文章编号:1004-4213(2010)08-1345-6

像素随机映射的快速算法及在 LSB 隐藏技术中的应用*

李俊昌,管一弘,蔡光程,樊则宾
(昆明理工大学 理学院,昆明 650093)

摘 要:提出一种像素随机映射的快速方法,将该方法与像素字节低位隐藏信息的最低有效位技术相结合,讨论了将 RGB 彩色图像作为载体隐匿真彩色图像、灰度图像、二值图像及全息信息的方法.研究结果表明,该方法加密及解密效率高,载体图像具有较好的抗破译及抗剪切能力.根据隐藏信息的性质合理使用 LSB 技术,能在基本不影响载体图像质量的情况下较好地隐匿多种信息.

关键词:数字图像处理,图像加密,全息存储,互联网信息传输
中图分类号:TN911.7 **文献标识码**:A **doi**:10.3788/gzxb20103908.1345

0 引言

随着计算机及互联网传输技术的进步,用互联网传播文字、声音及图像的技术正飞速发展,通过网络获取信息已经成为当今信息传播的一种重要手段.在互联网为通讯提供了极大的方便的同时,信息传播的保密问题逐渐成为人们关注并积极研究的课题,在该研究领域,根据光学原理,利用计算机进行图像加密及解密的技术获得广泛研究.1995 年,基于 4f 系统的光学变换原理,在系统的输入平面及焦平面插入随机相位板后,Réfrégier 和 Javidi 提出双随机相位图像加密技术[1].该技术一度被认为是不容易被破译的信息隐藏技术.成为多年来人们的一个研究热点[2-8].然而,最近的研究表明[9-10],双随机相位加密系统存在安全隐患.研究新的加密方法,或者对双随机相位加密系统进行改进,成为新的研究课题.

在图像加密研究领域,最低有效位(Least Significant Bit,LSB)技术[11]是将隐藏信息融入载体图像像素的低位字节的技术.由于处理方法简单,能准确复原隐匿信息而成为一种很流行的技术.然而,如何提高隐匿信息的抗破译能力始终是人们需要解决的问题[11].本文提出一种像素随机映射的快速算法,用长度为 M 和 N 的两个不重复整形随机序列为密钥,能将 $M\times N$ 个元素的数据阵列一次映射为元素位置随机变换的 $M\times N$ 阵列,经过随机映射变换的信息融入载体图像像素的低位字节中,能较好地保证隐藏信息的安全性.

以 BMP 图像为隐藏信息的载体,本文讨论隐藏真彩色图像、灰度图像、二值图像及全息信息的方法,研究隐藏信息的载体图像的抗剪切能力.

1 像素位置的随机映射方法讨论

像素位置的随机映射也称为像素置乱,在同类研究中,存在初等矩阵变换[4]及行列置换变换[11]等方法,这些方法通常需要通过多次迭代才能达到充分置乱,多次迭代不但增加了加密运算量,同时也降低了解密速度.以下介绍置乱及复原速度优于以上两种方法的随机映射法.

对于 $N\times M$ 像素构成的图像,通过计算机生成整形随机序列 $P_x(i)$,$P_y(j)$,当 $i=0,1,2\cdots N-1$ 以及 $j=0,1,2\cdots M-1$ 时,$P_x(i)$,$P_y(j)$分别是 $0,1,2\cdots N-1$ 及 $0,1,2\cdots M-1$ 中取值不重复的随机排列序列.随机映射图像 $\Psi(i,j)$与原图像 $\psi(i,j)$的关系可以简单地表为

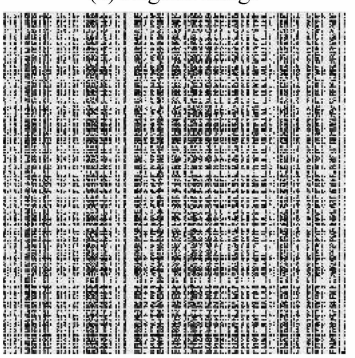
$$\Psi(i,j)=\psi(P_x(i),P_y(j)) \tag{1}$$

像素置乱效果可用置乱后图像功率谱是否为白噪声功率谱来衡量[5].图 1 给出一个随机映射实例.图中用 0~255 灰度等级分别表示出 $N=M=256$ 的原图像、随机映射图像及该映射图像的功率谱.其中,映射图像功率谱是映射图像减去平均灰度后进行离散傅里叶变换作出的.分析映射图像的功率谱可以看出,频谱在横轴及纵轴取均匀分布,说明映射图像已经较好地成为一个随机分布的图像.由于随机映射的可能情况为 $A_M^M\times A_N^N$ 种,不知道密钥 $P_x(i)$,$P_y(j)$很难对随机映射破解.

