第 34 卷 第 2 期 计 算 机 工 程 2008 年 1 月
Vol.34 No.2 Computer Engineering January 2008
·安全技术· 文章编号：1000—3428(2008)02—0095—02 文献标识码：A 中图分类号：TP391

一种利用插值实现的信息隐藏方法

赵鸿冰[1]，林代茂[1,2]，郭云彪[2]
(1. 中国科学院长春光学精密机械与物理研究所，长春 130033；2. 北京电子技术应用研究所，北京 100091)

摘 要：基于安全的信息隐藏范式的思想，提出利用插值的方法，将秘密信息组织为图像的插值点插入到图像中，实现了安全隐写，并且在隐写过程中引入随机性，使隐写系统变得更加安全。现有多数方法是利用原图中已存在的冗余进行信息隐藏，该文提出的利用插值的方法相当于增加冗余，为信息隐藏提供了新的思路。

关键词：隐写；安全范式；插值；安全性；随机性

Information Hiding Method Using Interpolation

ZHAO Hong-bing[1], LIN Dai-mao[1,2], GUO Yunbiao[2]
(1. Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun 130033;
2. Beijing Institute of Electronic Technology and Application, Beijing 100091)

【Abstract】 Based on the thought of secure paradigm, a secure steganographic system using interpolation is achieved. It inserts interpolation points that denote secret into images. Besides, randomicity is imported during the steganographic process to make the system more secure. At present, the majority of information hiding methods utilize redundancy that has been existent in the original image; however, the method using interpolation is different. It carries out information hiding utilizing additive redundancy.

【Key words】 steganography; secure paradigm; interpolation; security; randomicity

1 概述

安全性是隐写考虑的第一要素。目前，与之对抗的隐写分析主要采取统计检测的方法威胁其安全。对此，可以将目前的隐写方法分为两种思路：一种是保持载体原有的统计特征，现在大多数隐写算法[1-2]都属这种思路；另一种是使隐写后的载体符合某种正常处理后的特征，使分析者没有充足的证据怀疑隐写存在。文献[3-4]提出的安全的信息隐藏范式思想即是第 2 种思路。图 1 具体解释了安全的信息隐藏范式的思想。X’为对载体 X 的正常处理结果，信息隐藏后的结果为 S，如果 S 与 X’的特性基本一致，就很难区分载体是经过了正常处理还是信息隐藏，从而实现安全的信息隐藏。

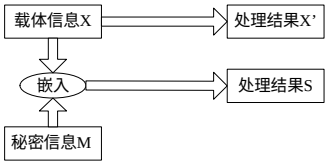

图 1 一种安全的信息隐藏范式

文献[5]根据信息论导出，增加载体的不确定性可以提高隐写系统安全性的结论，依据此结论，在隐写系统中引入了非决定论的概念。结合图 2 说明，在某些隐写系统中，没有 f_P 这个预处理过程，即给定一载体 cover 经过嵌入算法 f_E 后产生一 stego，再经过解密算法 f_E^{-1} 恢复出密信。

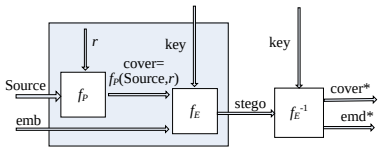

图 2 安全的隐写系统模型

在图 2 的隐写系统模型中，引入了预处理 f_P，这是一个不确定的随机过程。这样，在嵌入前输入的载体会变成一个载体集，也使得输入、输出间的传递函数不仅仅由 f_E 决定，也决定于 f_P 这个随机过程，从而提高了系统的安全性。

本文利用上述的第 2 种隐写思路，借鉴安全范式的思想，利用对图像的插值处理操作，实现了对图像的信息隐藏。

2 安全范式的插值实现

实现安全信息隐藏范式的关键之一是选择某种合适的正常操作，找到其处理结果边界的波动范围，使信息隐藏处理结果在此范围之内，以符合其规律。

2.1 算法原理

图像插值是图像处理中的一项重要的基本操作，广泛用于改善图像质量等方面，例如医学上常用插值来提高图像分辨率，以获得更多的图像细节。常见的插值方法有最近邻插值、双线型插值、双三次插值、三次 B-样条插值[6]等。

本文利用插值操作隐藏秘密信息，在原图像素点间加入插值点，利用插值点的奇偶性代表密信。如果随机事件集合 X 含有 N 个元素，那么熵 $H(X)\leq \log n\ N$。插值相当于增加了图像集合中元素的个数，使得图像的熵 $H(X')\geq H(X)$(X'表示插值后的集合)，这无疑增加了寻找密信的难度。

