一种基于密钥的图像掩密算法*)

石 鹏 陈 丹 王育民

(西安电子科技大学综合业务网国家重点实验室 西安710071)

摘 要 本文提出了一种新的LSB掩密算法。该算法采用基于线性同余算法的伪随机数发生器生成掩密和提取所需的密钥,通过该密钥在GIF图像中随机选取所要嵌入信息的位置来实现秘密信息比特的嵌入。实验结果表明该掩密算法可有效地抵御可视攻击和χ^2攻击。

关键词 掩密技术,伪随机数发生器,可视攻击,χ^2攻击

A New Image Steganography Based on Key

SHI Peng CHEN Dan WANG Yu-Min

(National Key Lab. of Integated Service Networks, Xidian Uni. Xi'an 710071)

Abstract A new LSB steganography algorithm is presented. In this algorithm, the key used to hide and extract information is generated by a pseudo-random generator based on linear congruent algorithm, the locations of message bits are chosen to complete steganography process with this key in a GIF image. The result indicates that this new steganoraphy is against Visual attack and Chi-square attack effectively.

Keywords Steganography, Pseudo-random generator, Visual-attack, Chi-square attack

1 引言

近年来,国际上提出一种新的关于信息安全的概念,开发设计出一种不同于传统密码学的技术,即将机密资料信息秘密地隐藏于普通的文件中,然后再通过网络传递散发出去。这样非法拦截者从网络上拦截下来的伪装后的机密资料,并不像传统加密过的文件那样是一堆乱码,而是看起来和其他非机密性的一般资料无异,因而十分容易欺骗非法拦截者。其道理如同生物学上的保护色,巧妙地将自己伪装隐藏于环境中,免于被天敌发现而遭受攻击。这一点是传统加解密系统所欠缺的,这便是掩密技术(Steganography)。保密通信、电子商务以及国家安全等方面的应用需求推动了信息掩密技术研究的开展。

现有的掩密算法大多采用LSB(Least Significant Bit)替换算法,即对所需处理的图像的每一个像素的最不重要比特进行相应的比特替换,由于现有算法大多采用顺序替换的方式,使得掩密算法的安全性大为降低,而图像自身也存在较大的失真,因此对于现有掩密攻击,诸如可视攻击和χ^2攻击来说,极易检测出图像中是否含有隐匿的信息。基于此,本文在分析现有掩密技术的基础上,提出一种抗可视攻击和χ^2攻击的掩密算法,大大提高了掩密的安全性。

2 掩密技术的研究现状

掩密技术就是将秘密信息隐藏于另一非机密的文件内容之中,其形式可以是任何一种数字媒体,如图像、声音、视频等等。掩密技术和传统的密码技术的区别在于:密码仅仅隐藏了信息的内容,而信息伪装不但隐藏了信息的内容而且隐藏了信息的存在。

根据掩密方式掩密算法可分为:顺序嵌入和随机嵌入。所谓随机嵌入即将所要嵌入的信息比特逐个嵌入到载体图像中的像素中,从载体图像的左上方至右下方,逐个处理直到将信息比特完全嵌入,现有的掩密算法大多采用顺序嵌入的方法,像EzStego、Jstego、Steganos和S-Tools;而随机嵌入则是在载体图像中随机选取一些位置,将所要嵌入的信息比特嵌入到这些随机选取的位置的像素中。随机嵌入方式将对图像像素的改变随机分散于图像当中,而不是像顺序嵌入那样过于集中在图像的前部,因此随机嵌入方式的采用不仅可以大大提高掩密信息的安全保密性,而且大大降低了因为对图像的改变所造成的失真,本文即采用随机嵌入的方式来达到此目的。

对掩密技术的攻击方法分为可视攻击和统计攻击两类,而χ^2攻击是一种很有效的统计攻击,本文提出的掩密算法可有效地抵御可视攻击和χ^2攻击。现将这两种攻击简介如下:

可视攻击 数字图像在隐匿信息后将显示出不同程度的失真:扭曲或变形。一些图像甚至在嵌入少量的信息后就会引起较大的失真,这种"可视噪音"将会泄漏所隐匿信息的存在,因而也就成为攻击者攻击掩密的基础和关键。所谓的可视攻击[4]是指滤除掩盖秘密信息的所有图像部分,人眼可直观地判断是所隐匿的信息还是原图像内容。滤除过程如图1所示。