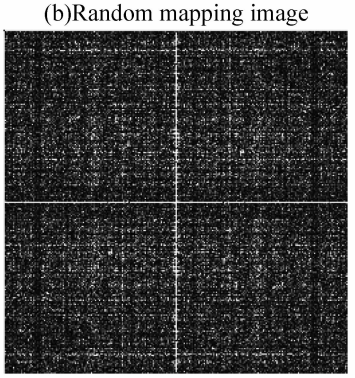
本文像素置乱方法编码及解码步骤简单,达到同一置乱效果时计算量低于需要迭代运算的文献[4]的初等矩阵变换法及文献[11]的行列置换变换法.

*云南省自然科学基金(2007F0028M)资助
Tel:0871-5162644 Email:jcli@vip.163.com
收稿日期:2008-11-12 修回日期:2009-02-06

(a)Original image



(b)Random mapping image



(c)Power spectrum of mapping image

图 1 原图像、随机映射图像及映射图像功率谱

Fig. 1 Original image, random mapping image and power spectrum of mapping image

2 加密研究实例

用三字节存储三个彩色分量的 BMP 真彩色图像是目前图像存储及传输的一种流行形式. 根据二进制知识，一个字节的 8 位二进制数能够表示 0～255 的量值，字节的每一位均为 1 时，每位表示的十进制数分别是 128、64、32、16、8、4、2、1. 对于一个饱和度较好的彩色图像，通常是字节的前 4 位或前 5 位体现图像的色彩信息. 换言之，更换字节低 4 位以下的内容，基本不影响人眼对图像的感觉.

根据对载体图像及隐藏信息质量的选择，可以有多种方式利用 BMP 真彩色图像像素字节低位的存储空间存储不同质量的图像. 设采用像素的低 k 位字节作为隐藏空间，一幅 $M\times N$ 字节的 BMP 图像能提供的比特数为 $3\times M\times N\times k$. 如果用 p 比特存储一个数据，则可以存储数据的个数为

$$S=3MNk/p \tag{2}$$

合理分配这个存储空间，不但能存储不同性质的图像或数据，而且存储方法还能构成新的密钥，增加隐藏信息的安全性. 以下分别给出隐藏真彩色图像、灰度图像、二值图像及全息信息的方法.

2.1 隐藏 BMP 真彩色图像实例

既然一幅 BMP 可以主要由三字节的前 4 位来描述，自然地，可以利用载体图的低 4 位隐藏另一幅彩色图的高 4 位信息. 图 2 给出 $M=N=256$ 的

(a)Original carrier image

(b)Eneryption image

(c)Hiding image of decryption

图 2 隐藏 BMP 真彩色图像

Fig. 2 Hiding BMP real colour image

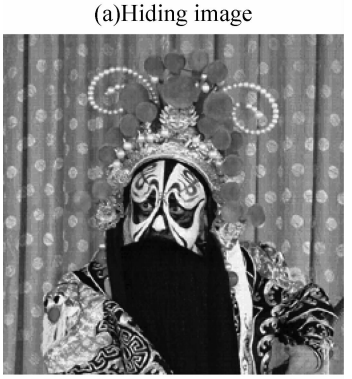
一隐藏实例. 其中，图 2(a)是原载体图；图 2(b)是采用了随机映射后隐藏了图 2(c)的加密图；图 2(c)是从图 2(b)解密出的隐藏图像. 不难看出，人眼很难觉察图 2(a)与图 2(b)的区别，图 2(c)仍然是一幅色彩艳丽的真彩色图像.

由于信息传播时不需要原载体图，只需要提供图 2(b)及密钥 $P_x(i)$，$P_y(j)$便能重建图 2(c). 该方法为信息的隐匿传播提供了方便.

2.2　隐藏灰度图像

仍然使用图 2(a)为载体图，现给出每像素 8 比特隐藏灰度图像的实例. 将隐藏图像像素经随机映射后，高 3 位及低 3 位分别放置在载体图红色分量及蓝色分量的低三位中，用绿色分量低 2 位隐藏字节的第 4 及第 5 两位，图 3 分别给出灰度层次 0～255 的隐藏图像、隐藏了信息的载体图像及通过解密重建的隐藏图像. 由于能够完全准确地重建隐藏信息，图 3(a)及图 3(c)事实上没有任何区别.

