基于图像二级置乱的信息隐藏技术

李 扬 樊养余 郝重阳
(西北工业大学电子与信息工程研究所,西安 710072)

摘 要 随着计算机网络及各种数字作品制作技术的迅速发展,信息隐藏技术越来越受到人们的关注。本文在分析了已有置乱方法优缺点的基础上,提出了图像的二级置乱法。它改进了原有方法中变换矩阵的形式,分别对原始图像的位置和灰度级进行不同类型的置乱,既改变了图像的纹理信息又改变了图像的统计特性,使其仅经过一次迭代就可以达到满意的效果。与其他方法相比,其计算量相对较小,且增强了图像的保密性,提高了保密信息的迷惑性,减小了攻击者的注意力。通过仿真实验证明,该方法具有较好的实用性。

关键词 位置置乱 灰度置乱 信息隐藏
中图法分类号: TP391 **文献标识码**: A **文章编号**: 1006-8961(2006)08-1088-04

Information Hiding Technology Based on Image Second-scrambling

LI Yang, FAN Yang-yu, HAO Chong-yang
(*The Institute of Electronic & Information Engineering, Northwestern Polytechnical University, Xi'an* 710072)

Abstract More and more people pay attention to the technology of information hiding because of the development of Internet and digital work. In the paper, a new scrambling method is introduced after analyzing the advantages and disadvantages of some other information hiding methods. It modifies the form of transformation matrix that is used to scramble the position and gray level of each pixel. This method changes not only the texture but also the statistical property of an image. Compared with other approaches, it has the following advantages: It improves the secrecy property of an image and reduces the attacker's notice; It has the less calculated capacity. Simulations show that it is practicable.

Keywords position scrambling, gray level scrambling, information hiding

1 引 言

网络通信技术和计算机处理能力的发展,使图像存储与传输变得越来越快捷。但是受到传播领域与传播方式的影响,一些保密信息(比如军事遥感图像,经济发展数据等)不能直接在公开网络或信道上传输,这就促进了信息隐藏技术的形成与发展,使其成为一个备受关注的前沿研究课题。所谓信息隐藏[1]是指将保密信息隐藏于另一个非保密载体中,以不引起检查者(攻击者)注意,从而实现隐蔽传输、存储、标注、身份识别等功能。与传统的密码学相比,信息隐藏具有更强的迷惑性。

在实际应用中需要通过图像预处理来满足迷惑性的要求,图像置乱就是一种常用的方法。目前研究较多的方法有基于 Arnold[2] 和 Fibonacci 变换[3]、骑士巡游[4]、生命游戏[5]、幻方置乱[6]、混沌序列[7]、仿射变换[8]和空间填充曲线[6](FASS 曲线)等等,这些方法都只是对图像位置信息进行置乱,而其统计特性(如灰度直方图)并未发生变化,因此攻击者有可能通过统计特性来判断或破坏保密信息,为此提出了基于图像二级置乱的信息隐藏算法,它采用两种不同的方法分别对图像的位置信息和颜色信息进行置乱,使处理后的保密图像与原图看似

基金项目:航空科学基金项目(04F53035)
收稿日期:2005-05-09;**改回日期**:2005-07-29

第一作者简介:李扬(1981~),女。西北工业大学信号与信息处理专业硕士研究生。感兴趣的研究方向有图像处理、信息隐藏、灰色系统理论及应用研究等。E-mail:liyang328@126.com

“面目全非”,具有较好的迷惑性,同时减少对掩体的要求,使其能隐藏于任意的公开图像中。

2　图像置乱的基本原理

2.1　位置空间的图像置乱

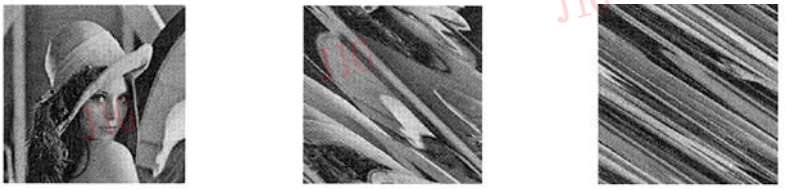
Arnold 变换是 Arnold 研究环面上的自同态时提出的,其 n 维变换矩阵 $|A|=1$,所以该变换具有周期性[9],且随着 n 取值的不同有多种应用。当 $n=3$时,可对 R、G、B 色彩分量或 3 维信息进行变换,$n=2$ 时,可用于图像位置置乱。但在实际应用中该方法需经过多次迭代才能达到满意的置乱效果,为了减少计算量,在满足 $|A|=1$ 的前提下对 A 中的元素值进行调整得到新的变换矩阵。

