防止核心關鍵技術外流-解析《國家安全法》修正重點

新竹市政府政風處副處長/李志強

清流 MJIB

◆ 新竹市政府政風處副處長 — 李志強

立法院於 2022 年 5 月 20 日三讀通過《國家安全法》修正案。

修法重點

由法務部說明可知，本次修法目的是為更周延保護我國高科技產業競爭力與鞏固國家經濟發展成果，並防止國家核心關鍵技術之營業秘密遭到境外敵對勢力或其所設立或實質控制之各類組織、機構、團體或其派遣之人侵害，政府積極建構國家核心關鍵技術營業秘密之層級化保護體系，並完備相關配套法制，解析如下。

保護國家核心關鍵技術

本次《國家安全法》第 3 條除增訂任何人不得為外國、大陸地區、香港、澳門、境外敵對勢力或其所設立或實質控制之各類組織、機構、團體或其派遣之人，為竊取、侵占、越權重製等侵害國家核心關鍵技術營業秘密之行為（即經濟間諜罪）外，[1] 為避免前述技術遭非法流至境外，同時也增訂國家核心關鍵技術營業秘密之域外使用罪。

[1] 依據《國家安全法》第 3 條第 1 項，違法行為有：一、以竊取、侵占、詐術、脅迫、擅自重製或其他不正方法而取得國家核心關鍵技術之營業秘密，或取得後進而使用、洩漏。二、知悉或持有國家核心關鍵技術之營業秘密，未經授權或逾越授權範圍而重製、使用或洩漏該營業秘密。三、持有國家核心關鍵技術之營業秘密，經營業秘密所有人告知應刪除、銷毀後，不為刪除、銷毀或隱匿該營業秘密。四、明知他人知悉或持有之國家核心關鍵技術之營業秘密有前三款所定情形，而取得、使用或洩漏。

《國家安全法》此次修法目的是為更周延保護我國產業競爭力與鞏固經濟發展成果，並防止核心關鍵技術之營業秘密遭到境外敵對勢力或其相關資組織人員侵害。（資料來源：行政院，https://www.ey.gov.tw/Page/9277F759E41CCD91/5d673316-5cc1-4b37-a756-8cd62a9e522d）

此外，為符合刑罰明確性原則，本次修法明定國家核心關鍵技術之定義及範圍，[2] 且規定其認定程序及其他應遵行事項之辦法，授權由國家科學及技術委員會會商有關機關定之，並應定期檢討。

加重級距強化課責機制

為發揮嚴懲及嚇阻效果，《國家安全法》第 8 條就侵害國家核心關鍵技術之營業秘密行為，增訂刑事處罰與科處罰金刑採取加重級距方式，如任何人為大陸地區竊取國家核心關鍵技術之營業秘密者，處 5 年以上 12 年以下有期徒刑，得併科新臺幣（下同）5 百萬元以上 1 億元以下之罰金。另因營業秘密可能涉及龐大之商業利益，所以本次參酌《營業秘密法》之規定，科罰金時，如犯罪行為人所得之利益超過罰金最多額，得於所得利益之 2 倍至 10 倍範圍內酌量加重。本法同時增列鼓勵自首、

[2] 依據《國家安全法》第 3 條第 3 項，所稱國家核心關鍵技術，指如流入外國、大陸地區、香港、澳門或境外敵對勢力，將重大損害國家安全、產業競爭力或經濟發展，且符合下列條件之一者，並經行政院公告生效後，送請立法院備查：一、基於國際公約、國防之需要或國家關鍵基礎設施安全防護考量，應進行管制。二、可促使我國產生領導型技術或大幅提升重要產業競爭力。

