第 57 卷 第 2 期 2008 年 2 月
1000-3290/2008/57(02)/0847-06

物 理 学 报
ACTA PHYSICA SINICA

Vol.57,No.2,February,2008

一种应用相息图对灰度图像信息进行隐藏的方法*

杨晓苹[1)2)] 翟宏琛[1)†] 王明伟[1)]

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

2)(天津理工大学电子信息与通信工程学院,天津 300191)

(2007 年 5 月 8 日收到;2007 年 6 月 19 日收到修改稿)

一幅灰度图像的相息图被隐藏于一幅宿主图像中,该相息图是采用基于相息图迭代的双随机相位加密技术得到的.由于采用仅含有位相信息的相息图作为待加密灰度图像信息的载体,因而与隐藏图像同时具有振幅和相位信息的情况相比较,需要隐藏的信息量大大降低,从而可在对宿主图像影响较小的情况下,提高提取信息的质量;并可有效地提高信息提取时的光学效率,并且对二元图像信息的隐藏也同样适用.水印图像的剪切对隐藏信息提取质量的影响也被分析,模拟实验结果证明了所采用方法的有效性.

关键词:灰度图像,相息图,信息隐藏

PACC:4225F,4230K

1. 引 言

信息的加密、隐藏和提取技术是信息安全研究领域中的重要组成部分.在国际上不断发展的新一代信息安全理论与技术的研究中,基于光学理论与方法的数据加密、隐藏和提取技术成为了一个重要的组成部分[1,2],光学信息处理技术在这些领域中也一直占据着重要的不可替代的地位[3—9].其中,Takai 等人[6]将光学全息概念应用到数字水印中,提出了数字全息水印,但由于只需作傅里叶逆变换就能够解出隐藏信息,因而其安全性较低.Kishk 和 Javidi[7—9]将双随机相位编码用于隐藏图像和数字全息水印,可用于二维或三维物体加密隐藏,安全性能较好.该方法的隐藏图像同时具有振幅和相位信息,当所需隐藏的原始信息为二元图像时,编码后信息的振幅较小,隐藏时对宿主图像影响较小,提取信息的质量较高.但当需要隐藏的信息为灰度图像时,编码后信息的振幅较大,隐藏时对宿主图像影响较大,解码信息质量迅速下降.此外,由于该方法的解码的光学效率低,因而限制了其实用性.

本文将一幅加权的灰度图像的相息图隐藏于一幅宿主图像中,即将一幅原始待加密灰度图像通过基于相息图迭代[10—12]的双随机相位加密技术,加密为仅含有位相信息的相息图,并将其隐藏于一幅宿主图像中.由于用于隐藏的相息图仅含有位相信息,因而与隐藏信息同时具有振幅和相位的情况相比较,需要隐藏的信息量大大降低,从而可在对宿主图像影响较小的情况下,提高提取信息的质量;并可有效地提高信息提取时的光学效率.此外,被隐藏的仅位相信息类似于白噪声,因此任何试图移开隐藏图像的企图都会导致对宿主图像的损害[9],且解码过程不依赖于原宿主图像.该方法也具有很高的安全性,因为采用双随机相位加密技术得到的相息图,在加密的过程中引进了随机相位因子,在不知密钥的情况下解密是几乎不可能的[12].同时,二元图像也可以被加密为相息图,所以本文提出的方法对二元图像同样适用.本文还讨论了隐藏信息的提取质量与宿主图像的信噪比之间的关系;水印图像被剪切后对隐藏信息提取质量的影响也被讨论.模拟实验

* 国家自然科学基金(批准号:60577017,60777007),天津市自然科学基金(批准号:05YFJMJC01700),光电信息技术科学教育部重点实验室开放课题(批准号:2005-14)资助的课题.

† 通讯联系人. E-mail:zhai@nankai.edu.cn

结果证明了本文所提出方法的有效性.