多数信息掩密算法要么以顺序的方式要么以某种伪随机的方式嵌入消息比特。在大多数程序中,非适应地选择与图像内容无关的消息比特,如果图像中含有单一颜色相连的区域或者以颜色值0或255来填充的相连的区域,那么能够在预先处理(如对图像中的调色板进行排序,然后根据LSB替换值进行黑白着色,最后恢复原有的调色板顺序)含有隐匿信息的图像后使用简单的可视检测来找寻所隐匿的信息。即使不能够轻易看到图像是否隐匿信息,也可构造一个比特平面(比如析取图像的LSB平面)仅仅检测比特平面本身。该攻击特别

*)基金项目:国家863项目(No.2002AA144060)和国家自然基金(项目编号:60173032)资助。石 鹏 硕士研究生,主要研究方向:信息与网络安全、信息隐藏。陈 丹 博士研究生,主要研究方向:信息与网络安全、信息隐藏。王育民 教授、博士生导师,主要研究领域:信息理论、编码及密码理论、通信网的安全。

适用于基于LSB嵌入的调色板图像。可视攻击的效果图如图2。可见可视攻击对于顺序改变图像空间域像素LSB的掩密技术有非常好的检测效果。

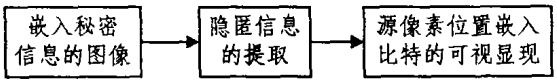

图1 滤除结构

图2 左图为未嵌入任何信息的图片的可视攻击效果图，右图是用EzStego嵌入占图像大小50%的信息后图像的可视攻击效果图

χ^2攻击 Pfitaman和Westfeld[4]针对利用一组固定的PoV(Pairs of Value)彼此相互对应来嵌入秘密信息的掩密算法，提出一种强有力的统计攻击[4]。由像素值、量化DCT系数或LSB中不同的调色板indices都可以构成PoV。在嵌入信息前，载体图像中每一对中的两个值非均匀分布；嵌入信息后，每一对值的出现呈现相等的趋势(独立于所嵌入消息的长度)。由于将一个值转换为另外一个值不会改变图像中两个颜色出现的总数，因此可用此事实来设计χ^2检验，即测试这样一个事实的统计显著性：每一对中两个值的出现是相同的。而且，如果从载体的左上角顺序地将消息比特嵌入到顺序的像素/indices/系数中，那么统计结果会有明显的变化。该检测的思想则是：将理论上所期望的频率分布和在可能改动的载体图像中所观测的某些样本分布做一比较从中发现变化。图3所示对于可视攻击效果不佳的掩密技术使用该统计分析方法可有效地检测图像中是否隐匿有秘密信息。

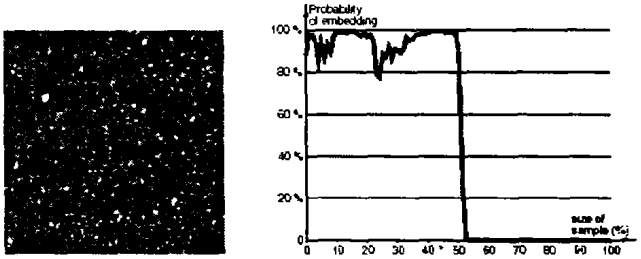

图3 左图是用EzStego处理过的背景图，右图是χ^2攻击分析图其中横坐标为图像的检测比例，纵坐标是嵌入信息的概率

3 基于密钥的掩密算法

基于空间域LSB的掩密算法可实现将秘密信息嵌入到载体(如文本、图像、声音等数字媒介)中，但不能有效抵抗现有前述各式各样的掩密攻击，像EzStego就不能有效地抵抗可视攻击和χ^2攻击。基于空间域LSB嵌入的算法思想，我们设计了一种以GIF图像为信息载体的抗可视攻击和χ^2攻击的掩密算法，其流程框图如图4所示。

