基于变步长量化的安全图像隐写

何军辉[1,2] 唐韶华[1] 邢宜博[1]
(华南理工大学计算机科学与工程学院 广州 510006)[1] (广东省信息安全技术重点实验室 广州 510006)[2]

摘 要 图像隐写通过将信息隐藏在载体图像中进行秘密传送,实现隐蔽通信。提出了VSQS图像隐写算法,利用密钥控制生成高斯序列并取整,用于对经伪随机排列后的图像像素进行变步长量化,根据量化像素与秘密信息之间的关系来修改像素,实现信息的嵌入。同时给出了该算法的一种扩展(称为TLQS隐写)。实验结果表明,VSQS和TLQS图像隐写可提供较大的隐藏容量,并能抵抗几种常见的隐写分析方法。

关键词 隐写术,高斯序列,量化,隐写分析
中图法分类号 TP391 **文献标识码** A

Secure Image Steganography Based on Step-varying Quantization

HE Jun-hui[1,2] TANG Shao-hua[1] XING Yi-bo[1]
(School of Computer Science and Engineering, South China University of Technology, Guangzhou 510006, China)[1]
(Guangdong Key Laboratory of Information Security Technology, Guangzhou 510006, China)[2]

Abstract Image steganography transfers message secretly by embedding the message into a cover image to implement covert communication. We presented an image steganographic algorithm called VSQS. A secret key dependent Gaussian sequence was generated and then rounded, which is used for the step-varying quantization of the pseudo-random permuted image pixels. Depending on the relationship between the quantized pixels and the secret message, the image pixels were modified to embed the message. Furthermore, an extension of this algorithm(called TLQS) was presented. Experimental results show that both the VSQS and TLQS image steganographic techniques may provide higher capacity and be resistant to several well-known steganalytic methods.

Keywords Steganography, Gaussian sequence, Quantization, Steganalysis

1 引言

多媒体(图像、音频和视频等)和互联网应用的不断普及,给人们的生活带来了诸多方便和快捷。互联网可能被用于私人秘密、商业文档和军事情报等涉密信息的传送,如何有效防止信息被窃听、盗用、篡改,保证通信安全,就成为需要首先解决的问题。

密码技术是一种用于解决通信安全的传统手段。但由于加密是通过把明文内容转换为密文来隐藏通信内容,难以掩盖通信发生的事实,而密文的传输易引起敌人或第三方的怀疑,进而可能被截获、攻击(如干扰或破坏通信设施)或破译。为了弥补密码技术隐蔽性的不足,近年来出现了一种新的通信安全技术——隐写术[1],并越来越受到学术界和工业界的重视。隐写术是信息隐藏的一个分支,通过将通信内容秘密地隐藏在公开载体媒体中进行传送,以掩盖真正的通信目的和通信发生的事实。

基于随机或连续替换的LSB(Least Significant Bit)隐写是一种相对简单的隐写算法,但在隐写术的发展中有着重要的地位。LSB隐写可达到的嵌入容量为1 bpp(bits per pixel)。互联网上许多可自由下载的隐写软件都可以归为此类,例如Steghide, S-Tools, Jsteg, Jphide, HIP和HideSeek等[2]。针对LSB隐写的攻击研究和分析比较多,典型的有χ^2统计检测[3]、广义χ^2统计检测[4]、RS方法[5]等,这些隐写分析算法可不同程度实施对LSB隐写的检测和攻击。隐写分析研究的深入,不断促进隐写术的改进和发展。文献[6]对传统LSB隐写进行了改进,提出了一种可抵抗RS检测的LSB隐写算法。为了避免给掩密图像直方图带来明显的"值对"现象,研究者T. Sharp提出了Hide隐写[7],该隐写术采用"±1"操作替换传统LSB隐写的翻转操作,抗检测性能得到了改善,但是由于在嵌入过程中会跳过某些可能会发生溢出的像素,其隐藏容量有所降低(一般小于1bpp)。此外,J. Fridrich也提出了一种称为随机调制的隐写算法[8],该算法通过在载体图像中嵌入与之相互独立并服从高斯分布的噪声来隐藏秘密消息。但随机调制隐写的隐藏容量一般建议不超过0.8bpp,因为要实现更大的隐藏容量,必须增大隐写噪声方差,而较大的隐写噪声方差可能会给载体图像带来明显的视