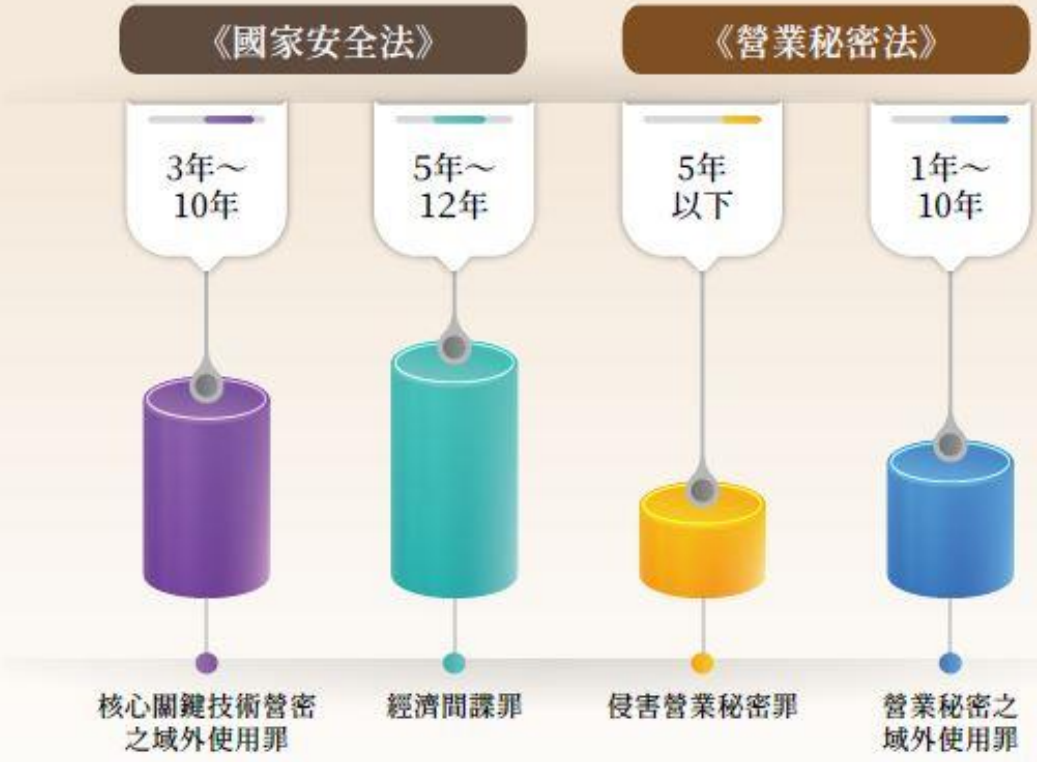


圖 1　《國家安全法》與《營業秘密法》刑責比較

自白等減輕或免除其刑之規定，亦即行為人自首者，得減輕或免除其刑，因而查獲其他正犯或共犯，或防止國家安全或利益受到重大危害情事者，免除其刑；對於偵查中及歷次審判中均自白者，[3]得減輕其刑，行為人若協助查獲其他共犯或預防危害有功者，亦減輕或免除其刑，以符合減免刑責之比例原則。

值得注意者，為更周延保障國家核心關鍵技術之營業秘密不受侵害，促使企業更加重視法令遵循與改善措施，本次增訂法人兩罰與舉證免責等規定。舉例來說，當受雇人因執行業務觸犯「經濟間諜罪」或「國家核心關鍵技術營業秘密之域外使用罪」，自當依法受罰，而為課予業者負有監督防止其員工不法侵害他人國家核心關鍵技術之營業秘密之責任，《國家安全法》明定對該雇主（即法人、非法人團體或自然人）亦科各該項之罰金，但雇主對於犯罪之發生，已盡力為防止行為者，則不在此限。

[3] 行為人於偵查審判中雖業供述內容者，不符減刑以利自新之精神，故《國家安全法》第 8 條第 6 項規定，於偵查中及歷次審判中均自白者，始得減免刑責。

導入偵查保密令之規定

鑑於涉及國家核心關鍵技術之案件，本質上亦為侵害營業秘密，且屬更核心重要之國家級營業秘密，所以《國家安全法》第 9 條增訂檢察官偵辦此類案件時，適用《營業秘密法》有關偵查保密令之規定，[4] 藉此周延保護此類營業秘密於偵查中不致發生二次外洩之風險，並促進偵查效率。另考量此類案件性質上為侵害營業秘密者，故歸屬《智慧財產案件審理法》之智慧財產案件。

此外，侵害國家核心關鍵技術之營業秘密案件，如有違反檢察官核發之偵查保密令者，考量危害程度較一般營業秘密嚴重，故《國家安全法》第 10 條增訂最重本刑 5 年以下有期徒刑、拘役或科或併科 1 百萬元以下罰金，以確保恪遵偵查保密令，且為強化偵查保密令之域外效力，降低發生二次外洩風險，又增訂於外國、大陸地區、香港或澳門違反偵查保密令者，不問犯罪地之法律有無處罰規定，亦適用前項規定。

《國家安全法》第 9 條增訂檢察官偵辦此類案件時，適用《營業秘密法》有關偵查保密令之規定，以保護此類營業秘密於偵查中不致發生二次外洩之風險，並促進偵查效率。

[4] 我國於 2020 年修正《營業秘密法》部分條文，主要是強化偵查過程中對於營業秘密之保護，特別是引進「偵查保密令」制度，重點有：一、檢察官偵辦營業秘密案件認有必要時，得依職權核發偵查保密令。二、受偵查保密令之人不得將偵查內容為偵查程序以外目的之使用，或揭露予未受偵查保密令之人。三、偵查保密令應以書面或言詞為之，且予營業秘密所有人陳述意見之機會；另制定偵查保密令得撤銷或變更之程序，以及面接法院秘密保持命令等。四、違反者課予刑罰。

