一种新的数据隐藏方法

田 源,程义民,王以孝
(中国科学技术大学电子科学与技术系,安徽合肥 230026)

摘 要: 本文提出一种新的数据隐藏方法,对于给定长为 n 比特的可修改宿主数据流,至多修改 1 比特宿主数据,可嵌入 $\log_2(n+1)$ 比特的数据. 嵌入/提取矩阵 H,还可作为密钥,使得嵌入数据具有较好的安全性. 该方法已在微机上进行了模拟,获得了预期的结果.

关键词: 数据隐藏; 嵌入/提取矩阵; 加密; 多媒体
中图分类号: TN918 **文献标识码**: A **文章编号**: 0372-2112 (2004) 09-1444-04

A Novel Method of Data Hiding

TIAN Yuan, CHENG Yi-min, WANG Yi-xiao
(Dept. of Electronic Science and Technology, University of Science and Technology of China, Hefei, Anhui 230026, China)

Abstract: This paper presents a novel data hiding method for concealing a piece of critical information in a host message. Given a host data stream of n bits size, the proposed method can embed as many as $[\log_2(n+1)]$ bits of data by changing, at most, one bit in host data stream. The matrix H for embedding and extracting data can also be used as a secret user key, which provides a higher security of the hidden data. With the proposed method, we gain satisfactory simulation results on PC.

Key words: data hiding; embedding-extracting matrix; encrypt; multimedia

1 引言

数据隐藏是近几年迅速发展起来的一个新兴技术领域[1],随着网络、多媒体和信息技术的迅速发展,以数字水印[2~4]和机密信息的隐秘传输[5~7]为代表的数据隐藏技术越来越多的应用于多媒体信息的版权保护及信息安全等领域.

对于声音、图像、视频等多媒体数字信息,常在对人听觉、视觉及侦测不敏感的数字段,选择适当的数位,生成可修改宿主二进制数据流,将待隐藏信息嵌入该数据中可有效提高隐秘性.

在一定长度的可修改宿主二进制数据流中,修改尽可能少的比特数,来嵌入尽可能多的信息数据是数据隐藏方法研究的重要目标之一. 通常的方法,如文献[8,9]中使用的奇偶调制法,要嵌入 1 比特信息,就选择宿主数据中 1 个比特(或一个象素)位来进行嵌入,这样,嵌入 1 比特信息时,至多修改 1 比特宿主数据(取反或不变). 2002 年,Tseng 等人给出了一种新颖的数据隐藏方法[10],可在长为 n 比特的可修改宿主数据中嵌入 $[\log_2(n+1)]$ 比特数据([*]表示取整数部分),最多只要修改 2 比特宿主数据,该方法大大提高了隐藏信息的有效性和隐秘性.

本文提出了一种新的算法,可在长为 n 比特的可修改宿主数据中嵌入 $[\log_2(n+1)]$ 比特数据最多只要修改 1 比特的宿主数据. 因此,在相同数据嵌入量的情况下,本文的算法对宿主数据的修改量更小,有更高的数据嵌入率和更好的隐秘性.

该方法已在计算机上进行了模拟,对文字、声音、图像等信息的隐藏实验获得了预期的结果.

2 数据嵌入/提取算法

这一部分将给出在任意长为 n 比特的可修改宿主数据中,至多修改 1 比特数据来嵌入 $\log_2(n+1)$ 比特信息数据的方法,先讨论 $n=2^m-1$ (m 为正整数)的情况.

2.1 输入输出表示

设 $a=(a_1,a_2,a_3,\cdots,a_n)$ 为信息数据嵌入前,n 比特可修改宿主数据组成的 n 维行向量; $r=(r_1,r_2,r_3,\cdots,r_n)$ 为信息数据嵌入后生成的宿主数据组成的 n 维行向量; $c=(c_1,c_2,c_3,\cdots,c_m)$ 为待嵌入信息数据组成的 m 维行向量,即需要隐藏的信息. 在数据嵌入/提取过程中还要用到 n 维加密密钥流行向量 $k=(k_1,k_2,k_3,\cdots,k_n)$ 和嵌入/提取矩阵 $H=(h_1,h_2,h_3,\cdots,h_n)_{m\times n}$.

