图像相位加密应用[5]。由它和计算机结合通过相位空间调制器就可实现光学图像加密密匙实时变化,而且密匙已不再是整个二维相位列阵,已变为确定系统的初始参数。如此不仅使密匙便于保存和传输,而且同时也起到压缩密匙数据量的作用。

* 国家自然科学基金(69687005)资助项目。

收稿日期: 1998-10-20; 收到修改稿日期: 1998-12-29

另外, 我们采用了一种新形式的环形相位列阵, 实现加密图像在解密时具有中心旋转不变性。而且还分别考虑了解密时仅采用部分环形相位来解密图像, 使除了起到部分解密功能外, 还具有一定的类似二值低通或高通滤波器的作用, 可以同时滤除噪声或提升边缘和轮廓。

1　原　理

频域相位加密的原理就是在图像的频域中对其进行一次相位调制, 改变频域中原有相位分布从而在空域中原始图像就会变成一片随机噪声而无法分辨。此时加密图像成为原始图像与加密相位傅里叶变换的卷积。

设被加密的图像用 $g(x, y)$ 表示, $M(u, v)$ 表示在$(-\pi, \pi)$ 范围内取值的二维混沌序列, 首先对 $g(x, y)$ 进行二维傅里叶变换得到相应的频谱分布 $G(u, v)$, 即

$$G(u, v) = \mathrm{FFT}[g(x, y)] \tag{1}$$

x, y 为空域坐标, u, v 为频域坐标。在频域对 $G(u, v)$ 叠加一个混沌相位分布 $\exp[jM(u, v)]$ 得到

$$I(u, v) = G(u, v)\exp[jM(u, v)] \tag{2}$$

再对上式进行一次逆傅里叶变换就获得

$$i(x, y) = \mathrm{FFT}^{-1}[I(u, v)] = \mathrm{FFT}^{-1}\{G(u, v)\exp[jM(u, v)]\} = g(x, y) * m(x, y) \tag{3}$$

其中 $m(x, y)$ 是 $\exp[jM(u, v)]$ 的逆傅里叶变换, $*$ 表示卷积, $i(x, y)$ 就是原图像 $g(x, y)$ 经过相位编码后获得的加密图像。

在识别加密图像 $i(x, y)$ 时, 采用解码相位 $\exp[-jM(u, v)]$ 对 $i(x, y)$ 在频域内进行滤波, 在输出面上就获得了原始图像 $g(x, y)$。这里 $\exp[-jM(u, v)]$ 就是识别过程中的密匙。在整个加密和解密过程中关键在于相位列阵 $M(u, v)$, 而它又是由确定性系统的离散混沌序列构造的, 从而就转换为确定非线性系统的初始状态。

由于整个加密相位和解密相位互为共轭相位, 因此在加密和解密过程中使用的相位列阵大小及形状不同, 那么最终的解密效果也会不同。为了进一步讨论, 可以把最终的解密图像 $j(x, y)$ 看作是原始图像 $g(x, y)$ 和一个噪声 $e(x, y)$ 的叠加

$$j(x, y) = g(x, y) + e(x, y) \tag{4}$$

这里 $e(x, y)$ 表示由于解密相位与加密相位不完全共轭引入的解密图像相对原始图像而言的解密噪声。当采用非法密匙解密就会使 $e(x, y)$ 非常大, 致使整个图像仍为一片噪声, 而若采用合法密匙则 $e(x, y)$ 就趋于零。根据上式可以引入解密图像的均方信噪比

$$(\mathrm{SNR})_{\mathrm{ms}} = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} j^2(x, y) \Big/ \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} e^2(x, y) \tag{5}$$

以及解密图像 $j(x, y)$ 和原始图像 $g(x, y)$ 间的均方误差

$$\mathrm{MSE} = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}[j(x, y) - g(x, y)]^2 \tag{6}$$

来分别衡量解密图像的质量。

2　模拟实验及分析

用计算机来模拟整个光学图像相位加密和解密的全过程。所用加密和解密的光学系统都是典型的 $4f$ 系统, 原始图像是 128 × 128 点阵的 256 级灰度图像, 如图 1(a) 所示, 加密相位为

