資訊隱藏技術之研究

左豪官[1] 戴鑑廷[1] 盧嘉鴻[2] 婁德權[3] 劉江龍[3] 吳嘉龍[4]

[1]陸軍軍官學校資訊系
[2]陸軍軍官學校電機系
[3]國防大學理工學院電機電子系
[4]空軍航空技術學院一般學科部航空通電系

摘要

由於網際網路及電腦技術的快速發展，使的數位資料的複製與傳送變得簡單而快速；但是卻衍生機密資料容易遭到非法者竊取及竄改等問題。如何確保資料傳輸時的安全性，成為非常重要的議題。而利用資訊隱藏技術來提供機密資料的保護，成為近年來熱門的研究主題。

一個良好的資訊隱藏技術可由幾個方面來評估：即強韌性、不可見性、容量及安全性等。然而這些特性幾乎都是互相衝突的，例如說提高隱藏資料的容量，即會降低資料的隱蔽性及強韌性。因此，發展可以同時滿足上述各項要求的隱藏技術，是目前研究者的最大挑戰。

本論文將針對近年來已發表的資訊隱藏文獻，進行重點式的整理與探討，以提供從事此研究之專家學者於設計資訊隱藏演算法之參考。

關鍵詞：資訊隱藏，強韌性，不可見性

一、前言

由於網路技術的蓬勃發展，無形之中縮短了世界各地的距離，越來越多的資訊均能透過網際網路快速的傳送至接收方，然而對於具有高度機密的資料，當其透過便利的網路傳送時，其安全性就面臨了高度的威脅，為了確保資訊的安全性，在網路上傳送資訊時，均會將資訊先行利用密碼技術進行加密後，再行透過網路傳送，此時若遭到有心人士截取，由於截取到的只是一堆亂碼，有心人士並無法得知你所要傳送的資訊是什麼，因此能夠避免有心人士解讀我們傳送的秘密資訊，進而確保資訊的安全性。

密碼學(cryptography)理論所使用的加解密系統，可以分為兩大類：秘密金鑰系統(secret-key cryptosystem)，如 DES[1]，及公開金鑰系統(public-key cryptosystem)，如 RSA[2]。不論是哪一種密碼系統或是其他影像加密的方法[3-7]，其運作的方式均是將機密文件經由加密運算處理成密文(ciphertext)後，成為無法辨識的亂碼。經過加密的資料在網路傳遞過程中即使遭到非法攔截者竊取，亦無法解密或很困難從中擷取機密訊息，進而達到資訊保密的目的[8]。

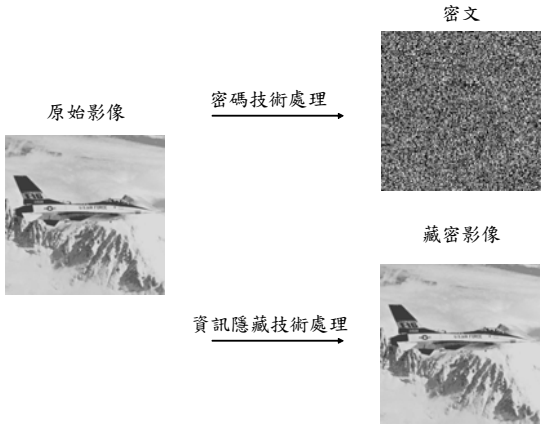
但是密碼技術對於提供資訊的保護性有以下兩種缺點:

1.機密資訊經過加密後是一堆無法辨識的亂碼，在網路傳送時容易增加有心人士破解的機會。

2.密碼技術只能夠對於資訊在傳輸階段提

供保護，無法對於解密後的資料提供永久的保障。

基於上述的缺點，實有必要提出一種安全的保護機密資訊的技術，除了不會讓有心人士產生疑心，並能夠降低資訊被竊取的可能性，資訊隱藏(information hiding)技術因此應運而生，基本上來說，密碼技術與資訊隱藏技術在意義上是有很大的不同，前者利用加密的方法使資訊變成密文，形成一堆無意義的亂碼，比較容易引起敵人的好奇與窺伺。後者則是由另一個觀點出發，利用媒體特性將資訊本身的存在性隱藏起來，令人察覺不到，圖一表示這兩種做法的不同之處，因此機密性的資訊可以利用這項技術來加強資訊傳輸時的安全性。