为进一步提高系统的安全性，在嵌入部分增加了图 2 中的预处理过程 f_P，即对欲嵌入的密信加密后，再混入不定长度的随机数。另外在嵌入部分设计了多种插值方法，在嵌入时随机地选择一种。两种做法共同的结果是使 cover 和 stego

基金项目：国家“973”计划基金资助项目(TG1999035804)
作者简介：赵鸿冰(1980－)，男，博士研究生，主研方向：信息安全；林代茂，研究员、博士生导师；郭云彪，副研究员、博士
收稿日期：2007-01-20 **E-mail：**hbing2399@sohu.com

建立起不确定的对应关系，进一步提高了隐写的安全性。

众所周知，可以把图像看作是由像素点组成的二维矩阵。插值后的图像是经过扩大的矩阵，此矩阵由两部分组成，即原矩阵的行、列和新插入的行、列。为确保隐藏后图像的视觉质量，需将插值行、列均匀地分布到图像中，基本不改变图像的长宽比。为方便起见，以下采取方阵加以说明。

2.2 嵌入过程

分别嵌入行、列会使嵌入变得相对简单，嵌入行与嵌入列的过程相似，在此以嵌入行为例说明。设 m 为原方阵行数，L 为密信长度，n 为嵌入后方阵的行数，则有 $n=\lceil\sqrt{L+m^2}\rceil$，其中$\lceil\ \rceil$为上取整。嵌入过程需要以下几个参数：

(1)总共需要插入的行数 $c=n-m$，这些行欲插入到 m-1 个间隙中。

(2)每个间隙需插入的行数 $h=c/(m-1)$。注意，h 可能是非整数，当越过更多的间隙时 h 会增加，间隙内实际插入的行数为 h 下取整，舍掉小数部分积累到下一个间隙。此参数用于确定原像素矩阵行在新矩阵中的位置。例如，原矩阵第 i 行 i_o 在新矩阵 N 中的位置应为在原 i_o 行的基础上加上前 i_o-1 个间隙内插入的$\lfloor(i_o-1)\times h\rfloor$行，即 $i_N=i_o+\lfloor(i_o-1)\times h\rfloor$。

(3)每个插入行所占间隙个数 $d=(m-1)/c$，此参数用于确定计算插值的行坐标以及该插值行在新矩阵中的位置。例如，当前欲插入第 j 行，$j\in[1, c]$，那么计算该插值行各点值时的行坐标应为 $p=1+d\times j$，计算出的该行加入到新矩阵 N 中的第 $\lceil d\times j\rceil+j$ 行，$\lceil d\times j\rceil$为插值行 j 前已存在的原矩阵行数。

嵌入过程有 4 个主要的步骤：

(1)对密信进行预处理 f_P，即加密并混入不定数量随机数。

(2)用式 $i_N=i_o+\lfloor(i_o-1)\times h\rfloor$，$i_o\in[1, m]$，将原矩阵像素复制到新矩阵。

(3)计算插值像素值。根据相邻像素值计算插入行内各点的插值，并对计算结果进行调整，用插值的奇偶表示密信内容。例如，计算出的某点的插值为 99.58，当密信为 1 时，下取整为 99，否则，上取整为 100。另外，插值点的值域为[0, 255]，当出现越界时可通过加减 2 进行调整。

(4)将步骤(3)的结果插入到新矩阵的$\lceil j/h\rceil+j$ 行。

至此，行嵌入已叙述完毕。列嵌入与行嵌入类似，不再赘述。

2.3 提取过程

由以上嵌入过程可以看出，提取的关键是找到插值行与插值列。这就要求提取方知道嵌入过程的一些参数分别对应于行、列嵌入的 c, h, d。实际上可以把这些参数看成嵌入密钥。

提取过程步骤如下：

(1)根据密钥定位插值列。

(2)根据列内点值的奇偶依次提取秘密信息，并删除插值列。

(3)定位插值行，根据行内点值的奇偶依次提取秘密信息。

(4)组合从行列中提出的密信，利用解密算法恢复密信。

注意，如果先插入行后插入列则提取过程应先提取列密信，删除插入列以后再提取行中的密信，即与嵌入时的顺序相反。

3 实验结果及安全性分析

图 3 为嵌入密信后的 Lena 图。从视觉效果看，无法分辨图像是否经过处理，说明隐写满足视觉安全。

同时，还对文中方法进行了抗统计分析的测试。利用文中方法对 100 幅图像嵌入了秘密信息(嵌入量为相对每幅图大小的 12.5%)。图 4～图 6 分别是 RS 分析、SamplePair 分析、最优逼近分析对隐秘图的检测结果(横坐标为图像编号，纵坐标为分析结果)。在 3 种统计检测方法的分析结果中，所有的图像都没有超过域值。结果表明，该方法可以抵抗统计检测。