到稿日期:2008-08-07 返修日期:2008-11-13 本文受广东省信息安全技术重点实验室基金(2006年度),国家大学生创新性实验计划(071056146)和华南理工大学SRP项目(Y1080280)资助。
何军辉(1976-),博士,讲师,主要研究方向为信息安全与多媒体技术,E-mail:hejh@scut.edu.cn;**唐韶华**(1970-),博士,教授,主要研究方向为信息安全;**邢宜博**(1988-),本科生。

觉失真。

本文提出一种基于变步长量化的图像隐写算法(Variable Step Quantization Steganography,下面简称为 VSQS 隐写),该隐写算法通过利用近似服从高斯分布的量化步长进行量化嵌入。同时给出了 VSQS 隐写算法思想的一种扩展,即采取两级量化模式得到 TLQS 隐写(Two Level Quantization Steganography)。通过实验对 VSQS 和 TLQS 隐写容量和安全性进行了深入分析和讨论,结果表明这两种算法可提供较大的隐藏容量,并且能有效抵抗常见的几种隐写分析方法。

2 VSQS 隐写算法

2.1 量化步长

假定载体图像为 8 比特 $M\times N$ 灰度图像并记为 $C_{i,j}$,其中 $C_{i,j}\in\{0,1,\cdots,255\}$,$i=1,2,\cdots,M$,$j=1,2,\cdots,N$。首先用密钥控制生成一个服从高斯分布 $N(0,\sigma)$的序列 S_l,$l=1,2,\cdots,L$,其中 L 为高斯序列的长度,然后对所生成的高斯序列取整,可得一个近似服从高斯分布的整数序列 Z_l,$l=1,2,\cdots,L$。高斯序列长度 L 与秘密信息长度 p(bpp)之间近似满足下式:

$$L\approx Round\left(\frac{p\times M\times N}{1-\mathrm{erf}\left(\frac{1}{2\sqrt{2}\sigma}\right)}\right)$$

$$\text{其中 erf}(x)=\frac{2}{\sqrt{\pi}}\int_0^x \mathrm{e}^{-t^2}\,\mathrm{d}t \tag{1}$$

2.2 嵌入和提取

对下标 $1,2,\cdots,M\times N$ 进行密钥控制的伪随机排列,可得新序列 $P_u\in\{1,2,\cdots,M\times N\}$,$u=1,2,\cdots,M\times N$。用序列 P_u 对载体图像像素进行伪随机排列,得到 I_v,$v=1,2,\cdots,M\times N$。顺序读入高斯整序列 Z_l、秘密信息序列 m_w($w=1,2,\cdots,p\times M\times N$)和载体图像像素伪随机排列序列 I_v,根据量化取整像素的 LSB 位与秘密信息是否相同来对像素进行更改,得到掩密图像像素序列 I_v',逆伪随机排列得到掩密图像 $S_{i,j}$。提取时,基本上按照嵌入逆过程来进行:生成相同的伪随机排列序列 P_u,用来对掩密图像进行伪随机排列。提取伪随机排列像素经过量化取整后的 LSB 位,即得所隐藏的秘密信息序列。VSQS 隐写算法嵌入和提取流程如图 1 所示,其中 $LSB(x)$表示取 x 的 LSB 位,$[x]$是对 x 取整。

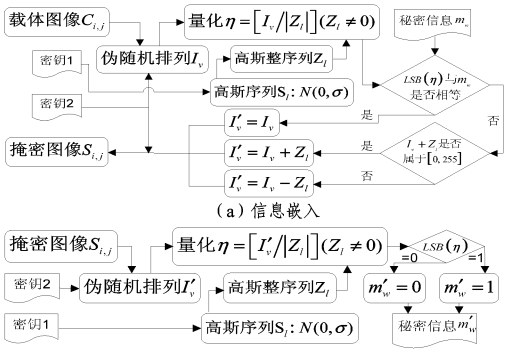
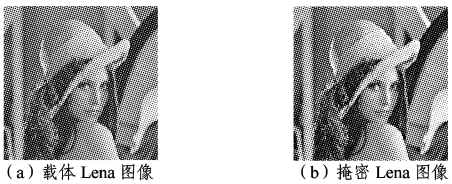


