基于像素置乱技术的多重双随机相位加密法*

陆红强 赵建林** 范 琦 徐 莹 宛晓闯
(西北工业大学理学院,光信息科学与技术研究所,西安 710072)

摘 要 提出一种基于像素置乱技术的多重双随机相位加密法,对该加密法中像素置乱操作的原理进行了阐述,并且提出在光学上实现像素置乱操作和解置乱操作的途径. 在计算机上模拟实现了该加密法,并且得到很好的加密解密结果. 仿真结果证实仅用部分加密图像来解密也能够得到原图像,并且得到随着待解密的加密图像像素的增加,解密图像的信号能量、噪声以及信噪比的变化曲线. 最后分析比较了该加密法与双随机相位加密法,得到该加密法与双随机相位加密法相比具有更高的保密性,而且解密图像的信噪比也不会因为引入像素置乱操作而降低.

关键词 图像加密;像素置乱;双随机相位加密;密钥
中图分类号 O438 **文献标识码** A

0 引言

随着互联网技术的迅速发展和对大量图像信息传输需求的日益增加,从信息安全角度考虑,图像加密技术已变得越来越重要. 如果单纯地利用现有各种加密算法对图像进行加密,那么随着高性能计算机的出现,只要利用现有的各种解密算法对被截获信息进行穷举运算,就很有可能提取出原图像,从而达不到真正加密的目的. 为此,有必要寻求更为安全的图像加密技术. 由于光学信息处理系统的高度并行性和超快处理速度,使得很多光学加密系统被提出并且运用于信息安全领域[1~10]. B. Javidi 等[1]于 1995 年首先提出双随机相位加密法. 在该方法的基础上,T. Nomura 等[2]提出用联合变换相关光路实现图像的双随机相位加密. N. Towghi 等[3]提出全相位加密法. O. Matoba 等[4]提出利用位于菲涅耳衍射区的随机相位掩模板对光学图像加密. C. C. Sun 等[5]提出在光折变晶体中利用角度复用来存储多幅加密的图像,利用相位共轭光读出加密图像. B. Javidi 等[6]还将双随机相位加密技术与数字全息技术相结合,提出了数字全息加密技术. T. Nomura 等[7]又提出运用二进制计算全息图作为密钥的加密法. 此外,也有人提出在分数傅里叶变换域中实现双随机相位加密的方法[8~10].

上述光学图像加密系统中,均未对被加密的图像进行预处理. 可以设想,如果在加密之前,将图像先按照一定的运算规则进行像素置乱处理,使原图像失去原有的面目,然后再将其加密到载体信息中,则可使所要传输的加密图像更安全. 基于此思想,本文提出基于像素置乱技术的多重双随机相位加密法,即将像素置乱技术和双随机相位加密法相结合,并且多次运用像素置乱技术和双随机相位加密法,以形成比双随机相位加密法更多重的密钥,使保密性更高. 文中将从理论和计算机仿真的角度,论证基于像素置乱技术的多重双随机相位加密法的可行性,并给出像素置乱的光学实现方法.

1 像素置乱与多重双随机相位加密原理

像素置乱技术可以等效为对图像进行分割和有限步的初等矩阵变换[11],从而打乱图像像素的排列位置. 对数字图像而言,像素的置乱实际上就是对应点之间灰度值或 RGB 颜色值的互换,即将(x, y)处的灰度值或 RGB 颜色值移到(x', y')处. 本文的模拟计算中通过把分割标序后的图像元进行随机地排列,从而来实现像素置乱. 图1是图像像素置乱和解置乱原理框图. 首先对待加密图像进行分割和标序,如图 1(a). 假定待加密图像被分割成 2×2 个图像元,对标序后的图像元进行置乱后得到图 1

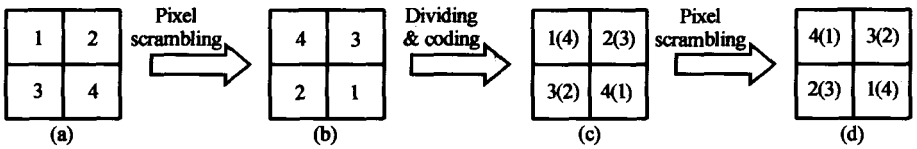


图 1 图像像素置乱与解置乱操作原理
Fig. 1 Principle of pixel scrambling and decoding

*西北工业大学研究生创业种子基金资助(z20040064)
** Tel:029-88495724-801 Email:jlzhao@nwpu.edu.cn
收稿日期:2004-05-14

(b). 进行解置乱时，首先对待解密图像进行再次分割和标序，如图 1(c). 其中图 1(c)中括号前的序号是新标定的序号，括号中的序号是原图像的序号. 对分割、标序后的图像元进行与加密过程中相同的置乱操作，最后得到图 1(d). 从图 1(d)中括号内的序号可以看出对加密的图像进行了正确的解密.