其中行向量 k 是从用户密钥经非线性运算生成的二进制加密密钥流中截取的 n 比特密钥流组成的. 而嵌入/提取矩阵 H 中的列向量 $h_i=(h_{1i},h_{2i},h_{3i},\cdots,h_{mi})^T$ 满足:

$$(h_{1i},h_{2i},h_{3i},\cdots,h_{mi})_{(10)}=i,\quad 1\le i\le n \tag{1}$$

式中 $(h_{1i},h_{2i},h_{3i},\cdots,h_{mi})_{(10)}$ 表示由 $h_{1i},h_{2i},h_{3i},\cdots,h_{mi}$ 组成的二进制数对应的十进制数值,即 $h_1=(0,0,\cdots,1,0)^T$、$h_2=(0,0,\cdots,1,0)^T$、$\cdots$、$h_{(n-1)}=(1,1,\cdots,1,0)^T$、$h_n=(1,1,\cdots,1,1)^T$, $(h_{1i},h_{2i},h_{3i},\cdots,h_{mi})_{(10)}$ 也可简记为 $(h_i)_{(10)}$. h_1、h_2、$\cdots$、h_n 分别为 H 的第 1 列、第 2 列、$\cdots$、第 n 列. 例如:当 $n=15$, $m=4$ 时, H 矩阵为一个 4 ×15 矩阵:

收稿日期:2003-06-16;修回日期:2004-03-29

$$H=\begin{pmatrix}0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\end{pmatrix}_{4\times 15} \tag{2}$$

2.2 算法原理

对任意给定的 n 维宿主行向量 $a=(a_1,a_2,a_3,\cdots,a_n)$ 和满足式(1)的 $m\times n$ 矩阵 H,计算 Ha^T 可以得到一个 m 维列向量,令

$$s^T=Ha^T=\begin{pmatrix}(h_{11}\,h_{12}\cdots h_{1n}) & a^T\\(h_{21}\,h_{22}\cdots h_{2n}) & a^T\\\cdots & \cdots\\(h_{m1}\,h_{m2}\cdots h_{mn}) & a^T\end{pmatrix}=\sum_{i=1}^{n}a_i h_i$$

其中 s 为一 m 维行向量,上标"T"表示转置运算,"$\sum$"为模 2 加运算(下同).

对任意给定的 m 维待嵌信息行向量 $c=(c_1,c_2,c_3,\cdots,c_m)$,它和行向量 s 的差值向量设为 d,即 $d=c\oplus s=(c_1\oplus s_2,c_2\oplus s_2,\cdots,c_m\oplus s_m)$. 若 $d=0$,则说明 $c=s$,此时不需对宿主向量进行修改,即 $r=a$,这时有 $c=rH^T$;若 $d\neq 0$,则列向量 d^T 一定可以在 H 矩阵列向量中找到,因为 H 矩阵有 $n=2^m-1$ 个 m 维列向量,这些列向量各不相同且不含有零向量. 又根据式(1)可知,该向量是 H 矩阵的第 $d=(d)_{(10)}$ 列,即 $h_d=d^T$. 将宿主行向量 a 的第 d 位取反,得到嵌入后向量 r,即:

$$r_i=\begin{cases}a_i, & i\neq d\\ \overline{a_i}=1\oplus a_i, & i=d\end{cases}$$

这时,计算 Hr^T 可得:

$$Hr^T=\sum_{i=1}^{n}r_i h_i=\sum_{i=1}^{d-1}a_i h_i\oplus[(1\oplus a_d)\,h_d]\oplus\sum_{i=(d+1)}^{n}a_i h_i=h_d\oplus\sum_{i=1}^{n}a_i h_i=d^T\oplus s^T=c^T$$

也即 $c=rH^T$. 因此从上面分析可以知道,无论 d 是否为零向量,均有 $c=rH^T$;而从向量 a 变成向量 r 最多只需将向量 a 其中 1 位取反即可.