(a)Hiding image



(b)Carrier image of encryption

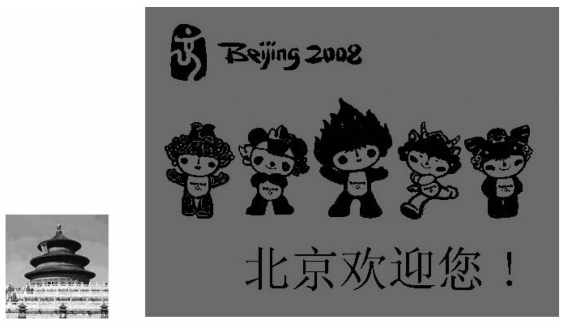
(c)Decryption image

图 3　隐藏灰度图像

Fig. 3　Hiding gray image

2.3　隐藏大尺度二值图像

隐藏二值图像可以视为隐藏灰度变化在 0～1 的图像的一个特例. 但是，由于每一像素只需要 1 个比特位存储，根据式(2)，能够使用较小的 bmp 图像存储尺寸较大的二值图像. 图 4 给出用 128×128 像素的真彩色图像素的低 4 位存储 512×384 像素的二值图像的实例. 在该实例中，将 512×384 像素的二值图像分解为 12 个 128×128 像素的子图像，载体图像的三个色彩分量的低 4 位依次存储这 12 幅子图.



(a)Carrier image (128×128pixels)　　(b)Decryption image(512×384pixels)

图 4　小尺寸真彩色图隐藏大尺寸的二值图像.

Fig. 4　A small scale real color image is hidden in big scale binary image

2.4　隐藏全息信息

利用带有随机映射加密的 LSB 技术，可以实现光全息存储. 设需要存储的光波场的实部和虚部是两个 $N\times N$ 点的数据阵列，该光波场是来自物体的光波经距离 d 衍射的结果. 用像素字节的低位来隐藏光波场数据时可以有多种方案[8]. 现介绍用 $N\times N$ 点真彩色图像素字节低 4 位隐藏信息的一种方案.

由于三个色彩分量能提供 12 个比特位的存储空间，可以分别用 6 个比特位存储光波场的实部及虚部. 鉴于衍射场实部和虚部是有符号的浮点数，二进制 6 个比特数据的变化范围为 0～63，必须对光波场数据作下述处理.

令经过随机映射的隐藏信息的实部和虚部分别为 $\mathrm{dif}R(i,j)$，$\mathrm{dif}I(i,j)(i,j=0,1,2,\cdots,N\text{-}1)$，首先求出衍射场振幅极大值 $A_{\max}$

$$A_{\max}=\max\left\{\sqrt{[\mathrm{dif}R(i,j)]^2+[\mathrm{dif}I(i,j)]^2}\right\} \quad (3)$$

再按式(4)和(5)将实部和虚部的浮点数变换为 0～63 范围变化的数据

$$\mathrm{Dif}R(i,j)=\mathrm{INT}\left[\frac{\mathrm{dif}R(i,j)}{A_{\max}}\times 31.5+31.5\right] \quad (4)$$

$$\mathrm{Dif}I(i,j)=\mathrm{INT}\left[\frac{\mathrm{dif}I(i,j)}{A_{\max}}\times 31.5+31.5\right] \quad (5)$$

式中，INT[]为对[]中的数值作最接近整数的取整运算.

此后，按 2 进制转换并分解出 $\mathrm{Dif}R(i,j)$，$\mathrm{Dif}I(i,j)$的高 2 位及低 4 位，将 $\mathrm{Dif}R(i,j)$的低 4 位存入红色分量字节的低 4 位中，高 2 位存入绿色分量字节低 4 位的前两位；将 $\mathrm{Dif}I(i,j)$的低 4 位存入蓝色分量字节的低 4 位中，高 2 位存入绿色分量字节低 4 位的后两位.

载体图像中获取 $\mathrm{Dif}R(i,j)$，$\mathrm{Dif}I(i,j)$的过程是上过程的逆过程. 当取出 $\mathrm{Dif}R(i,j)$，$\mathrm{Dif}I(i,j)$的

高 2 位及低 4 位后，按照二进制恢复出对应的十进制整数，再用下式恢复衍射数据的符号及量值

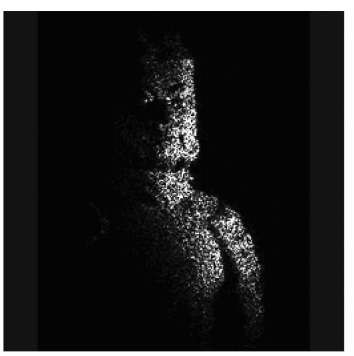
$$\mathrm{Dif}R(i,j)=\frac{\mathrm{Dif}R(i,j)-31.5}{31.5}\times A_{\max} \tag{6}$$

$$\mathrm{Dif}I(i,j)=\frac{\mathrm{Dif}I(i,j)-31.5}{31.5}\times A_{\max} \tag{7}$$

