基于LSB图像隐藏系统的设计与实现

邹 娟,贾世杰
(大连交通大学 电气信息学院,辽宁 大连 116028)

摘 要:文中运用Matlab实现了基于空域LSB(Least Significant Bit)的灰度图像隐藏与提取系统。图像隐藏系统由置乱模块、加密模块和嵌入模块组成。置乱模块采用基于行列置换的置乱算法,经过多次迭代处理,将原始图像变换为灰度均衡的灰度图像,迭代的次数作为密钥一。加密模块借鉴通信系统中常用的伪随机序列加密的方法,运用软件产生m序列对置乱后的图像进行加密处理。m序列的初始值作为密钥二。经过置乱、加密后的图像进入嵌入模块,采用最低位隐藏方法将数据信息嵌入到载体图像中。图像信息提取系统则由解隐藏、解密和反置乱三部分组成。

关键词:图像隐藏;LSB算法;m序列
中图分类号:TP391.41 **文献标识码**:A **文章编号**:1673-629X(2007)05-0114-03

Design and Implementation of Image Hiding System Based on LSB

ZOU Juan, JIA Shi-jie
(Electronic and Information College of Dalian Jiaotong University, Dalian 116028, China)

Abstract: Utilizes Matlab to realize the system of the intensity image hiding and extraction which based on spatial domain LSB (Least Significant Bit). The image hiding system contains three modules: the chaotic module, the encryption module and the embedded module. The chaotic module uses the chaotic algorithm based on the ranks replacement, and iterates many times. Then the primitive image is inversed to the intensity balanced image, the iteration number is considered as the secret key one. Encryption module commonly uses pseudo-random sequence encryption method of communication system for reference, and the m sequence is produced by Matlab software to encrypt the image in disorder. The initial value of m sequence is the secret key two. The image information extraction system is composed of three parts: the decipher module, the decryption module and the anti-chaotic module.

Key words: image hiding; LSB algorithm; m sequence

0 引 言

近几年来,国际上提出一种新的关于信息安全的概念——信息隐藏技术。所谓信息隐藏是利用多媒体信息普遍存在的冗余特性,将秘密信息隐藏到一般的非秘密数字媒体文件(如图像、声音、文档文件,通常称之为掩护媒体)中,从而不让对手发觉的一种方法[1]。隐藏的动作称为嵌入,掩护媒体经嵌入信息后称为伪装媒体。信息隐藏的本质是:利用人眼(或人耳)是一个不太灵敏的检测器,将信息本身的存在性隐藏起来,使人察觉不到有信息隐藏在媒体之中。由于人对视觉的不敏感性及图像文件本身的数据量很大,因此,图像文件是信息隐藏很好的载体。

实现图像隐藏的算法主要有空间域算法和变换域算法两种。变换域方法,如DCT(离散余弦变换)域、DWT(小波变换)域等利用某种数学变换,将图像用变换域表示,通过改变图像的某些变换域系数加入待隐藏的信息,然后再利用反变换来生成隐藏有秘密信息的图像[2],具有较强的不可见性和稳健性,隐藏信息量小,实现难度较大。空间域算法是使用最不重要的比特位和噪声控制来把秘密图像嵌入到载体图像中去,抗攻击力较弱,但隐藏信息量大,且容易实现[3]。文中运用Matlab实现了基于空域LSB(Least Significant Bit)的灰度图像隐藏与提取系统。图像隐藏系统由置乱模块、加密模块和嵌入模块组成。置乱模块采用基于行列置换的置乱算法,经过多次迭代处理,将原始图像变换为灰度均衡的灰度图像,迭代的次数作为密钥一,加密模块借鉴通信系统中常用的伪随机序列加密的方法,运用软件产生m序列对置乱后的图像进行加密处理。m序列的初始值作为密钥二。经过置乱、加密后的图像进入嵌入模块,采用最低位隐藏方法将数据信息嵌入到载体图像中。图像信息提取系统则由解

收稿日期:2006-08-13
作者简介:邹 娟(1978-),女,辽宁大连人,硕士,助教,研究方向为网络安全;贾世杰,硕士,副教授,研究方向是网络与多媒体信息处理技术。