128 × 128 列阵, 它是由许多同心圆环构成的, 见图 1(*b*) 。各圆环的相位取值由一维圆映像 $x_{k+1} = \alpha + \beta\cos x_k$ 的混沌序列给出, 其中 α 和 β 为控制参数, 分别取为 6.39 和 2.556 。该序列取值范围已被归化在(- π, π) 之间 。所以虽然相位列阵的相位分布形状存在一定的规律, 但相位值仍是随机的, 它依然是一个随机性的相位列阵, 是不易被非法仿造的 。用图 1(*b*) 形状的相位分布对图 1(*a*) 在其傅里叶频域内进行调制, 则在空域中得到加密的图像 。图 1(*c*) 和(*d*) 分别是加密图像的振幅和相位分布, 显见它已是一片无法分辨的噪声 。接着将加密图绕 4*f* 系统光轴旋转任意角度, 不失一般性我们将其旋转 90° 再在解密光学系统中用解密相位解调, 最终获得和图 1(*a*) 完全一样但旋转了 90° 的图 1(*e*) 。由此可见, 采用同心圆环形状的相位列阵作为密匙可导致加密图像具有旋转不变性, 该性质使图像解密对方向性不敏感 。不仅使解密中不再对加密图像限制取向, 而且又能使原始图像不同旋转样本的加密图可用统一的解密密匙还原 。

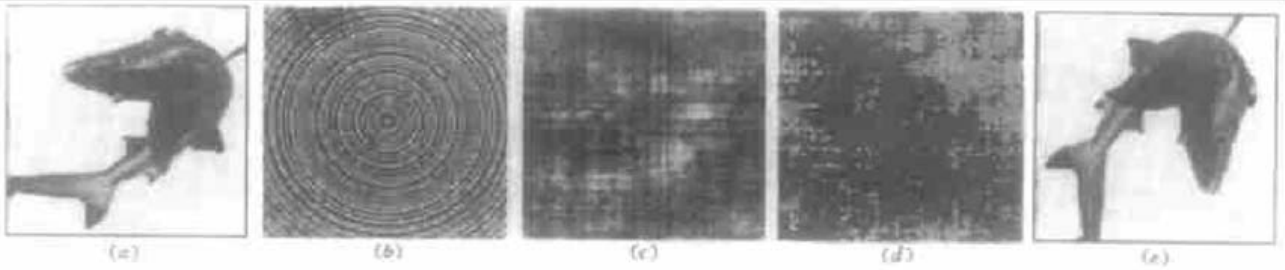

图 1 (*a*) 原图; (*b*) 环形加密相位列阵; (*c*) 加密图像的振幅分布;
(*d*) 加密图像的相位分布; (*e*) 加密图像绕中心旋转 90° 后的解密图像

Fig. 1 (*a*) Original image; (*b*) Phase-ring array for encryption; (*c*) Amplitude distribution of encrypted image;
(*d*) Phase distribution of encrypted image; (*e*) Decrypted image after the encrypted image rotates 90° around its centre