2. 基于相息图的信息隐藏

2.1. 用于隐藏的相息图

本文用于隐藏的相息图由一幅原始待加密灰度图像采用基于相息图迭代[12]的双随机相位加密技术获得.所谓相息图,即它的复振幅分布是一个仅相位分布,若用 $g(x,y)$ 表示,则 $|g(x,y)|=c$,c 为任意常数.设 $f(x,y)$ 表示待加密图像的复振幅分布,则将 $f(x,y)$ 加密为 $g(x,y)$ 的过程可表示为

$$\begin{aligned} g(x,y) &= FT^{-1}\{FT\{f(x,y)\exp[\mathrm{i}2\pi p(x,y)]\} \\ &\quad \times \exp[\mathrm{i}2\pi b(u,v)]\} \\ &= |g(x,y)|\exp[\mathrm{i}\psi(x,y)], \end{aligned} \tag{1}$$

其中,FT 为傅里叶变换,FT^{-1} 为傅里叶逆变换,(x,y) 表示二维空间坐标,(u,v) 为二维频域坐标,$p(x,y)$ 和 $b(u,v)$ 分别代表两个在 $[0,1]$ 之间均匀分布的二维随机阵列.$g(x,y)$ 的相位分布 $\psi(x,y)$ 及附加的相位分布 $b(u,v)$ 可通过迭代算法求出[12].$b(u,v)$ 一经确定,即可用 $H(u,v)=\exp[\mathrm{i}2\pi b(u,v)]$ 作为从相息图 $g(x,y)$ 本身来恢复 $f(x,y)$ 的密钥.由于 $p(x,y)$ 是随机噪声,因而 $b(u,v)$ 也是随机的,只不过这一随机相位的分布会与 $p(x,y)$ 和图像 $f(x,y)$ 紧密相关.所以,用 $H(u,v)$ 作为密钥,有很高的安全性.

2.2. 宿主图像的滤波

设 $C_0(x,y)$ 为原始宿主图像,$C_1(x,y)$ 为包含有隐藏图像的水印图像.我们将加权的相息图隐藏于宿主图像中,则有

$$C_1(x,y) = C_0(x,y) + \alpha g(x,y), \tag{2}$$

其中,α 即为隐藏信息的权值,它是一个小于 1 的常数.α 的合理选择可以在保证隐藏图像的不可见性的前提下,增强它的抗失真能力.

为了恢复隐藏图像,我们需要将 $C_1(x,y)$ 进行傅里叶变换,乘以 $\exp[-\mathrm{i}2\pi b(u,v)]$,然后进行逆傅里叶变换,再乘以 $\exp[-\mathrm{i}2\pi p(x,y)]$,则解密后的隐藏图像可表示为

$$\begin{aligned} \bar{f}(x,y) &= \alpha f(x,y) + FT^{-1}\{FT[C_0(x,y)] \\ &\quad \times \exp[-\mathrm{i}2\pi b(u,v)]\} \\ &\quad \times \exp[-\mathrm{i}2\pi p(x,y)], \end{aligned} \tag{3}$$

上式中右边第二项可表示为

$$\begin{aligned} \Delta f(x,y) &= FT^{-1}\{FT[C_0(x,y)] \\ &\quad \times \exp[-\mathrm{i}2\pi b(u,v)]\} \\ &\quad \times \exp[-\mathrm{i}2\pi p(x,y)]. \end{aligned} \tag{4}$$

$\Delta f(x,y)$ 可认为是一个均值为 0,具有一定方差的高斯噪声[9].对于解密后的隐藏信息来说,它与(3)式中右边的第一项的比值越小,解密图像的质量越高.

事实上,对于灰度隐藏信息来说,即使将其加密为相息图,$g(x,y)$ 的值比用文献[9]的方法得到的已经小了很多,但是仍然足够大(比用文献[9]的方法得到的二元图像加密后的值大很多).为保证隐藏信息的不可见性,(2)式中的 α 值必须足够小,这就使得 $\Delta f(x,y)$ 与(3)式中右边的第一项的比值较大,因此,由公式(3)得到的解密隐藏信息信噪比小,质量差.为解决这一问题,考虑到隐藏信息类似于白噪声,我们在加入隐藏信息前,先对宿主图像进行了低通滤波,即滤掉宿主图像的高频部分,再将隐藏信息加入,相当于将原宿主图像中的高频部分用隐藏信息的频谱来代替,提取时采用这一高频部分来解密,可大大提高解密图像的质量.

