基于直接位平面替换的LSB信息隐藏技术*)

孙文静[1] 孙亚民[1] 张学梅[2]

(南京理工大学计算机学院 南京 210094)[1] (南京信息工程大学 南京 210044)[2]

摘 要 针对经典LSB信息隐藏技术隐蔽性较低的情况,提出了基于直接位平面替换的LSB信息隐藏技术。实验表明,该算法隐蔽性强,信息嵌入量高,抗干扰性好,具有良好的应用前景。

关键词 信息隐藏,LSB,位平面替换,局部灰度特征,隐蔽性

Information Hiding Technology of LSB Based on Direct Bit-plane Replacement

SUN Wen-jing[1] SUN Ya-min[1] ZHANG Xue-mei[2]

(School of Computer, Nanjing University of Science & Technology, Nanjing 210094, China)[1]

(Nanjing University of Information Science & Technology, Nanjing 210044, China)[2]

Abstract The invisibility of classical LSB information hiding technology is poor. This article presented an information hiding technology of LSB based on direct bit-plane replacement. Experimental results show that this algorithm has better invisibility, great embedding quantity and better robustness. It will have good application in the future.

Keywords Information hiding, Least significant bit, Local gray-level feature, Invisibility

现代信息隐藏是一种将特定的信息(如图像、文本、声音、认证、注释、版权等)隐藏在数字化宿主信息(如文本、数字化的声音、图像、视频信号等)中的技术。1993年Tirkel发表了名为"Electronic Wartermark"的研究论文;1996年第一届国际信息隐藏大会(First International Workshop on Information Hiding)在英国剑桥大学举行,会议对信息隐藏的部分英文术语和学科分支进行了统一和规范。此后十多年,信息隐藏技术飞速发展,研究内容从空域信息隐藏逐步转向频率域的信息隐藏,以数字水印为主的研究正逐步转向与数据压缩、数据融合、神经网络等学科相结合[1-3]。

LSB(Least Significant Bit)是一种经典的数据隐藏方法,其利用人的视觉系统(HVS)对于图像的微小改动不敏感和图像的LSB平面的类噪声特性,通过信息比特去替换载体图像流的最低二进制位实现信息的嵌入,具有对载体文件改动小、嵌入量大、简单易行、实用性强的特点,得到了较多的应用。

但是,LSB会使图像的灰度直方图分布产生较为明显的变化,遗留下隐蔽通信的痕迹,使得通过分析直方图统计特征的改变,可以检测出隐蔽信息的存在并对其大小做出估计。

有鉴于此,本文提出了基于直接位平面替换的LSB信息隐藏技术。实验表明,该算法隐蔽性强,信息嵌入量高,抗干扰性好,具有良好的应用前景。

1 传统的LSB信息隐藏原理

经典LSB嵌入算法的思想是各个颜色分量的灰度上增1(偶数的情况)或减1(奇数的情况),人的视觉不会感觉到。一般情况下,各个颜色分量在计算机中都用一个字节表示,载体图片看作是字节流,而隐秘消息看作是二进制数0或1的位流,设载体文件图像数据部分为:

$$C=B_1B_2\cdots B_n, B_i=b_{i1}b_{i2}\cdots b_{i8} \quad (i=1,2,\cdots,n) \tag{1}$$

待嵌入的秘密信息为:

$$M=m_1m_2\cdots m_l \tag{2}$$

其中,$b_{ij}, m_k\in\{0,1\}, j=1,2,\cdots,8; k=1,2,\cdots,l$。LSB替换算法就是从载体图片中选择嵌入位置,用$m_k$来代替对应位置上的$b_{i8}$,嵌入后生成的隐秘图像可以表示为$S=B_1B_2\cdots B_n$,其中

$$B_i^*=\begin{cases} b_{i1}b_{i2}\cdots b_{i7}m_i & (1\leqslant i\leqslant l) \\ B_i & (l\leqslant i\leqslant n) \end{cases} \tag{3}$$

若秘密信息嵌入到位图BMP(24位彩色图像)文件中的最低位,那么该BMP文件所能容纳的秘密信息最大容量M=图像高度×图像宽度×3/8字节。对于8位的灰度图像,M=图像高度×图像宽度/8字节。

2 基于直接位平面替换的LSB算法

基于灰度图像的直接位平面替换的LSB算法的核心是,在嵌入区域选择上,考虑图像的局部灰度特征和嵌入的信息量。本文将图像分为4×4窗口,通过计算该窗口中各像素之间的灰度差值来决定替换像素的最低1位还是最低2位。