图 1 VSQS 隐写算法流程

2.3 容量与失真

采用 VSQS 算法在 128×128Lena 图像中嵌入 1 bpp 的秘密信息,所使用的高斯噪声序列的方差为 1,即 $p=1,\sigma=1$,结果如图 2 所示。可以看出,掩密图像的失真不是很明显。



(a) 载体 Lena 图像　　(b) 掩密 Lena 图像

图 2 VSQS 隐写前后图像($p=1,\sigma=1$)

从式(1)可以看出,VSQS 隐写隐藏容量取决于高斯序列的方差及其长度。一方面,可使方差保持不变,通过调整高斯序列长度来改变 VSQS 隐写的隐藏容量;另一方面,也可通过改变方差来对隐藏容量进行调整。但是方差的增大势必给图像带来更大的失真(我们在实验中发现,当 $\sigma^2=9$,$p=1$ 时,8 比特 128×128Lena 图像平滑区域的失真已经变得比较明显)。

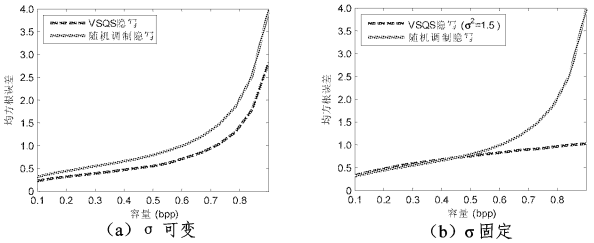
为了衡量由隐写造成的图像失真与高斯序列方差之间的关系,选用掩密图像和载体图像之间的均方根误差(RMS Error)作为标准。均方根误差定义为

$$e=\sqrt{\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(C_{ij}-S_{ij})^2} \tag{2}$$

对下面两种情形中均方误差与隐藏容量之间的变化关系进行了实验,并与随机调制隐写进行了比较。

(a)通过改变高斯序列方差来调整隐藏容量,使 VSQS 隐写所用高斯序列方差与随机调制隐写高斯噪声方差保持一致,实验结果如图 3(a)所示。

(b)保持 VSQS 隐写中高斯序列方差不变($\sigma^2=1.5$),通过调整高斯序列长度来调整隐藏容量,实验结果如图 3(b)所示。



(a) σ 可变　　(b) σ 固定

图 3 VSQS 隐写隐藏容量与均方根误差失真

从图 3(a)可看出,当 VSQS 隐写和随机调制隐写隐藏容量和高斯序列方差一致时,VSQS 隐写带来的图像失真略小一些。从图 3(b)可看出,当需要达到较大的隐藏容量(如 0.8bpp以上)时,VSQS 隐写带来的图像失真比随机调制隐写要小得多。

2.4 TLQS 隐写算法

TLQS 隐写算法对载体图像进行两级量化,量化步长依次为高斯序列和常数 2,实现了每像素 2 比特的嵌入容量(即 2 bpp)。TLQS 隐写算法与 VSQS 隐写算法类似,在进行秘密信息嵌入的时候,首先利用高斯整序列取值对伪随机排列图像像素进行量化,根据像素第一次量化取整后的 LSB 位与二进制秘密信息比特位是否吻合以及第二次量化取整后的 LSB 位与下一消息比特位的匹配情况,对图像像素进行修改,实现秘密信息的嵌入。

提取时,先产生与嵌入时相同的高斯整序列,用高斯整序列对像素进行第一次量化,提取像素量化取整后的 LSB 位,即可得到 1 位秘密信息比特。然后将第一次量化的结果再用

常数 2 进行第二次量化，提取量化取整后的 LSB 位，可得到另外 1 位秘密信息比特，从而从 1 个像素提取 2 比特信息。

3 讨论分析

与数字水印着重考虑鲁棒性以对抗各种可能的主动攻击不同，隐写术的重点是如何实现信息伪装，使攻击者难以知道秘密信息的存在。一般来说，隐写的主要要求包括不可见性、抗检测性和隐藏容量，其中不可见性是隐写的基本要求，是指在图像、音频或视频等载体媒体中嵌入秘密信息后，并不引起载体媒体主观质量的明显下降，从而不易被察觉。从前面实验已知 VSQS 隐写满足这一基本要求(如图 2 所示)。下面对 VSQS 隐写和 TLQS 隐写的隐藏容量和安全性进行讨论。