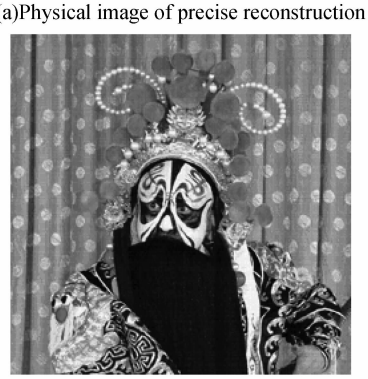
经随机映射的逆运算获得光波场的实部和虚部后，利用距离 d 的衍射逆运算[13]便能重建物平面信息.

分析加密及解密过程可以看出，解密误差主要起因于式(4)和(5)的取整运算. 由于采用 6 位 2 进制的存储空间，取整运算引入的相对误差小于1/63.

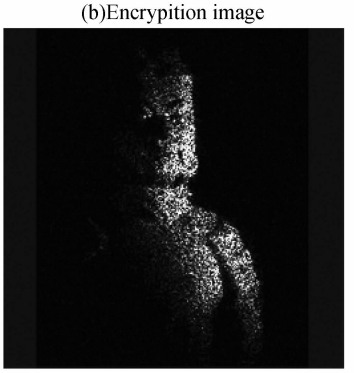
用一个身高 150 mm 的仿制陶兵马俑为物体，选择 d=1 320 mm，经数字全息实验获得衍射场数据后，图 5 给出相应的加密及解密图像. 其中图 5(a)是使用准确衍射场数据重建的物体像；图5(b)是隐匿有物体全息信息的载体图；图 5(c)是用图 5(b)解密获取的衍射场数据重建的物体像. 可以看出，由于只存在 1/63 的取整误差，图 5(a)及图 5(c)的差别很难辨别.



(a)Physical image of precise reconstruction



(b)Encrypition image



(c)Reconstruction physical of image decryption

图 5 BMP 图像隐藏全息信息实例

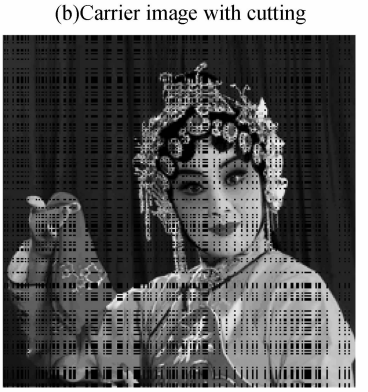
Fig. 5 A example of BMP image with hiding holographic information

3 载体图像的抗剪切研究

由于随机映射图像的每一位置具有获取来自原图像不同位置信息的相同概率，引入随机映射的 LSB 加密载体图像与双随机相位加密的载体图像一样，能保持较好的抗剪切能力. 模拟的"剪切"可以理解为在数字传输过程中的成块数据丢失，这在网络传输信息时是时有发生的问题. 用图 2 隐藏真彩色图像为例，图 6 给出有缺损的载体图像及相应的解密结果.

(a)Original hiding image

(b)Carrier image with cutting



(c)Decryption image

图 6 抗剪切能力考查

Fig. 6 Test of resistance to cutting

4　结论

本文提出一种像素随机映射的快速方法，并将该方法与像素字节低位隐藏信息的技术 LSB 相结合，讨论了将 RGB 彩色图像作为载体隐匿不同性质的图像及全息信息的方法. 研究结果表明，该方法加密及解密效率高，载体图像具有较好的抗剪切能力. 根据隐藏信息的性质合理使用 LSB 技术，能在基本不影响载体图像质量的情况下较好地隐匿多种信息.

应该指出，本文提出的方法可以方便地移植于图像水印技术中. 例如，用像素随机映射的快速方法代替文献[13]的混沌置乱法，在保持同等解密难度的情况下，能够有效提高图像水印系统的加密及解密效率.

对于互联网传输隐匿信息及图像水印技术的研究，本文所做的工作是一个有益的参考.

参考文献

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

[2] NOMURA T. Optical encryption using a joint transform correlator architecture[J]. *Opt Eng*, 2000, **39**(8): 2031-2035.

