

基于图片的数字密写设计与实现

王海春^{1,2}, 邱寄帆^{1,2}, 邱敦国¹

(1. 四川大学计算机学院, 成都 610065; 2. 成都航空职业技术学院计算机工程系, 成都 610021)

摘 要: 提出了一种基于图片的数字密写设计与实现方法, 介绍了应用程序的实现方案, 给出了系统组成方框图。通过对图片的数字密写来进行汉字文本信息传输, 较好地解决了在互联网上信息传输的通信安全问题。实践表明, 系统具有推广和应用价值。

关键词: 数字密写; 信息隐藏; 图片

Design and Implementation of Steganography Based on Picture

WANG Haichun^{1,2}, QIU Jifan^{1,2}, QIU Dunguo¹

(1. College of Computer, Sichuan University, Chengdu 610065;

2. Department of Computer Engineering, Chengdu Aeroautic Vocational & Technical College, Chengdu 610021)

【Abstract】 This paper proposes one kind of design and implementation of a steganography system based on the picture, introduces the application program realization plan, produces the system composition block diagram. A new transmission method of the Chinese character text information based on the picture solves the communication security problem of the information transmission at Internet. The practice indicates the system has the promotion and the application value.

【Key words】 Steganography; Information hiding; Picture

数字密写是将秘密信息嵌入到载体信号中, 通过公众媒体传输而不被察觉, 以实现信息的隐藏, 载体信号可以是文本、图像、声音等。在实验中, 需要在公用信道上传输保密的文字材料, 采取了将重要信息隐藏在图片中, 通过公用信道发送出去, 接收方再从图片中提取隐藏信息。

彩色图片的每一个像素点均由 RGB 颜色组成, 每一种颜色的取值范围由 8bits 二进制数表示, 在 0~255 中, 0 代表黑色, 255 代表白色。对一幅自然图片, 相邻像素的颜色差别往往不大, 也就是说相邻颜色的相关性比较强。把每个像素位的 RGB 值按二进制数位抽取出来, 每种颜色可构成 8 个不同的位平面(bit plane), 最高位平面的颜色值为 128, 对图片的色彩贡献最大, 最低位平面的颜色值为 1, 对图片的色彩贡献相对较小, 最接近黑色。当颜色的 8bits 二进制数存在高位数时, 其低位数仅仅表示某一色彩的变化范围, 对整个图形的影响相对较小, 在视觉上不易察觉。实验表明, 颜色值的第 4~7 位组成的位平面对图片视觉影响较大, 而第 0~3 位组成的位平面对图片的视觉影响较小。本文介绍的数字密写方法, 就是用欲嵌入的秘密信息取代载体图像的颜色值的较低比特位, 与原来图像颜色值的 7 个较高位平面组成含隐藏信息的新图像, 实现基于图片的数字密写。

1 密写信息的嵌入设计

在密写前, 首先将欲嵌入的信息转化为比特流, 例如将汉字转换成相应的二进制 4B 编码, 再对这个二进制数进行加密和置乱。如果欲嵌入的二进制比特流小于载体图像的像素数, 可采取在较低位平面上用伪随机游走的方法建立起秘密信息比特流与载体图像较低比特位的对应关系, 然后进行替换嵌入。

当秘密信息的接收者从网络上得到经密写过的图片后, 便可直接取出较低比特位平面, 根据密钥对置乱的比特流进

行解密, 得到秘密信息, 再将其从二进制编码转换成汉字。

由于秘密信息经过加密和置乱后近似于随机噪声, 而载体图片的较低位平面也类似于随机噪声, 因此嵌入秘密信息后, 图片的统计特性并没有明显改变。而且较低比特位对像素值影响较小, 视觉上基本无法察觉图片的微小改变。图 1 显示了数字密写与解密过程。

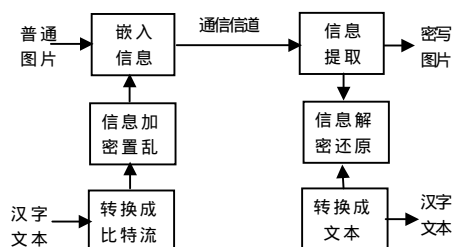


图1 数字密写与解密过程

2 信息密写与信息提取的程序实现

本文采用微软的 VB 6.0 程序设计语言, 设计了一个基于数字图片的数字密写编码器和数字密写解码器。采用 2 个 Picture Box 控件进行图片的装入与输出, 选择了一幅宽为 469 像素、高为 349 像素、名为 pic01.bmp 的位图图片作为载体图片, 将载体图片装入 Picture Box 控件内, 对图片进行数字密写, 加入要密写的信息, 生成一幅含有密写信息的新图片 new3.bmp。将新图片经互联网发送给对方, 对方收到新图片后, 将新图片重新装入 Picture Box 控件, 从中取出密写的信

基金项目: 四川省 2004 年基金资助重点项目(04GG006-032)

作者简介: 王海春(1957 -), 男, 副教授、硕士, 主研方向: 智能控制, 语音与图像处理, 嵌入式应用; 邱寄帆, 副教授、硕士; 邱敦国, 硕士

收稿日期: 2006-04-13 **E-mail:** whc700@163.com

息。如果在图片的 RGB 的每一个颜色分量的每个像素位上隐藏 1 个二进制数位, 这幅图片理论上可存储 $3 \times 469 \times 349 = 491\,043$ 个二进制比特位。如果隐藏汉字的二进制编码, 此幅图片可隐藏约 15 000 个汉字。