3.1 隐藏容量

隐藏容量是隐写的实用要求，隐藏量太小的隐写意义不是很大。传统 LSB 替换隐写隐藏容量可达 1 bpp，而 Hide 隐写在嵌入过程中会跳过发生溢出的像素，隐藏容量一般小于 1 bpp。随机调制隐写的隐藏容量分为两种情况：(a)使用 1 个高斯序列，其容量记为 c_1；(b)使用 2 个高斯序列，其容量记为 c_2，根据文献[8]可知：

$$c_1=1-\mathrm{erf}\frac{1}{2\sqrt{2}\sigma},c_2=1-\mathrm{erf}\frac{1}{4\sigma} \tag{3}$$

从上式和图 3(b)可以看出，对随机调制隐写来说，为了获得较大的隐藏容量，需要明显增加高斯噪声的方差。而当隐藏容量达到一定数值时(0.8 bpp 以上)，方差的较大增加并不能给随机调制隐写隐藏容量带来明显的升高，这与随机调制隐写作者在文献[8]中建议不超过 0.8 bpp 是吻合的。

VSQS 隐写：由于采用变步长量化取代随机调制隐写的特殊奇偶函数来实现秘密信息的嵌入，使得隐藏容量不仅与高斯序列方差有关，还受高斯序列长度的影响。这可以从图 3(b)看到：虽然高斯序列方差保持不变($\sigma^2=1.5$)，但可通过增加高斯序列长度获得较大的隐藏容量(可达 1 bpp)，而对图像带来的失真只是很少的增加，肉眼难以察觉。

TLQS 隐写：是对 VSQS 隐写算法思想的扩展，采取两级量化模式，进一步提高了 VSQS 隐写算法的隐藏容量，最大可达 2 bpp，且不会给图像带来明显的失真。

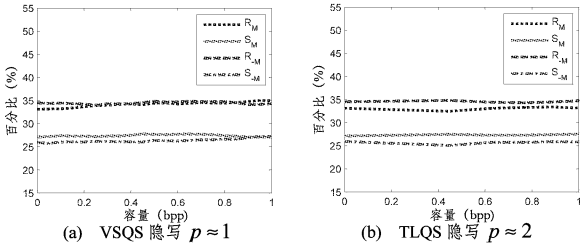
3.2 安全性

隐写的安全性首先体现为抗检测性，是隐写术的核心要求。如果第三方或监控者能以较高的概率(>50%)判断掩密图像中秘密信息的存在性，则所对应的隐写算法被认为失效。下面对 VSQS 隐写和 TLQS 隐写在面临常见的几种隐写被动攻击时的安全性进行分析。

3.2.1 RS 检测

一般来说，自然灰度图像相邻像素之间具有较强的相关性。对空域 LSB 替换隐写来说，所隐藏的秘密信息与载体图像互相独立，并且消息比特之间可认为不具有相关性，因此 LSB 隐写会削弱或破坏载体图像像素值之间的相关性。RS (Regular & Singular Groups)检测算法利用此特性来检测图像中的秘密消息。该算法将图像像素按照某种方式进行分组(例如同一行上连续的 4 个像素)，借助统计判别函数和置换函数将图像像素组分为正常组、异常组和不变组 3 类。定义 R_M，S_M，R_{-M}，S_{-M}分别为正向模板、负向模板操作下正常组、异常组在所有像素组中所占的百分比例。自然载体图像的像素组存在近似关系：$R_M\cong R_{-M}$，$S_M\cong S_{-M}$，但是随着所嵌入秘密信息长度的增加，R_M，S_M，R_{-M}，S_{-M}之间的近似关系会被破坏，表现出与隐藏容量 p 相关的规律曲线(具体参见文献[5])，从而可通过曲线拟合的方法求解秘密信息长度。

为了检验 RS 算法对 VSQS 隐写和 TLQS 隐写的有效性，我们在实验中所采用的正向模板为 $M=[0,1,1,0]$和负向模板 $-M=[0,-1,-1,0]$，然后对 VSQS 和 TLQS 图像隐写算法生成的掩密图像都进行 RS 统计量计算，发现 R_M，S_M，R_{-M}，S_{-M}之间的分布不再满足 RS 检测算法的假设(如图 4(a)、(b)所示)，而与载体图像的近似关系($R_M\cong R_{-M}$，$S_M\cong S_{-M}$)基本吻合，因此可以推断 VSQS 和 TLQS 隐写对 RS 检测算法是安全的。