图 3 隐写后 Lena 图

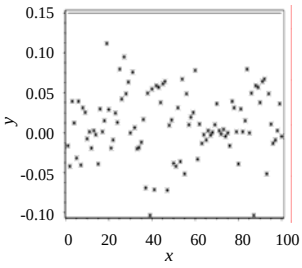

图 4 RS 分析检测结果

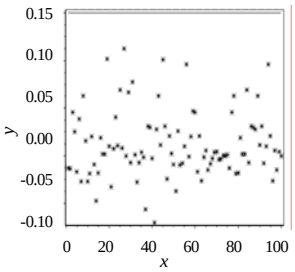

图 5 SamplePair 分析

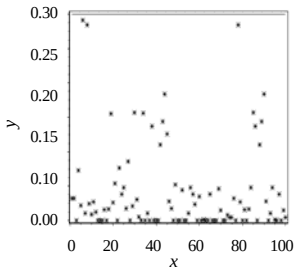

图 6 最优逼近分析

除此之外，笔者考虑将安全性做 3 个层次的假设：

(1)分析者察觉不到图像的变化。当嵌入较少的密信时，图像中绝大多数都为原图像素点，在统计特性上与原图基本一致，这样使得分析者察觉不到图像的变化。

(2)分析者没有充足的证据怀疑图像经过隐写。当嵌入大量密信时，图像的统计特性可能发生变化，引入了插值特征。但是，由于插值是一个常用的、基本的图像处理操作，因此，分析者仅凭插值特征不能证明图像经过隐写。

(3)假设图像被发现是含密的，攻击者提取密信的可能性也是非常小的。攻击者首先要攻破隐写算法找到密信流，再攻破在密信中掺入冗余的算法确定真实的密信流，还得攻破高强度的加密算法提取密信。

由此可以看出，攻击者提取密信的可能性甚小。综上 3 个层次的安全性分析，可以说该隐写系统具有较高的安全性。

本文方法会使图像变大，所以应注意选择载体图像的大小和嵌入密信的长度，如果图像过大也会引起分析者猜疑。另外，应选择应用插值较多的领域中的图像，如医学图像，这样会更好地消除分析者对插值特征的猜疑。

4 结束语

笔者利用插值实现了一个安全的隐写系统，它是图 1 所示范式的一种实现。利用插值的方法实现信息隐藏，是一个新思路，也是本文的创新之处。它不仅把秘密信息置于图像的冗余部分，而且在图像的主要成分上了做了改变，仍可以实现安全的信息隐藏，这与传统的信息隐藏方法有较大的区别。另外，本思路也一定程度地借鉴了广义信息隐藏[7]的思想，将秘密信息赋予像素值的含义，起到了隐藏通信存在的作用。

(下转第 99 页)

钥已经收到，可以开始正式通信了。然后会话进入全特征阶段，进行 iSCSI 命令和数据的交互。最后，启动端向目标端发送退出请求结束本次会话。

4 实验及结果分析

4.1 实验环境配置

本文中 iSCSI 协议及 SSL 的实现均在 Linux 平台下完成，启动端和目标端均采用 RedHat Linux 8.0，内核版本为 2.4.18-7。启动端 CPU 为 Intel P4 2.8，1 GB 内存；目标端 CPU 为 Intel P4 2.0，512 MB 内存，4 块 72 GB Ultra 160 SCSI 硬盘。启动端和目标端直接连接到百兆以太网交换机上。

本文还使用 FreeSWAN 2.05 实现了在 IP 层对数据包进行加密，为了两种安全机制的性能比较的公平性，在两种机制中都使用了 3DES 加密算法。

4.2 性能测试与结果分析

考虑到 iSCSI 是一种数据块级的传输协议，本文采用 Intel 公司的 IOmeter 来测试 iSCSI 的 I/O 性能和 CPU 占用率。测试时，设置读写操作各占 50%，顺序和随机各占 50%，I/O 数据块大小从 1 KB～1 024KB。先后对不加安全机制的 iSCSI、使用 SSL 的 iSCSI 和使用 IPSec 的 iSCSI 进行了测试，得到的 I/O 速率和 CPU 占用率结果分别如图 3、图 4 所示。

从图中可看出，采用 iSCSI+IPSec 模式，与不加安全机制的 iSCSI 相比，I/O 性能明显下降，降幅在 40%左右。而在 iSCSI+SSL 模式下，I/O 速率下降的幅度明显减小，在 15%左右。在 CPU 占用率方面，使用 IPSec 时 CPU 占用率增加了 1 倍，而使用 SSL 时 CPU 占用率增加了 50%。因此，与 IPSec 相比，基于 SSL 的安全 iSCSI 方案在保证相同安全性的同时，I/O 速率可以提高 25%，而 CPU 占用率可以降低 50%。

