基于随机区域移位和随机像素映射的图像加密

黄 飞,冯少彤,王 亮,聂守平

(南京师范大学 江苏省光电技术重点实验,江苏 南京 210097)

[摘要] 提出基于随机区域移位和随机像素映射的图像加密算法. 该算法首先对待加密图像进行分割,然后将分割出来的图像单元顺序随机打乱,扰乱了图像的原始信息;然后再对每个图像单元进行像素映射扰乱,切断了各个单元像素值之间的联系. 该算法结合了区域移位算法和像素映射算法的优点. 计算机模拟表明该算法自由度大、保密性强,对二值图像和灰度图像加密都取得了很好的效果.

[关键词] 图像加密,区域移位,像素映射

[中图分类号] TP391 [文献标识码] A [文章编号] 1672-1292(2006)03-0066-04

Image Encryption Based on Region Shifting Encoding and Pixel Mapping

HUANG Fei, FENG Shaotong, WANG Liang, NIE Shouping

(Jiangsu Province Key Laboratory of Optoelectronic Technology, Nanjing Normal University, Nanjing 210097, China)

Abstract Based on region shifting encoding and pixel mapping, the paper proposes image encryption algorithm. The image to be encrypted is divided into several units, and the positions of these units are changed randomly. Then each unit is disturbed by the pixel mapping, cutting the relations between the values of pixels in every unit. The algorithm is based on the virtues of the region shifting and pixel mapping. The results of computer simulation show that this method is flexible in the freedom and strong in secrecy, especially for the binary images and grayscale images.

Key words image encryption; region shifting encoding; pixel mapping

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,图像加密技术已变得越来越重要,为此,有必要寻求安全的图像加密技术. 图像加密[1-6]就是通过一系列操作后,使原来的图像信息变为类似的随机噪声信息,这些信息在不知道密钥的条件下不易被破解,进而有效地保护了图像数据. 加密操作可以分成空域加密和变换域加密. 空域加密可以通过附加随机噪声等来实现,变换域加密可以通过离散余弦变换、傅立叶变换等来实现. 目前变换域加密技术有双随机位相加密,即在图像的空域和频域上附加两个随机位相掩模板来实现图像的加密.

本文的加密方法是作用于空间领域. 在随机像素映射法和随机区域移位法加密图像的基础上,提出基于随机区域移位和随机像素映射的图像加密算法. 计算机模拟表明该加密算法能有效地对图像进行加密.

1 图像加密算法

1.1 像素映射法

像素映射法是一种简单的加密方法,对于一幅灰度图它首先建立从原灰度值到新灰度值的映射表,然后把图像中所有原灰度替换成在映射表中该灰度对应的新灰度,打乱图像中原来的像素分布,从而达到加密图像的目的;而在解密时只要依照映射表用旧灰度替代加密后图像中的新灰度,就可以还原出原来的图

收稿日期: 2006-04-12

基金项目: 江苏省教育厅自然科学基金资助项目(05KJB140065).

作者简介: 黄飞(1982-),硕士研究生,主要从事光学信号处理和图像信号处理的学习与研究. E-mail: huangfei82@126.com

通讯联系人: 聂守平(1967-),博士,教授,主要从事光学信息处理、数学图像处理等方面的教学与研究. E-mail: nieshouping@njnu.edu.cn

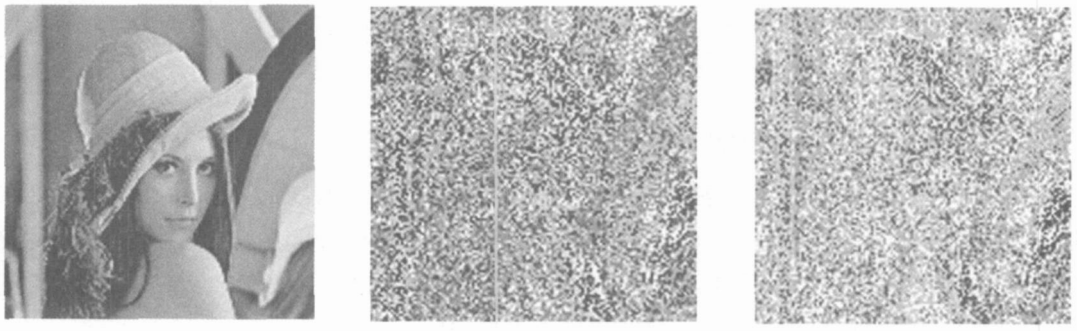
像, 完成解密.