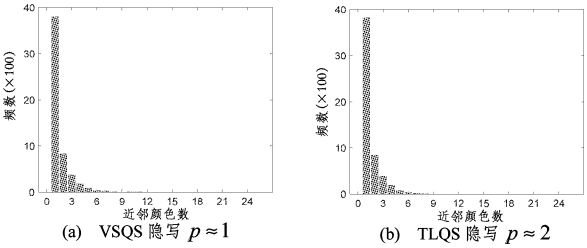
(a) VSQS 隐写 $p\approx1$　　(b) TLQS 隐写 $p\approx2$

图 4　VSQS 和 TLQS 掩密 Lena 图像 RS 统计量分布($\sigma=1$)

3.2.2 近邻颜色直方图分析

邻近颜色直方图分析方法[9]是 A. Westfeld 所提出的，可对“±1”模式隐写算法(如引言部分提到的 Hide 隐写)实施一定程度上的检测。而本文提出的两种基于高斯序列量化的 VSQS 隐写和 TLQS 隐写上对载体图像所带来的失真中，也是以“±1”为主的，因此有必要采取近邻颜色直方图分析方法对本算法进行安全性的分析。

近邻颜色直方图分析的基本思想是：LSB 隐写可使图像中每一种颜色最多产生 7 种近邻颜色(关于近邻颜色的定义参见文献[9])，而“±1”模式隐写可使每一种颜色最多产生 26 种近邻颜色。通常情况下，如果载体图像的原始格式是 JPEG 或中间存储经历过 JPEG 压缩(如将 TIFF/BMP 格式图像压缩成 JPEG 格式再解压缩成 TIFF/BMP 格式)，则载体图像中近邻颜色数不会太多，尽管不同的图像格式会有稍微的差异。如果采用“±1”模式隐写(如 Hide)在载体图像中嵌入一定量的秘密信息时，近邻颜色直方图会产生明显的“拖尾”现象，也就是说近邻颜色数大大增加。此外，文献[9]也提到，对灰度图像，可以将 3 个连续灰度值看作一种颜色的 3 个组件来进行近邻颜色分析。



(a) VSQS 隐写 $p\approx1$　　(b) TLQS 隐写 $p\approx2$

图 5　VSQS 和 TLQS 掩密 Lena 图像近邻颜色分布($\sigma=1$)

在实验中，我们首先利用 VSQS 和 TLQS 隐写在 128×128 灰度 Lena 图像中分别嵌入约 1bpp 和 2bpp(都是满容量)的秘密信息，嵌入过程中所使用的高斯序列方差等于 1。然后对所生成的掩密 Lena 图像进行近邻颜色数统计分析，得到

如图 5 所示的直方图。从图 5 可以看出，这两种算法都不存在明显的“拖尾”现象，可以预见本文提出的两种隐写算法能在一定程度上抵抗近邻颜色直方图分析方法的检测。

3.2.3 广义 χ^2 检测

χ^2 检测算法首先由 A. Westfeld 提出，可用于检测连续嵌入秘密信息的 LSB 隐写。后来 N. Provos 对该算法进行了扩展，能成功检测连续或随机嵌入秘密信息的 LSB 隐写，一般将其称为广义 χ^2 检测。广义 χ^2 检测算法能成功检测的基础是 LSB 类隐写算法在秘密信息嵌入过程中主要进行 0-1 “翻转”操作。因为“翻转”操作的存在，会给掩密图像像素直方图带来异常：“值对”之间出现的频数会随着消息的嵌入越来越接近。从本算法的嵌入思想可知，VSQS 和 TLQS 隐写的基本操作是对像素加减高斯整序列，不会产生明显的“值对”现象，从而可预见广义 χ^2 检测难以对 VSQS 和 TLQS 隐写实施成功的检测。

结束语 本文提出了一种基于高斯序列量化的图像隐写算法——VSQS，该算法可进一步扩展成 TLQS。对这两种隐写算法的隐藏容量和安全性进行了实验分析和讨论，结果表明，它们不仅可提供较大的隐藏容量（隐藏容量分别为 1 bpp 和 2 bpp），并且能有效抵抗几种常见的隐写分析方法。

