软件水印

软件水印(Software WaterMarking)是数字水印技术的分支，是近年来出现的软件产品版权保护技术，可以用来标识作者、发行商、所有者、使用者等信息，并携带有版权保护信息和身份认证信息，可以鉴别出非法复制和盗用的软件产品。

技术介绍

根据软件水印的提取技术来分，可分为静态水印和动态水印。静态水印存储在可执行程序代码中，比较典型的是把水印信息放在安装模块部分，或者是指令代码中，或者是调试信息的符号部分。对于 Java 程序，水印信息也可以隐藏在类文件（包括常量池表、方法表、行号表）的任何部分中。

静态水印又可以进一步分为静态数据水印和静态代码水印。区别于静态水印，动态水印则保存在程序的执行状态中，而不是程序源代码本身。这种水印可用于证明程序是否经过了迷乱变换处理。

动态水印主要有 3 类：Easter Egg 水印、数据结构水印和执行状态水印。其中，每种情况都需要有预先输入，然后根据输入，程序会运行到某种状态，这些状态就代表水印。

评价标准

在保证嵌入水印后的软件，与原软件在功能一致的前提下，衡量软件水印技术好坏的标准主要有以下 3 个:

(1) 隐藏信息量(adatote):表示程序代码中嵌入的水印数据量。

(2) 隐蔽性 (staeh)h:表示嵌入数据对于观察者的不可察觉程度。

(3) 弹性 (resilecn)e:表示嵌入数据对攻击的免疫程度。

对水印的攻击 :攻击者必须在保证攻击后的软件功能不变的前提下对水印进行一系列操作。水印需要具备一定的弹性以抵御这些攻击。主要的攻击方式有以下 4 类:

(1) 去除攻击(subtractiveattack):将水印信息从软件中去除。

(2) 变形攻击(disotrtiveattack):对水印程序进行模糊变换，使攻击后的软件不能提取出水印，或者使提取的水印不再具有版权证明作用。

(3) 添加攻击(addilivealtack):往软件中添加新的水印使原水印无法提取，或者使提取的水印不再具有版权证明作用。

(4) 共谋攻击(collusiveattack):通过比较几个不同软件，找出嵌入的水印，从而破坏它。

软件水印技术是近几年来国际学术界才兴起的一个前沿研究领域，处于迅速发展阶段，而软件水印又是其中的一个重要组成部分，因此作为软件安全领域中的新生事物，具有很高的技术含量和很强的生命力，而成为保护软件所有权的有力武器。