首先计算窗口中16个像素$S_1, S_2, \cdots, S_{16}$的平均灰度值G

$$G=\frac{S_1+S_2+\cdots+S_{15}+S_{16}}{16} \tag{4}$$

然后计算各个像素灰度值与G之差的平方和,即

$$AVE=\frac{1}{16}\sum_{i=1}^{16}(S_i-G)^2 \tag{5}$$

在第1个分块中用秘密信息流嵌入窗口中的各像素的最低1位,记$n=1$(n是二进制数);以后,若$AVE\leqslant K$(K值根据载体图像的整体灰度分布和嵌入信息量来选定),将秘密信息的1位嵌入窗口中的各像素的最低1位,并记$n=n\times2$;否则,将秘密信息流嵌入窗口中各像素的最低2位,修改$n=n\times$

*)基金项目:江苏省产业技术研究与开发基金,苏发改高技发[2006]1106号。**孙文静** 博士生,研究方向为信息安全。

2+1，依次进行下去，直至秘密信息流嵌入完毕，把 n 保存好作为提取时的密钥。AVE 越大，表示该区域的灰度值越丰富，适宜嵌入更多的信息；K 值越大，表示选取灰度值越丰富的分块嵌入较多的信息，K 值越小，嵌入的信息总量越大，但信息的不可见性就差。提取时，根据 n 的值进行提取。从 n 的最高位开始，若该位为 1 则从对应的 4×4 窗口中各像素点的最低 1 位提取信息，若该位为 0 则从对应的 4×4 窗口中各像素点的最低 2 位提取信息，依次进行 L 次（L 为 n 的长度），秘密信息流提取完毕。

在嵌入方法上，文献[4]提出了一种基于 LSB 的图像字节各位的异或算法，用来对秘密信息进行隐藏，使攻击者不能轻易取得秘密信息。设 S 为秘密信息的一个位，它对应的一个位图数据字节为 $X_7\ X_6\ X_5\ X_4\ X_3\ X_2\ X_1\ X_0$。

嵌入算法：顺序读取秘密信息的各个 S，将它分别与即将放置于载体图像中的该字节的高 7 位进行异或运算，得到 X_0'。将 X_0 丢弃不做处理，用 X_0' 来代替。即

$$X_0'=X_7\oplus X_6\oplus X_5\oplus X_4\oplus X_3\oplus X_2\oplus X_1\oplus S \quad (6)$$

提取算法：设提取后的信息为 S'，则

$$\begin{aligned}S'&=X_7\oplus X_6\oplus X_5\oplus X_4\oplus X_3\oplus X_2\oplus X_1\oplus X_0'\\&=(X_7\oplus X_6\oplus X_5\oplus X_4\oplus X_3\oplus X_2\oplus X_1\oplus X_7)\oplus\\&\quad(X_6\oplus X_5\oplus X_4\oplus X_3\oplus X_2\oplus X_1\oplus S)\\&=(X_7\oplus X_6\oplus X_5\oplus X_4\oplus X_3\oplus X_2\oplus X_1\oplus X_7)\oplus\\&\quad(X_6\oplus X_5\oplus X_4\oplus X_3\oplus X_2\oplus X_1)\oplus S\\&=S\end{aligned} \quad (7)$$

本文借鉴文献[5]的思想，提出了一种新的嵌入算法，即只用图像数据的每个字节的最高 1 位 X_7 与秘密信息的一位 S 进行异或运算，结果放置到载体图像数据字节的最低位。即

$$X_0'=X_7\oplus S \quad (8)$$

嵌入算法如图 1 所示。

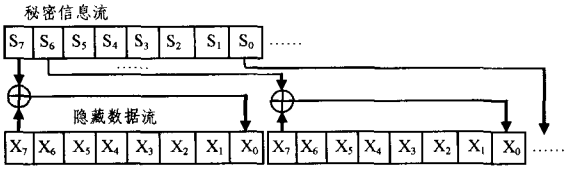


图 1　1 位信息嵌入示意图

信息提取过程（图 2）是

$$S'=X_7\oplus X_0'=X_7\oplus(X_7\oplus S)=S \quad (9)$$

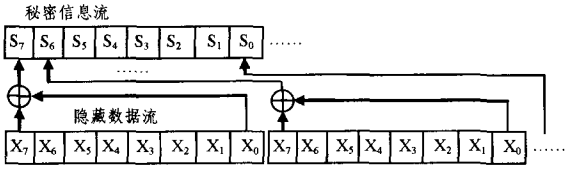


图 2　1 位信息提取算法示意图

如果采用最低 2 位嵌入信息，则将秘密信息的 2 位依次与载体数据流的最高两位分别异或再嵌入载体数据流的最低 2 位（图 3），提取时分别用隐藏数据字节的最低 2 位与最高 2 位异或（图 3）。