为了减少运算量，实验中无须对每一个像素进行置乱，而是对分割后的图像元进行置乱. 例如，待加密图像为 256×256 个像素，将该图像分割成 256 个图像元，每个图像元为 16×16 个像素. 被加密图像分割得越小越好，如果分割成 256×256 个图像元，就转变成对每个像素进行置乱，这样置乱后的图像保密效果最好，但是运算量也随之剧增.

假定被加密图像是 $f(x, y)$，空域中的随机相位掩模板为 $\exp[\mathrm{j}2\pi\phi_i(x, y)]$，频域中的随机相位掩模板为 $\exp[\mathrm{j}2\pi\varphi_i(u,v)]$. 其中，$x$ 和 y 是空域坐标，u 和 v 是频域坐标，$\phi_i(x, y)$和 $\varphi_i(u,v)$是分布于[0, 1]之间互不相关的随机白噪声序列. 对图像进行第 i 次置乱和解置乱操作分别表示为 $J_i\{\}$和 $J_i^{-1}\{\}$，傅里叶变换和逆傅里叶变换分别表示为 FFT{}和 $\mathrm{FFT}^{-1}\{\}$. 首先对待加密图像进行像素置乱得到 $J_1\{f(x, y)\}$，置乱后的图像与空域随机相位掩模板 $\exp[\mathrm{j}2\pi\phi_1(x, y)]$相乘，再作一次傅里叶变换变换 FFT{}，得到

$$\mathrm{FFT}\{J_1\{f(x,y)\}\exp[\mathrm{j}2\pi\phi_1(x,y)]\} \quad (1)$$

对所得变换结果进行第二次像素置乱 $J_2\{\}$，并使其与频域随机相位掩模板 $\exp[\mathrm{j}2\pi\varphi_1(u,v)]$相乘，然后作一次逆傅里叶变换 $\mathrm{FFT}^{-1}\{\}$，得到

$$\mathrm{FFT}^{-1}\{J_2\{\mathrm{FFT}\{J_1\{f(x,y)\}\exp[\mathrm{j}2\pi\phi_1(x,y)]\}\}\exp[\mathrm{j}2\pi\varphi_1(\mu,\nu)]\} \quad (2)$$

再对上述结果进行第三次像素置乱 $J_3\{\}$，得到

$$R_1 = J_3\{\mathrm{FFT}^{-1}\{J_2\{\mathrm{FFT}\{J_1\{f(x,y)\}\cdot \exp[\mathrm{j}2\pi\phi_1(x,y)]\}\}\exp[\mathrm{j}2\pi\varphi_1(\mu,\nu)]\}\} \quad (3)$$

上述过程就是一个加密周期，得到的加密图像为 R_1. 多次循环上述操作就可以得到保密性更高的加密图像. 如果进行 n 次上述操作，则最后的加密图像为

$$R_n = J_{3n}\{\mathrm{FFT}^{-1}\{J_{3n-1}\{\mathrm{FFT}\{J_{3n-2}\{R_{n-1}\}\cdot \exp[\mathrm{j}2\pi\phi_n(x,y)]\}\}\exp[\mathrm{j}2\pi\varphi_n(\mu,\nu)]\}\} \quad (4)$$

解密过程是加密过程的逆过程. 首先对待解密图像进行解置乱 $J_{3n}^{-1}\{\}$，再进行一次傅里叶变换 FFT{}得到

$$J_{3n-1}\{\mathrm{FFT}\{J_{3n-2}\{R_{n-1}\exp[\mathrm{j}2\pi\phi_n(x,y)]\}\}\cdot \exp[\mathrm{j}2\pi\varphi_n(\mu,\nu)] \quad (5)$$

