文章编号 1004-924X(2002)03-0243-04

基于噪声抽取的信息隐藏方法研究

隋永新[1], 杨英慧[2], 杨怀江[1], 曹健林[1]
(1. 中国科学院长春光学精密机械与物理研究所, 吉林 长春 130022;
2. 辽宁省营口中专教务科, 辽宁 营口 115000)

摘要: 信息隐藏技术是在只具平凡意义的载体中隐藏需要进行保密通信的敏感信息, 只要人类感觉系统无法察觉由此所引起的载体变化, 则此通信中对外表现的只是载体的属性, 除了通信双方之外的任何第三方并不知道在此平凡载体通信过程中存在着隐蔽信道, 由此以减少敏感信息在信道传输过程中受到攻击的可能性, 因此本文认为若将信息隐藏与加密技术结合使用则可以较为完善地解决高强度的保密通信问题。文中利用所提出的基于噪声抽取信息隐藏方法实现了上述方案, 算法设计过程中主要考虑了图像质量、全比特恢复能力、保密性、反检测能力等方面的因素, 最后给出了实验结果和反检测分析。

关 键 词: 信息隐藏; 噪声抽取; 保密通信
中图分类号: TP391 文献标识码: A

1 引 言

随着通信技术的飞速发展, 信息的表现形式和传播方式都发生了根本变化, 数字化、网络化使信息流通更为迅捷, 信息传播更为顺畅, 然而由于信息本身所具有的脆弱性, 使其在存储与传播过程中易于受到非法获取、修改以及删除等形式的攻击, 特别是在计算机网络成为通信的重要方式后, 信息安全已经成为信息科学中急需解决的问题。

众所周知对信息进行加密处理是最为常用的信息安全防护方法。一般而言, 信息经加密处理后其随机性显著增强, 使未授权者无法解读以达到信息安全的目的, 然而其不可解读性却较易引起恶意攻击者的注意, 随着计算机计算速度和存储方面的飞速发展, 以及通过网络实现并行计算破解技术的日益成熟, 加密处理的安全性面临空前的挑战。即使攻击者无法破译加密的信息, 却可以采用篡改和删除的手段以破坏通信的进行。因此, 仅凭加密技术难以使信息受到完全保护, 但若与信息隐藏技术配合使用则信息安全问题可望得到更为理想的解决。

信息隐藏技术是将待隐藏的敏感信息有机地编码耦合到宿主信息之中, 同时又保证隐藏信息后宿主的表观变化不会引起人类的感觉差异, 因此隐藏敏感信息的宿主在公用信道上传输时, 因其平凡的表观亦不会引起攻击者的格外注意, 从而减小受到攻击的可能性, 由此解决信道安全问题。

目前, 国际上关于信息隐藏的研究主要集中在用于版权及数据完整性保护的数字水印方面[1,2], 针对信息安全领域的信息隐藏研究报道较为少见。结合人类视觉系统的特性在数字图像的变换域和空间域中隐藏信息是数字水印技术最常采用的方法。在图像中嵌入数字水印要求在保证图像视觉质量的同时力求获得较强的鲁棒性, 即嵌入水印的图像经过滤波、压缩、几何变换等操作后仍然可以恢复出可鉴别的水印信息, 另外在提取数字水印时一般不要求全比特的恢复能力, 因而在变换域中隐藏信息更适合于数字水印。

当信息隐藏技术应用到信息安全领域之时, 除了要求宿主图像在隐藏信息后其表观变化不会引起人类的感觉差异之外, 更重要的是能够保证

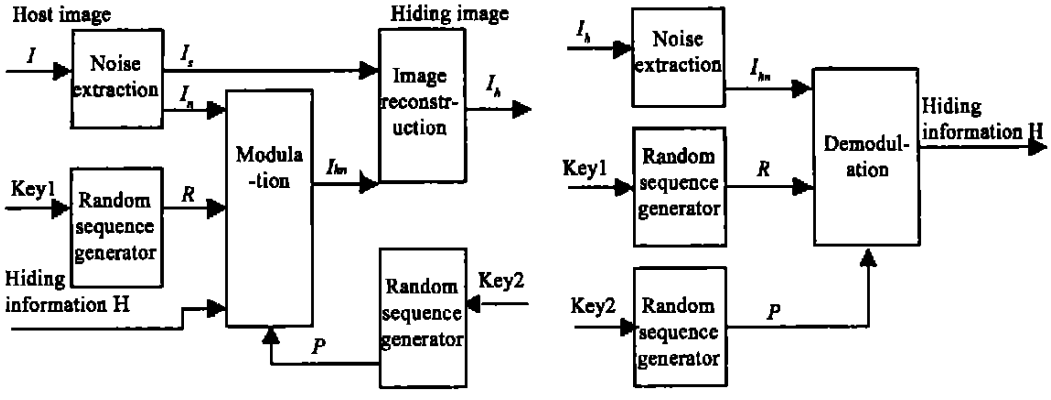
收稿日期: 2001-08-10; 修订日期: 2002-02-01
基金项目: 国家自然科学基金, 吉林省杰出青年基金资助

