相信裡的另類玄機

◆ 社團法人台灣 E 化資安分析管理協會、朝陽科技大學資訊管理系教授 — 呂慈純

「資訊隱藏」對一般民眾而言是個陌生的字辭，感覺好像是有了網路、電腦後才聽聞過。然而，它可是在久遠的時代就存在了！

資訊隱藏大小事

西元前 4 百年左右，斯巴達的來山得（Lysander）將軍接獲了一個木條和一個上面寫滿字的皮條，當時的他一臉疑惑，完全不曉得發生什麼事。經過了 3 天 3 夜的思考，終於讓他發現，原來只要按照一定的方向和角度，將皮條繞在木條上，就可以順利看到皮條上面的訊息。這個就是資訊隱藏的精髓，將資訊隱藏在看不到的地方，躲過敵人的耳目，成功進行資訊傳遞。這就是資訊隱藏存在的目的之一——**機密訊息傳遞**。

這個木棒稱之為「斯巴達密碼棒」（Scytale）。著名的卡通《名偵探柯南》就有一集劇情是利用紙條和雨傘當作媒介，使用旋轉溜滑梯提示紙條旋轉的角度，組合出破案的關鍵。

知名動畫《名偵探柯南》中使用斯巴達密碼棒概念構成的隱藏訊息。（圖片來源：青山剛昌；TMS 娛樂）

斯巴達密碼棒是由一條加工過、夾帶著訊息的皮革纏繞在一根木棒上所組成。（Photo Credit: Wikimedia, https://w.wiki/5ZGT）

由於這項資訊隱藏的手法讓人拍案叫絕，因此也常被使用在各種影劇中。例如電影《達文西密碼》，羅浮宮館長利用隱形墨水在地上、蒙娜麗莎的微笑、岩窟中的聖母後面，留下訊息給男女主角。

留下的訊息“O, Draconian Devil”（啊！嚴峻的魔鬼），其實是利用變位字的“Leonardo da Vinci”（李奧納多·達文西）；訊息“Oh, Lame Saint”（啊！跛足的聖人）則藏入了“The Mona Lisa”（蒙那麗莎）等訊息，變位字技巧如圖所示，它巧妙的安排在不同的位置上，將字抽取出來就可以拼出原來的訊息。

古代中國也有相同的技巧，稱之為離合詩（Acrostic），此種詩體每一行的首字母、尾字母或其他特定處的字母能夠組合成一個詞或一句話。

周星馳著名的電影《唐伯虎點秋香》，唐伯虎為秋香寫的情詩：

《我愛秋香》

我畫藍江水悠悠，
愛晚亭上楓葉稠。
秋月融融照佛寺，
香煙裊裊繞經樓。

就用了首字藏字技巧，藏了「我愛秋香」告白字句，該詩收錄在明代唐寅的著作中。

此外，剛剛談到的隱形墨水，也是常見的資訊隱藏技術，我們可以利用筆沾取常見的牛奶、橘子汁、醋等，在白紙上寫字，等液體乾掉後，紙上面的字便會消失不見，形成無字天書。等到需要解密時，再利用火進行加熱，寫在紙上面的字就會顯現出來。其主要的原因是上述的液體含有豐富的碳元素，當碳元素接觸到熱就會炭化留下黑色的字跡。

電影《達文西密碼》中，慘遭殺害的羅浮宮館長利用隱形墨水在地上留下隱藏訊息（左），亦有透過變位字技術將訊息藏入文字中的場景（右）。（Photo Credit: Columbia Pictures; Sony Pictures）

資訊隱藏手法大解密

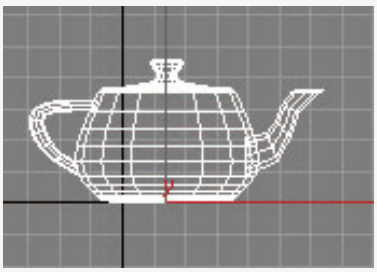
上述的資訊隱藏大概都是技術型的資訊隱藏手法，將訊息放到特定的媒體上，讓它跟原來的媒體差不多，因此躲過第三者的懷疑，成功達到訊息傳遞的目的。

