用水印实现溯源同时防止盗版泄露的一种设想

Hollow Man

(一)　需要解决问题的分析

对于在屏幕上加水印来追踪泄露源头，实现防止泄密，最保险的方法是做一个自己编写的特殊文档阅读器，从源头进行打水印，增强安全性。同时，为了防止文件盗版泄露，文件必须是加密的，并且每次文档被打开时记录打开者的身份信息。只有用这种方法我们才能确保别有用心的人无法用其他方法规避使用我们的特殊文档阅读器打开文档。同时对于打水印，我们需要想到，截图者完全可以用 OCR 等一些文字识别软件，将图片识别成文字进行盗取文章内容。因而水印必须对类似的一些识别软件的识别产生干扰。

(二)　我的设想

首先为了确认身份和追踪溯源，阅读者必须获得文档发布者的一个授权的账号和密码来打开文件。文档发布者在发布文档时使用密钥进行加密。阅读器在被打开后，要求用户输入账号和密码，进行登录，登陆时使用 RSA 和 HTTPS 进行服务器和软件之间的加密传输，同时发送软件自身的 MD5 码进行校验，以确保软件自身没有被恶意者非法篡改，并且同时发送设备的机器识别码（根据硬件环境生成，这种技术已经被用于许多软件的防盗版，如果是手机端则发送 IMEI 号）给服务器进行校验，如果该设备不在授权的设备列表里，则进行二次确认，防止授权账号被盗号。

如果服务器确认没有异常，则发送给阅读器解密文档的密钥和在文件中记录阅读者设备和账号信息的加密文档，阅读器可以用解密密钥解密文档供阅读者进行阅读，同时再次确认文档中包含的阅读者设备和账号信息是否跟本设备当前信息一致，防止恶意用户打开从非法渠道获取的文件，这样就可以实现文件泄露的溯源（泄露的文件里记录着阅读者阅读设备和账号信息）。同时根据设备的机器识别码和账号信息产生类似于二维码的水印，这种水印同时也具有二维码的功能，还必须要有极强的容错能力，使得即使恶意者将截图中的水印进行破坏时也能进行溯源。这种水印由杂乱的彩色像素点构成，在阅读者能识别出文字的情况下，干扰文字识别软件的工作（类似于现在的一些防验证码破解技术）。如果发生了截图泄露事件，我们便可以通过水印来获知泄露设备和账号的源头，及时止损。