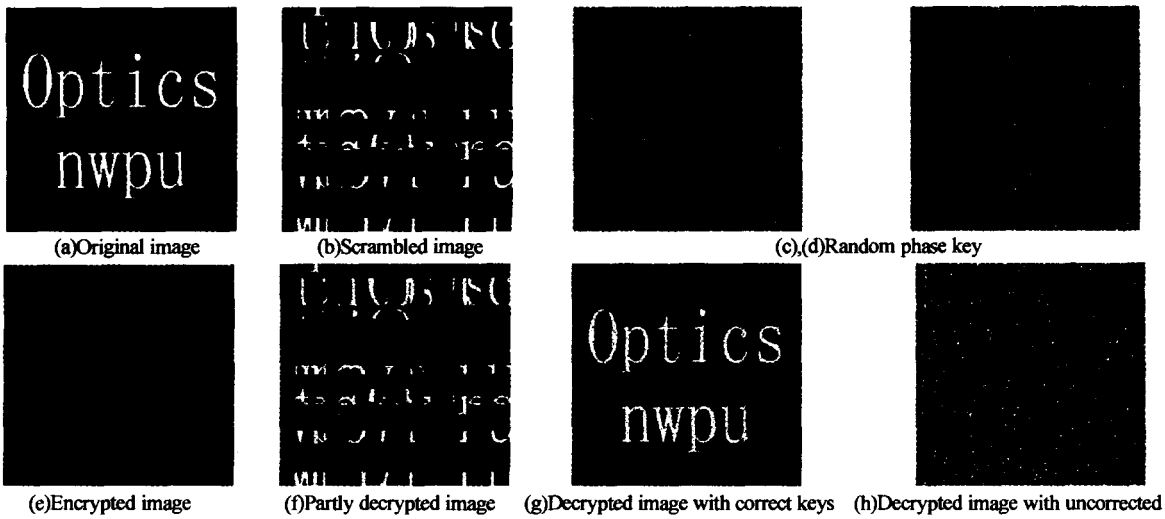
与频域相位掩模板的复共轭 $\exp[-\mathrm{j}2\pi\varphi_n(u,v)]$相乘，进行一次解置乱 $J_{3n-1}^{-1}\{\}$后做一次逆傅里叶变换 $\mathrm{FFT}^{-1}\{\}$得到

$$J_{3n-2}\{R_{n-1}\}\exp[\mathrm{j}2\pi\phi_n(x,y)] \quad (6)$$

乘以空域相位掩模板的复共轭 $\exp[-\mathrm{j}2\pi\phi_n(x, y)]$，再做一次解置乱操作 $J_{3n-2}^{-1}\{\}$，最后得到 R_{n-1}. 上述过程是一个解密周期，对加密图像进行 n 次解密操作就可以得到被加密图像 $f(x, y)$.

2 实验结果

图 2(a)是待加密的二值化图像，其大小为 256×256 个像素，图中字母的像素数为 4988. 图 2(b)是将图 2(a)分割成 16×16 个图像元并且进行第一次置乱后的结果. 图 2(c)和图 2(d)分别是空域和频域中的密钥. 图 2(e)是得到的加密图像，可以看



(a)Original image (b)Scrambled image (c),(d)Random phase key

(e)Encrypted image (f)Partly decrypted image (g)Decrypted image with correct keys (h)Decrypted image with uncorrected keys

图 2 基于像素置乱技术的多重双随机相位加密的实验结果

Fig. 2 Experimental results of iterative double random phase encryption based on pixel scrambling

到加密的效果很好．需要说明的是，该加密过程仅运用了一个周期的加密操作．图 2(f)是部分解密后的图像，该解密图像缺少最后一步解置乱操作．图 2(g)是完全解密后得到的图像．由于待加密图像主要是低频信息，能量集中分布在频谱面上的中心区域，而在本仿真计算中相对于频谱密度而言抽样间距较大，从而导致该图中有噪声．通过减小抽样间距或对解密图像的去噪、滤波可以减少解密图像的噪声对解密图像后续处理的影响．图 2(h)是第一步解置乱错误，其它两步解置乱正确，并且密钥也是正确的情况下后得到的解密图像．从图中可以看到只要解置乱错误，即使频域和空域中的密钥正确也得不到原图像．