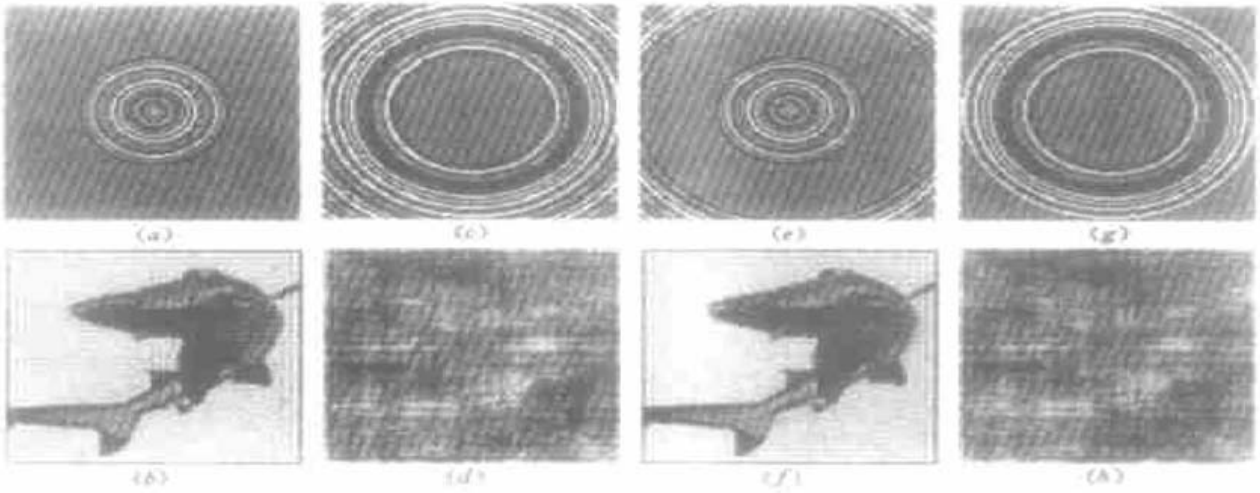

图 2 不同形状的环形解密相位列阵和对应的解密图像

Fig. 2 The different types of decryption phase array and the decrypted images

另外使用部分且形状不同的解密相位列阵来进行解密 。首先使用图 2 (*a*) 作为解密相位, 它是保留以零频为中心以 R = 36 个像素为半径圆域内的解密相位, 而取圆外所有相位为零的相位列阵 。它的作用是仅对加密图像在频域半径为 R 的圆域内实现部分解调 。这一作用极类似于二值滤波中理想的低通滤波, 它将导致图像平滑且存在振铃现象, 如图 2(*b*) 所示 。反之, 图 2(*c*) 形状的解密相位列阵类似于理想的高通滤波器, 它将导致图像边缘增强, 这一点在图 2(*d*) 中明显反映出来 。如果我们在图 2(*a*) 中增加一些相位调制的高频分量, 见图 2(*e*), 或

在图 2(*c*) 中去掉一些高频分量, 见图 2(*g*), 则获得解密图像 2(*f*) 和(*h*) 。将它们同图 2(*b*) 和 (*d*) 进行比较不难看出增加或减少解密相位的部分高频分量对滤波解密的效果影响不大, 重要的加密图像信息都集中在频域的低频范围内 。正因为如此, 使我们能够仅用部分低频相位解密就能获得可以分辨的图像 。当然随着对解密图像质量要求的提高, 就需增加更多解密相位的高频分量从而将加密图像更多的高频信息解调出来 。

我们进一步来讨论解密图像和原始图像之间的均方差以及解密图像的信噪比 。首先将解密相位列阵分为两种, 第一种仅保留半径为 R 的圆内原有的解密相位, 其他部分相位取为零; 第二种是保留圆外原有的解密相位, 圆内相位取为零 。此外还分别考虑加密图像受高斯白噪声污染和未污染两种情况 。通过计算得到均方差随半径 R 变化的曲线和解密图像信噪比与R 的关系, 分别见图 3 和 4 所示 。

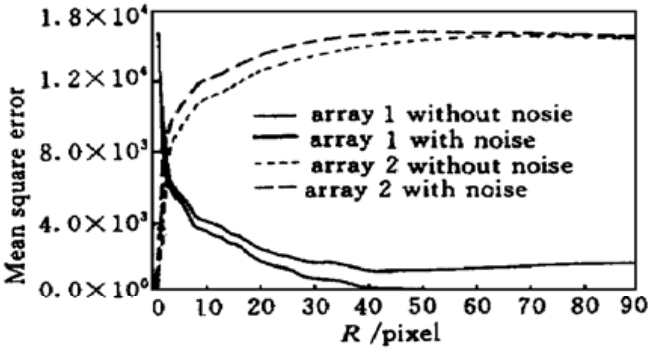

图 3　解密图像与原始图像之间均方差同环形解密相位半径的关系

Fig. 3　The mean square error between the decrypted image and original image versus the radius for different types of decryption phase array

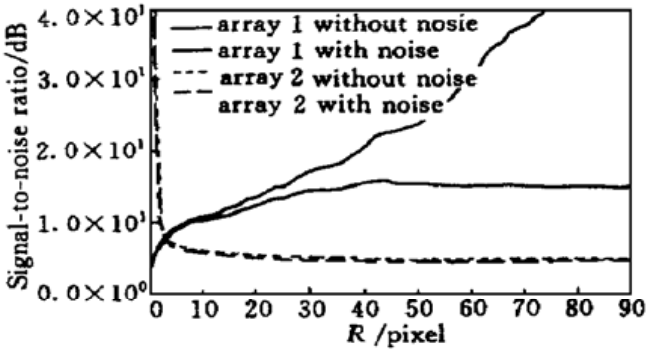

图 4　解密图像信噪比同环形解密相位半径的关系

Fig. 4　The signal-to-noise ratio of decrypted image versus the radius for different types of the decryptionphase array