圖一 密碼技術與資訊隱藏技術之比較

二、資訊隱藏技術分類及特性

近代的科學文獻中對資訊隱藏的討論非常熱烈。而且都提出各種方法來滿足其應用所需特性，但主要可以分成以下兩類作法：

1.空間域(spatial domain)技術：在空間域的方法主要是以直接改變數位媒體資料來達成隱藏目的，通常此類方法可在不破壞原始影像的視覺效果下達成高容量的資訊隱藏。常見的空間域方法有：補丁法(patchwork) [9]、紋理區塊(texture block)編碼法[9]、最低位元置換法(least significant bit insertion, LSB insertion)[10]、向量量化(vector quantization, VQ)編碼藏密法[11]等。

2.轉換域(transform domain)：主要是把空間域中各影像的像素值轉換成頻率域中的係數，再將秘密訊息加入所選定的係數中。通常高頻係數易受資料壓縮技術處理的影響產生誤差，破壞隱藏的資訊，而低頻係數是影像能量集中的地方，稍作修改就容易造成影像的失真，所以一般是將要嵌入的資訊放在中頻係數的部份。常用的轉換方法有離散餘弦轉換(discrete cosine transform，DCT) [12-15]、離散傅立葉轉換(discrete fourier transform，DFT) [16]、小波轉換(discrete wavelet transform) [17-19]等。

一個成功的資訊隱藏系統，其需求與特性因應用領域的不同而異。以下所敘述的是資訊隱藏系統的一般化特性，然而一個安全且可信賴的資訊隱藏技術應該要盡可能達到以下的要求。

1.不可察覺性(imperceptibility)

隱藏之資訊必須為人類感官所難以察覺，對於掩護媒體品質的影響應減至最低，使得非法者不至起疑，如此才能達到隱藏的目的。亦可以說，隱藏之資訊對於原始媒體有良好的透通性(transparency)。

2.強韌性(robustness)

隱藏之資訊必須能承受一些常見非惡意的信號處理，例如：失真壓縮、量化編碼、數位類比轉換、雜訊干擾等，或是經過濾波、剪裁、變形、再取樣、印出再掃描等處理後，仍能存在於媒體之中，不會被移除。甚至一般使用者故意的操作處理，但機密隱藏之資訊仍應不受影響。

3.容量(capacity)

隱藏技術對於資訊的隱藏容量越大越好，較大的容量亦表示有較佳的隱藏性，即在相同的不可察覺性的條件下，能夠隱藏更多的資訊是較佳的隱藏方法。

4.不可偵測性(undetectability)

利用資訊隱藏技術進行秘密通訊時，即使嵌入的資訊無法被人類感覺所察知，並不代表安全無虞，因為媒體本身具有一些與媒體內容相關的性質，當嵌入時更改了這些特性，便可能被以統計方式分析出來，曝露秘密通訊的行為。

5.安全性(security)

隱藏的資訊必須能抵抗非法者的偵測或解碼，不易或不能被非法者從掩護媒體中移除，即使在已知有資訊隱藏的情況下，仍然要保證資訊的安全。

6.有效及簡易(efficiency and simpleness)

隱藏技術要簡單且有效率，資訊的藏入(embedding)與取出(extraction)要快速省時。同時，系統的執行時間和維護成本要盡可能降低。

然而上述六點需求，在實際應用時彼此會有些衝突。例如說提高隱藏資訊的容量，即會降低資訊的隱蔽性及強韌性。一般而言，機密資訊的隱藏容量對於強韌性與不可見性是處於互補的情況[9]，只有在這兩個因素之間取得平衡，才有最佳之藏密效果。因此在資訊隱藏的應用上，必須考量隱藏的容量與其他因素來作比較與取捨。發展可以同時滿足上述各項要求的隱藏技術，是目前研究者的最大挑戰。

三、資訊隱藏技術之回顧

由於轉換域技術比空間域技術更具強韌性，因此，以下均針對轉換域技術進行探討。在 1999 年，Hsu 和 Wu[20]提出一種將資訊隱藏進入影像 DCT 中頻係數的方法，來達成不可見性與強韌性的要求，他們的方法說明如下:

1. 首先產生一個亂數種子(seed)，並利用亂數產生器將浮水印打亂。

2. 將浮水印區分成區塊，然後計算與排序每個區塊黑點的數目，再計算原始影像每個 8×8 區塊的變異數，並進行排序，最後將浮水印與原始影像進行配對與重新排列

3. 將影像區分成 8×8 區塊後，再利用 DCT 轉換成頻率係數。

4. 取出每個區塊的 16 個中頻係數後，組成一個縮減(reduce)後的影像。

5. 修改 DCT 係數

(1)首先計算相鄰區塊中係數的極性(polarity)，如果該區塊係數比前一個區塊係數大，將極性設為 1，否則為 0。最後會得到一個與浮水印大小相同的二元數值方塊 P，然後再與經過排列的浮水印方塊 W_b 進行互斥或運算，得到 $\hat{P}$ 。

(2)根據 $\hat{P}$ 區塊的係數值決定是否修改現行區塊內的係數，如果 $\hat{P}$ 區塊係數值為 1，則該區塊係數值必須比前一區塊內相對應的係數值大，同樣的，如果 $\hat{P}$ 區塊係數值為 0，則該區塊係數值必須比前一區塊內相對應的係數值小，經過上面的調整規則後，就完成了隱藏的動作。

6. 將隱藏後的係數回存至相對應區塊的位置。

7. 將所有係數進行反 DCT 轉換後，就得到隱藏資訊的影像。

浮水印資訊的取出流程需要原始影像的輔助，說明如下:

1. 將原始影像與藏密影像分別區分成 8×8 區塊，並進行 DCT 轉換。

2. 分別取出每個區塊的中頻係數後，產生縮減後的影像。

3. 將縮減後的影像進行兩極化的處理後得到二值化區塊 P 及 $\tilde{P}$ 。

4. 將 P 及 P' 進行互斥或運算後，就能夠取出隱藏的資訊。

5. 利用隱藏程序中步驟 2 的方式還原經亂數擾亂的資料。

6. 利用隱藏程序中步驟 1 所產生的亂數種子(seed)後，利用亂數產生器將資訊還原。

Choi 等人[21]提出一種利用相鄰像素關係來隱藏資訊的方法，他們的方法說明如下:

1.首先將包含 RGB 三色的彩色影像轉換至 YCRCB 的色彩空間。

2.將亮度成分 Y 區分成為 8×8 區塊後，利用 DCT 轉換至頻率係數。

3.取出相鄰 9 個區塊中的 4 個區塊 DC 值 C(0,0)，並計算他們的平均值 M，然後進行資訊的隱藏。

4.將隱藏後的係數取代原先的係數。

5.執行反 DCT 與反 YCRCB 轉換後得到藏密影像。

取出流程則非常簡單，說明如下:

1.首先將包含 RGB 的彩色藏密影像轉換至 YCRCB 的色彩空間。

2.將亮度成分 Y 區分成 8×8 區塊後，利用 DCT 轉換至頻率係數。

3.取出相鄰 9 個區塊中的 4 個區塊 DC 值，並計算他們的平均值，然後取出隱藏的資訊。

Shih 和 Wu[12]提出一種組合空間域與頻率域的資訊隱藏技術，他們的做法是將要隱藏的訊息切成兩個部分，然後將訊息分別隱藏於空間域及頻率域的 LSB，以增大隱藏資訊的容量。

詳細的隱藏方法如下:

1. 將要隱藏的訊息區分成兩個部分 A 和 B。

2. 將訊息 A 取代原始影像的 LSB 後，得到藏密後影像。

3. 將藏密後影像區分成不重疊的 8×8 區塊。

4. 將每個區塊利用 DCT 轉換成為頻率係數。

5. 將訊息 B 隱藏於頻率係數的 LSB。

6. 執行反 DCT 轉換後得到藏密影像。

至於資訊的取出則是隱藏程序的相反過程。

Cheng 等人[13]提出一種基於修改量化表的資訊隱藏技術，他們的做法如下:

