第 52 卷 第 10 期 2003 年 10 月
1000-3290/2003/52(10)/2462-04

物 理 学 报
ACTA PHYSICA SINICA

Vol.52, No.10, October, 2003

基于相息图迭代的随机相位加密*

刘福民[1)] 翟宏琛[1)] 杨晓苹[2)]

[1)] (教育部光电信息技术科学重点实验室,南开大学现代光学研究所,天津 300071)

[2)] (天津理工学院光电信息与电子工程系,天津 300191)

(2002 年 5 月 1 日收到;2003 年 1 月 3 日收到修改稿)

提出了一种将随机相位加密和相位恢复算法中的求解附加相位分布分二步实施的加密方法.由于该方法的实质是通过在随机谱和相息图之间进行相位恢复迭代以确定相息图和密钥的相位分布,因而能够减小图像的解密误差.在相息图相位离散化的迭代过程中,采用增大设计冗余度的方法,降低了由相位离散化所带来的解密误差.最后,通过计算机模拟实验验证了该方法在减小图像解密误差方面的有效性.

关键词:随机相位,光学图像加密,相息图,二元光学,离散化误差,相位恢复算法

PACC:4225F,4230K

1. 引 言

由于随机噪声有最大的熵,而且再生一个相同的随机噪声是非常困难的,因而随机噪声用于图像加密时,具有很高的保密性[1].Javidi 等人[2—4]提出了一种双随机相位加密方法,使加密的图像在光学防伪的应用中有很高的保密性.但该方法需要同时记录加密图像的振幅和相位信息,因而在图像解密时的光学效率不高.Wang 等人[5]提出了将图像加密为随机产生的仅相位图像,省去了对振幅的记录,从而保证了光学实现的高效率[6],这在防复制方面无疑会具有很大的吸引力[7].然而,我们的研究发现,该方法的解密图像存在着很大的噪声,特别是对于二元图像,其解密图像的噪声更大.此外,作者在文章中只考虑了相位的模拟分布的情况,因而在光学实现中,由实际二元光学制造工艺中相位的离散化所引起的误差必然导致实际解密图像的噪声进一步加大,从而容易在后续的对图像的识别中引起误判.为此,本文提出了一种将图像加密成由原图像和某一加密随机相位产生的相息图的新方法.由于在本方法中对求解密钥所必需的相位恢复迭代是在相息图和一个含有随机相位信息的傅氏谱之间进行的,因而这种方法能够降低解密图像特别是二元图像的噪声.此外,本方法还在应用相位恢复算法获得密钥的过程中,采用了增加计算冗余度的方法,降低了离散化引起的误差,从而降低了解密图像的噪声.本文还通过计算机模拟实验,验证了这一方法在应用二元光学相息图实现防伪中对降低解密图像噪声的有效性.

2. 随机相位的加密方法

本文提出的二步随机相位加密方法与文献[1]的方法不同,加密后的图像是一个仅相位分布的相息图,此加密过程的框图如图 1 所示.

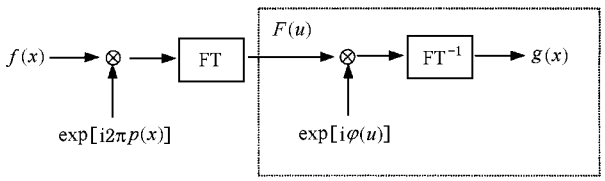

图 1 基于相息图迭代的随机相位加密方法框图(虚框内为迭代计算区域)

图中 $f(x)$ 表示待加密图像的复振幅分布,x 表示二维的像空间坐标,$p(x)$ 代表一个在 $[0,1]$ 之间均匀分布的二维随机阵列.全部加密过程分为以下两步:

* 国家自然科学基金(批准号:60177004)资助的课题.

1)把 $f(x)$ 乘以一个随机相位函数 $\exp[\mathrm{i}2\pi \times p(x)]$,然后再将这个乘积 $f(x)\exp[\mathrm{i}2\pi p(x)]$ 作傅氏变换,得到一个随机谱 $F(u)$.