專業考量設定管轄法院

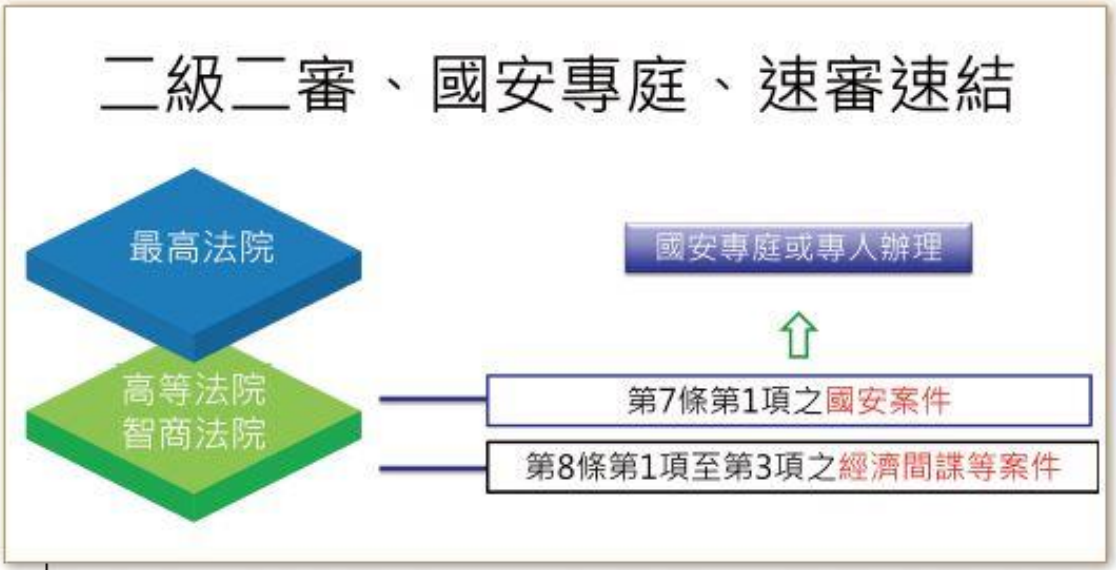
本次修法增訂「經濟間諜罪」及「國家核心關鍵技術營業秘密之域外使用罪」，兩者雖非屬內亂、外患及妨害國交罪之行為態樣，然其對國家法益之侵害程度亦應等同視之。所以《國家安全法》第 18 條增訂上開案件之第一審管轄權屬於智慧財產及商業法院。

在偵查實務上，對與前述兩罪之案件有裁判上一罪或《刑事訴訟法》第 7 條第 1 款（即一人犯數罪者）所定相牽連關係之第一審管轄權屬於高等法院之其他刑事案件，由於檢察官起訴或合併起訴時，究應由高等法院管轄，抑或由智慧財產及商業法院管轄，因法無明文，易生疑義，故本次增訂前開案件經檢察官起訴或合併起訴者，應向智慧財產及商業法院為之。

此外，基於專業考量，第 19 條則增訂法院為審理違反本法之犯罪案件，得設立專業法庭或指定專股辦理，期能速審速結以重懲不法，進而確保我國產業之競爭優勢及更周延保護國家安全。

結語

本次修法不僅攸關國家核心關鍵技術，也與國家安全緊密相關，而直接影響者則是我國高科技產業。如報載因業界至感憂慮與關切，故修法通過後不久，國內



《國家安全法》第 18 條增訂「經濟間諜罪」及「國家核心關鍵技術營業秘密之域外使用罪」第一審管轄權歸屬於智慧財產及商業法院，另於第 19 條增訂法院得設立專業法庭或指定專股辦理，期能速審速結以重懲不法。（資料來源：行政院，https://www.ey.gov.tw/Page/9277F759E41CCD91/5d673316-5cc1-4b37-a756-8cd62a9e522d）