1. 首先將要隱藏的訊息透過加密演算法進行加密。

2. 將原始影像區分成為不重疊的 8×8 區塊。

3. 利用 DCT 轉換技術將每個區塊轉換成頻率係數。

4. 利用修改後的量化表對頻率係數進行量化。

5. 將秘密訊息隱藏於選取的中頻係數的最後兩個位元(LTSB)。

6. 對每個區塊執行熵編碼，就產生了經過壓縮的藏密影像。

7. 將密鑰和藏密影像送至接收方。

資訊的取出程序則是隱藏過程的相反程序，說明如下:

1. 對於藏密影像進行反熵編碼的動作。

2. 由選取的中頻係數中，將每個係數的最後兩個位元取出。

3. 透過相同的加密演算法和密鑰將取出的訊息解密後，就能夠得到正確的訊息。

Tseng 和 Chang[14]提出了另一種修改量化表的資訊隱藏技術，不同之處是在量化後的 DCT 係數中，0 的係數越多，隱藏的資訊也越多，詳細的隱藏程序可以區分成為 3 個部分，說明如下:

1.DCT 係數的選取:

(1)首先將影像區分為 8×8 區塊。

(2)利用 DCT 轉換每個區塊成為頻域係數。

(3)利用量化表對於區塊的每個係數進行量化。

(4)計算區塊中係數為 0 的數目，如果大於門檻 T，則該係數就被選為隱藏的係數。

2.量化表的修改:

修改量化表的目的是為了改善隱藏資訊後的影像品質，也就是說隱藏後的影像品質的失真度可以在我們的控制之下。

3.資訊的隱藏:

將被選取 DCT 係數進行反量化後，即進行秘密訊息的隱藏。

Wang 和 Pearmain[15]提出利用估測係數的概念來進行資訊隱藏，他們提出兩種(空間域及頻率域)資訊隱藏技術，在空間域技術上，以 1024×768 的影像來說，若是區分成為 3×3 區塊的話，隱藏容量可以達到 87296 位元，但是影像的品質較差，若是區分成為 9×9 區塊的話，隱藏容量雖然比較低(9605 位元)，但是影像的品質較佳，而且而在頻率域技術上，以 1024×768 的影像來說，隱藏容量可以達到

6720 位元，以 512×512 的影像來說，隱藏的容量則為 2205 位元，雖然頻率域的隱藏容量較少，但是頻率域技術在經過 80%壓縮因子的 JPEG 壓縮後，仍然可以取回全部的資訊。

Chang 等人[22]提出一種利用碎型壓縮(fractal compression)方法的 DCT 技術，首先將要隱藏的資訊利用碎型壓縮方法進行壓縮，然後利用 DES 加密技術進行加密，最後隱藏進入影像的 DCT 中頻區域，由於資訊事先經過壓縮程序，因此可以隱藏較多的資訊進入影像，他們的方法說明如下:

1.利用碎型影像壓縮技術將要隱藏的資訊進行壓縮。

2.利用 DES 加密技術將壓縮過的資料進行加密。

3.區分原始影像成為 8×8 區塊後，利用 DCT 轉換至頻率域。

4.選取中頻區域的係數準備進行隱藏。

5.利用隨機亂數產生器選取不同的區塊。

6.使用隨機亂數產生器由區塊中選取中頻係數。

7.如果選取的係數為 C_i，則可將 C_i 表示如下:

$$C_i = b_7 b_6 ... b_0,\ b_i = \{0,1\}$$

8.將要隱藏的資訊取代 3 個位元 $b_4 b_3 b_2$。

9.為避免影像處理攻擊所造成的資訊遺失，將最後兩個位元 $b_1 b_0$ 修改為“10”。

10.重複上述的隱藏程序直到所有的資訊均完成隱藏後，進行反 DCT 轉換得到藏密影像。

以下敘述如何取出隱藏的資訊:

1.區分原始影像成為 8×8 區塊後，利用 DCT 轉換至頻率域。

2.與隱藏程序一樣，選取隱藏資訊的係數。

3.將選取的係數與“00011100”進行 AND 運算後，就可以獲得 3 個隱藏的資訊。

4.將所有取出的位元集合在一起後，再利用 DES 解密。

5.利用碎型解碼技術恢復秘密的資訊。

四、技術分析

Hsu 和 Wu[20]提出一種將資訊隱藏進入影像 DCT 中頻係數的方法，來達成不可見性與強韌性的要求，他們的方法能夠隱藏的容量為 16384 位元的資訊，然而他們提出的方法需要原始影像才能夠恢復原始的隱藏資訊，這種做法在藏密技術上較不具實用性。