设 $C_F(u,v)$ 为宿主图像 $C_0(x,y)$ 的频谱函数,则滤波函数可以表示为[13]

$$\begin{aligned} C_1(u,v) &= C_F(u,v)\left\{0.08 + 0.46\left[1 - \cos\left(\frac{\pi\sqrt{(u-u_c)^2+(v-v_c)^2}}{R} - \pi\right)\right]\right\} \\ &\qquad \sqrt{(u-u_c)^2+(v-v_c)^2} \leqslant R, \\ C_1(u,v) &= 0 \qquad \sqrt{(u-u_c)^2+(v-v_c)^2} > R, \end{aligned} \tag{5}$$

其中,(u_c,v_c) 是滤波器的中心点,对应于 $C_F(u,v)$ 的中心;R 是滤波半径,可表示为

$$R = (\mathrm{ROW}/4)\times\sqrt{2}, \tag{6}$$

其中 ROW 是宿主图像的列数.

采用该函数的优点是,它对集中了宿主图像大部分信息的低频部分影响很小,对宿主图像的损坏

也就较小.

2.3. 基于相息图的信息隐藏

现在，我们就将加权的相息图隐藏到已滤过波的宿主图像 $C_I(x,y)$ 中，则有

$$C_{FI}(x,y) = C_I(x,y) + \alpha g(x,y), \quad (7)$$

解密后的隐藏图像就可表示为

$$\overline{f_F}(x,y) = \alpha f(x,y) + FT^{-1}\{FT[C_{FI}(x,y)] \times \exp[-i2\pi b(u,v)]\} \times \exp[-i2\pi p(x,y)]. \quad (8)$$

加入隐藏信息后的宿主图像与原宿主图像之间的关系，以及解密后得到的隐藏图像的质量，可分别用归一化的相关系数 r_c 和 r_f 来评价. 若 $g_1(x,y)$ 与 $g_2(x,y)$ 分别代表两个函数，则它们之间的相关系数 r 可定义为

$$r = \frac{\sum\sum g_1(x,y)\, g_2(x,y)}{\sqrt{\sum\sum g_1^2(x,y) \sum\sum g_2^2(x,y)}}, \quad (9)$$

显然，r 的值越大，两个图像的相关性越大，这两个图像就越接近.

3. 模拟实验结果及分析

我们对以上算法进行了计算机模拟实验. 图 1(a)为一幅 128×128 像素的原始待加密灰度图像，图 1(b)为采用基于相息图迭代的双随机相位加密技术得到的该图像的相息图，图 1(c)为 128×128 像素的宿主图像.

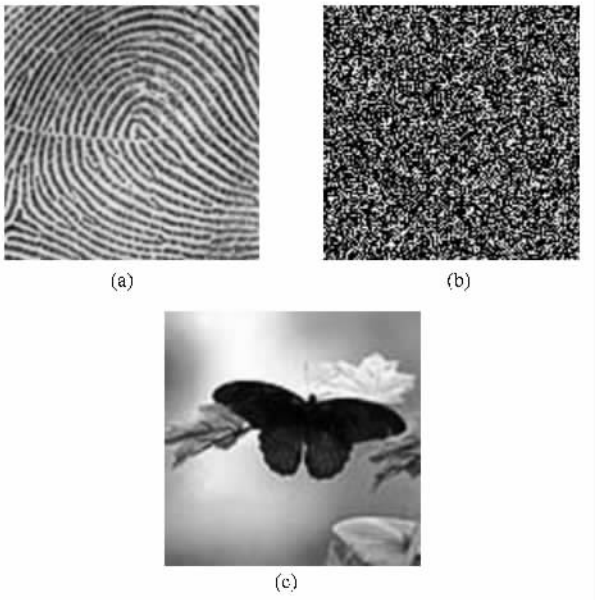

图 1　模拟实验用图像　(a)待加密图像；(b)图(a)的相息图；(c)宿主图像

3.1. 参数 α 的选取

我们分别计算了不同 α 值的情况下，加入隐藏图像的水印图像和原宿主图像之间的相关度 r_c，以及解密后的隐藏图像与原隐藏图像之间的相关系数 r_f，计算结果如表 1 所示.