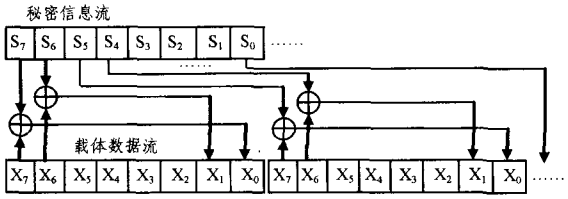


图 3　最低 2 位信息嵌入示意图

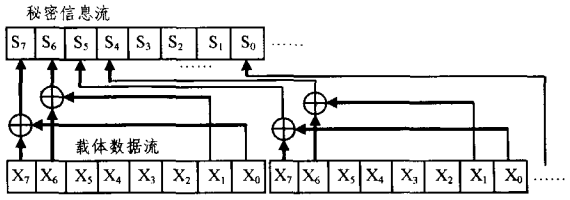


图 4　最低 2 位提取算法示意图

基于灰度图像的直接位平面替换的 LSB 算法流程如下：

（1）将随机待隐信息转化为二进制数据码流，存入数组 secret[N]，N 为秘密信息的长度；

（2）计算载体图像每个 4×4 窗口中像素点 AVE 值，若 $AVE\leqslant K$，将窗口各像素点的字节的第 7 位与 secret [N]数据码流异或后的结果写入最低位。比如，对秘密信息的第 i 比特位，若掩体图像的相应字节为 cover [8]，隐藏后的图像为：

$$\text{cover}[0]=\text{cover}[7]\oplus\text{secret}[i] \quad (10)$$

否则，将窗口各像素点的字节的第 7，6 位与 secret[N]数据码流每 2 位分别异或后的结果写入窗口对应像素点最低 2 位，即

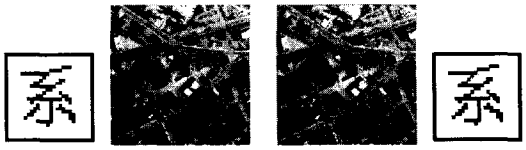
$$\text{cover}[1]=\text{cover}[7]\oplus\text{secret}[i] \quad (11)$$

$$\text{cover}[0]=\text{cover}[6]\oplus\text{secret}[i+1] \quad (12)$$

（3）新产生的图像即为嵌入信息后的图像。

3　实验结果

在 Matlab 中编写实现上述算法的应用程序[6]。首先把秘密信息的长度 N 隐藏到载体图像的第一行数据中，然后从载体图像的第二行开始进行 4×4 分块，按照上述算法的嵌入过程顺序嵌入载体图像的最低 1 位或 2 位。提取时，首先从隐秘图像的第一行获得嵌入信息的长度 N，然后从第二行开始按照上述算法的提取过程提取字节的最后 1 位或 2 位，并和该字节的最高 1 位或 2 位异或，异或的结果即为嵌入的秘密信息位。按照此方法执行 L 次，从隐秘图像中提取的信息位流即是嵌入的秘密信息流。



(a)秘密图像　(b)载体图像　(c)隐藏图像　(d)提取图像

图 5　图像的 LSB 嵌入示例

图 5(a) 是要隐藏的图像，即秘密信息，(b)是没有嵌入秘密信息的载体图像，(c)是嵌入秘密信息的隐藏图像，(d)是提取出的秘密图像。图(c)和图(b)图相比较，人眼完全不能分辨其差异，证明了本算法的有效性和可行性。图 (a) 和图 (d) 相比较，说明本程序能够完全准确地提取出被隐藏的数据信息，证明了本算法的有效性和正确性。