从图 3 可以看出, 当 R 取 3 个像素点时第一种相位列阵解密图和原图之间的均方差由最大值降低到一半以下, 反之对于第二种相位列阵, 均方差由最小值增大到最大值的一半 。这就说明频域中最低频分量包含最重要的信息, 它对解密质量起到决定性的作用 。而当 R 大于 42 个像素点之后, 再增大 R, 均方差反而趋于不变 。这也就说明频域中最高频分量对还原图像的质量影响非常微弱 。在 R 等于 42 个像素点, 即实际解密相位有效部分占原图像的 33. 8% 时, 受噪声污染的加密图像经过两种相位列阵解密后, 解密图像和原图之间的均方差取极值 。对应第一种相位列阵取最小值, 而对应第二种相位列阵取最大值 。

由图 4 发现对于第一种相位列阵, 半径 R 越小则无论噪声污染加密图与否, 经相位列阵解密还原的图像信噪比之间彼此越接近 。但当 R 增大后, 加密图像无噪声污染的情况下解密图像具有很高的信噪比且随 R 增大而增大; 对于加密图像有噪声污染的情况, 解密图的信噪比同 R 之间不存在单调关系 。在 R 等于 42 个像素点时取最大值, 继续增大 R 反而导致信噪比降低, 并且同加密图像无噪声污染情况下解密图像的信噪比之间差距变大 。这是由于相位列阵在 R 较小时具有低通性质使噪声降低 。对于第二种相位列阵, 解密图像的信噪比随 R 增大下降很快, 在 R 大于几个像素点后解密图像的信噪比都低于 6 dB, 并且对于加密图像有无噪声污染区别不大 。这就再次表明影响解密图像信噪比大小的关键在于加密图像频域中的低频分量 。

3 结 论

在光学图像频域内对其进行相位调制可以起到加密图像的功能,同时如果采用混沌序列来构造相位列阵还可以压缩密匙的数据量,使密匙的保存和传输既可靠又方便。如果采用环形相位分布又能使加密图像具有中心旋转不变性,该性质使解密过程中不必再考虑加密图像输入时的方向性,图像绕解密光学系统光轴旋转任意角度都能被正确解密。在此方法中图像傅里叶域中的超低频分量对提高解密质量和解密图像信噪比十分关键,低频分量的作用大于高频分量,因此可以仅对部分加密图像的低频分量解调就能获得较好的解密图像,同时又使解密相位具有低通滤波器的功能用来降低噪声。这种高低频分量所起作用大小的差异使非法破译密匙低频部分就能得到一定质量的解密图像,理论上讲它在一定程度上降低了保密性,但是加密图像和密匙的相位属性使此不足不影响应用。

参 考 文 献

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

2 E. G. Johnson, J. D. Brasher, D. Gregory *et al.*. Optical recognition of phase-encrypted biometrics. *Opt. Eng.*, 1998, **37**(1): 18~ 26

3 B. Javidi, A. Sergent. Fully phase encoded key and biometrics for security verification. *Opt. Eng.*, 1997, **36**(3): 935~ 942

4 L. G. Neto, Y. Sheng. Optical implementation of image encryption using random phase encoding. *Opt. Eng.*, 1996, **35**(9): 2459~ 2463

5 P. Zhang, Y. Li, M. Hu *et al.*. The influence of noise on optical image encryption & decryption using chaotic phase array. *Acta Photonica Sinica* (光子学报), 1998, **27**(7): 593~ 597 (in Chinese)

Study on the Rotative Invariance in the Phase Encrypted Image and the Phase-ring Decryption

Zhang Peikun[1,2] Li Yulin[1] Liu Jiaying[2] Liu Jifang[1] Hu Manli[1] Qiao Xueguang[1]

[1] *Xi' an Institute of Optics and Precision Mechanics, The Chinese Academy of Sciences, Xi' an* 710068

[2] *Xi' an Applied Optics Institute, Xi' an* 710065

Abstract The phase encryption and decryption of optical image in Fourier domain are studied by computer simulation. The chaotic sequence is used to construct the phase array to compress the data of decryption key to make it saving and transferring conveniently. A novel phase-ring distribution is used to make encrypted image with a rotative invariance so that the orientation of encrypted image is unconsidered during decryption. The noise can be reduced and the edges can be enhanced because this type of phase array has some functions as same as high-pass or low-pass filters. In this encryption method the ultra-low-frequency components of encrypted image in Fourier domain is more important and has a greater influence on the quality and signal-to-noise ratio of decrypted image than the high-frequency components do.

Key words optical image, phase-ring array, encryption and decryption