表 1　α 与宿主图像的相关度及隐藏图像的相关度之间的关系

α	0.02	0.03	0.04	0.05	0.06
r_c	0.9975	0.9968	0.9958	0.9945	0.9930
r_f	0.7743	0.8308	0.8664	0.8883	0.9023

由表 1 可见，当 α 值较小时，加入隐藏信息前后的宿主图像的相关度高一些；而 α 值较大时，宿主图像的相关度较低. 而隐藏信息提取质量情况正好相反，α 值较小时，隐藏图像的相关程度较低，即所提取的隐藏信息质量较差，α 值较大时，隐藏图像的相关程度较高，即所提取的隐藏信息质量较好.

选取 $\alpha = 0.04$ 以提高隐藏图像的解密质量，同时兼顾宿主图像的视觉效果. 此时，水印图像与原宿主图像的相关度为 0.9958，解密后的隐藏图像与原图像之间的相关度为 0.8664，其隐藏和解密效果如图 2 所示. 图 2(a)为包含有隐藏信息的水印图像，图 2(b)是解密后得到的隐藏图像.

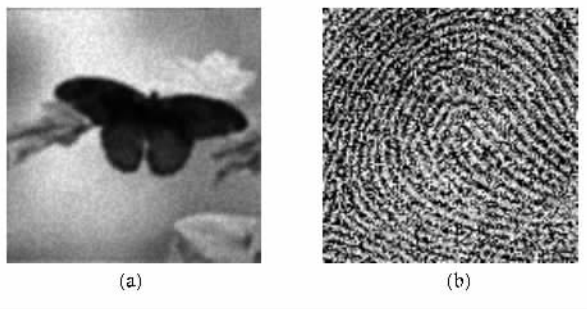

图 2　解密结果　(a)含有隐藏信息的水印图像；(b)解密后得到的隐藏图像

我们还采用文献[9]的方法进行了模拟实验，以便与本文提出的方法进行比较. 表 2 是不同 α 值的情况下，加入隐藏图像的水印图像和原宿主图像之间的相关度 r_{cj}，以及解密后的隐藏图像与原隐藏图像之间的相关系数 r_{fj}. 由表 2 可见，当 α 取 0.05 时，r_{cj} 与表 1 中 α 取 0.04 时的 r_c 近似相等，但此时解密图像的质量很差，如图 3 所示. 其中图 3(a)为包含有隐藏信息的水印图像，图 3(b)是解密后得到的

隐藏图像.而继续增加值 α,并不能提高解密图像的质量(α 为 0.06 时,r_{fj}的值反而下降).

表 2 采用文献[9]的方法得到的 α 与宿主图像的相关度及隐藏图像的相关度之间的关系

α	0.02	0.03	0.04	0.05	0.06
r_{cj}	0.9989	0.9977	0.9976	0.9960	0.9956
r_{fj}	0.7456	0.7777	0.7804	0.7883	0.7828

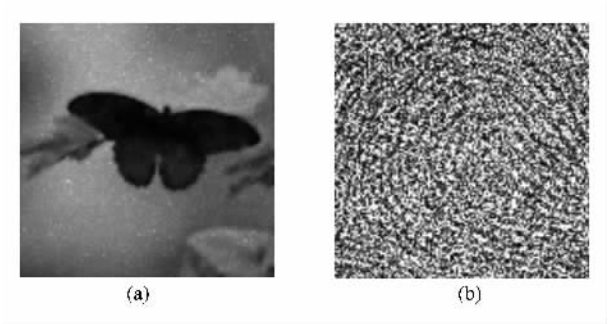

图 3 采用文献[9]的方法得到的解密结果 (a)含有隐藏信息的水印图像;(b)解密后得到的隐藏图像

3.2. 水印图像的剪切对隐藏信息提取的影响

我们对不同剪切程度的水印图像分别进行了隐藏信息的提取,如图 4 所示,实验中,仍然选取 α = 0.04.图 4(a),4(c),4(e)是将水印图像 6.25%,12.5%,25% 的像素剪切后得到的图像,图 4(b),4(d),4(f)分别是与之对应的解密图像,各解密后的隐藏图像与原图像之间的相关度分别为 0.7926,0.7587,0.7349.由图 4 可见,当水印图像 25% 的像素被剪切后,恢复的图像中噪声较大,质量较差,此时解密后的隐藏图像与原图像之间的相关度也较低.