文献[12～14]证明，从加密图像中取出一部分进行解密也可以得到原图像，但解密出的图像带有一定噪声，其大小为 $M(\Omega^2-\Omega^4)/N$. 这里 Ω 为待解密图像的归一化长度，M 为被加密图像中灰度不为 0 区域(本实验所给图像中的字母)的像素数，N 为整个加密图像的像素数．这一结论在基于像素置乱技术的多重双随机相位加密方法中也得到证实．图 3 是从不同大小的部分待解密图像得到的解密图像，图 4 和图 5 分别为解密图像信号能量和噪声与待解密图像像素的大小关系曲线．可以明显看出，待解密图像像素数目越大，解密图像的信号越强．其次，图 3(a)中图像的噪声不大，图 3(b)和图 3(c)中图像的噪声明显增加，但随着待解密图像像素数目的继续增加，解密图像的噪声反而减小，如图 3(d)．这种噪声的变化趋势与理论计算结果完全一致．图 5 中虚线为理论计算结果，实线为解密图像平均噪声的拟合结果．在计算解密图像的噪声时运用了式(7)[14]

(a)50×50pixels　(b)100×100pixels　(c)200×200pixels　(d)250×250pixels

图 3　由不同像素数目的加密图像所得解密图像

Fig. 3　Decrypted images from encoded images

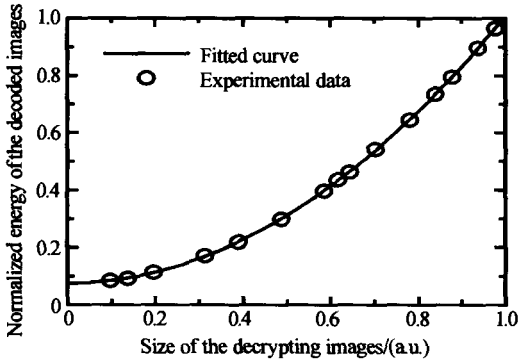


图 4　解密图像信号能量与待解图像像素数目的关系

Fig. 4　The relationship of the energy of the decoded images via the pixels number of the decrypting images

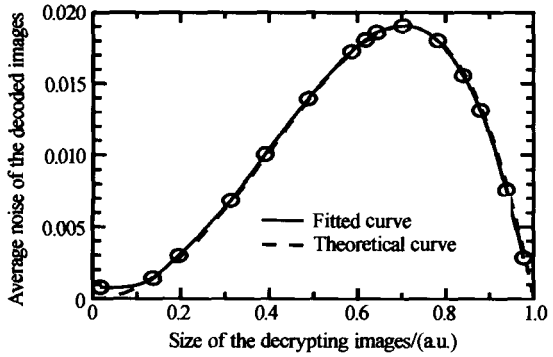


图 5　解密图像噪声能量与待解图像像素数目的关系

Fig. 5　The relationship of the noise of the decoded images via the pixels number of the decrypting images

$$\mathrm{Ave}\{\mathrm{noise}\}=\frac{\sum_{ij}|f_{ij}(x,y)|^2}{(N-M)},\quad i,j\in[0,\cdots,255]$$

$i,j\notin$图像字母所处像素坐标　　(7)

需要说明的是，虽然解密图像的噪声随着待解密图像的大小呈开口向下的抛物线，但由于解密图像的信号能量随着待解密图像的增加而增加，所以并不能因为图 3(b)和图 3(c)中噪声能量较大而认为图 3(b)和图 3(c)的解密效果不好．因为通常衡量图像质量的标准是其信噪比(SNR)，而不是绝对噪声大小．事实上，如果比较 3(a)、图 3(b)、图 3(c)和图 3(d)的信噪比就可以看出，解密图像的质量随着待解密图像像素的增多而提高，这一点也可由图 6 给出的信噪比曲线得以证实．此外，由于像素置乱操作在解密过程中能够完全解密，所以像素置乱预处理对解密图像的信噪比没有任何影响．图 7 比较了施加像素置乱和未施加像素置乱操作情况下解密图像的信噪比．可以看出，两条曲线几乎完全重合，略有差别的原因是每次计算时运用的随机相位掩模板不同所引起的．