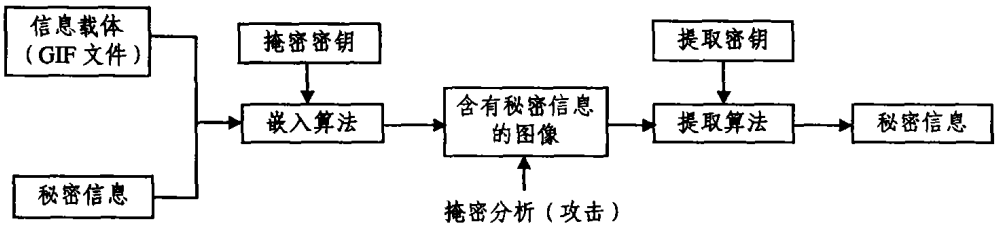

图4 算法流程框图

该算法所实现的功能是：发送与接收双方共享掩密密钥，发送方以GIF格式的图像文件为信息载体，将多种格式的文件(如文本、图像、声音等)在密钥控制下嵌入载体图像中，在视觉上载体图像没有失真，从而难以检测；接收方可以与发送方所共享的掩密密钥从已嵌入信息的GIF文件中将信息无损失的恢复出来。下面具体介绍该算法：

3.1 掩密载体的选用

对于该掩密算法，选用基于调色板的GIF格式的图像作为载体图像。GIF文件中包含一个256种颜色的调色板，共计2^{24}种可能的颜色和一个调色板索引的Lempel-Ziv-Welch(LZW)压缩矩阵。采用的该掩密算法将产生一个重新排序的调色板，使得在重新排序后的调色板中从视觉角度上几乎不能区分相邻的两种颜色。由于该算法采用随机处理的方式，使得所隐匿在载体图像中的信息随机分散于载体图像的各个像素中，无论载体图像色彩单调，内容单一，都使得图像被改变的部分不会出现较为明显的失真，因此，采用该算法进行信息的掩密不需要对载体图像的选择有苛刻的要求。

3.2 掩密密钥

该掩密算法所需的密钥是一个对称密钥，它用于通信双方为秘密信息比特在载体中随机选取嵌入和提取的位置，在掩密秘密信息前需要通信双方共享该掩密密钥，否则在接收方难以提取嵌入在载体中的秘密信息。在这里我们假设该掩密密钥的交换是安全的。

我们用掩密密钥来初始化一个伪随机序列产生器，以便于由此种子密钥产生一系列伪随机数来用于在载体中随机选取所要嵌入秘密信息的位置。这里采用线性同余(Linear Congruent)算法[5]，选模$m=2^{19}-1=524287$，$c=0$，$a=3$，则线性同余的迭代函数为：

$$x_{i+1}=3x_i \bmod m \quad 0\leqslant x_i\leqslant m$$

其中x_0为初始值，即种子密钥。这样即实现了LSB随机嵌入，将所要嵌入的信息比特分散到随机选择的载体图像的各个像素中，极大地改进了图像中因所嵌入信息过于集中而造成失真较大的问题，同时增加了掩密的安全保密性。提取算法中添加相同的伪随机发生器。只要嵌入与提取过程中使用相同的种子密钥，则可完整地嵌入和提取秘密信息。

3.3 所嵌入秘密信息的准备

在嵌入秘密信息前，对所要嵌入的秘密信息进行加密可提高掩密的保密度和安全性；而且在嵌入前可将秘密信息进行压缩处理，这样可在载体中嵌入更多的秘密信息，也减少了载体自身的失真，同时，秘密信息也有较好的随机特性，使得0

和1呈均匀分布。

3.4 嵌入秘密信息

我们采用空间域LSB替换作为基本的掩密算法。需要强调的是LSB可用于空间域和变换域当中，空域上实现LSB算法，不需要将图像载体中的像素做任何技术上的处理，不改变原有图像的存贮格式，直接将所要嵌入的信息比特替换载体图像中相应位置的像素值，因而其实现相当简单，信息在载体图像中的嵌入/提取速度也很高。

基于LSB的嵌入函数不打破原有的载体单元(如图像的像素)顺序，在嵌入过程完成后，载体中的每一个单元含有一个掩密值(比如1比特秘密信息)。嵌入函数将掩密值与所要嵌入位置的比特进行匹配，如果需要替换的话，则将该位置的颜色用与该颜色最为接近的颜色进行替换从而达到嵌入掩密值的目的。图5示出了以图像作为载体的LSB替换函数示意图。