为了验证该文算法的鲁棒性，对嵌入了信息的图像分别进行 JPEG 压缩、加噪、中值滤波等操作，之后再提取秘密信息。

（1）JPEG 压缩

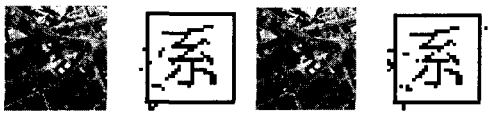
JPEG 压缩是图像处理中最常见的操作，对含密图像分

（下转第 219 页）

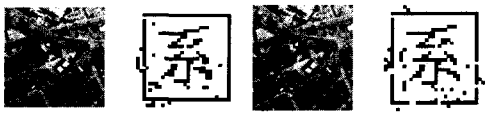
graphics modeling, rednering and animation. 叶修梓, 万华根, 张引, 译. 电子工业出版社, 2004
[2] 苏延辉, 韦欢, 费广正, 等. 非真实感绘制技术研究. 中国传媒大学学报: 自然科学版, 2006, 13(2): 15-21
[3] Lansdown J, Schofield S. Expressive rendering: a review of non-photorealistic techniques. IEEE Computer Graphics and Applications, 1995, 15(3): 29-37
[4] 钱小燕, 肖亮, 吴慧中. 基于多分辨率的非真实感绘制. 南京理工大学学报, 2006, 30(3): 348-351
[5] Pang Y J. Combining computer graphics with Chinese traditional painting. Computer & Graphics, 1987, 11(1): 63-68
[6] Pang Y J, Zhong H X. Drawing Chinese Traditional Painting by Computer// Pro. IFIP WG5. 10 Working Conference on Modeling in Computer Graphics. Tokyo, Japan, 1991: 321-328
[7] Pang Y J, Zhong H X. Drawing Chinese traditional painting by computer// Proc. IFIP WG5. 10 Working Conference on Modeling in Computer Graphics. Tokyo, Japan, 1991: 321-328
[8] 王相海, 庞云阶. 模拟绘画的三维几何纹理生成研究. 计算机学报, 2002, 25(9): 982-986

(上接第 208 页)

别进行了不同质量因子的压缩后，再分别进行信息提取。图 6 给出了质量因子为 90, 75, 60, 50 压缩后的实验结果，实验结果表明，在图像质量已经严重失真的情况下，仍然能提取出信息，可见该算法具有较好的抗压缩的性能。



(a) Quality=90　　(b) Quality=75



(c) Quality=60　　(d) Quality=50

图 6　图像 JPEG 压缩攻击示例

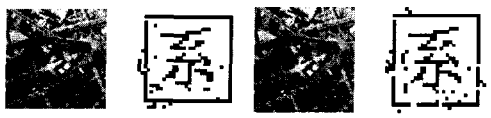
(2)中值滤波

中值滤波是把数字图像或数字序列中的一点的值用该点的一个窗口(window)中心的像素值代换。图 7 给出了中值滤波后的隐秘图像以及恢复的秘密图像。

图 7　5×5 中值滤波攻击示例

(4)加噪攻击

图 8 是分别在含密图像中加入乘性噪声、高斯噪声，然后提取秘密图像。可以看出，在加入随机噪声后，仍能很好地提取秘密信息。



(a)乘性噪声 0.01　　(b)高斯噪声 0.01

图 8　加噪攻击示例

结束语　基于直接位平面替换的 LSB 算法可有效实现信息隐藏，较传统 LSB 算法相比较，具有以下特点：

(1) 隐蔽性强。由于考虑到了图像中相邻像素间灰度值的变化差异，选择了像素间灰度值变化大的分块嵌入较多的信息，而像素间灰度值变化小的分块嵌入较少的信息。隐藏图像与载体图像相比较，像素间灰度值变化大的分块，每字节的值最大变化 3，该字节代表的像素最多只变化了 3/256，而像素间灰度值变化小的分块，每字节的值最大变化 1，该字节代表的像素最多只变化了 1/256，这样的变化不会引起视觉差异。

(2) 信息嵌入量高。在像素间灰度值变化大的分块中，用秘密信息的 2 位来替换掉各个像素的最低 2 位，大大提高了信息的嵌入量。

(3) 抗干扰性好，对 JPEG 压缩、加噪、中值滤波等操作有良好的适应特性。

(4) 嵌入效率高。若秘密图像有 N 个字节，对每个字节将有 7 次异或运算，时间复杂度为 $O(7N)$；而本文提出的改进算法进行信息的隐藏与提取，秘密图像的每个字节将有 1 次异或运算，时间复杂度为 $O(N)$。

参 考 文 献

[1] Katzenbeisser S, Petitcolas F A P. Information Hiding Techniques for Steganography and Digital Watermarking[M]. Artech House, Inc, 2004
[2] Lu C S, Liao H Y. Multipurpose watermarking for image authentication and protection. IEEE Transaction on Image Processing, 2001, 10(10): 1579-1592
[3] Queluz M P. Content-based integrity protection of digital images //Proceedings of SPIE: Security and Watermarking of Multimedia Contents I. 1999, 3657: 85-93
[4] 徐献灵, 崔楠. 信息隐藏技术及其应用[J]. 信息安全, 2007, 3: 27-30
[5] 高明, 陈丹, 王育民. 一种改进的空域 LSB 掩密算法[J]. 网络安全技术与应用, 2004, 8: 34-36
[6] 郑婷婷, 叶哲江, 戚勇. DES 数据加密算法的研究及其 matlab 实现[J]. 信息通信, 2007, 5: 48-60
[7] 徐江峰, 李昊, 杨有. 一种基于多变换的 LSB 隐写算法. 计算机科学, 2007, 34(10): 106-109