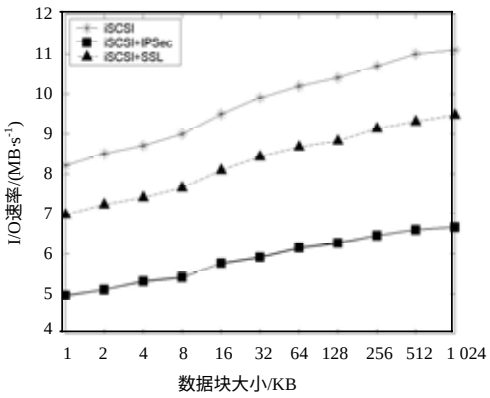

图 3 I/O 速度比较

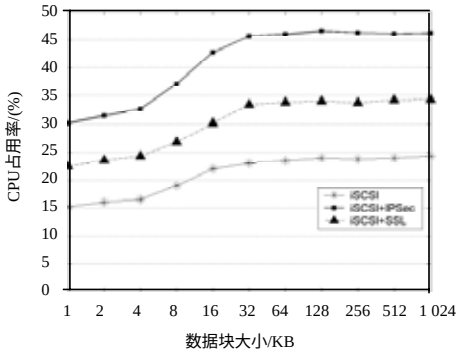

图 4 CPU 占用率比较

5 结束语

基于 TCP/IP 的 iSCSI 协议面临着和因特网相同的安全威胁，本文在 iSCSI 实现中引入了 SSL 安全机制。实验表明，与基于 IPSec 的安全 iSCSI 方案相比，本文的方案在 I/O 速率和 CPU 占用率两方面都具有明显优势，在保证安全性的同时提高了性能。

本方案的不足是在 iSCSI 实现时，要同时实现 SSL 的功能，增加了协议实现的复杂性，但这种修改相对来说很小，是能够容忍的。iSCSI 技术是 CPU 密集型的业务，加入安全机制后对 CPU 的占用更严重。因此，建议不要在 iSCSI 软件实现方式中加入安全功能，而应该在智能网卡或 iSCSI HBA 卡中集成安全功能，这样可大大减少对 CPU 的占用。下一步将研究如何在 iSCSI HBA 卡中实现 SSL 的功能。

参考文献

[1] Smith S. iSCSI[Z]. (2002-09-09). Internet Draft, http://www.ietf.org/internet-drafts /draft-ietf-ipiSCSI-16.txt.

[2] Satran, Meth J, Sapuntzakis K, et al. Internet Small Computer Systems Interface(iSCSI)[EB/OL]. (2004-04-08). http://www.ietf.org/rfc/rfc 3720.txt.

[3] Tang Shuangyi, Lu Yingping. Performance Study of Software-based iSCSI Security[C]//Proceedings of the 1st IEEE International Workshop on Security in Storage. [S. l.]: IEEE Press 2002: 70-79.

[4] 刘卫平, 蔡皖东. 基于 IPSec 的分级安全 iSCSI 技术研究[J]. 计算机工程, 2006, 32(9): 162-164.

[5] 谢长生, 傅湘林, 韩德志, 等. 一种基于 iSCSI 的 SAN 的研究与实现[J]. 计算机研究与发展, 2003, 40(5): 746-751.

[6] 周敬利, 杨 光, 余胜生, 等. iSCSI 存储系统中的安全性能研究及其模型实现[J]. 计算机工程, 2005, 31(2): 160-162.

(上接第 96 页)

参考文献

[1] Sallee P. Model-based Steganography[C]//Proc. of International Workshop on Digital Watermarking. Berlin: Springer-Verlag, 2004: 154-167.

[2] 赵鸿冰, 林代茂, 杨怀江. 利用反馈控制直方图失真的隐写方法[J]. 光学机密工程, 2006, 14(4): 720-724.

[3] 林代茂, 郭云彪. 一种安全的信息隐藏范式及其在二值图像上的实现[J]. 电子学报, 2005, 33(9): 1537-1540.

[4] Elke F, Andreas P. Steganography Secure Against Cover-stego-attacks[C]//Proc. of IH'99. Dresden: [s. n.], 2000: 29-46.

[5] Zöllner J, Federrath H. Modeling the Security of Steganographic Systems[C]//Proc. of IH'98. Portland, Oregon: [s. n.], 1998: 344.

[6] 李将云. 图像处理中的插值和缩放若干技术研究[D]. 杭州: 浙江大学, 2002.

[7] 林代茂, 胡 岚. 广义信息隐藏技术的安全问题[J]. 中山大学学报, 2004, 43(增 2): 14-16.