

档案守护者 CryptoDefender

钟天乐 / 香港玛利诺神父教会学校
指导教师 陶婉雯

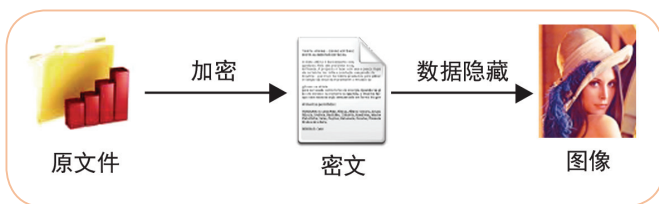


图 1 CryptoDefender 保护文件的流程

◎ 研究背景

直接储存商业档案且意外地被他人开启，这实在是十分危险的。其实，现在市面上有很多加密软件能够解决以上问题。可是，它们始终未能吸引使用者使用。有调查数据显示，67% 的公司没有将储存在 U 盘的商业文件加密，所以推出一种方便使用者保护档案的软件是十分必要的。

直接将文件加密并不够安全，因为文件加密后，乱码数据还会引起不怀好意者的疑心，他们可能会尝试破解文件真正的内容。因此需要更好地隐藏加密文件，使人们不会发现其中包含有一些机密信息。因此，我研发了 CryptoDefender 来解决这个问题，它只需一键点击就可为文档加密。该软件可以作为插件添加到各种应用软件中，如 Word、Excel 和 Access 等。一次点击后保护文件的程序就可以执行，自动加密和更改待加密文档的格式，以减少他人对文件的疑心。

◎ 工作原理

使用 CryptoDefender 加密文件时，使用者只需输入密码和选择图像，之后

待加密文件就会加密为一张图像。换言之加密后的数据会储存在图形文件中而不是原来的文件格式。

在恢复文件时，使用者需要选择含有加密文件的图像文件并输入密码，CryptoDefender 就会把档案解密从而得出原来的文件。保护和解密的流程都很简单，使用者额外的工作就是只需要输入密码及选择图像，非常方便。

图 1 显示了 CryptoDefender 保护文件的工作流程：

- ◆ 用 CryptoDefender 保存文件；
- ◆ 该文件被加密成密文（这是一个包含无意义字符的文件）；
- ◆ 由于密文会引起他人疑心，因此密文会被收藏于图像里。

如果密文不是存放在图像文件里，则使用普通的应用软件开启密文文件后会出现一些乱码，这就会引起别人的疑心。CryptoDefender 进一步把密文储存在图像中，其他人就不容易知道哪张图像包含经过加密的密文，从而减低疑心。

◎ CryptoDefender 的程序实现

➤ 插件与功能区界面

CryptoDefender 是多种应用软件

的附加插件，它给软件提供了更多的功能且不会影响软件原本的功能。在功能列上，它是一个按键，并提供另一种方法去储存及开启档案。CryptoDefender 适合各类支持插件的应用软件。

CryptoDefender 已可以在微软 Office 2007 下成功运行，例如 Word、Excel 等。安装 CryptoDefender 后，在这些软件界面的功能区中，会增加一个功能列“CryptoDefender”，功能列上有 3 个功能：“Protect（加密）”、“Decrypt（解密）”以及“Quick Protect（快速加密）”，见图 2。使用者只需要按下相应按键，档案就能够加密和解密，而不会占用太多的时间，因此这是一个安全又方便的工具。

➤ 加密

CryptoDefender 的加密操作中，会进行几个步骤去增加文件的复杂性。它们是重新排列、数据与密码相加及哈希函数处理。用 CryptoDefender 加密后，数据经过了 2 次重新排列，因此它的复杂性增加。程序使用了哈希函数（散列函数）来保护密码。它将密码转化为乱码，而且乱码不能通过比较操作来破解密码。此外，加密和解密的速度亦相当之快，所以 CryptoDefender 的加密



图2 Microsoft Word 2007 功能区中的插件

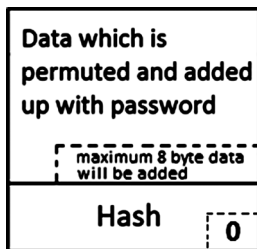


图3 加密后的数据结构

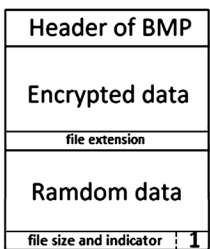


图4 保护后的文件结构

方法是安全又快捷的。

➤ 数据隐藏

数据隐藏的第一种方法是程序直接读取数据，再把数据转化为 24 位位图一个个像素的颜色值。因此，3 个字节的数据会组成一个像素，而这些像素就会组成一张图像。这个方法能够产生好像电视机上的雪花一样的图像，而且不会直接让人看到加密后的数据。可是因为它实在太特别，一般人不会制作这样的图，所以图像依然会引起别人的注意，因此这个方法并不太适合用来收藏数据。