2)将 $F(u)$ 再乘以一个特定的随机相位函数 $H(u)=\exp[\mathrm{i}\varphi(u)]$,以使 $F(u)H(u)$ 经过逆傅氏变换,能得到一个仅相位分布的加密相息图 $g(x)$,即要求

$$|g(x)| = c, \tag{1}$$

其中 c 为任意常数.上述加密过程在空域中的表示为

$$g(x) = FT^{-1}\{FT\{f(x)\exp[\mathrm{i}2\pi p(x)]\} \times \exp[\mathrm{i}\varphi(u)]\}, \tag{2}$$

其中 $g(x)$ 的相位分布 $\psi(x)$ 及附加的相位分布 $\varphi(u)$ 可以通过迭代的相位恢复算法如 IFTA 迭代求出.这样,$\varphi(u)$ 一经确定,便可作为从相息图 $g(x)$ 本身来恢复 $f(x)$ 的密钥.由于 $p(x)$ 是随机噪声,因而通过相位恢复算法求出的密钥 $\varphi(u)$ 也是随机的,只不过这一随机相位的分布会与 $p(x)$ 和图像 $f(x)$ 紧密相关.所以,用 $\varphi(u)$ 作为密钥,有很高的安全性.

在利用迭代傅里叶算法计算相息图的相位分布以及密钥 $\varphi(u)$ 的过程中,每次迭代过程结束时,即用本次迭代得到的密钥 $\varphi'(u)$ 将图像解密,并采用归一化的价值函数 MSE 作为信噪比的描述,来判断迭代是否收敛.其定义为

$$\mathrm{MSE} = 10\log\frac{\sum_x [I_0(x) - \alpha I_r(x)]^2}{\sum_x I_0^2(x)}, \tag{3}$$

其中 $I_0(x)=|f(x)|^2$ 表示被加密图像的强度分布,$I_r(x)$ 表示解密的图像的强度分布,系数 α 是一个缩放因子,其定义为[8]

$$\alpha = \frac{\sum_x I_0(x) I_r(x)}{\sum_x I_r^2(x)}. \tag{4}$$

当 MSE 低于某一设定值时,即可作为迭代过程结束的条件.

图 2 对比了用本文的加密方法和应用 Wang 的加密方法进行图像加密时解密图像的 MSE 随迭代次数变化的曲线.从中可以看出,解密图像的误差本文方法明显低于 Wang 方法.对于灰度分布图像,应用本文的方法的第 250 次迭代的解密图像的 MSE 比用 Wang 的方法下降了 5.9 dB;而对于二元图像,则下降得更多,约 30 dB.这是因为二元图像中 0 值像素所占的比例一般要大于灰度图像中 0 值元素所占的比例.这表明本文提出的加密方法应用于二元图像要比应用于灰度图像时对图像的改善明显得多.

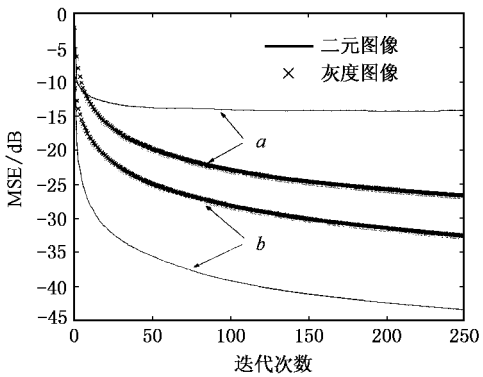

图 2　本文与 Wang 两种加密方法的 MSE 收敛情况比较
a 为用 Wang 的方法;b 为用本文的加密方法

3. 相息图及密钥相位的离散化

出于对实际应用中的技术性考虑,一般须将相息图 $g(x)$ 的相位及密钥 $\varphi(u)$ 离散化.因而在上节所涉及的相位恢复迭代过程就应修正为寻找同时满足(1)式和(2)式的离散化的相位对的过程.

一般而言,对一个模拟的相位分布直接进行离散化,会引入很大的误差,因而可以采用迭代的方式进行[9],即在相位恢复迭代过程中,对每一次迭代的结果都要进行离散化,并利用这个离散化的相位进行下一次迭代.

由于目前尚未从数学上证明相位恢复问题解的存在性和惟一性,而相位离散化条件又给相位恢复问题增加了一个额外的限制,因而其迭代的结果必然会使解密图像存在很大的散斑噪声[9].为解决上述问题,本文通过增大相息图的面积,即增加设计冗余度的方法[9—11]来降低相息图的离散化误差.即在谱面上 $F(u)$ 周围增加了一部分无信号区,在迭代过程中,在无信号区内可以保留一定的振幅,而且这部分区域内的相位也可以不必离散化,因而可以利用这部分区域复振幅的自由度来防止迭代过程的停滞.由于该无信号区仅用于迭代过程而不参与迭代后的解密过程,因而在不影响实质应用效果的前提下,保证了由 $F(u)$ 区内的谱值所决定的再现像有较小的误差.