Choi 等人[21]提出一種利用相鄰像素關係來隱藏資訊的方法，他們的方法在 3×3 區塊中隱藏 1 個位元，最多能夠隱藏 5 個位元，以 512×512 影像來說，影像資訊的容量只有 2205 位元。

Shih 和 Wu[12]提出一種組合空間域與頻率域的資訊隱藏技術，他們的做法是將要隱藏的訊息切成兩個部分，然後將訊息分別隱藏於空間域及頻率域的 LSB，以增大隱藏資訊的容量，在他們的方法中，以 256×256 的影像而言，隱藏資訊的容量是 65536 位元，若是要增加隱藏容量則可以達到 131072 位元，但是影像的品質也會因而降低。

Cheng 等人[13]提出一種基於修改量化表的資訊隱藏技術，此種方式的優點是改善了 Jpeg-Jsteg 軟體隱藏容量小的缺點，而且輸出的檔案是經過壓縮後的影像，比較符合目前網路的實際應用。

Tseng 和 Chang[14]提出了另一種修改量化表的資訊隱藏技術，他們提出的方法比 Jpeg-Jsteg 軟體的隱藏容量大，但是最大的缺點就是取回資訊時需要原始圖像的輔助，這在應用上比較不具實用性。

Wang 和 Pearmain[15]提出利用估測係數的概念來進行資訊隱藏，他們提出兩種(空間域及頻率域)資訊隱藏技術，在空間域技術上，以 1024×768 的影像來說，若是區分成為 3×3 區塊的話，隱藏容量可以達到 87296 位元，但是影像的品質較差，若是區分成為 9×9 區塊的話，隱藏容量雖然比較低(9605 位元)，但是影像的品質較

佳，而且而在頻率域技術上，以 1024×768 的影像來說，隱藏容量可以達到 6720 位元，以 512×512 的影像來說，隱藏的容量則為 2205 位元，雖然頻率域的隱藏容量較少，但是頻率域技術在經過 80%壓縮因子的 JPEG 壓縮後，仍然可以取回全部的資訊。

Chang 等人[22]提出一種利用碎型壓縮方法的 DCT 技術，首先將要隱藏的資訊利用碎型壓縮方法進行壓縮，然後利用 DES 加密技術進行加密，最後隱藏進入影像的 DCT 中頻區域，由於資訊事先經過壓縮程序，因此可以隱藏較多的資訊進入影像，在他們的方法中，以一個 M×M 的影像來說，如果每個區塊有 k 個係數可以隱藏，則可以隱藏的資訊量為 $3M^2k/64$ 位元，如果以一個 512×512 的影像來說，每個區塊隱藏 16 個位元，則隱藏容量為 98304 位元。

在上面提出的方法中，以 Tseng 和 Chang[14]提出的修改量化表的方法，其隱藏容量最高(316259 位元)，但是取回資訊時需要原始圖像的輔助，Chang 等人[22]提出利用碎型壓縮方法提高資訊隱藏容量(196608 位元)的方法次之，然而影像品質較差，而 Cheng 等人[9]提出的修改量化表的方法，其隱藏容量雖然比前面的方法低(53248 位元)，但是取回資訊時不需要原始圖像的輔助，而且輸出為 JPEG 影像，是最符合網路上傳輸的實際應用。

五、結論

資訊隱藏技術與密碼技術相較起來，對於機密資訊更能夠提供進一步的保護，因此近年來吸引許多研究者的注意，然而要提出一種滿足所有需求的資訊隱藏技術卻是非常困難的，有鑑於此，本論文對於近年來提出的資訊隱藏技術作一概略性的整理，期望能提供從事此一領域的研究者有新的思考方向。

參考文獻：

[1] NBA FIPS PUB 46-1, Data encryption standard, National Bureau of Standards, Department of Commerce, USA, Jan. 1988.

[2] Rivest, R, Shamir, A., and Adleman, L., “A method for obtaining digital signature and public-key cryptosystems,” Communications of the ACM, Vol. 21, No. 2, pp. 120-126, Feb. 1978.