为了使数据隐藏后有一定的安全性,可在嵌入过程中进行加密,加密可以有下面两个方面:

(1)对信息数据进行加密. 此时可以使用任何一种密码学中的加密方法,将其加密成二进制密文数据流,然后对密文数据进行嵌入;接收方在提取出隐藏的密文数据后,对密文数据进行解密,即可得到明文信息数据.

(2)对宿主数据进行加密. 可以在嵌入过程中引入加密密钥流向量 k,设 $b=a\oplus k$,可将 b 看成加密宿主向量进行嵌入,从上面的分析可以知道,b 最多只需将其中 1 位取反即可,不妨设是第 d 位$(1\le d\le n)$,也就是 a 的第 d 位取反,也即 $\overline{a_d\oplus k_d}$ 变成$\overline{a_d\oplus k_d}$,又:

$$\overline{a_d\oplus k_d}=(1\oplus a_d)\oplus k_d=1\oplus(a_d\oplus k_d)=\overline{a_d\oplus k_d},$$

上式表明,对 a 的第 d 位取反,也即对 b 的第 d 位取反. 因此,将 a 的第 d 位取反得到 r 后,提取时计算 $(r\oplus k)\,H^T$ 即可得到嵌入向量 c.

2.3 嵌入/提取步骤

数据嵌入步骤如下:

(1)计算校验向量 $s^T=H(a\oplus k)^T$; (3)

(2)计算误差向量 $d=c\oplus s$;

(3)若 $d=0$,则不需对宿主数据进行任何修改,即 $r=a$;若 $d\neq 0$,令 $d=(d)_{(10)}$,将向量 a 中的第 d 位取反即为 r.

例如 $n=15$ 时,宿主数据向量 $a=(0,0,1,0,1,1,0,0,1,0,1,0,0,0,0)$,密钥向量 $k=(1,0,0,0,1,1,0,1,1,1,1,1,0,1,0)$,则 $a\oplus k=(1,0,1,0,0,0,0,1,0,1,0,1,0,1,0)$,嵌入/提取矩阵 H 如(2)所示,则校验向量 $s^T=\sum_{i=1}^{n}(a_i\oplus k_i)\,h_i$,即:$s=(0,0,1,0)$. 若此时待嵌入的数据向量 c 也为$(0,0,1,0)$,则误差向量 $d=0$,则宿主数据向量 a 不需进行任何修改;若待嵌入的数据向量为其它值,例如 $c=(0,1,1,1)$,则误差向量 $d=(0,1,0,1)$,这时 $d=(d)_{(10)}=5$,表明将宿主向量 a 的第 5 位数据进行修改,即把 1 改为 0 即可,得到隐藏 4 比特数据后的宿主向量 $r=(0,0,1,0,0,1,0,0,1,0,1,0,0,0,0)$.

数据提取过程只需计算下式即可:

$$c=(r\oplus k)\,H^T \tag{4}$$

例如接收方得到向量 $r=(0,0,1,0,0,1,0,0,1,0,1,0,0,0,0)$,用密钥生成解密密钥向量 $k=(1,0,0,0,1,1,0,1,1,1,1,1,0,1,0)$,则 $r\oplus k=(1,0,1,0,1,0,0,1,0,1,0,1,0,1,0)$,再计算$(r\oplus k)\,H^T$ 提取出信息 $c=(0,1,1,1)$.

从嵌入算法第 3 步可知整个嵌入过程中,$n$bit 的宿主数据最多只需进行 1bit 的修改,即可嵌入 $m=\log_2(n+1)$ bit 的信息数据.