3.3. 二元图像的隐藏

由于二元图像也可以被加密为相息图,本文所提出的方法对二元图像同样适用,如图 5 所示.其中,图 5(a)为待隐藏的二元图像,图 5(b)为加入隐藏信息以后的宿主图像,图 5(c)为解密结果.此时,水印图像和原宿主图像之间的相关度为 0.9911,解密后的隐藏图像与原图像之间的相关系数为 0.9908.

4. 结 论

本文采用基于相息图迭代的双随机相位加密技

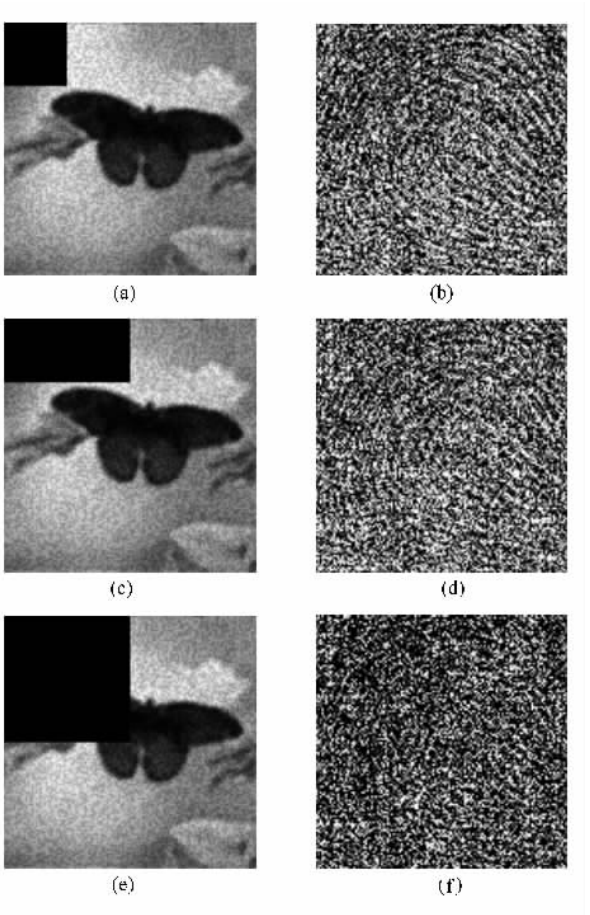

图 4 剪切水印图像的隐藏信息提取 (a)6.25%的像素剪切后得到的水印图像;(b)用(a)的水印图像解密得到的解密图像;(c)12.5%的像素剪切后得到的水印图像;(d)用(c)的水印图像解密得到的解密图像;(e)25%的像素剪切后得到的水印图像;(f)用(e)的水印图像解密得到的解密图像