从原灰度值到新灰度值的映射函数可以表示如下, 假设 G_{old} 表示原图中某一灰度, G_{new} 表示新灰度, 构造一个函数 $f(\cdot)$, 使:

$$G_{new} = f(G_{old}) \tag{1}$$

建立了映射函数后, 用新灰度去取代对应的旧灰度, 实现对原图像的加密. 该函数可以任意选取, 选取的函数不同, 加密的效果就会不同, 所以为了达到加密图像的目的, 需选用合适的映射函数. 本文所采用的映射函数是随机产生的, 就是用随机像素映射法来加密图像.

随机像素映射法是将 256个灰度值随机排列产生新的灰度值, 在这里用到 rand(·) 函数, 该函数能产生一个值在 0到 1的随机数; 把函数 $y = \mathrm{fix}(\mathrm{rand}(x) \cdot 255)$ 的值作为新灰度值, 当每一次产生新灰度值的时候, 要和之前产生的所有新灰度值进行比较, 如果当前灰度值已经出现过了, 那么该新灰度值不入选, 重新产生新灰度值, 直到产生的新灰度值包含 256个灰度值为止, 这样就产生了随机排列的 256个灰度值, 与它们对应的位置序号一起构成随机像素映射表.

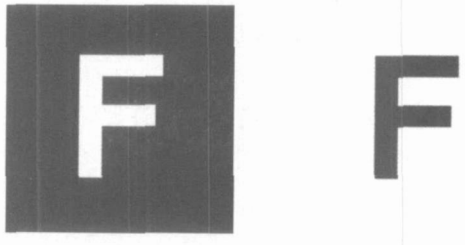


(a)　(b)　(c)

图 1　随机映射法加密灰度图像

图 1(b)是用随机像素映射法来加密图 1(a)的效果, 加密后图像已经失去了表示原事物的能力; 图 1(c)是用错误的映射表来解密的图像, 从结果来看, 用错误的映射表来解密得不到原图像的信息.

然而随机映射法有着很大的缺陷, 如果对一个二值图进行加密, 那么它就无能为力了. 图 2(b)是用随机像素映射法来加密字符二值图图 2(a)的效果, 由于原图像的对比度很强, 灰度等级二级 (即只有二个灰度值)的性质从而导致了加密后图像的对比度仍然很大 (仍然是两个灰度值), 原图的信息依稀可见, 从而违背了图像的加密原则[1].



(a)　(b)

图 2　随机像素映射法加密二值图像

1.2　区域移位法

区域移位法[7]是一种基本的加密算法, 它是先把待加密的图像分割成 $N * N$ 个单元块, 然后对分割后的单元块进行移位, 形成加密图像, 其中涉及到一张移位表用来放单元块移位的信息, 解密时仍将图像分割成 $N * N$ 个单元块, 根据移位表还原回去, 得到原图像.

图 3是区域移位法的示意图, 假设将原图像分割成 4个单元块如 (a), 按照移位表 (e)将单元块进行移位 (见 (b))得到加密的图像; 解密时仍将图像分割成 4个单元块如图 (c), 括号中是原图像单元块序号, 通过移位表将单元块移位, 得到解密的图像 (d), 由括号中的序号可知, 图像已经恢复成原图像.