在实验过程中发现，VSQS 和 TLQS 两种隐写算法虽然具有类似高斯噪声的失真，但由于加性高斯白噪声在自然图像中很常见，使其安全性得到一定程度的保证。但是当秘密信息嵌入量接近满容量时，在图像的平滑区域可能会产生比较明显的失真。这是由于这两种算法都没有充分利用载体图像本身的统计特性来进行自适应嵌入，使得对载体图像的更改可能发生在平滑区域。如何结合载体图像的统计特性进行隐写和盲提取，是今后的研究重点。

参 考 文 献

[1] Anderson R J，Petitcolas F A．On the limits of steganography [J]. IEEE Journal on Selected Areas in Communications，1998，16(4)：474-481

[2] Steganography Information，Software，and News to Enhance Your Privacy [URL]. http://www.stegoarchive.com

[3] Westfeld A，Pfitzmann A．Attacks on Steganographic Systems [C]// The Third International Workshop on Information Hiding. Dresden，Germany，September-October，1999：61-76

[4] Provos N，Honeyman P．Detecting Steganographic Content on the Internet [C]// BISOC NDSS'02. San Diego，CA，February 2002

[5] Fridrich J，Goljan M，Du R. Detecting LSB steganography in color and gray-scale images [J]. IEEE Multimedia，2001，8(4)：22-28

[6] 徐江峰，李昊，杨有．一种基于多变换的 LSB 隐写算法 [J]．计算机科学，2007，34(10)：106-109

[7] Sharp T．An Implementation of Key - based Digital Signal Steganography [C]// The 4th International Workshop on Information Hiding. LNCS 2137. Pittsburgh，PA，April 2001：13-26

[8] Fridrich J，Goljan M. Digital Image Steganography Using Stochastic Modulation [C]// Security and Watermarking of Multimedia Contents. SPIE 5020. 2003：191-202

[9] Westfeld A. Detecting Low Embedding Rates [C]// The 5th International Wokshop on Information Hiding. LNCS 2578. Noordwijkerhout，Netherlands，Oct. 2002：324-339

（上接第 41 页）

表 1 2-终端可靠性计算表

前栏包含节点、链路	Rel(G)
节点 1	50%
节点 1，2	25%
节点 1，2，3	12.5%
节点 1、2、3 和 4 及边{2，4}，不含链路{3，4}	12.5%
节点 1、2、3 和 4	31.25%
包含节点 1、2、3、4、6	28.13%
包含节点 1、2、7	29.29%

结束语 如果计算出每个网络设备的平均修复时间，就可以决定服务所需部分集合的大小和维护队列的大小。另一个发展方向是，在设备失效概率范围很大的情况下，计算尽可能接近的上下界，如果考虑到地面作业期间的网络行为，这一点很重要，因为这种情况下某些设备更没有保障。以上问题将是下一步重点完成的工作。尝试提出一套新型的网络可靠性测量与评价模型及方法，将对网络安全提供技术支撑，可视化的可靠性评估软件可被用于网络管理系统，提供直观的、动态的网络可靠性显示，对及时修复网络结构问题、提升网络节点的性能、合理部署网络节点，具有重要的指导意义。

参 考 文 献

[1] 郑龙，罗鹏程，周经伦．网络可靠性研究综述[J]．中国科技信息，2006(1)：9-11

[2] Gebre B，Ramirez-Marquez J. Element substitution algorithm for general two-terminal network reliability analyses[J]. IIE Transactions，2007，39(3)：265-275

[3] Satitsatian S，Kapur K. An algorithm for lower reliability bounds of multistate two-terminal networks[J]. IEEE Transactions on Reliability，2006，55(2)：199-206

[4] Galtier J，Laugier A，Ponst P. Algorithms to evaluate the reliability of a network[J]. IEEE Trans Reliab，2005：93-100

[5] Krivoulets V G，Polesskii V P．Monotone Structures．The Best Possible Bounds of Their Reliability[J]. Information Processes，Toml，2001，2：188-198

[6] Younes A，Girgis M. A tool for computing computer network reliability [J]. International Journal of Computer Mathematics，2005，82(12)：1455-1465