第二种方法有所进步。这个方法会把数据先变为图像，每 3 个字节的数据会组成一个像素，图像的效果与方法一相同；然后，程序会把颜色值分开到 2 张图像，当 2 个图像的对应点的颜色值相加，就可以得出原来的颜色值。例如，以方法一生成的原图某个像素的 RGB 颜色值是 90、60、30，分成 2 张图后第一张图的 RGB 颜色值是 30、50、10，第二张图的 RGB 颜色值是 60、10、20。如果将两图片重叠，颜色值相加，程序就能得出加密后的数据 90、60、30。这个方法以 2 张图像输出，当这 2 张图像的 RGB 颜色值相加后，就会得出加密后资料的 RGB 颜色值。而这两张图的效果与方法一生成的图一样。加密后的数据会收藏于 2 张分开的图像，因此数据比方法一得出的数据更不容易被破解。但这个方法对于使用者

实在不方便，而且加密后的数据还是容易引起人们的注意，因为图像所显示的是没有意义的内容。

第三种隐藏方法需要一张现成的图像进行加密。程序会将原图的每一个像素扩展至几个像素使它们组成一个正方块。而正方块的大小是按加密后的数据量而定的。在正方块里，一半的像素会用来储存加密后的数据，而余下的一半则保留它原来的颜色。而这些像素的正方块就会组成一张新的图像。

例如：档案 A 需要加密，而图像 A 会用来隐藏数据。程序把图像 A 的每个像素扩展成 4、9、16 等等大小的正方块，有些像素会用来隐藏数据，有些就会被保留。例如在一个 4 个像素的正方块中，2 个像素会用来收藏加密数据，2 个像素会保留它的颜色以维持原来图像 A 的颜色。这个方法以正常的图像作输出，图像的质量亦比方法一、二要好。这种方法能降低黑客的疑心，因为图片显示的内容是真实且较普通的。可是，图像还是带有雪花，还有可能引起黑客的疑心。此外，使用这种方法，文件最小也是原文件的 4 倍。

CryptoDefender 所采用的方法与以上三种都不同，它利用 RGB 的概念来隐藏数据。在 24 位的位图中，RGB 是代表每个像素的颜色，它们各为 8 位。每个字节最左边的位拥有最高的值，而最右则拥有最小的值。因此，转变最右位（低位）的影响对整个字节及颜色的

影响都是十分小的。此外，人类的肉眼对红色最敏感，因此对于红色只改变最低 2 位，绿色和蓝色则改变最低 3 位，因此 1 个像素会储存 1 个字节的加密后的数据。如果图像大于加密后的数据，余下的像素就用随机的数据做相同的取代处理。与上述三个方法相比，这个方法产生的图像质量最高，数据隐藏的压缩率也很高。最后得出的图与原图一样大小，图像的颜色转变也很小，肉眼是不容易辨认出图像的变化。这个方法的唯一限制就是不要选择一些太有名或太流行的图像，这样他人便很难知道图像有所改变。

➤ 数据结构

图 3 显示了加密后的数据的结构。加密后的数据会分为两部分。第一部分是经过重新排列及加上密码的数据。为满足重新排列的需要，可能要添加最多 8 个字节。第二部分是由密码转化的 32 个字节的乱码信息。如果使用者只选择加密，文件最后的字节就会写作“0”，以分辨档案只进行加密或同时进行加密与数据隐藏。加密后，数据会隐藏于一张位图。图像的结构又会分作 5 部分。图 4 为保护后的文件结构。第一部分是位图的文件头。第二部分是加密后的数据。第三部分用 1 个字节储存档案的格式。第四部分是当位图给予储放数据的空间多于加密的数据时添加的随机数据。在第五部分，用 8 个字节来储存档案的大小，G 值用来储存档案的格式，