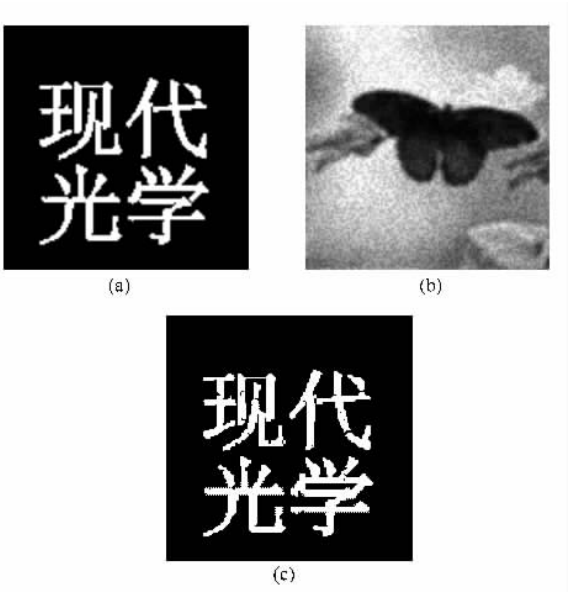

图 5 隐藏信息为二元图像时的解密结果 (a)待隐藏的二元图像;(b)加入隐藏信息以后的宿主图像;(c)解密结果

术，将一幅灰度图像加密为一幅相息图，并将其加权后隐藏于一幅宿主图像中.采用双随机相位加密技术得到的相息图，在加密的过程中引进了随机相位因子，使密钥也具有随机性.而该随机相位因子来自于一个随机噪声，再产生一个与它相同的随机噪声是几乎不可能的[14]，所以在不知密钥的情况下解密相息图是很困难的，因而该方法具有很高的安全性，并可有效地提高信息提取时的光学效率.此外，被隐藏的仅位相信息类似于白噪声，因此任何试图移开隐藏图像的企图都会导致对宿主图像的损害，且解码过程不依赖于原宿主图像.模拟实验结果表明，由于采用相息图作为待加密灰度图像信息的载体，而相息图仅含有位相信息，与隐藏信息同时具有振幅和相位的情况相比较，需要隐藏的信息量大大降低，在对宿主图像影响较小的情况下，隐藏灰度图像信息的提取质量得到了提高.同时，二元图像也可以被加密为相息图，所以本文提出的方法对二元图像同样适用.在文章最后部分，对加入的隐藏信息的权值与宿主图像的关系以及它对隐藏信息提取质量的影响进行了讨论，还分析了水印图像的不同剪切度对隐藏信息提取质量的影响，分析结果表明，该方法有一定的抗剪切性.

[1] Rosen J, Javidi B 2001 *Appl. Opt.* **40** 3346

[2] Yamamoto H, Hayasaki Y, Nishida N 2003 *Opt. Lett.* **28** 1564

[3] Dittmann J, Ferri L C, Hologram C 2001 *Vielhauer IEEE: Information Technology Coding and Computing* 2001 *Proceedings International Conference* [C]

[4] Apolinar J M R, Ramon R V 2004 *Opt. Commun.* **236** 295

[5] Peng X, Yu L, Cai L 2003 *Opt. Commun.* **226** 155

[6] Takai N, Mifune Y 2002 *Appl. Opt.* **41** 865

[7] Kishk S, Javidi B 2003 *Opt. Lett.* **28** 167

[8] Kishk S, Javidi B 2003 *Opt. Exp.* **11** 874

[9] Kishk S, Javidi B 2002 *Appl. Opt.* **41** 5462

[10] Yang X P, Zhai H C 2005 *Acta Phys. Sin.* **54** 1578 (in Chinese) [杨晓苹、翟宏琛 2005 物理学报 **54** 1578]

[11] Yang X P, Zhai H C, Liu F M 2003 *Journal of Optoelectronics Laser* **14** 1187 (in Chinese) [杨晓苹、翟宏琛、刘福民 2003 光电子激光 **14** 1187]

[12] Liu F M, Zhai H C, Yang X P 2003 *Acta Phys. Sin.* **52** 2462 (in Chinese) [刘福民、翟宏琛、杨晓苹 2003 物理学报 **52** 2462]

[13] Gonzalez R C, Woods R E 2002 *Digital Image Processing* 2nd ed (Englewood Cliffs, NJ: Prentice-Hall)

[14] Refregier P, Javidi B 1995 *Opt. Lett.* **20** 767

Gray-image information hiding based on kinoform *

Yang Xiao-Ping[1)2)] Zhai Hong-Chen[1)†] Wang Ming-Wei[1)]

1) (*Institute of Modern Optics, Nankai University, Key Laboratory of Opto-electronic Information Science & Technology, Ministry of Education of China, Tianjin* 300071, *China*)

2) (*School of Electronics Information and Communications Engineering, Tianjin University of Technology, Tianjin* 300191, *China*)

(Received 8 May 2007; revised manuscript received 19 June 2007)

Abstract

In this paper, a new method of hiding gray-images in a host image by using double-random phase encryption method based on kinoform iterative is presented, through which not only the volume to be hidden can be compressed, but also the optical efficiency in the information extracting can be improved. The decoding process of which will not rely on the original host image, and this method can also be applied to the hiding of binary-images. In the last part of this paper, the efficiency and the robustness of this method is analyzed. Computer simulations are presented to illustrate the effectiveness of this method.

Keywords: gray-image, kinoform, information hiding

PACC: 4225F, 4230K

* Project supported by the National Natural Science Foundation of China (Grant Nos. 60577017, 60777007), the Natural Science Foundation of Tianjin, China (Grant No. 05YFJMJC01700) and the Opening Subject of Key Laboratory of Opto-electronic Information Science & Technology, Ministry of Education of China (Grant No. 2005-14).

† Corresponding author. E-mail: zhai@nankai.edu.cn