定义 1　设 $F=[f(x,y)]$ 表示一幅数字图像,(x,y) 表示像素的坐标,则位置置乱变换为

$$\begin{bmatrix}x'\\y'\end{bmatrix}=\begin{bmatrix}2 & 1\\3 & 2\end{bmatrix}\cdot\begin{bmatrix}x\\y\end{bmatrix} \bmod N \quad (1)$$

其中,$x,y\in\{0,1,2,\cdots,N-1\}$,$N$ 为图像矩阵阶数,称式(1)定义的变换为非对称矩阵变换,它表示将原图 (x,y) 处的像素移动到置乱后图像的 (x',y') 处。

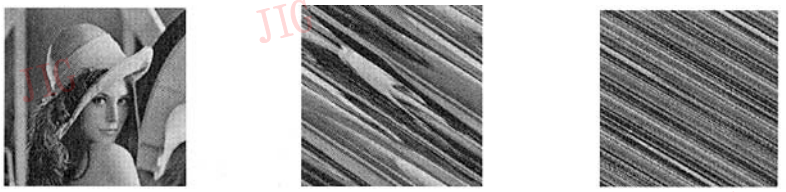
图 1、图 2 分别是采用 Arnold 变换和本文算法得到的置乱效果图,其中,t 表示迭代次数。从图中可以看出,Arnold 变换经过一次迭代后,仍能够从置乱图中得到一些原始信息,而本文提出的方法已经基本改变了原图中的纹理,无法找到有用信息。



(a) 原始图像　(b) $t=1$　(c) $t=2$

图 1　采用 Arnold 变换的位置置乱效果

Fig. 1　Result of Arnold scrambling



(a) 原始图像　(b) $t=1$　(c) $t=2$

图 2　本文算法的位置置乱效果

Fig. 2　Result of Asymmetric scrambling

2.2　灰度空间的图像置乱

除了图像的纹理信息,其统计特性也是分析图像的重要指标,但是目前有关灰度置乱的研究方法相对较少。对 Gray 编码技术进行改进,产生一个新的变换矩阵,以增强灰度置乱效果。

定义 2　任意灰度值 g 的二进制数表达形式为 $g=(g_0g_1g_2\cdots g_7)_2$,其中 $g_i=1$ 或 0,$i=0,1,\cdots,7$,令

$$h_i=(g_i+g_{i-1}) \bmod 2,\ i=1,2,\cdots,6 \quad (2)$$

当 $i=0$ 时,$h_0=(g_0+g_7) \bmod 2$,$i=7$ 时,$h_7=(g_0+g_6+g_7) \bmod 2$,称以上变换为改进的 Gray 编码变换,$h(g)=(h_0h_1\cdots h_7)$ 为灰度变换结果,即同一位置像素点经过灰度置乱后的值,用矩阵形式可将该运算表示为

$$\begin{bmatrix}h_0\\h_1\\\vdots\\h_6\\h_7\end{bmatrix}=\begin{bmatrix}1 & 0 & \cdots & 0 & 1\\1 & 1 & \cdots & 0 & 0\\\vdots & \vdots & \ddots & \vdots & \vdots\\0 & 0 & \cdots & 1 & 0\\1 & 0 & \cdots & 1 & 1\end{bmatrix}\cdot\begin{bmatrix}g_0\\g_1\\\vdots\\g_6\\g_7\end{bmatrix} \bmod 2 \quad (3)$$

虽然它与原 Gray 编码的变换矩阵只有两个元素值的差异,但是灰度置乱的效果却相差较大,如图 3所示。

(a) 原始图像 (b) Gray 编码 (c) 改进 Gray 编码

图 3 灰度置乱结果比较

Fig. 3 Comparison of gray scrambling result

3 基于置乱的信息隐藏技术

LSB(least significant bit)算法是常用的信息隐藏方法,缺点是抗噪能力差。因此,本文将保密信息隐藏于不重要的低两位,以提高算法的适应能力。具体步骤如下:

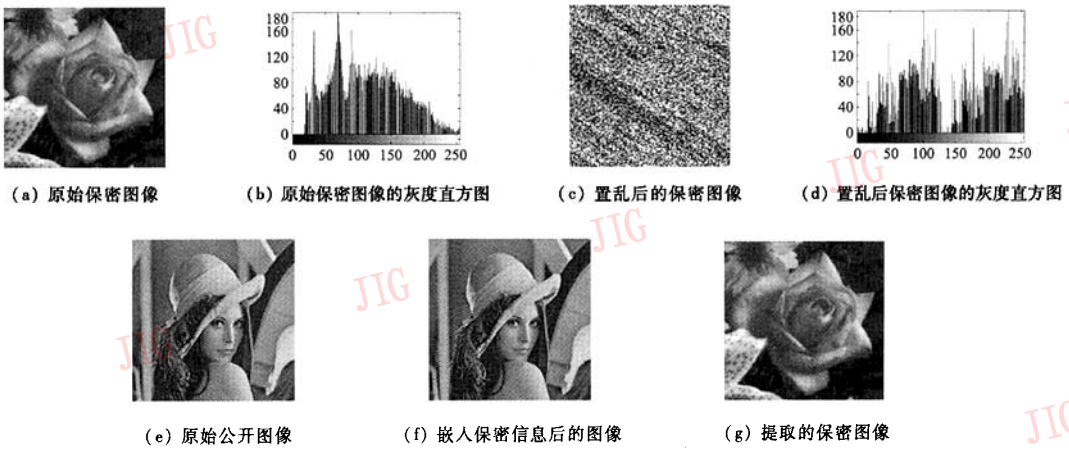
(1) 隐藏过程 设公开图像 $\boldsymbol{P}$ 和保密图像 $\boldsymbol{S}$ 分别表示为

$$\boldsymbol{P} = \{p(x,y) \mid 1 \leqslant x \leqslant M_1, 1 \leqslant y \leqslant N_1\} \quad (4)$$

$$\boldsymbol{S} = \{s(x,y) \mid 1 \leqslant x \leqslant M_2, 1 \leqslant y \leqslant N_2\} \quad (5)$$

首先对保密图像进行位置置乱得到矩阵 $\boldsymbol{S}_1$,变换过程如式(1)。其次根据本文提出的改进 Gray 编码方法对 $\boldsymbol{S}_1$ 中像素点的灰度值进行二级置乱,得到矩阵 $\boldsymbol{S}_2$。最后将 $\boldsymbol{S}_2$ 嵌入公开图像 $\boldsymbol{P}$ 中像素点灰度值的低两位(最不重要位和次不重要位),从而得到可以在公共网络或信道中传输的矩阵 $\boldsymbol{P}_S$,其中嵌入位置的选择可以由随机数组产生,产生随机数组的种子将作为密钥传输。

(2) 提取过程 保密信息的提取与嵌入是互逆过程。首先利用密钥确定隐藏位置,根据双方共知的隐藏原则从 $\boldsymbol{P}'_S$(信息传输过程中会受到多种干扰,因此接收的图像与发送图像可能有一定的差异,所以文中在表示方法上做了区别)中提取隐藏内容 $\boldsymbol{S}'_2$。然后对其进行灰度值和位置的逆置乱,由此恢复出保密信息 $\boldsymbol{S}'$。理想情况下为 $\boldsymbol{S}' = \boldsymbol{S}$,但实际应用中只能尽力做到二者在视觉效果上没有差别。图 4是采用本文算法进行信息隐藏的结果图。



(a) 原始保密图像 (b) 原始保密图像的灰度直方图 (c) 置乱后的保密图像 (d) 置乱后保密图像的灰度直方图

(e) 原始公开图像 (f) 嵌入保密信息后的图像 (g) 提取的保密图像

图 4 基于二级置乱的图像信息隐藏算法

Fig. 4 Result image of information hiding based on second-scrambling

4 结 论

随着计算机网络的不断发展,信息隐藏技术必然会有更大的研究空间。基于二级置乱的信息隐藏方法充分利用了图像隐藏的迷惑性,首先对保密图像进行位置及灰度的共同置乱,使其与原始图像不具有任何相似性;其次采用不重要位的方法将已经