有關國家核心關鍵技術之定義與要件，立法時應與產業界進行充分溝通，然而科技產業趨勢瞬息萬變，對於法條中所列之技術也應適時滾動式調整修正。

高科技廠商即召開會議以研商因應之道。為協助業者釐清疑義，俾利本法推動，最後提出幾點淺見：

首先，本次修法保護之客體為國家核心關鍵技術，雖於法條中有所界定，惟實際上包含哪些技術，依法尚待行政院公告後送請立法院備查，因影響高科技產業之研發、列管人員及業者責任等，所以有關國家核心關鍵技術之定義與要件，應與產業界進行充分溝通，復因科技產業趨勢瞬息萬變，對於核列之技術亦應適時滾動式調整修正。

再者，本法明文國家核心關鍵技術之認定程序，係授權由國家科學及技術委員會會商有關機關決定，所以建議應建立合法可行且可受公正檢驗之審查機制，避免標準或要件不一致使適用範圍過大，造成業者困擾，並提供便民措施，俾利業者提出申請或接受審查。

最後，因現行政府機關常委託、補助或與業者合作開發技術，故在簽訂委託或補助契約時，即應明列國家核心關鍵技術之範圍。相信未來若結合以上方式，將有助業者願意充分配合，始能有效達到修法之目的。

本文摘自清流雙月刊中華民國111年9月 號P10-P15

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）

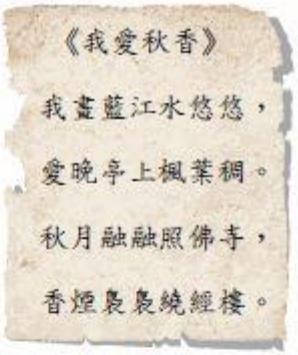
斯巴達密碼棒是由一條加工過、夾帶著訊息的皮革纏繞在一根木棒上所組成。（Photo Credit: Wikimedia, https://w.wiki/5ZGT）

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：



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

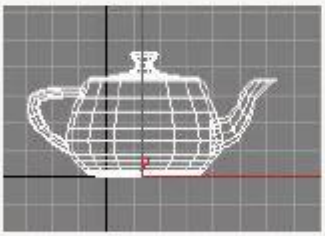
上述的資訊隱藏大概都是技術型的資訊隱藏手法，將訊息放到特定的媒體上，讓它跟原來的媒體差不多，因此躲過第三者的懷疑，成功達到訊息傳遞的目的。

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。

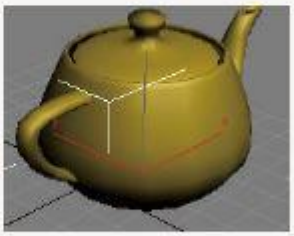
在談到如何隱藏訊息於數位媒體前，要先了解什麼是數位媒體？舉凡影像、圖片、聲音、文字、執行檔、二位元檔等，這些可以儲存在電腦裡面的檔案都可以稱為數位媒體。其中影像最常見的儲存方式有兩種：向量影像和點陣式影像。

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

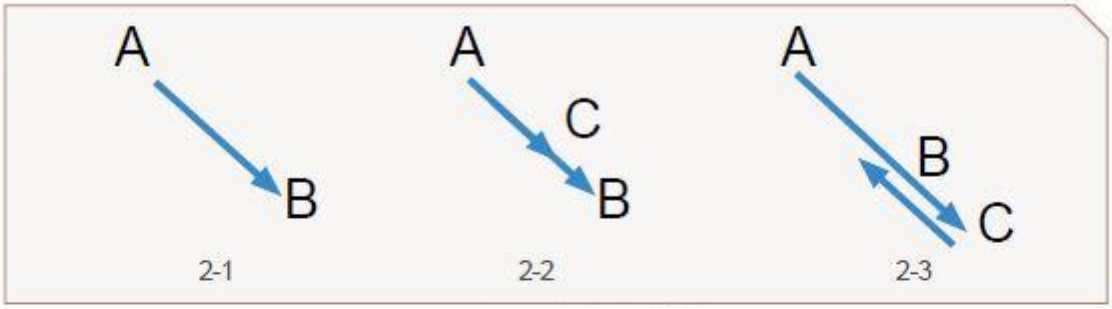
圖 1　向量影像

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

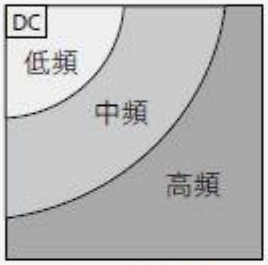
172	172	171	173	171	171	174	172
172	174	174	173	174	174	173	174
170	174	173	172	173	173	171	170
169	172	171	170	171	170	171	174
168	170	174	171	172	173	174	174
169	171	172	172	171	171	172	173
168	171	170	169	169	169	170	174
171	171	169	168	168	171	173	172

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）

本文摘自清流雙月刊中華民國111年9月 號P55-P60