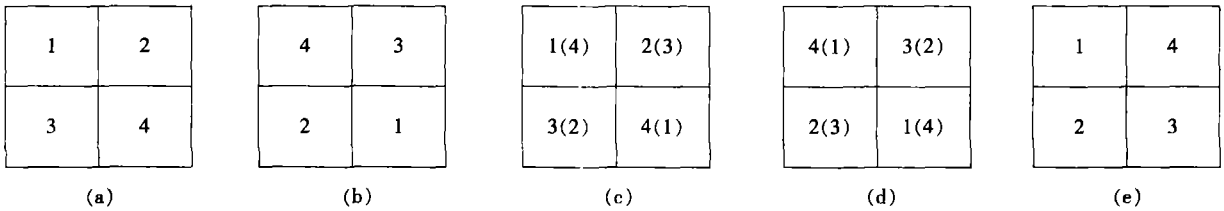


图 3　区域移位法示意图

对于区域移位表的选择可以是任意的, 但一定要起到图像加密的效果, 本文的移位表仍是用 1. 1所论述的产生随机像素映射表的原理得到, 即为随机区域移位法的图像加密.

图 4是用随机区域移位加密图像图 1(a)的效果, 图 4(a)将原图像分割成 4×4个单元块进行区域移位加密; 图 4(b)将原图分解成 8×4个单元块进行图像加密.

(a)　　(b)

图 4　区域移位法加密图像

作为一种基本加密技术的随机区域移位法, 若将原图像分成 4×4单元块, 则有 16! 加密方式, 其中有一部分是起不到加密效果的, 因为加密效果不好, 容易被非授权者破解, 这势必要增加分割单元块数, 通过这个方法虽然能使图像保密性增强, 但同时也会增加计算量, 导致加密速度的降低 (特别对于视频信号); 另外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, 则很有可能破解出原图像, 所以要寻找其它加密方法, 该方法一方面运算量不是很大, 另一方面又要有很好的保密性.

2　基于随机区域移位和随机像素映射的图像加密

基于随机区域移位和随机像素映射的图像加密法结合了像素映射法和区域移位法这两种方法, 该法充分发挥了两种方法的各自加密优点, 在运算量不大的同时提高了图像的保密性. 该方法首先用随机区域移位法对待加密的图像进行加密, 初步置乱图像区域位置, 然后对每一个分割单元块进行随机映射法加密, 使像素信息再一次置乱, 最后得到的图像就是加密后的图像.

下面来讨论该图像加密法的保密性程度, 如果把图像仍分成 4×4个单元块, 则共有 16! 种区域移位方式; 然后用像素映射法对每一个单元块进行加密, 则共有 256! 种映射关系, 由于每一个单元块都对应一个映射表, 且每个单元块的映射表都是独立的, 所以 4×4个单元块就有 (256!)^{16}种加密方式, 那么总共有 (256!)^{16} × 16! 种加密方式, 由此可见该方法比单一的随机区域移位法具有更好的保密性能, 不仅运算量不大而且图像保密性更好, 自由度更大.

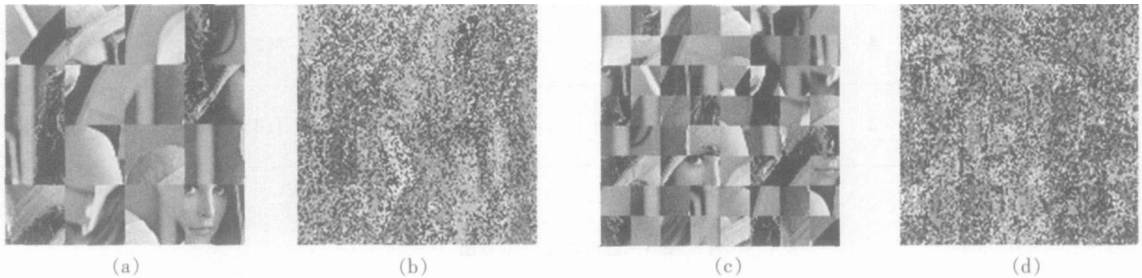
由于移位表和映射表都是一一对应的关系, 授权者只要知道了“钥匙”, 就可以依照“钥匙”还原出原图像. 而非授权者在没有得到“钥匙”的条件下, 试图得到原图信息是非常困难的. 传输“钥匙”时, 可以将移位表和映射表组成一张表传输, 并且可以制定“规则”来隐藏表的信息, 这样就更能提高图像的安全性, 本文没有进行相关研究.

基于随机区域移位和随机像素映射的图像加密法不仅具有很强的保密性, 同时还克服了随机映射法对二值图加密无效的缺陷 (见图 2和图 6), 这也说明该加密方法具有很好的通用性.