然而在電腦資訊化的時代，人們不可能再用飛鴿傳書和送藏密筒的方式傳遞私密訊息。因此，如何在數位化的環境下，成功的將訊息藏到數位媒體中，就是現代資訊隱藏面臨的問題。

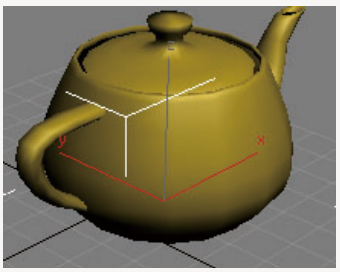
在談到如何隱藏訊息於數位媒體前，要先了解什麼是數位媒體？舉凡影像、圖片、聲音、文字、執行檔、二位元檔等，這些可以儲存在電腦裡面的檔案都可以稱為數位媒體。其中影像最常見的儲存方式有兩種：向量影像和點陣式影像。

向量影像藏入

向量影像中每一個物件都是使用數學式來表達。如圖 1 中的茶壺，是由多個不同的矩形、梯形、三角形、圓形等所組成（圖 1-1），再透過軟體將向量轉成擬真的圖形（圖 1-2）。



1-1 向量影像模型



1-2 擬真向量影像

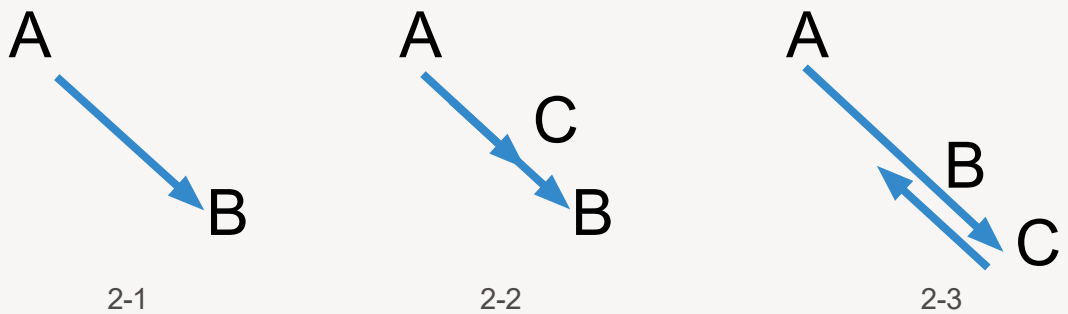
圖 1　向量影像

要在向量圖像中藏入資訊可以利用改變向量影像座標位置，或是放大縮小比例等方式進行，常見的方法有轉置隱藏（Hide Transform）、位移隱藏（Hide Move）、顏色隱藏（Hide Color）、矩陣隱藏（Hide Matrix）等。以位移隱藏法為例，繪製一條線段 A → B（圖 2-1）；如果要藏入的訊息是 0，則讓路徑的順序是 A → C → B，C 點在 A 和 B 點中間（圖 2-2）；反之，若為藏 1 則 C 點在 B 點之後（如圖 2-3）。

頻率域隱藏法

點陣式圖形的資訊隱藏方法有分直接在像素上面做手腳，或者是將這些數值轉換到另一個空間，再進行藏入的，我們稱轉換過去的空間為頻率域（Frequency Domain）。轉換的方式有非常多種，例如博立葉轉換（Transformation de Fourier）、離散餘弦轉換（Discrete Cosine Transform, DCT）、小波轉換（Wavelet Analysis）等。轉換的特性是當轉到另一個空間後，必須要能夠百分之百還原到原始數值，我們稱之為反轉換。科學家利用頻率空間能夠將能量集中的特性，把訊息藏到不易被查覺或是清除的區域，達到訊息交換或是嵌入版權浮水印的目的。例如，圖 3-1 的像素值經過 DCT 轉換後，得到如圖 3-2 的係數值。

DCT 係數的特性是越靠近左上角越重要，如圖 4-1，DC 值是整個區塊最重要的



2-1　2-2　2-3

圖 2　向量影像位移隱藏法

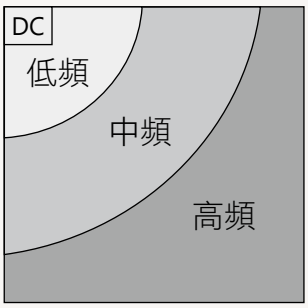
172	172	171	173	171	171	174	172
172	174	174	173	174	174	173	174
170	174	173	172	173	173	171	170
169	172	171	170	171	170	171	174
168	170	174	171	172	173	174	174
169	171	172	172	171	171	172	173
168	171	170	169	169	169	170	174
171	171	169	168	168	171	173	172