置乱的保密图像嵌入到公开图像中。与其他方法相比,具有以下优点:

(1) 置乱效果好　不仅对图像中各个像素的位置进行了置乱,而且还通过灰度值的置乱改变了图像的灰度级分布,使其与原图像在视觉效果及统计特性上都发生了变化。这样即使恶意的攻击者从传输图像中发现了异常,也无法利用截获信息来寻找和判断出真正的保密信息。

(2) 逆过程求解简单　在进行置乱的过程中都定义了相应的变换矩阵,因此接收方在恢复的过程中只需要求出相应的逆矩阵就可以得到结果。

(3) 与 LSB 算法相比,本文采用的不重要位嵌入方法在一定程度上增强了抗攻击能力,也提高了算法的嵌入容量。

参考文献(References)

1 Ding W, Yan W Q, Qi D X. Digital image information hiding technology and its application based on scrambling and amalgamation [J]. Journal of Image and Graphics, 2000, **5**(8):644 ~ 649. [丁玮,闫伟齐,齐东旭. 基于置乱与融合的数字图象隐藏技术及其应用[J]. 中国图象图形学报(A 版), 2000,**5**(8):644 ~ 649.]

2 Zou Jian-cheng, Ward Rabab K. Introducing two new image scrambling methods [A]. In: Proceedings of the IEEE PacRim Conference on Communications, Computers and Signal Proceedings [C], Victoria, Canada, 2003, **2**:708 ~ 711.

3 Zou Jian-cheng, Ward Rabab K, Qi Dong-xu. A new digital image scrambling method based on fibonacci number[A]. In: Proceeding of the IEEE Inter Symposium on Circuits and Systems[C], Vancouver, Canada, 2004, **3**:965 ~ 968.

4 Bai Sen, Cao Chang-xiu, Cao Long-han, *et al*. Digital image details hiding technology based on knight-tour transformation[J]. Journal of Image and Graphics, 2001,**6**(11):1096 ~ 1100. [柏森,曹长修,曹龙汉等. 基于骑士巡游变换的数字图象细节隐藏技术[J]. 中国图象图形学报, 2001,**6**(11):1096 ~ 1100.]

5 Ding Wei, Yan Wei-qi, Qi Dong-xu. Digital image scrambling and digital watermarking technology based on conway's game[J]. Journal of North China University of Technology, 2000,**12**(1):1 ~ 5. [丁玮,闫伟齐,齐东旭. 基于生命游戏的数字图像置乱与数字水印技术[J]. 北方工业大学学报, 2000,**12**(1):1 ~ 5.]

6 Ding Wei, Qi Dong-xu. Digital image transformation and information hiding and disguising technology[J]. Chinese Journal of Computers, 1998,**21**(9):838 ~ 843. [丁玮,齐东旭. 数字图像变换及信息隐藏与伪装技术[J]. 计算机学报,1998,**21**(9):838 ~ 843.]

7 Yi Kai-xiang, Sun Xin, Shi Jiao-ying. An image encryption algorithm based on chaotic sequences[J]. Journal of Computer-Aided Design & Computer Graphics, 2000,**12**(9):672 ~ 676. [易开祥,孙鑫,石教英. 一种基于混沌序列的图像加密算法[J]. 计算机辅助设计与图形学学报,2000,**12**(9):672 ~ 676.]

8 Zhu Gui-bin, Cao Chang-xiu, Hu Zhong-yu, *et al*. An image scrambling and encryption algorithm based on affine transformation [J]. Journal of Computer-Aided Design & Computer Graphics, 2003,**15**(6):711 ~ 715. [朱桂斌,曹长修,胡中豫等. 基于仿射变换的数字图像置乱加密算法[J]. 计算机辅助设计与图形学学报,2003,**15**(6):711 ~ 715.]

9 Qi Dong-xu, Zou Jian-cheng, Han Xiao-you. A new scrambling method and its application in image information hiding[J]. Science China(Series E), 2000,**30**(5):440 ~ 447. [齐东旭,邹建成,韩效宥. 一类新的置乱变换及其在图像信息隐蔽中的应用[J]. 中国科学(E 辑),2000,**30**(5):440 ~ 447.]