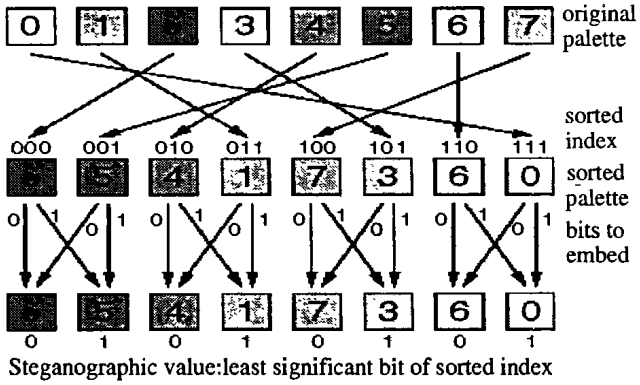

图5 LSB替换函数

图5用一个简单的调色板来说明LSB替换过程。例如在载体图像中存在一个索引值为7的颜色，想要在该位置中嵌入"1"，则用索引值为3的颜色来替换索引值为7的颜色；而如果想要嵌入"0"则不作任何改变。这是由于载体图像中索引值为7的颜色经最短路径原则排序后其索引值变为100(=4)，而索引值为3的颜色在排序后的调色板中索引值变为101(=5)，这两种颜色在排序后的调色板中彼此相邻，在视觉上很难区分除非直接与原图比较。

3.5 掩密信息的提取

当接收方接收到隐匿有秘密信息的载体时，使用与发方所共享的掩密密钥，使得同一伪随机序列发生器产生与发方相同的伪随机序列相对应的嵌入位置，采用与嵌入函数相同的提取方法对载体中相应位置的比特进行逐个提取，最后还原为秘密信息的原貌。

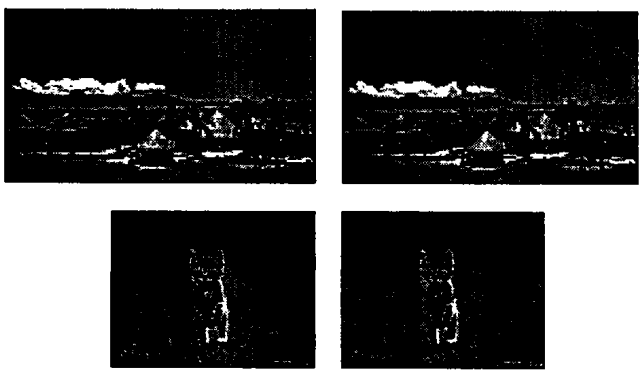

图6 左上图是嵌入小猫图像前的载体图像，右上图是嵌入后的载体图像，左下图是所要嵌入的小猫图像，右下图是从载体图像中提取出来的小猫图像

使用该算法无论是将文本、图片还是声音文件隐匿在GIF格式的图像中，均有较好的掩密效果，人的视觉难以觉察出载体图像有任何形式的失真。图6便是将一幅JEPG格式的图像嵌入在GIF图像当中的效果图。

4 安全性能测试

4.1 可视攻击

采用可视攻击的方法，对经过该掩密算法处理的图像进行分析，欣喜地看到该分析方法不能产生应有的效果，即有效的检测出载体图像中是否隐匿秘密信息，下图是载体图像即掩密图像的可视攻击效果的比较：