隐藏、解密和反置乱三部分组成。如图 1~3 所示。

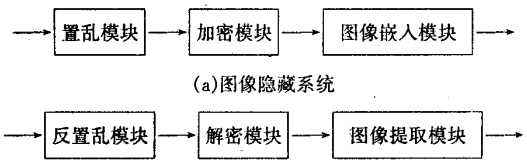
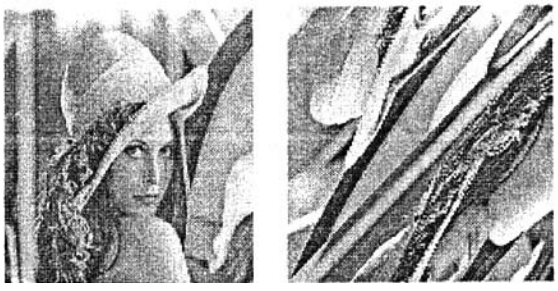
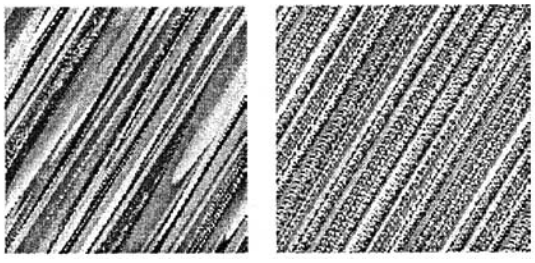


图 1　图像隐藏与还原系统



(a) 原图像　　(b) 一次置乱后的图像

图 2　一次置乱处理结果



(a)　迭代三次后的图像　　(b) 迭代六次后的图像

图 3　多次迭代处理结果

1　基于行列变换的图像置乱与反置乱算法

1.1　图像置乱算法

图像可看作是平面区域上的二元函数 $Z = F(x, y), (x, y) \in R$。在绝大多数情况下区域 R 中任意的点 (x, y)，则 $F(x, y)$ 代表图像的信息(如灰度值，RGB分量值等)，表示图像的二元函数有其特殊性，这就是相关性[4]。在图像被数字化之后，$Z = F(x, y)$ 则相应于一个矩阵，其元素所在的行与列对应于自变量取值，元素本身代表图像信息。离散化的数字图像相应于元素之间有相关性的一类特别的矩阵。矩阵的初等变换可以将图像转换成为另一幅图像，但其置乱作用较差，非线性交换则有可能增强置乱作用[5]。

基于行列式计算方法的图像置乱算法：

设置原始图像 $A = [a(i, j)]$，用置乱方法得到的图像为 B，则行列式置乱方法构造思想可表述为：

按某种规则 R，在 A 中选取不同行不同列的 N 个灰度值，再按另一种规则 r 放入 B 的第 1 行或者第 1 列中；

按规则 R，在 A 中剩余的元素中，选取不同行不同列的 N 个灰度值。再按规则 r 放入 B 的第 2 行或者第 2 列；

按规则 R，在 A 中剩余的元素中，选取不同行不同列的 N 个灰度值。再按规则 r 放入 B 的第 3 行或者第 3 列；

……

依次类推，进行到 N 步，则可以得到置乱后的图像 B，显然选取规则 R 不同或者放入规则 r 不同时，得到的置乱方法也不同。该类算法即为：行列式图像置乱加密法。如果每一步选取的规则 R 与放入规则 r 均不同，可以想象，这样的置乱算法是无穷多的。

下面具体构造一个比较简单的该类方法：

将 A 中主对角线上的元素依次放入 B 的第一行，既 B 的第一行：$B(1, j) = 1, 2, \cdots, N$；将主对角线下面紧靠它的 $N-1$ 元素依次放入 B 的第 2 行，后面用 A 中第 1 行第 N 列卡选的元素 $A(1, N)$ 补齐，即 $B(2, j) = A(j+1, j) = 1, 2, \cdots, N-1$；$B(2, N) = A(1, N)$；以此类推，可以得到该置乱算法的数学描述为：

$$B(i, j) = A(i + j - 1, j),\ i = 1, 2, \cdots, N;\ j = 1, 2, \cdots, N - i + 1$$

$$B(i, j) = A(i + j - 1 - N, j),\ i = 1, 2, \cdots, N;\ j = N - i + 2, N - i + 3, \cdots, N$$