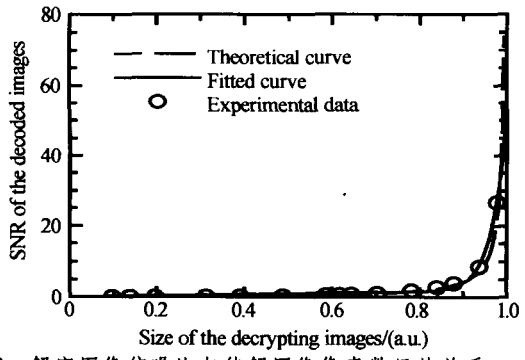


图 6 解密图像信噪比与待解图像像素数目的关系

Fig. 6 The relationship of the SNR of the decoded images via the pixels number of the decrypting images

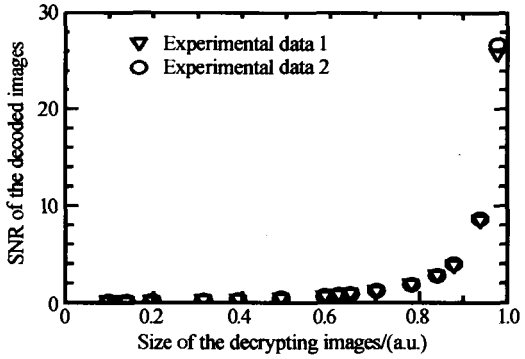


图 7 施加和未施加像素置乱技术时的双随机相位加密法比较

Fig. 7 Comparison of the double random phase encryption with and without pixel scrambling

3 讨论

基于像素置乱技术的多重双随机相位加密法的特点之一是多重密钥．假设被加密的图像大小为 256×256 个像素，空域和频域中的密钥也是 256×256 个像素，加密后的图像被非法获取．现在要通过计算机运算来解密该加密图像，并假定运算一半就能解密，那么对双随机相位加密法得到的加密图像进行解密需运算的次数为 $2^{256\times255}\times2^{[15]}$．现在考虑解像素置乱操作，在本文进行的计算机仿真实验中，图像被分割成 256 个图像元，那么一次解置乱操作要运算 256！/2 次，而且运用了三次像素置乱操作．故在不知道密钥的前提下，通过穷举运算来解密基于像素置乱技术的多重双随机相位加密法得到的加密图像需要运算 $2^{256\times255}\times2\times(256!/2)^3$ 次．与没有像素置乱操作的双随机相位加密法相比，其运算量增加了 $(256!/2)^3$ 倍．如果将图像分割成 256×256 个图像元，其运算量将增加 $(65536!/2)^3$ 倍．其次，每次分割后图像元的像素数也是密钥．在本文进行的计算机仿真实验中，每个图像元包含 16×16 个像素，在解置乱时，只有对 $16/n\times16/n$（n 为正整数，并且要求 $16/n$ 为正整数）大小的图像元进行解置乱才有可能得到正确的解密图像，这同样增加了解置乱操作的运算量．

由于在计算机上进行像素置乱操作运算量很大，影响图像的加密处理速度．故可考虑利用光学方法实现像素置乱操作，如采用光纤置乱器．光纤面板是由很多根平行排列的光学纤维，经熔压形成的高分辨率传像元件，其输入图像和输出图像点与点对应．因此，在布置光纤时人为地让光纤的两端在光纤面板上的相对位置随机排列，则输出图像就会发生置乱．在解密过程中根据光路可逆原理，只要运用和加密过程中相同的光纤置乱器就能解像素置乱操作．

此外，加密图像通过互联网传输前要进行压缩，在解密之前必须先对加密图像进行解压缩．如果解压缩得到的图像没有任何信息损失，那么该压缩、传输过程对解密图像质量没有任何影响；如果加密图像在传输过程中引入了噪声，或者是解压缩过程是有损压缩，那么在解像素置乱时就不能够得到正确的解密图像，从而会影响解密图像的质量甚至得不到正确解密图像．

4 结论

本文提出了基于像素置乱技术的多重双随机相位加密法，把像素置乱技术和双随机相位加密法紧密地结合起来，对该加密法中的像素置乱操作进行了原理性的阐述，并且提出在光路中实现像素置乱操作和解置乱操作的方法．从计算机上模拟实现该加密法，并且得到很好的加密解密效果．仿真结果证实了仅用部分加密图像来解密也能够得到解密图像．而且随着用于解密的加密图像像素的增加，解密图像的信号能量和信噪比也增加，解密图像的噪声则呈开口向下的抛物线变化．在最后分析比较了该加密法与双随机相位加密法，得到该加密法与双随机相位加密法相比具有更高的保密性，而且解密图像的信噪比也不会因为引入了像素置乱操作而降低，同时指出分割后图像元的像素数也可以作为密钥．