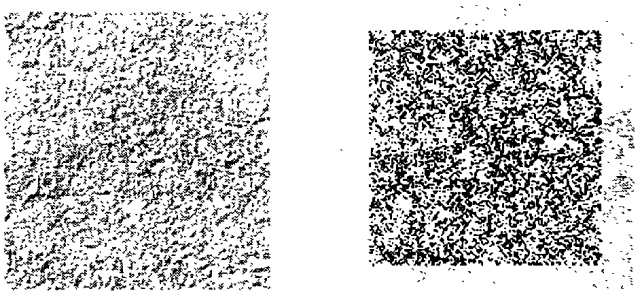

图7 纯背景图案及其可视攻击的效果图

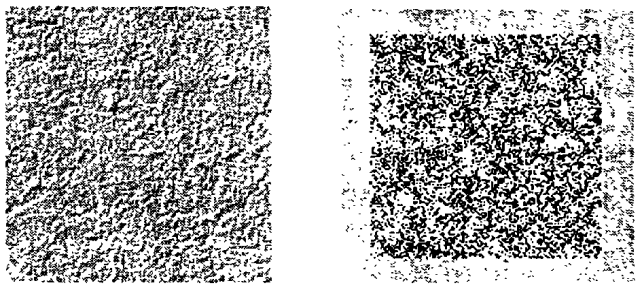

图8 应用该掩密算法嵌入秘密信息后的图案及其可视攻击效果图

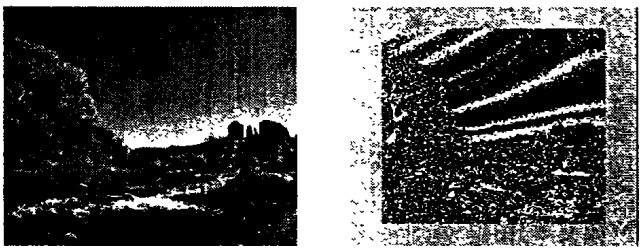

图9 载体图像及其可视攻击的效果图

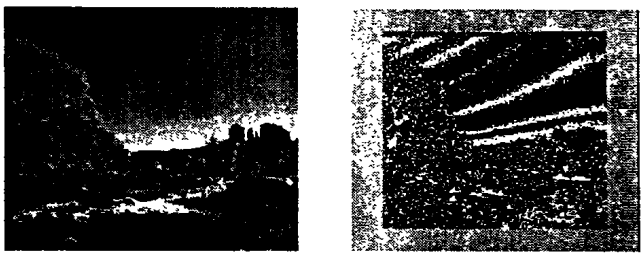

图10 嵌入秘密信息后的载体图像及其可视攻击的效果图

对比图8、图10与图2，同是对GIF图像空间域LSB替换进行可视攻击，可是效果却截然不同，图8和图10没有出现图2所显现的效果，同各自未嵌入任何信息的载体图像的可视效果图比较，没有出现较大的差异，因而用可视攻击难以检测用

该掩密算法处理的 GIF 图像。图10所示，将一幅120×90的JPEG 格式的图像文件嵌入图9所示的载体图像中，从原载体图像的可视攻击的效果图和嵌入信息后载体图像的可视攻击效果图的比较可知，可成功地抵抗此攻击。

4.2 χ^2攻击

采用前述 χ^2攻击方法，对一幅100×93的纯色背景图用该掩密算法嵌入一段文本信息，嵌入信息前后的 χ^2攻击效果比较如图11、12所示。

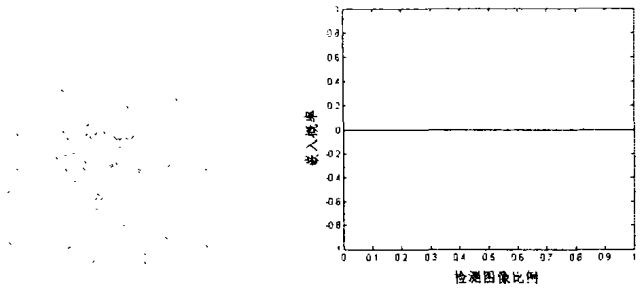

图11 嵌入文本信息前的纯色背景图及其 χ^2攻击

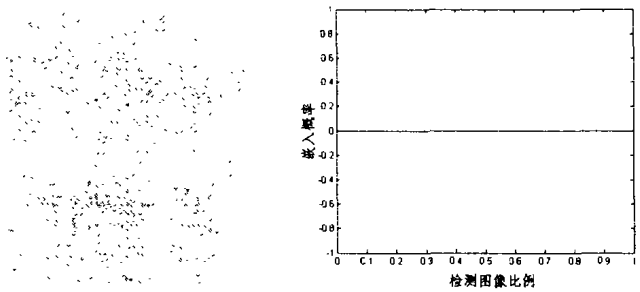

图12 嵌入文本信息后的纯色背景图及其 χ^2攻击

由上述结果显示，在嵌入秘密信息前后图像的 χ^2攻击结果相同，其检测的嵌入概率均为零，这足以说明用该掩密算法可有效地抗 χ^2攻击。

对大量 GIF 格式的图像做同样的测试，其结果显示：使用该掩密算法可有效地抗可视攻击和 χ^2攻击。

今后的研究方向 我们提出了上述抵御可视攻击和 χ^2攻击的掩密算法，进行了相应的安全性能测试，产生了非常好的效果。在该领域我们将深入地在以下几个方向进行研究与开发：