4. 模拟实验及其结果

本文用计算机对应用上述加密方法进行图像加密/解密的结果进行模拟.在应用相位恢复算法的过程中,采用分步离散化[9]的方式,采用 240 步逐步确定离散化的相位分布,以避免迭代离散化的停滞.从前面的分析可知,离散化的阶数越高,离散化误差越小.由于离散化的阶数应在技术允许的条件下选取,因此把相息图的相位分布取 16 阶离散化量值,而作为解密密钥的相位 $\varphi(u)$,则取与售品空间光调制器对应的 64 阶离散化量值.图 3(a)是像素数为 128 × 128 的待加密图像,图 3(b)至(d)分别给出不引入无信号区,引入无信号区使总面积为原图面积的 4 倍及 16 倍时的最终再现图像.从中可以看出,增加的无信号区面积越大,对解密图像的质量改善就越明显.当然,随着面积的增大,计算量也会相应增大.所以,增大面积的多少要在图像解密质量与计算开销之间进行权衡.对于本文中的例子,面积增加到 16 倍时的解密图像(图 3(d))与期望图像(图 3(a))之间的差异用肉眼已几乎难于分辨了.因此,可以认为在此例中,增大到 16 倍面积已能得到满意的结果.

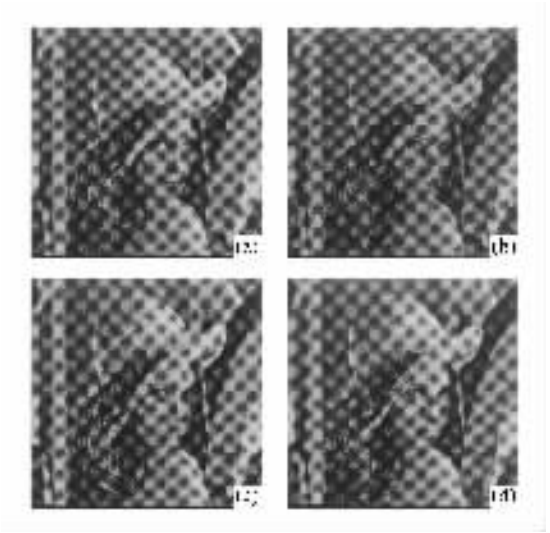

图 3 要加密的图像与解密图像 (a)要加密的图像;(b)未增加无信号区的解密像;(c)增加无信号区后面积为原图 4 倍时的解密像;(d)增加无信号区后面积为原图 16 倍时的解密像

图 4 给出了在上述三种情况下,迭代过程中解密图像的均方差函数 MSE 随迭代次数的变化情况.由于采用分步离散化,在最初的几次(约 35 次)迭代

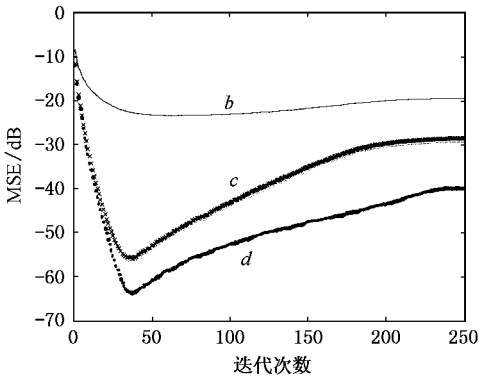

图 4 在不同的相息图面积情况下,MSE 随迭代次数的收敛情况比较(三条曲线分别对应于图 3 中的(b),(c),(d))

中,离散化对 MSE 影响很小,因而 MSE 主要受相位恢复算法的误差递减特性[7]的影响,表现出了下降的趋势.此外,由增大面积使振幅自由度的增加也进一步导致了 MSE 的下降.但随着迭代次数的增加,离散化对 MSE 的影响开始增大,故而 MSE 开始增大.可以看出,在迭代 240 次以后,迭代已经停滞,MSE 不再变化.从以上收敛结果可以看出,对于增大到 16 倍面积的相息图的解密图像,其 MSE 比未引入无信号区的情况下降了 2 个数量级.