2.1 数字密写编码器程序设计

在一幅位图上进行信息密写的示意子程序如下:

```
Public sub process1()  
Dim s(469, 349) As Integer  
//定义一个二维数组, 存储要密写的信息  
i = 93 //例如要密写的是一个二进制数 10010011  
s(1, 1) = 8 //可选 0-3 位的位平面作为隐藏位  
s(1, 2) = 0 //案例中选取的是第 3 位平面, 8 代表“1”  
s(1, 3) = 0  
s(1, 4) = 8  
s(1, 5) = 0  
s(1, 6) = 0  
s(1, 7) = 8  
s(1, 8) = 8  
Picture1.Picture = LoadPicture("d:\vbtest\pic01.bmp")  
//装入载体图片  
Picture2.ScaleHeight = Picture1.ScaleHeight  
//设置新生成的图片高度  
Picture2.ScaleWidth = Picture1.ScaleWidth  
//设置新生成的图片宽度  
For Y = 0 To Picture2.ScaleHeight - 1  
For X = 0 To Picture2.ScaleWidth - 1  
r0 = Picture1.Point(X, Y) //提取原图片 R 像素分量值  
r = r0 And &HF0 //清除低 4 位像素值  
r1 = r Or s(X, Y) //在第 3 位嵌入隐藏信息  
g = (r0 And 65280) / 256 //提取原图片的 G 分量像素值  
b = (r0 And &HFF0000) / 65536 //提取原图片的 B 分量像素值  
Picture2.PSet (X, Y), RGB(r1, g, b) //生成新图片的像素  
Next X  
Next y  
dddd = "d:\vbtest\new3.bmp"  
SavePicture Picture2.Image, dddd //输出嵌入了隐藏信息的新  
//图片文件  
End Sub
```

2.2 数字密写解码器程序设计

从一幅隐藏了密写信息的位图上提取密写信息的子程序如下:

```
Public sub process2()  
Dim s2(469, 349) As Integer //定义二维数组, 存储提取的信息  
Picture1.Picture = LoadPicture("d:\vbtest\new3.bmp")  
//打开载体图片
```

```
For Y = 0 To Picture1.ScaleHeight - 1  
For X = 0 To Picture1.ScaleWidth - 1  
r0 = Picture1.Point(X, Y) //提取像素值  
r = r0 And &H08 //抽取隐藏的第 3 位信息  
s2(X, Y) = r //提取的信息存入数组  
Next X  
Next Y  
End Sub
```

3 结论

上述程序给出了在图片的每一个像素位置密写二进制比特位的方法, 比起通过文本进行的信息密写, 使用更方便、密写量更大、密写效果更好。大量实验统计表明, 该数字密写的峰值信噪比(peak signal-to-noise ratio, PSNR)为 53dB, 而人们往往不易察觉峰值信噪比大于 38dB 的数字密写对图片产生的影响。特别是当需要密写的比特数较少时, 密写比特位在图片上可随机游走, 加上对汉字的二进制编码的数字扰乱, 系统在进行的安全测试中, 顺利通过了 RS 分析法和 GPC 分析法的检测。

本文的创新点:

(1)通过对图片的数字密写来进行汉字文本传输, 较好地解决了在互联网上信息传输的通信安全问题, 具有一定的实用价值。由于互联网上图片传输的海量和随意性, 使密写分析者的难度达到了无法估计的程度。

(2)通过 VB 的 picture Box 控件进行图像处理, 使系统的实现更方便和快捷, 具有一定的参考价值。

(3)通过汉字编码、信息扰乱、二进制信息在图片上的随机游走和密写, 使系统具有了较高的安全性能, 实现了互联网上文本信息安全传输方式上的突破。

参考文献

- 1 Kalker T, Ro Y M, Cox I J. Digital Watermarking: the 2nd International Workshop[J]. Lecture Notes in Computer Science, Springer-Verlag, 2004, 10(2).
- 2 Garvin A. The Debate over Online Steganography[J]. The Digital Beat, 2001, 21(2).
- 3 张路平, 喻波. Visual Basic 6.0 编程案例精解[M]. 北京: 电子工业出版社, 2005.
- 4 张新鹏, 王朔中, 张开文. 数字密写和密写分析[M]. 北京: 清华大学出版社, 2005.
- 5 刘显德, 唐国维, 富宇等. 一种基于 Word 文档的信息隐藏方法[J]. 电子技术应用, 2005, 31(4): 16-17.
- 6 张新鹏, 王朔中, 张开文. 基于统计特性的 LSB 密写分析[J]. 应用科学学报, 2004, 22(1): 16-19.

(上接第 154 页)

参考文献

- 1 Arbaugh W A, Gvan B, Doorn L. Signed Executables for Linux[R]. University of Maryland, Tech.Report: CS-TR-4259, 2001.
- 2 Catuogno L, Visconti I. A Format-independent Architecture for Run-time Integrity Checking of Executable Code[C]. Proceedings of the 3rd Conference on Security in Communication Networks, 2002.
- 3 Catuogno L, Visconti I. An Architecture for Kernel-level Verification of Executables at Run Time[J]. The Computer Journal, 2004, 47(5).
- 4 Tool Interface Standard(TIS) Committee. Executable and Linking Format (ELF) Specification (Version 1.2)[Z]. 1995.
- 5 胡希明, 毛德操. Linux 内核源代码情景分析[M]. 杭州: 浙江大学出版社, 2001.
- 6 Krawczyk H, Bellare M, Canetti R. HMAC: Keyed-Hashing for Message Authentication[S]. RFC2104, 1997.
- 7 Devik S. Linux On-the-fly Kernel Patching Without LKM[Z]. <http://www.phrack.com>, 2001.
- 8 Schneier B. 吴世忠, 祝世雄译. 应用密码学: 协议、算法与 C 源程序[M]. 北京: 机械工业出版社, 2000.