·设计大容量无失真(或失真较小)的掩密算法，改进现有掩密软件，使其含有嵌入信息长度信息；

·开发适用于在 JPEG 图像中嵌入信息、可抗可视攻击和各种统计攻击的掩密软件；

·开发频域掩密算法及相应的软件；

·针对现有掩密分析工具，设计更为隐秘的掩密技术。

参 考 文 献

1 Zollner J, Federrath H, Klimant H, et al. Modeling the Security of Steganographic Systems[M]. 1998, Springer-Verlag Berlin Heidelberg IH'98. 344～354

2 Katznbeisser S, Fabien A, Petitcolas P. Information Hiding Techniques for Steganography and Digital Watermarking[M]. Artech House. Boston London, 2000

3 Petitcolas F A P, Anderson R J, Kuhn M G. Information hiding—a survey[J]. Proceedings of IEEE, 1999, 87(7): 1062～1078

4 Westfeld A, Pfitzmann A. Attacks on Steganographic Systems. IHW'99, Dresden, Germany, Sept. 1999

5 王育民，刘建伟. 通信网的安全——理论与技术. 西安：西安电子科技大学出版社，1999

(上接第168页)

参 考 文 献

1 Wilks S S. Mathematical Statistics [M]. New York: Wiley, 1962

2 Belhumeur P N, Hespanha J P, Kriegam D J. Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1997, 19(7): 711～720

3 Foley D H, Sammon J W, Jr. An optimal set of discriminant vectors [J]. IEEE Transactions on Computers, 1975, 24(3): 281～289

4 Liu Ke, Cheng Yong-qing, Yang Jing-yu. An efficient algorithm for Foley-Sammon optimal set of discriminant vectors by algebraic method [J]. International Journal of Pattern Recognition and Artificial Intelligence, 1992, 6(5): 817～829

5 Liu Ke, Cheng Yong-qing, Yang Jing-yu. A generalized optimal set of discriminant vectors [J]. Pattern Recognition, 1992, 25(7): 731～739

6 郭跃飞，杨静宇. 求解广义最佳鉴别矢量集的一种迭代算法及人脸识别[J]. 计算机学报，2000, 23(11): 1189～1195

7 Vapnik V N. The Nature of statistical Learning Theory [M]. New York: Springer-Verlag, 1995

8 Baudat G, Anouar F. Generalized discriminant analysis using a kernel approach [J]. Neural Computation, 2000, 12(10): 2385～2404

9 Roth V, Steinhage V. Nonlinear discriminant analysis using kernel functions [A]. In: S. A. Solla, T. K. Leen, K.-R. Müller, eds. Advance in Neural Information Processing Systems 12 [C]. Cambridge, MA: MIT Press, 2000. 568～574

10 Mika S, Rätsch G, Weston J, et al. Fisher discriminant analysis with kernels [A]. In: Y.-H. Hu, J. Larsen, E. Wilson, eds. Neural Networks for Singal Processing IX [C]. Piscataway, NJ: IEEE, 1999. 41～48

11 Müller K-R, Mika S, Rätsch G, et al. An introduction to kernel-based learning algorithms [J]. IEEE Transactions on Neural Networks, 2001, 12(2): 181～201

12 甘俊英，张有为. 模式识别中广义核函数 Fisher 最佳鉴别[J]. 模式识别与人工智能，2002, 15(4): 429～433

13 吴小俊. 图像特征抽取与识别理论及其在人脸识别中的应用[D]. 南京：南京理工大学，2002

14 李士进. 人脸检测与识别方法研究：[博士学位论文][D]. 南京：南京理工大学，2000

15 程云鹏. 矩阵论[M]. 西安：西安工业大学出版社，1989

16 Liu Ke, Cheng Yong-qing, Yang Jing-yu. Algebraic feature extraction for image recognition based on an optimal discriminant criterion [J]. Pattern Recognition, 1993, 26(6): 903～911