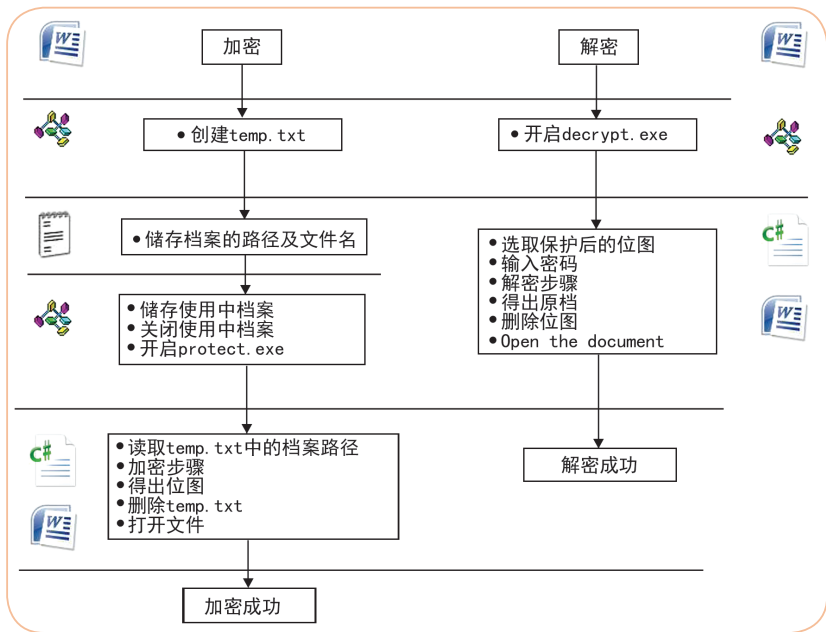


图5 CryptoDefender 程序工作流程图

最后一个字节会被写为“1”。

➤ 程序结构

这个插件的主要3个档案分别是：CryptoDefender.docm、protect.exe及encrypt.exe，它们是用VBA和C#编写出来的。其工作流程见图5。

➤ 安全测试

安全测试时使用brute-force attack（穷举法攻击）去破解加密后的档案。这个方法是最流行的破解方法。破解计算机使用的CPU是Intel core i7。在这种硬件条件下，破解加密后的文件理论上需要的时间约为9万年。实际上，真正破解所需的时间会比预期的短，因为CPU的技术会每年提升。例如，如果预期的破解时间是100年，最后可能只需10年。即便如此，破解的时间也是可以接受的。

◎ 总结及发展设想

CryptoDefender的出现让使用者能够更方便地防止数据外泄的意外发生。CryptoDefender是一个应用软件中的插件，其一键保护的操作方式节省了使用者的时间，能够保护档案及防止

档案被他人直接打开阅读。

在数据加密时，CryptoDefender把数据重新排列2次去增加数据的复杂性。此外，数据会与密码相加组成密文，又用哈希函数作为密码的保护。因此加密的数据及密码都十分安全。

在数据隐藏时，CryptoDefender使用了24位位图去隐藏数据。高质量的图像输出、高压缩比率及图像输出的大小与原图大小一样是它来做数据隐藏的好处。数据隐藏最好的方法是减低别人的疑心，CryptoDefender恰好做到了这一点。

CryptoDefender下一步的改进就是当使用者要保护文件时，只需按下按键，计算机的摄像头便会立即拍摄图像进行保护。这既方便使用者使用，安全度也相对增加。因为被加密文件打开后，只是一张使用者的自拍照，没有什么特别，他人不会知道图像里面隐藏了数据。

其次，程序不但应该能够在Windows中使用，还希望在更多的平台中使用，例如Linux、Windows Mobile等不同操作系统中的更多应用软件中都应该可以安装

CryptoDefender，使该软件能够得到普及。

接着，CryptoDefender应该能够给使用者提供更多选择，让使用者可以把加密后的文件转为不同的文件格式，比如声音文件（mp3）、压缩图文件（jpg）、视频文件（mp4）等。如果一个文件夹中存放了不同格式的文件，就更加不易引起他人的疑心。

最后，程序的结构还可以优化，使得运算的工作量减少，使用户可以更加快捷方便地使用。

该项目获得第25届全国青少年科技创新大赛创新成果竞赛项目中学组计算机科学一等奖。

专家评语

该项目创新性地设计了一种数据加密方法，提出了一种新颖的文件隐藏方式，即降低他人的疑心。该选题具有重要的应用价值，具有产品化前景，希望进一步完善。■