3-1 隱蔽區塊

1372	-4	1	-3	-2	-1	0	0
6	2	-3	1	0	0	0	0
0	1	2	2	0	1	-1	-1
0	-1	0	-1	1	1	0	0
-1	-1	2	0	0	1	0	0
-4	0	1	-1	1	-1	-1	0
0	1	-1	1	0	1	0	0
0	0	-1	0	-1	0	0	0

3-2 DCT 係數

圖 3　DCT 頻率係數值



4-1 頻率能量

1372	-4	1	-3	-2	-1	0	0
6	2	-3	1	0	0	0	0
0	1	2	2	0	1	-1	-1
0	-1	0	-1	1	1	0	0
-1	-1	2	0	0	1	0	0
-4	0	1	-1	1	-1	-1	0
0	1	-1	1	0	1	0	0
0	0	-1	0	-1	0	0	0

4-2 可以藏入的空間

圖 4　可供藏入訊息的係數值

數值，其他依序為低頻、中頻及高頻，高頻係數可以用來藏入訊息。例如圖 4-2 右下角框起來的區域，即可用來加入訊息。藏入訊息後，再使用反轉換的方式轉回像素值域，以求得最後藏入訊息的偽裝圖。

文字隱藏

前述的藏頭詩就是一個例子，將訊息巧妙的藏入字首、字尾或字中。現代的文字隱藏方法則是利用不同語言轉換時偷偷進行藏入，例如，將中文的「我愛你」譯成英文時，可以譯成“I love you”，也可以譯成“I like you”，二個的意思表示差不多。我們就可以設定，當要藏入的位元是 0 時使用“love”，如果是要藏 1 則使用“like”。

若是從英文轉成中文，則可以利用中文的一音多字特性進行藏入，一樣使用“I love you”進行翻譯，可以譯成「我愛你」，也可以譯成「我愛妳」，當要藏入的位元是 0 時使用「你」，如果是要藏 1 則使用「妳」。只要字面意思不變，即可達到在不被人發現的情況下，偷偷將訊息藏入的目的。

可逆及不可逆的資訊隱藏

訊息藏入多媒體後稱之為偽裝媒體，當收方收到偽裝媒體，可以利用相對應的取出技術將訊息取出。若當初藏入的方法是以直接破壞原始載體的方式進行，則收方只可單純取出藏在裡面的訊息，而原始載體就只能丟棄不能使用了，這樣的藏入方法，我們稱之為不可逆（Non-Reversible）式資訊隱藏方法。反之，若收方在取出祕密訊息後，還能夠將載體還原到原始狀態，這樣的技術就稱之為可逆（Reversible）式資訊隱藏方法。

可逆式資訊隱藏方法主要應用於醫學、軍事或是數位典藏領域，例如，要將病人的病歷資料放到病患的 MRI 掃描圖中，如圖 5-1，得到偽裝影像圖 5-2。若因藏入訊息導致有些像素變成線條或是出現

5-1 原始影像　5-2 偽裝影像　5-3 回復影像

圖 5　可逆式資訊隱藏技術

白點，則醫生在取出病患病歷資料後，該圖就不能再使用了，因為可能會造成醫生誤判。若使用的是可逆式資訊隱藏技術，則不但可以取出藏入的訊息，還可以將影像還原到原始的狀態，如圖 5-3。

由於可逆式資訊隱藏技術需要顧慮影像是否可以還原，有些技術需要犧牲一些隱藏空間，儲存一些還原的額外訊息，或是藏入的訊息可能不能太多，以維持影像品質及達到可以還原的目的。

結論

資訊隱藏技術無奇不有，從古至今不管是科學家或是一般民眾都可利用隨手可得的物品進行訊息藏匿。資訊隱藏不但提供人們有效的機密訊息交換管道，也可應用在日常的著作保護、竄改偵測等事項中，甚至我們每天都要接觸的紙幣也都可以看到資訊隱藏技術——浮水印的存在。

然而，此項技術也有可能被拿來從事不法行為，造成巨大的災難。例如 911 恐怖攻擊事件，據傳蓋達組織首腦就是利用資訊隱藏技術，將攻擊的時間點、行動訊息藏在網路聊天室、拍賣或色情網站的照片中。

學習資訊隱藏技術不但可了解不法攻擊的方法，提早破解並且做好準備，也可應用在各種不同領域。期望資訊隱藏技術能夠被運用在正途，追求和平、增進人民福祉與便利。

在日常生活中經常接觸的紙幣也可以看到許多資訊隱藏的技術。（圖片來源：中央印製廠，https://www.cepp.gov.tw/Page?key=00ccc&key2=00iqf）

社團法人台灣 E 化資安分析管理協會（ESAM）