3 $n\neq 2^m-1$ 的情况及 H 矩阵的讨论

上面给出在 $n=2^m-1$ 时,至多修改 1 比特宿主数据来嵌入 $\log_2(n+1)$ 比特信息数据的算法步骤;对于 $n>2^m-1$ 时,一个简单的方法就是从 $n$bit 中任选 2^m-1 比特作为宿主数据,其中 $m=[\log_2(n+1)]$,这样即可嵌入$[\log_2(n+1)]$bit 的信息数据. 另一种方法,可对 H 矩阵进行修改,此时,H 矩阵需要满足如下关系:

(1) H 矩阵是一个 $m\times n$ 矩阵;

(2) H 矩阵所有列向量 h_i 对应的十进制数$(h_i)_{(10)}$组成的集合满足:$\{1,2,\cdots,2^m-1\}$中每个元素至少在该集合中出现一次,即 n 个列向量中,满足上述条件的每一列向量至少有一个.

这样,嵌入/提取算法步骤要略作修改,只需将数据嵌入过程中第 3 步 $d\neq 0$的情况修改成:查找和向量 d 相等的 h_i 在矩阵 H 中的位置,然后将宿主向量 a 中的相应位置数据取反即为 r. 同样提取时计算出 r 的校验向量为 $s\oplus d$,由于 $d=c\oplus s$,所以 r 的校验向量值为 c.

从上面的分析知道,H 矩阵可以有许多种选择,从而 H 矩阵也可作为一个用户密钥. 若宿主数据长为 $n(n>2^m-1)$ 比特,待隐藏数据长为 m 比特,H 矩阵约有 $C_n^{2^m-1}\times(2^m-1)!\times(2^m-1)^{(n-2^m+1)}$ 种选择,其中 $m=[\log_2(n+1)]$. 若 $n=2^m-1$,则 H 矩阵有 $(2^m-1)!$ 种选择.

4 实验及结果

为了验证上述方法,我们将其应用到以二值图像和视频为宿主的数据隐藏方法中,并在微机上进行了模拟,获得了预期的结果,下面给出部分实验结果.

4.1 二值图像隐藏汉字

图 1 给出了将上述方法应用于二值图像隐藏汉字的实验结果,其中图 1(*a*)是原始二值图像,大小为 240 ×288,在对宿主图像进行数据隐藏时,以正方形图像块为单元进行嵌入. 为了有较好的主观图像质量,对所有象素为全黑或全白的正方形单元块,不进行数据嵌入,接收方接收到数据后,将认为全黑或全白的单元块不隐藏有数据. 同时考虑到,在数据隐藏过程中,单元块可能在修改 1 个象素后变成全黑或全白,这时,该单元块作为未隐藏数据块,将其变成全黑或全白的图像块,这样可保证提取时数据正确.

图 1(*b*)和(*c*)分别是以 3 ×3 象素块和 4 ×4 象素块为单元进行数据嵌入后得到的图像. 其中图 1(*b*)中隐藏了 94 个汉字,对原始图像 437 个象素进行了的修改,平均修改一个象素嵌入 3.47 比特的数据;图 1(*c*)则隐藏了 95 个汉字,对原始图像 359 个象素进行了修改,平均修改一个象素嵌入 4.23 比特数据.

图 1 二值图像数据隐藏结果

表 1 二值图像数据隐藏实验相关数据

二值图像	图像大小	单元块大小	嵌入数据量/bits	修改象素数	提取正确率/%
1 cards	168 ×176	4 ×4	1432	329	100
		8 ×8	714	117	100
2 logo	336 ×336	4 ×4	1940	454	100
		8 ×8	1764	290	100
3 mickey	584 ×544	4 ×4	12432	2911	100
		8 ×8	7266	1189	100

我们对其它图像进行了实验,部分实验相关数据如表 1 所示. 其中因为没有考虑隐藏有信息的图像在传输过程中的噪声影响问题,所以提取正确率均为 100 %.

4.2 视频中隐藏彩色图像

图 2 给出了在 MPEG-2 视频中隐藏彩色图像的实验结果,数据嵌入过程中以一个 8 ×8 图像块为单元进行嵌入,数据嵌入到图像块 DCT 域的中频部分,每个图像块最多修改一个中频系数的最低位. 实验所用视频是从 MPEG 官方网站下载的测试视频. 图中给出了在 Susi_080 视频中隐藏 Lena 彩色图像的实验结果. Susi_080 视频每帧大小为 704 ×480,共 450 帧,其中图 2(*a*)是未隐藏信息时三帧原始视频图像,图 2(*b*)是隐藏信息后相应的视频帧. 图中可见,隐藏信息前与隐藏信息后视频图像人眼很难分辨出差异. 图 3(*a*)是隐藏的原始彩色图像,图 3(*b*)是提取出的彩色图像,这里因为没有考虑噪声等影响,原始彩色图像和提取出的图像完全相同(实验用的图像和视频均为彩色,为印刷方便,这里给出的是相应的灰度图像,下同).