参考文献

1 Refregier P, Javidi B. Optical image encryption using input plane and Fourier plane random encoding. *Proc SPIE*, 1995, **2565**: 62～68

2 Nomura T, Javidi B. Optical encryption using a joint transform correlator architecture. *Optical Engineering*, 2000, **39**(8): 2031～2035

3 Javidi B, Towghi N. Fully phase techniques for optical security and encryption. *Proc SPIE*, 1999, **3714**: 40～56

4 Matoba O, Javidi B. Encrypted optical memory system using three-dimensional keys in the fresnel domain.

Optical Letters, 1999, **24**(11): 762～764

5 Sun C C, Su W C, Wang B. Lateral shifting sensitivity of a ground glass for holographic encryption and multiplexing using phase conjugate readout algorithm. *Optics Communications*, 2001, **191**(3-6): 209～224

6 Javidi B, Nomura T. Securing information by use of digital holography. *Optical Letters*, 2000, **25**(1): 28～30

7 Nomura T, Javidi B. Optical encryption system with a binary key code. *Applied Optics*, 2000, **39**(26): 4783～4787

8 Unnikrishnan G, Singh K. Double random Fractional Fourier-domain encoding for optical security. *Optical Engineering*, 2000, **39**(11): 2853～2859

9 Zhang Y, Zheng C H, Tanno N. Optical encryption based on iterative fractional fourier transform. *Optics Communications*, 2002, **202**(4-6): 227～285

10 于力，朱邦和，刘树田. 用于光学图像加密分数傅里叶变换双向位编码. 光子学报, 2001, **30**(7): 904～907
Yu L, Zhu B H, Liu S T. *Acta Photonica Sinca*, 2001, **30**(7): 904～907

11 李昌刚，韩正之，张皓然. 图像加密技术综述. 计算机研究与发展, 2002, **39**(10): 1317～1324
Li C G, Han Z Z, Zhang H R. *Journal Of Computer Research And Development*, 2002, **39**(10): 1317～1324

12 Wang B, Sun C C, Su W C. Improvement of the shift tolerance to the double random phase encoding encryption system. *Proc SPIE*, 1999, **3804**: 215～221

13 Wang B, Sun C C, Su W C, *et a*. Shift-tolerance property of an optical double-random phase-encoding encryption system. *Applied Optics*, 2000, **39**(26): 4788～4793

14 Wang B, Sun C C. Enhancement of signal-to-noise ratio of a double random phase encoding encryption system. *Optical Engineering*, 2001, **40**(8): 1502～1506

15 Lai S, Neifeld M A. Digital wavefront reconstruction and its application to image encryption. *Optics Communications*, 2000, **178**(4-6): 283～289

Iterative Double Random Phase Encryption Based on Pixel Scrambling Technology

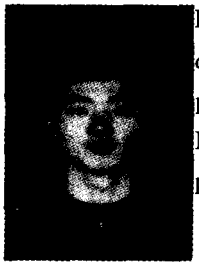
Lu Hongqiang, Zhao Jianlin, Fan Qi, Xu Ying and Wan Xiaochuang

Institute of Optical Information and Technology, School of Science, Northwestern Polytechnical University, Xi'an 710072.

• Received date: 2004-05-14

Abstract A novel encryption based on iterative double random phase encoding and pixel scrambling technology is proposed. The principle of pixel scrambling method is described, and good results are given by numerical simulation used the proposed method. It is shown from numerical simulation that the original image can been reconstructed only when part of the encrypted image is used by this method. The relationship curves of the energy, noise and SNR of the decoded image via the pixels number of the decrypting image is given. By comparing the proposed method with the double random phase encryption, it comes to the conclusions that this method has better performance than the double random phase encryption, and the SNR of the decoded image will not decrease due to pixel scrambling. Finally an optical approach to realize the pixel scrambling is also proposed.

Keywords Image encryption; Pixel scrambling; Double random phase encryption; Secret key



Lu Hongqiang was born on November 21, 1979, in Zhejiang Province. He received B. S. degree from Northwestern Polytechnical University in 2002. Then he was recommended to pursue his M. S. degree in Institute of Optical Information and Technology of Northwestern Polytechnical University. His main research fields are optical information processing and image encryption.