5. 讨论与结论

1. 应该指出,虽然本文提出的这种方法和 Wang[5]的随机相位加密方法都是将图像加密成纯相位图像,但是二者有很大的不同.其中最主要的是,后者获得密钥的相位恢复迭代是在一个随机谱分布和待加密图像之间进行的.由于在待加密的图像中占有一定比例的强度为 0 的像素所对应的相位对迭代的自由度没有贡献,因此必然导致相位恢复迭代赖以进行的相位自由度的不足,进而导致迭代的停滞[9],使相位恢复迭代所获的解的精度下降.这一问题对于二元图像尤其严重[8];而在本文的方法中,相位恢复的迭代是在一个待加密图像与一个随机相位因子乘积的傅氏谱 $F(u)$ 和一个相息图 $g(x)$ 之间进行的.由于随机相位有均化傅氏谱的功能[12],因而 $F(u)$ 中的零值区所占比例几乎为 0,从而确保了迭代过程能够利用所有的相位自由度,使相位恢复迭代所得的解有较高的精度,即较小的图像解密误差.

2. 由于在相位离散化的过程中,在谱面 $F(u)$

周围增加的无信号区并不参与后续的解密过程,因而在迭代中无需对该区的振幅作任何限制,也不需要对该区的相位进行离散化处理,因而能更有效地利用该区的复振幅自由度,防止离散化迭代过程的停滞,从而保证能获得较高的解密质量.当然,图像解密质量的提高是以增加计算量为代价的,而且,由于允许在无信号区内保留一定的振幅值,也必然会引起光学实现中效率的下降,因而在具体的操作中,还要在这三者之间进行权衡,选择最优化的实验条件.

[1] Refregier Ph and Javidi B 1995 *Opt. Lett.* **20** 767

[2] Horner J L and Javidi B 1994 *Optical Pattern Recognition* (Proc. Soc. Photo-Opt. Instrum. Eng.) **2237** 193

[3] Javidi B, Sergent A, Zhang G *et al* 1997 *Opt. Eng.* **36** 992

[4] Johnson E G, Bresher J D, Gregory D *et al* 1998 *Opt. Eng.* **37** 18

[5] Wang R K, Watson I A and Chris Chatwin 1996 *Opt. Eng.* **35** 2464

[6] Liang W X, Zhang J J, Lu J F and Liao R 2001 *Chin. Phys.* **10** 1129

[7] Fienup J R 1982 *Appl. Opt.* **21** 2758

[8] Liu F M, Zhai H C, Yang X P and Huang G L 2003 *Acta Opt. Sin.* **23**(6) (in Chinese) [刘福民、翟宏琛、杨晓苹、黄桂岭 2003 光学学报 **23**(6)]

[9] Wyrowski F 1990 *J. Opt. Soc. Am.* A **7** 961

[10] Akahori H 1986 *Appl. Opt.* **25** 802

[11] Shiyuan Yang and Teruo Shimomura 1998 *Appl. Opt.* **37** 6931

[12] Wyrowski F and Bryngdahl O 1988 *J. Opt. Soc. Am.* A **5** 1058

Kinoform-based iterative random phase encryption*

Liu Fu-Min[1)] Zhai Hong-Chen[1)] Yang Xiao-Ping[2)]

[1)] (*Key Laboratory of Optoelectronic Information Science & Technology, Ministry of Education, Institute of Modern Optics, Nankai University, Tianjin* 300071, *China*)

[2)] (*Department of Phtoelectronics and Devices, Tianjin University of Technology*, 300191, *China*)

(Received 1 May 2002; revised manuscript received 3 January 2003)

Abstract

We propose a kinoform-based iterative random phase encryption method, in which the phase retrieval algorithm is divided into two steps: 1) random phase encryption and 2) iteration solving for phase distributions of both the key phase plate and the kinoform. Since the iterations are executed between a Fourier spectrum and the kinoform, the decryption errors can be effectively depressed. By the quantization process for the phase distributions during the iterations, a method of increasing the abundance of design is used to depress the decryption errors. The simulation results are presented at the end, which agree well with the theoretical analysis.

Keywords: random phase, optical image encryption, kinoform, binary optics, quantization error, phase retrieval algorithm

PACC: 4225F, 4230K

* Project supported by the National Natural Science Foundation of China (Grant No. 60177004).