图 2 原始视频帧和隐藏数据后视频帧的比较

图 3

表 2 给出了不同码率下三个视频的实验结果. 从实验数据可知,该方法具有较高的平均 PSNR,这是因为在数据嵌入过程时对每个视频图像块的修改量都很小;同时,数据嵌入码率也较高,算法在修改量很小的情况下仍然可以嵌入较多的数据. 所有实验因没有考虑噪声及远距离传输对数据的影响,其正确提取率均为 100 %,未在表中列出.

4.3 视频中隐藏声音数据

图4是视频图像中隐藏声音数据的实验结果,数据嵌入

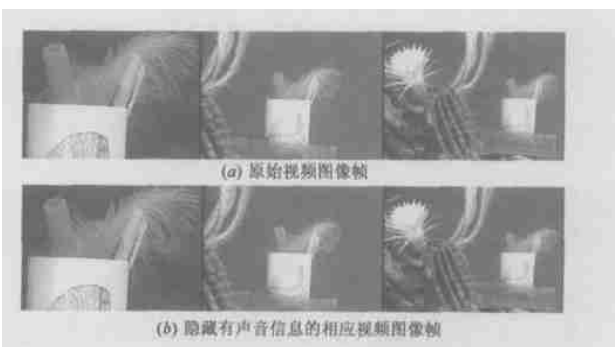

图 4 原始视频帧和隐藏数据后视频帧的比较

方法和嵌入彩色图像时相同. 图中所示是 Cact. 060 视频中隐藏声音的实验结果,所隐藏的音频是 mpeg-2 格式的音频. Cact. 060 视频每帧大小为 704 ×480,共 450 帧,其中图 4(a)是未隐藏信息时三帧原始视频图像,图 4(b)是隐藏信息后相应的视频帧.

表 3 给出了不同码率视频中隐藏声音的实验结果.

5　结论

本文提出了一种新的数据隐藏算法,该算法可以实现在任意长为 n 比特的宿主数据中嵌入 $\lfloor \log_2(n+1) \rfloor$ 比特的数据而最多只要修改 1 比特的宿主数据. 因此,在嵌入量一定的情况下,该算法有着更好的隐秘性及更高的数据嵌入率. 算法在嵌入过程中可对待隐藏信息数据和宿主数据进行加密,H 矩阵也可作为一个密钥,使得隐藏的数据具有较好的安全性.

该方法已在计算机上进行了模拟,对文字、声音、图像等多种信息隐藏在二值图像、视频等信息中的实验表明,该方法嵌入/提取步骤简单有效,有较好的效果.

本文主要讨论信息隐藏方法,噪声及远距离传输对隐藏信息的影响尚待进一步研究.

表 2　不同视频隐藏图像实验相关数据

视　频	视频帧数	嵌入数据大小/ bits	平均数据嵌入码率/ Kbits/ s	原视频大小/ MB	嵌入数据后视频大小/ MB	平均 PSNR/ dB
Cact. 015(1.5Mbits/ s)	450	693691	46.2	2.68	2.71	46.60
Cact. 040(4.0Mbits/ s)	450	1623620	108.2	7.17	7.24	40.27
Cact. 080(8Mbits/ s)	450	4084070	272.3	14.3	14.4	41.05
Susi. 015(1.5Mbits/ s)	450	805519	53.7	2.68	2.71	45.07
Susi. 040(4.0Mbits/ s)	450	1779062	118.6	7.16	7.23	44.75
Susi. 080(8Mbits/ s)	450	4240152	282.7	14.3	14.4	43.77
Tens. 015(1.5Mbits/ s)	450	721451	48.1	2.68	2.71	40.86
Tens. 040(4.0Mbits/ s)	450	1816274	121.1	7.17	7.24	37.77
Tens. 080(8.0Mbits/ s)	450	3962435	264.2	14.3	14.4	39.57