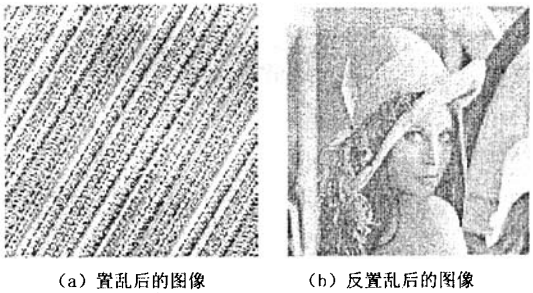
即置乱后的图像 B 的每一行的灰度值来自 A 的不同行，而列保持不变。

运行结果见图 2。

图 3 是迭代三次和六次后的效果图。可以看出，经过多次迭代处理后的图像与原图像相似度接近于 0。

1.2　图像反置乱算法

反置乱算法是置乱算法的逆过程。实验结果如图 4 所示。



(a) 置乱后的图像　　(b) 反置乱后的图像

图 4　反置乱处理结果

2　基于 m 序列的图像加密与解密算法

文中使用 Matlab 产生 15 位的 m 序列。在这里，

产生 m 序列的初始值就是加密算法中的密钥,为避免产生输出的全 0 序列,就不能将寄存器的初始值全设为 0。

从 m 序列产生器可以看出只要初始值改变,m 序列就不同。这就满足随机性。以上初始值的运行结果为:111010110010001。

然后,将 m 序列与原图像像素的各位相异或,就能达到加密的效果,产生加密后的图像。

同样,图像解密是图像加密的逆过程。根据异或的特点 $A = A \oplus B \oplus B$,所以,解密就是将加密后的图像与 m 序列再异或一下就可以实现。运行结果就是加密前的图像。只要接收者使用此算法和密钥就可以实现解密,读出原图像。

3 基于 LSB 的图像嵌入与提取算法

选取原图像大小为:32 * 32(见图 4(a));选取载体图像大小为:128 * 128,如图 5(b)所示;隐藏 1～4 位后的图像如图 5(c)～(f)所示。信息隐藏比和峰值信噪比的计算如表 1 所示。

表 1 信息隐藏比和峰值信噪比计算结果

隐藏位数	信息隐藏比	峰值信噪比(PSNR)
1	0.125	75.4dB
2	0.25	69.4dB
3	0.375	58.2dB
4	0.5	33.8dB

由图 5 可以看出,隐藏 1～3 位后的图像与载体图像相比在视觉上没有什么差别或差别不大,而隐藏 4 位后的图像出现比较明显的伪轮廓。

4 结束语

图像信息隐藏技术和图像加密技术都是新兴的技术,具有极大的发展潜力,两者的结合可以克服目前的信息隐藏技术中的很多弱点。文中运用 Matlab 实现了基于空域 LSB(Least Significant Bit)的灰度图像隐藏与提取系统。由于在进行图像隐藏前对原始图像信息进行了置乱和加密处理,具有较高的安全强度,能满足隐蔽通信等应用要求。

(a) 原图像 (b) 载体图像

(c) 隐藏一位后的图像 (d) 隐藏二位后的图像

(e) 隐藏三位后的图像 (f) 隐藏四位后的图像

图 5 基于 LSB 的图像嵌入算法实验结果

参考文献:

[1] 韩杰思,汤光明,马晓煜.基于图像的信息隐藏安全性分析[J].微计算机信息,2006,22(1-3):19-21.

[2] Provos N, Honerman P. Hide and Seek: An Introduction to Steganography[J]. IEEE SECURITY & PRIVACY, 2003, 5/6:32-44.

[3] 汪小帆,戴跃伟,茅耀斌.信息隐藏技术——方法与应用[M].北京:机械工业出版社,2001.

[4] 王聪丽,平西建.矩阵编码的实现及其在图像信息隐藏中的应用[J].计算机工程与应用,2005(34):146-148.

[5] 夏 煜,郎荣玲,戴冠中,等.基于图像的信息隐藏分析技术综述[J].计算机工程,2003,29(7):1-3.

(上接第 113 页)

程,2006,32(3):164-166.

[4] Adi K, Debbabi M, Meiri M. A New Logic for Electronic Commerce Protocols[C]// AMAST 2000, LNCS. [s.l.]:[s.n.],2000:499-513.

[5] 史国庆.利用组合加解密方案改进 SET 协议的研究[J].计算机工程与应用,2002,38(2):43-45.

[6] Shen Jau—Ji, Lin Iuon—Chang, Hwang Min—Shiang. A secure LITESET scheme[J]. Inst. Electron. Inf. & Commun. Eng,2004(11):2509-2521.

[7] 何 胜.电子商务中安全支付协议的对比及应用[J].计算机时代,2004(2):29-30.