关于信息技术隐藏及其应用的综述

马思腾 20171110349

Abstract

With the development of science and technology and the arrival of the information age, information security has become the focus of attention. And the information hiding technology that emerged at the historic moment has become an emerging information security technology in recent years. The principle is to use the redundant part of the host information with random characteristics to embed important information in the host information without being discovered by others. It is not only important in the field of information security, but also in information warfare. Has played an extremely important role, this article is to summarize and summarize the current existing information hiding technology, and study how information hiding technology is applied to information security and confidentiality, including steganography technology based on GAN image generation, Deep learning multimedia information hiding technology, etc.

keywords: Information hiding, information security, steganography, GAN image, deep learning

摘要

随着科学技术的发展，信息时代的到来，信息的安全已经成为众人关注的焦点。而随之应运而生的信息隐藏技术成为了近年来的一项新兴的信息安全技术。其原理便是利用宿主信息中具有随机特性的冗余部分，将重要信息嵌入宿主信息之中，而不被其他人发现的一项技术，不仅在信息安全领域举足轻重，而且在信息战中也发挥出了极其重要的作用，本文就是对目前现有的信息隐藏技术进行归纳和总结，并研究信息隐藏技术是如何应用到信息安全和保密工作上的，包括基于 GAN 图像生成的隐写技术、基于深度学习的多媒体信息隐藏技术等。

关键字: 信息隐藏 信息安全 GAN 图像 隐写技术 深度学习

1 信息隐藏技术的概述

1.1 信息隐藏技术组成

信息隐藏技术作为一门新兴的信息技术 [1]，现已应用到各个领域。在这方面，我们将保密的信息称为嵌入对象，将用于隐藏嵌入对象的非保密载体称为掩体对象。而隐藏对象是产生在嵌入对象通过嵌入过程被隐藏在掩体对象的过程中。我们将嵌入对象添加到掩体对象中得到隐藏对象的过程成为信息的嵌入，嵌入过程中所需要的算法，我们称为嵌入算法。在此过程中，从隐藏对象中重新获得嵌入对象的过程我们称为信息的提取，即信息嵌入的逆过程。其中涉及到的算法我们称之为提取算法。

对于信息隐藏系统，我们可以将其一般模型归纳如图 1 所示：

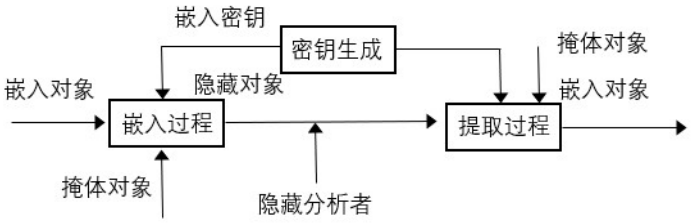

图 1: 信息隐藏系统的一般模型

其中可以看出，系统包括一个嵌入过程和一个提取过程。隐藏对象在传输过程中会面临可能存在的隐藏攻击者的信息攻击及分析。在提取过程中，掩体对象不是必要的。在军事应用中，为了提高保密性一般需要预先对待隐藏信息进行预处理，如：加密，相应的也需要在提取后对得到的嵌入对象进行后处理，如：解密，恢复原始信息。

信息隐藏技术的研究主要分为隐藏技术和隐藏分析技术两部分 [2]。前者的主要内容是寻求向掩体对象中秘密地添加嵌入对象的方法；而后者的主要内容则是考虑如何将发掘隐藏对象中嵌入对象的存在，进而能够破解出嵌入对象，或者可以对隐藏对象进行处理，达到破坏嵌入对象或阻止对方提取嵌入对象的目的，在此过程中使用的算法我们称之为分析算法，其中，用于隐藏信息检测的算法我们又称为检测算法 [3]。