3　计算机仿真

本文在 M atlab7. 0软件平台上对以上提到的基于随机区域移位和随机像素映射的图像加密法进行了仿真.

图 5展示用基于随机区域移位和随机像素映射法加密图像 (图 1(a))的效果, 图 5(a)是将原图分成了 4×4个单元块进行区域移位, 图 5(b)是对移位后的图像中每一个单元块进行随机像素映射法置乱像



(a)　　(b)　　(c)　　(d)

图 5　基于随机区域移位和随机像素映射法的灰度图像加密

素, 得到最后的加密图像; 图 5(c)和 图 5(d) 是将原图分成 8×8个单元进行图像加密.

图 6用基于随机区域移位和随机像素映射法对二值图进行加密, 图 6(b)是将图分割成了 4×4个单元块进行区域移位, 在加密图中可以看见原图的主特征; 图 6(c)是对图 6(b)中每个单元块进行随机像素映射来置乱像素, 得到加密图像. 从图中可看到图 6(b)中的主特征已经被湮灭, 在加密后的图像中已找不到任何关于原图的相关信息, 这就说明了该方法克服了随机映射法对二值图加密无效的缺陷, 具有很好的通用性.

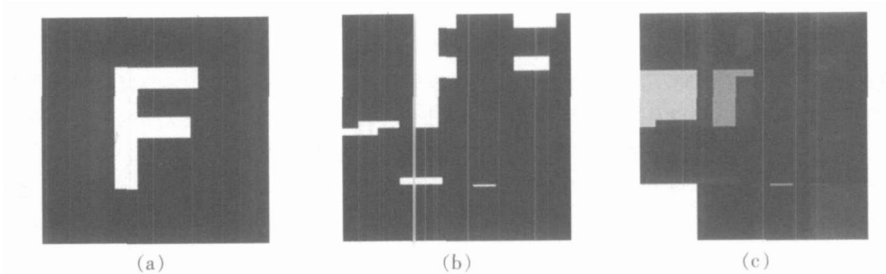


图 6　基于随机区域移位和随机像素映射法二值图像加密

4　结论

本文提出了基于随机区域移位和随机像素映射的图像加密算法. 它首先把图像分割成一定的单元数, 把每个单元随机移位, 初步失去原来的图像信息; 然后在每一单元块中运用随机像素映射法进一步扰乱图像信息, 得到了加密后的图像. 由上面分析可知该算法结合了随机像素映射法和随机区域移位法的优点, 不仅操作步骤简单, 有较好的通用性, 而且还具有很好的图像保密性, 是一种实用的图像加密方法.

[参考文献] (References)

[1] CHUNG K L, CHANG L C. Large encryption binary images with higher security[J]. Pattern Recognition Letters, 1998, 19(5): 461-468.

[2] REFREGIER P, JAVIDI B. Optical image encryption based on input plane and fourier plane random encoding[J]. Optics Letters, 1995, 20(7): 767-769.

[3] NOMURA T, JAVIDI B. Optical encryption system with a binary key code[J]. Applied Optics, 2000, 39(26): 4783-4787.

[4] UNNIKRISHNAN G, SINGH K. Double random fractional fourier-domain encoding for optical security[J]. Optical Engineering, 2000, 39(11): 2853-2859.

[5] ZHANG Y, ZHENG C H, TANNO N. Optical encryption based on iterative fractional fourier transform[J]. Optics Communications, 2002, 202(4): 227-285.

[6] JAVIDI B, NOMURA T. Securing information by use of digital holography[J]. Optical Letters, 2000, 25(1): 28-30.

[7] 陆红强, 赵建林, 范　琦, 等, 基于像素置乱技术的多重双随机相位加密法[J]. 光子学报, 2005, 34(7): 1069-1073.
LU Hongqiang, ZHAO Jianlin, FAN Qi, et al. Iterative double random phase encryption based on pixel scrambling technology [J]. Acta Photonica Sinica, 2005, 34(7): 1069-1073. (in Chinese)

[责任编辑: 刘　健]