保密通信有效安全地进行,因此以下三个方面亦绝不能忽视。首先,因为待隐藏的基本上都是敏感信息,任何误码都可能导致无法估量的损失,所以必须保证全比特地恢复隐藏的信息;其次,即使截获者已知隐藏算法,亦不能恢复出隐藏的信息,在此引入符合密码学要求的密钥控制是保证隐藏算法保密性的根本途径;最后,隐藏算法的反检测能力越强,则籍此实现的保密通信越安全。

本文所提出的基于噪声抽取隐藏方法是在空间域中隐藏信息,如此可以保证全比特地恢复隐藏的信息。

2　基于噪声抽取进行信息隐藏

基于噪声抽取的隐藏算法如图1所示,图1(a)为信息嵌入过程,包括噪声抽取、随机控制、信息调制和图像合成四个部分,图1(b)为信息恢复过程,包括噪声抽取、随机控制、信息解调三个部分。



(a) 嵌入信息过程
(a) Information embedding process

(b)恢复信息过程
(b)Information recovering process

图1　基于噪声抽取的信息隐藏算法

Fig. 1　Algorithm of information hiding based on noise extraction.

2.1　噪声抽取

色度学及视觉理论的研究结果证明人类视觉系统对于亮度及色度变化的分辨能力是有限的,因而针对图像I可以构造其相似变换空间:

$$\Omega(I) = \{I' : \mathrm{dis}(I, I') \leqslant \mathrm{dis}_{th}, \qquad (1)$$

其中 $I' = I + N$ 为注入噪声后所得图像,$\mathrm{dis}(I, I')$ 为图像 I 与 I' 的距离,dis_{th} 为人类视觉系统可以分辨的最小图像距离,由此可以计算最大允许噪声强度 N_{th}:

$$I'_{th} = I + N_{th},\ \mathrm{dis}_{th} = \mathrm{dis}(I, I'_{th}), \qquad (2)$$

只要注入噪声小于最大允许噪声强度 N_{th},则可保证经过噪声注入后图像的变化不会引起视觉差异。通常数字图像在存储和显示过程中是以一定位数的数据来表示的,此数据的各比特位对于图像象素亮度和色度的贡献随着位平面的降低而逐渐减小。具体的噪声抽取方法是根据最大允许噪声强度,选取图像像素的 m 位较小意义位(LSBs)进行噪声抽取。

经过噪声抽取后宿主图像 I 分解为信号 I_s 和噪声 I_n 两部分,将待隐藏信息根据一定规则代换图像的噪声以实现信息嵌入。

2.2　基于密钥的随机控制

信息隐藏之目的是为了增强保密通信在信道传输过程中的安全性,然而,如果隐藏算法没有密码保护,只凭借对算法本身的保密其安全性是不可靠的,一方面在使用过程中要杜绝算法被跟踪或反汇编在技术上是极其困难的,另一方面无法保证攻击者不能根据隐藏的结果回溯出算法的细节,因此在算法中必须引入具有密码学意义上的基于密钥的随机控制方可确保其保密性。在本算法中提供了两方面的随机控制,key2控制在图像中隐藏信息的位置,以key1为种子的随机序列发生器运转产生 $GP(2^m)$ 域上的随机序列,而后此随机序列代换图像中指定位置的m位较小意义位。在key2的控制下隐藏的信息将分散到整个图像之中,如此可以改善隐藏信息后图像的局部区域的统计特性。算法的保密性将主要取决于key1为种子的随机序列发生器的密码学性质,在

此采用混沌加密技术实现此发生器[3,4]。

2.3 隐藏信息的调制与解调

当噪声抽取原则确定以后, 即根据图像的最大允许噪声强度确定较小意义位数 m 后, 隐藏信息的调制与解调可以利用 $GP(2^m)$ 域上的模加运算实现:

调制:

$$I_{hn} = (H + R) \bmod (2^m), \qquad (3)$$

解调:

$$H = (I_{hn} + R) \bmod (2^m), \qquad (4)$$

2.4 图像合成

图像的噪声部分在调制了待隐藏信息后与图像的信号部分 I_s 合成得到隐藏信息的图像。

3 测试结果与分析

利用上述方法, 将一 8k 字节的英文文本隐藏到 lena 测试图像的结果如图 2 所示, 其中所选取的较小意义位数 m 为 1。

(a) 原始 lena 图像

(a) Original lena image

(b) 嵌入信息后的 lena 图像

(b) Lena image embedded information

图 2　隐藏信息前后的 lena 测试图像

Fig. 2　Lena images before and after hiding information.

本方法可以全比特地恢复信息, 因而恢复后的信息没有误码, 图 3 为恢复后的部分英文文本。

> Data hiding, a form of steganography, embeds data into digital media for the purpose of identification, annotation, and copyright. Several constraints affect this process: the quantity of data to be hidden, the need for invariance of these data under conditions where a "host" signal is subject to distortions, e. g., lossy compression, and the degree to which the data must be immune to interception, modification, or removal by a third party.

图 3　恢复后的部分英文文本

Fig. 3　Part of recovered English text.