[3] SITU Guo-hai, ZHANG Jing-Juan. Double random phase encoding in the Fresnel domain[J]. *Opt Lett*, 2004, **29**(14): 1584-1586.

[4] LU Hong-qiang, ZHAO Jian-lin, FAN Qi, *et al*. Iterative double random phase encryption based on pixel scrambling technogy[J]. *Acta Photonica Sinica*, 2005, **34**(7): 1069-1072.
陆红强，赵建林，范琦，等，基于像素置乱技术的双随机相位加密法[J]，光子学报，2005，**34**(7)：1069-1072.

[5] DEN Xiao-pen. Research and progress of optical image encryption using random phase mask [J]. *Laser & Optoelectronics Progress*, 2005, **42**(9): 11.
邓晓鹏. 随机相位编码光学图像加密研究进展[J]. 激光与光电子学进展，2005，**42**(9)：11.

[6] SUN Liu-Jie, ZHUANG Son-lin, Anti-Fake technique by double random phase encrypted holographic mark[J]. *Acta Optica Sinica*, 2007, **27**(1): 31-34.
孙树杰，庄松林. 双随机相位加密全息标识防伪技术研究[J]. 光学学报，2007，**27**(1)：31-34.

[7] WANG Hon-xia, ZHAO Wei, LIU Chang-wen, *et al*. Six security key for image encryption based on anamorphic fractional fourier transform[J]. *Acta Photonica Sinica*, 2007, **36**(4): 759-762.
王红霞，赵玮，刘长文，等. 基于变形分数傅里叶变换的六重密钥图像加密[J]. 光子学报，2007，**36**(4)：759-762.

[8] SUN Min, SU Xian-yu. Technology of double random encode data hidden in RGB image[J]. *Acta Photonica Sinica*, 2008, **37**(2): 320-324.
孙敏，苏显渝. 基于 RGB 图像传输的双随机相位加密隐藏技术[J]. 光子学报，2008，**37**(2)：320-324.

[9] PENG Xiang, ZHANG Peng, WEI Heng-zheng, *et al*. Known-plaintext attack on optical encryption based on double random phase keys[J]. *Opt Lett*, 2006, **31**(8): 1044-1046.

[10] WEI Heng-zheng, PENG Xiang, ZHANG Peng, *et al*. Chosen-Plaintext attack on double phase encoding encryption technique[J]. *Acta Optica Sinica*, 2007, **27**(5): 824-829.
位恒政，彭翔，张鹏，等，双随机相位加密系统的选择明文攻击[J]. 光学学报，2007，**27**(5)：824-829.

[11] ZOU Juan, JIA Shi-jie, Design and implementation of image hiding system based on LSB[J]. *Computer Technology and Development*, 2007, **17**(5): 114-116.
邹娟，贾世杰，基于 LSB 图像隐藏系统的设计与实现[J]. 计算机技术与发展，2007，**17**(5)：114-116.

[12] LI Jun-chang, PENG Zu-jie, FU Yun-chang. Diffraction transfer function and its calculation of classic diffraction formula[J]. *Opt Commun*, 2007, **280**(2): 243-248.

[13] HU Yu-feng, ZHU Shan-an. Research of chaos scrambling in Image watermarking system[J]. *Chinese Journal Of Electron Devices*, 2008, **31**(5): 1457-1459.
胡裕峰，朱善安，混沌置乱在图像水印系统中的研究[J]. 电子器件，2008，**31**(5)：1457-1459.

A Fast Method for Pixel Random Mapping and Application on the Hiding Technology of LSB

LI Jun-chang, GUAN Yi-hong, CAI Guang-cheng, FAN Ze-bin
(*Faculty of Science, Kunming University of Science and Technology, Kunming* 650093, *China*)

Abstract: A novel fast method for pixel random mapping is proposed. Combining with the technology of information hiding of Least Significant Bit(LSB), the RGB colour image used as a carrier image to hide real colour image, gray image, binary image and holography information are discussed. The experimental results show that this method has a high efficiency of encryption and decryption, and is robust to resist the attack of interference and image cutting. While the technology of LSB is applied properly according to the property of information hiding, the multiple information can be hidden well in carrier image while the quality of image is almost not influenced.

Key words: Digital image processing; Image encryption; Holographic storage; Information transform on internet

LI Jun-chang was born in 1945. Now he is a Doctoral Supervisor at Kunming University of Science and Technology and at three France engineering Universities (Ecole Centrale de LYON, INSA de LYON, Université du MAINE). His research interests focus on optical information processing and interaction between laser and materials.