1.2 信息隐藏技术分支

信息隐藏技术作为一门综合交叉学科，所涉及的领域与应用非常广泛，我们可以将其归纳如图 2：

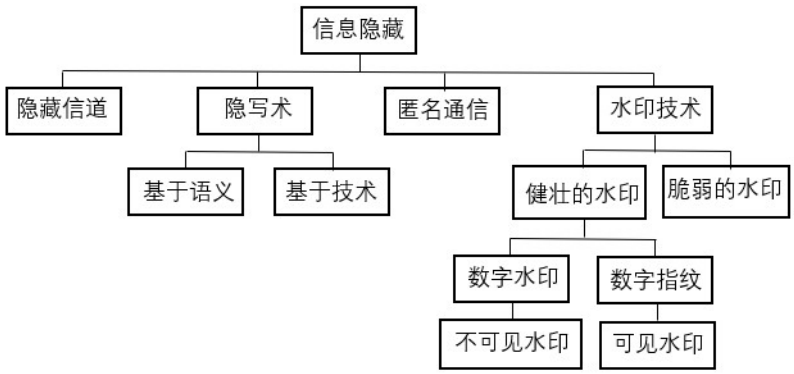

图 2: 信息隐藏的主要分支

其中隐蔽信道是指在多级安全水平的系统环境中，并不是专门设计且不应用于传输信息的通信路径称为隐蔽信道。匿名信道指的是寻求各种途径来隐藏通信的主体，即信息的发送者和接收者。隐写术是信息隐藏学的一个重要分支。相比叫密码学研究如何保护信息内容，隐写术更多的侧重于研究如何隐藏实际存在的信息。主要分为基于语义的隐写术和基于技术的隐写术。而最后一大类水印技术与隐写术不同，它并不总是要隐藏起来，而是需要增加健壮性以应对各种可能的攻击。当水印信息不是数字产品的版权信息，而是购买者的身份识别信息，这种水印技术被称为数字指纹，目的就是为了鉴别产品的非法分发者。

2 国内外研究现状

自信息隐蔽技术提出之后十几年的研究和反战，信息隐蔽技术已经成为当下信息安全领域中一个热门的研究方向，众多优秀的成熟学科如：密码学、信息论等相关学科中的理论资源都可以运用到信息隐蔽技术中来。自从 1994 年信息隐蔽技术在国际上被提出来，发展迅速。1996 年，在英国剑桥牛顿研究所召开了第一届国际信息隐蔽学术研讨会，至今已在许多西方国家举办了多届国际研讨会。国际学术界也有许多关于信息隐蔽技术的文章

发表，几个国际学术期刊也相继出版了有关的专题。

在国内，信息隐蔽技术也是热门的研究方向。1995 年 5 月，在北京组织召开了“网络计算和信息安全论坛”，强调了研究信息隐蔽的重要性。国家“863”计划也包含有信息隐蔽方面的专项课题。国内的学术期刊，近几年来也陆续发表了大量的有关信息隐蔽技术的文章。

不过总的来说，信息隐藏技术还未完全成熟，依然不能实现大规模的推广，从理论和实践上都还存在着许多问题。并且目前为止，自身也没有一套完整的理论体系。对于理论研究，技术开放和实用性方面的发展还不成熟。

3 信息隐藏技术的应用

3.1 基于 GAN 图像生成的信息隐藏技术

目前深度学习技术取得了很大的突破，这些模型一般都是建立在对判别模型的改进优化和利用上 [4]，而生成式对抗网络则是在关注判别器的同时，也对生成器进行了改进，生成式对抗网络 [5] 是由 Goodfelllow 等人提出的一种生成模型。GAN 模型 [6] 中含有一个生成器 G 和一个判别器 D，生成器和判别器同时被训练，二者不断进行对抗博弈，最终达到纳什均衡，输出的结果可以高度拟合原图像。事实上，生成对抗网络就是对学习训练数据的近似拟合。

生成式对抗网络在研究应用中最广泛的就是用于图像的生成 [7]。GAN 模型生成图像的基本过程如图 3 所示:

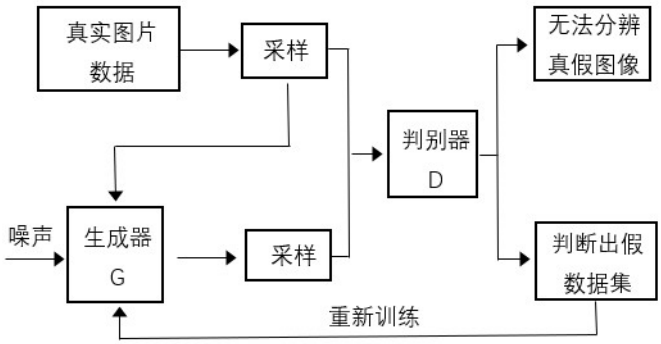

图 3: GAN 模型

在图像生成系统中，生成器 G 根据输入的随机噪声，通过训练生成假图像，

而判别器 D 的工作就是将数据集和生成器 G 生成的加图片集进行对比。在整个对抗博弈过程中，如果判别器 D 不能分别出伪造的图像，则证明前面的生成器的参数和学习方法有效，反之，则需重新修改生成器 D 的参数和训练方法，提高和真实数据的拟合度。在无监管情况下，GAN 还有很大的发展空间，但是由于无监管学习机制会导致生成器产生的图片严重违背常理，而判别器会出现判别失误分数过高的情况，所以说明生成式对抗网络的原始模型在控制图像的内容上有着很大的局限性。因此很多新的方法应运而生。

GAN 在隐写上的一些具体应用 [8]，大致可以分为两种，一种是有载体，一种是无载体。前者首先需要做的就是构造载体，我们可以将其具体分为 3 种不同的类型：1）SGAN；2）SSGAN；3）StegoWGAN。针对这三种基于图片为载体的隐写方式我们做了比较，如表 1 所示:

隐写方式	模型	判别器 S	隐写效果
SGAN	DCGAN	类似 DCGAN 判别器	有一定的抗隐写分析能力
SSGAN	WGAN	GNCNN	图片质量较好，抗隐写分析能力较强
StegoWGAN	WGAN	GNCNN	训练时间最短，抗隐写分析能力最强

表 1: 3 种隐写方式对比

3.2 基于深度学习的多媒体信息隐藏技术

随着深度学习近些年来的迅速发展，在信息隐藏领域，很多研究是利用深度神经网络来进行隐写分析的，而专门利用深度学习来对信息进行隐藏处理的比较少，所以该方法在一定程度上推动了深度学习与信息隐藏两者之间的结合。

首先，衡量现代信息隐藏技术质量的指标大致有三点，分别是：容量，透明性和鲁棒性。容量在这里指的就是在单位时间惑着一幅作品中能够实际嵌入的隐藏消息数；透明性指的是所嵌入信息不被探测到的程度，也称不可感知性；鲁棒性指的是隐写载体抵抗不同种类信号处理攻击的能力，是数字水印比较注重的特征。这三个指标它们之间的关系往往是相互对立的，不

能同时满足，高鲁棒性的算法往往修改了图像的重要部分以抵御攻击，因此对图像的改动比较大，会导致透明性指标下降。

其所用到的深度网络结构如图 4 所示 [9]，原始音频 A_0 首先经过频域变换，变换后即进入编码层网络，在这里进行秘密信息的嵌入，以及频域的反变换，完成后即可得到编码完成的音频 A_e；然后进入解码层网络 [10]，由此处进行隐藏信息的重建，得到 M_e。

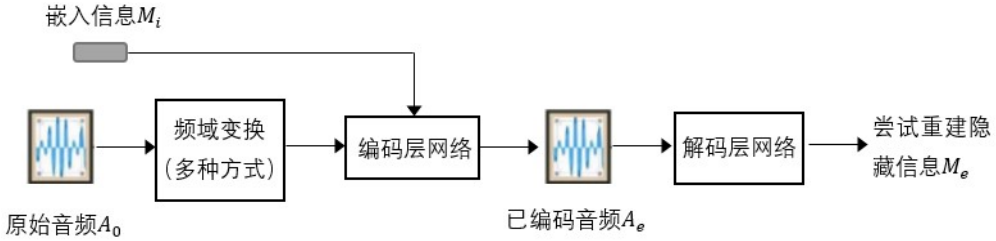

图 4: 音频信息隐藏的深度网络结构

4 总结和展望

本文主要介绍了信息隐藏技术目前的发展现状以及部分应用，简单了解了基于 GAN 的图像信息隐藏技术和基于深度学习的多媒体信息隐藏技术等。随着信息技术的高速发展，信息隐藏技术也面临着更大的挑战，在隐写技术不断提高的环境下，对于隐写技术也应该顺应时代的变化进行更进一步的研究。随着多种技术引入信息隐藏技术领域，如深度学习技术，我们更应该广泛的将其应用到信息隐藏技术的方方面面，进一步完善和优化生成式对抗网络的模型，引入新的架构，并将其应用到隐写技术上。

参考文献

[1] 李强, 郭震华, 晁冰. 信息隐藏技术及其应用 [J]. 安徽电子信息职业技术学院学报,2004,003(005):30-32.

[2] 刘峰, 张鹏. 信息隐藏技术及其应用 [J]. 天津通信技术,2001,000(001):1-4.

[3] 张卫明, 田辉. 信息隐藏技术及应用 [J]. 网信军民融合,2017,000(006):P.75-77.

[4] 周琳娜, 吕欣一. 基于 GAN 图像生成的信息隐藏技术综述 [J]. 信息安全研究,2019,5(09):771-777.

[5] 刘佳, 柯彦, 雷雨等. 生成对抗网络在图像隐写中的应用 [J]. 武汉大学学报 (理学版),2019,65(02):139-152.

[6] 宋好娴. 基于生成模型的无载体信息隐藏 [D]. 河南师范大学,2018.

[7] 王耀杰, 钮可, 杨晓元. 基于生成对抗网络的信息隐藏方案 [J]. 计算机应用,2018,38(10):2923-2928.

[8] 刘明明, 张敏情, 刘佳等. 基于生成对抗网络的无载体信息隐藏 [J]. 应用科学学报,2018,36(02):371-382.

[9] 雷朴承. 基于深度学习的多媒体信息隐藏技术 [J]. 电子技术与软件工程,2019(11):250.

[10] Goodfellow I., Pouget-Abadie J., Mirza M, et al[OL]. Generative Adversarial Networks. (2014-06-11)[2019-04-28] In: Advances in Neural Information Processing Systems, Springer, Berlin, 2672-2680.