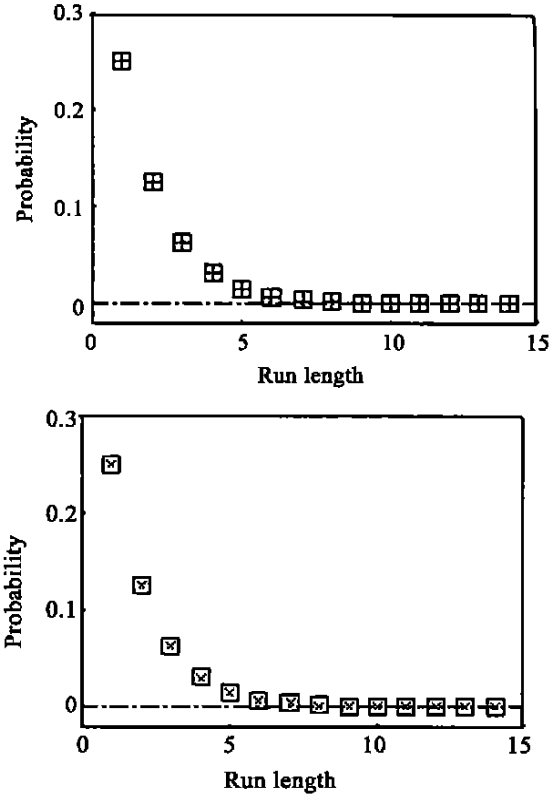


图 4　隐藏信息后最小意义位的游程特性
(此图中□表示理想随机序列的游程特性 + 表示隐藏信息后 1 序列的游程特性× 表示隐藏信息后 0 序列的游程特性)

Fig. 4　Probability of run length of the least significant bit after hiding information.
(Where □ denotes the probability of run length of ideal random sequence;
+ denotes the probability of run length of 1 sequence;
× denotes the probability of run length of 0 sequence.)

在图像的较小意义位上直接隐藏信息将改变其原有的统计特性,据此可以利用数理统计的方法检测一幅图像是否隐藏了信息[5]。图像在较小意义位上的数据可视为随机变量,只要在隐藏信息后这些数据依然保持其随机分布,则可抵抗依据统计特性检测隐藏信息的方法。在本算法中,信息并不是直接代换较小意义位,而是经过一个随机序列调制后代换较小意义位,因此在隐藏前后较小意义位的随机分布并未发生改变。图4所示为lena图像在隐藏信息后最低数据位的游程统计,可以看出在隐藏信息后最低数据位与理想随机序列的统计特性十分接近。

4 结论

利用噪声抽取实现了在数字图像中隐藏信息,能够全比特地恢复隐藏的信息,在隐藏过程中引入了具有密码学意义的随机控制,一方面提高了隐藏的保密性,另一方面增强了反检测能力。由此可见,信息隐藏技术通过隐匿通信过程本身,因而可以发展成为一种新型的保密通信手段,然而信息隐藏技术必须借鉴密码技术或者与其相结合才能保证通信的保密性和安全性。

参考文献:

[1] Bender W, Gruhl D, Morimoto N, Lu A. Techniques for data hiding[J]. *IBM System Journal*, 1996,(35):313-335.

[2] Petitcolas F A P, Anderson R J, Kuhn M G. Information hiding-A survey[J]. *Proceedings of IEEE*, 1999,(87): 1062-1078.

[3] 周红. 混沌前馈型流密码的设计[J]. 电子学报,1998,(26):98-101.

[4] 石文孝, 荆涛, 杨怀江. 混沌序列的神经网络实现[J]. 光学 精密工程,2000,(8):231-233.

[5] 尤新刚, 郭云彪, 周琳娜. 信息隐藏对图像空域数据特性的影响[A]. 全国第二届信息隐藏学术研讨会论文集[C]. 北京,2000.

Study of information hiding algorithm based on noise extraction

SUI Yong_xin[1], YANG Ying_hui[2], YANG Huai_jiang[1], CAO Jian_lin[1]

(1. *Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun* 130022, *China*;
2. *Liaoning Yingkou Technical Secondary School, Yingkou* 115000, *China*)

Abstract: Information hiding, a form of information processing, embeds data into trivial media for the purpose of concealing the secret communication. Provided that the change due to the above_mentioned process cannot to be detected by human vision system, only the two parties of communication know the covered channel within the traffic, thus it arouses less suspicion. In this paper the authors believe that information hiding combined with encryption techniques can provide a perfect scheme for high strength secure communications. Utilizing a new information hiding algorithm based on noise extraction, the above_mentioned scheme has been realized, to design the algorithm the factors including image quality, ability of whole bits restoration, security, performance of anti_detection have been taken into account. Finally, the experiment and analysis of anti_detection are given.

Key words: information hiding; noise extraction; secure communications

作者简介:隋永新(1970-),男,黑龙江虎林人,1993年毕业于长春光学精密机械学院,现为中科院长春光学精密机械与物理研究所应用光学国家重点实验室博士生,主要从事混沌保密通信、信息隐藏等方面的研究工作。