表 3　不同视频隐藏声音实验相关数据

视　频	视频帧数	嵌入数据大小/ bits	平均数据嵌入码率/ Kbits/ s	原视频大小/ MB	嵌入数据后视频大小/ MB	平均 PSNR/ dB
Cact. 015(1.5Mbits/ s)	450	693691	46.2	2.68	2.71	40.00
Cact. 060(6.0Mbits/ s)	450	2835090	189.0	10.7	10.8	40.68
Cact. 080(8Mbits/ s)	450	4084070	272.3	14.3	14.4	40.97
Flwr. 015(1.5Mbits/ s)	450	759788	50.7	2.68	2.71	36.66
Flwr. 060(6.0Mbits/ s)	450	2999474	200.0	10.7	10.8	35.51
Flwr. 080(8Mbits/ s)	450	4047226	270.0	14.3	14.4	36.82
Mobl. 015(1.5Mbits/ s)	450	759626	50.6	2.68	2.71	35.15
Mobl. 060(6.0Mbits/ s)	450	2884672	192.3	10.7	10.8	34.93
Mobl. 080(8.0Mbits/ s)	450	3876885	258.5	14.3	14.4	36.14

参考文献:

[1] F A P Petitcolas, R J Anderson, M G Kuhn. Information Hiding ——A Survey[J]. Proceedings of the IEEE, 1999, 87(7): 1062 - 1078.

[2] D Kirovski, H S Malvar. Spread-spectrum watermarking of audio signals [J]. IEEE Transaction on Signal Processing, 2003, 51(4): 1020 - 1033.

[3] J A Bloom, I J Cox, et al. Copy protection for DVD video[J]. Proceedings of the IEEE, July 1999, 87(7): 1267 - 1276.

[4] 汪春生,程义民,王以孝. 一种基于块分类的自适应数字水印算法[J]. 计算机工程及应用, 2002, 38(21): 106 - 109.

[5] Gang Pan, Zhaohui Wu, Yunhe Pan. A data hiding method for few-color images[A]. Acoustics, Speech, and Signal Processing, Proceedings[C]. Orlando, Florida: IEEE, 2002, 4. IV-3469 - IV-3472.

[6] J Chou, K Ramchandran, A Ortega. High capacity audio data hiding for noisy channels[A]. Information Technology: Coding and Computing[C]. Las Vegas, Nevada: IEEE, 2001. 108 - 112.

[7] 陆红琳,程义民,王以孝,田源. 一种基于 ICA 的汉字信息隐秘传输方法[J]. 中文信息学报, 2003, 17(4): 59 - 65.

[8] R G van Schyndel, A Z Osborne. A digital watermark[A]. IEEE International Conferenca on Image Processing (Vol. 2)[C]. Austin, TX USA: IEEE, Nov 1994. 86 - 90.

[9] Min Wu, E Tang, B Lin. Data Hiding in digital binary image[A]. Multimedia and Expo, 2000[C]. New York: IEEE, 2000, 1. 393 - 396.

[10] Yu-Chee Tseng, Yu-Yuan Chen, Hsiang-Kuang Pan. A secure data hiding scheme for binary images[J]. IEEE Transactions on Communications, Aug 2002, 50(8): 1227 - 1231.

作者简介:

田　源　男,1980 年 10 月生于安徽和县,现为中国科学技术大学电路与系统专业硕士研究生,主要研究方向为信息隐藏.

程义民　男,1945 年 11 月生于陕西西安,1969 年毕业于中国科学技术大学无线电电子学系计算机专业,1984～1985 年英国 Hull 大学为访问研究员,现为中国科学技术大学教授,博士生导师,主要研究领域为信息隐藏、计算机视觉和网络多媒体技术等.