[3] Bourbakis, N., and Alexopoulos, C., “Picture data encryption using scan patterns,” Pattern Recognition, Vol. 25, No. 6, pp. 567-581, June 1992.

[4] Chang, H. K.-C. and Liu, J.-L., “A linear quadtree compression scheme for image encryption,” Signal Processing: Image Communication, Vol. 10, No. 4, pp. 279-290, Sep. 1997.

[5] Chen, T.-S., Chang, C.-C., and Hwang, M.-S., “Virtual image cryptosystem based upon vector quantization,” IEEE Transactions on Image Processing, Vol. 7, No. 10, pp. 1485-1488, Oct. 1998.

[6] Jan, J.-K., and Tseng, Y.-M., “On the security of image encryption method,” Information Processing Letters, Vol. 60, No. 5, pp. 261-265, Dec. 1996.

[7] Schwartz, C., “A new graphical method for encryption of computer data,” Cryptologia, Vol. 15, No. 10, pp. 43-46, 1991.

[8] Schneier, B., Applied cryptography, John Wiley & Sons, New York, USA, 1993.

[9] Bender, W., Gruh, D., Morimoto, N., and Lu, A., “Techniques for data hiding,” IBM Systems Journal, Vol. 35, pp. 313-336, 1996.

[10] Walton, S., “Image authentication for a slippery new age,” Dr. Dobb’s Journal, Vol. 20, No. 4, pp. 18-26, Apr. 1995.

[11] Chen, T.-S., Chang, C.-C., and Hwang, M.-S., “Virtual image cryptosystem based upon vector quantization,” IEEE Transactions on Image Processing, Vol. 7, No. 10, pp. 1485-1488, Oct. 1998.

[12] Shih, F.-Y., and Wu, S. Y.-T., “Combinational image watermarking in the spatial and frequency domains,”

Pattern Recognition, Vol. 36, No. 4, pp. 969-975, Apr. 2003.

[13] Chang, C.-C., Chen, T.-S., and Chung, L.-Z., “A steganographic method based upon JPEG and quantization table modification,” Information Sciences, Vol. 141, pp. 123-138, 2002.

[14] Tseng, H.-W., and Chang, C.-C., “Steganography using JPEG-compressed images,” Proceedings of The Fourth International Conference on Computer and Information Technology, pp. 12-17, 2004.

[15] Wang, Y., and Pearmain, A., “Blind image data hiding based on self reference,” Pattern Recognition Letters, Vol. 25, pp. 1681-1689, 2004.

[16] Alturki, F., and Mersereau, R., “Secure blind image steganographic technique using discrete fourier transformation,” Proceedings of IEEE International Conference on Image Processing, pp. 542-545, 2001.

[17] Joo, S., Suh, Y., Shin, J., Kikuchi, H., and Cho, S.-J., “A new robust watermark embedding into wavelet DC components,” ETRI Journal, Vol. 24, No. 5, pp. 401-404, 2002.

[18] Hsieh, M.-S., Tseng, D.-C., and Huang, Y.-H., “Hiding digital watermarks using multiresolution wavelet transform,” IEEE Transactions on Industrial Electronics, Vol. 48, No. 5, pp. 875-882, 2001.

[19] Lee, W.-B., and Chen, T.-H., “A public verifiable copy protection technique for still image,” Journal of Systems and Software, Vol. 62, pp. 195-204, 2002.

[20] Hsu, C.-T., and Wu, J.-L., “Hidden Digital Watermarks in Images”, IEEE Transaction on Image Processing, Vol. 8, No. 1, pp. 58-68, Jan. 1999.

[21] Choi, Y., Aizawa, k., and Hatori, M., “Digital watermarking using inter-block correlation,” Proceedings of IEEE International Conference on Image Processing, Vol. II, pp. 216-220, 1999.

[22] Chang, C.-C., Chiang, C.-L., and Hsiao, J.-Y., “A DCT-domain system for hiding fractal compressed images,” Proceedings of IEEE International Conference on Advanced Information Networking and Applications, pp. 1-4, 2005.

Study of information hiding techniques

Hao-Kuan Tso[1], David Chien-Ting Tai[1]. Chia-Hung Lu[2], Der-Chyuan Lou[3], Chia-Long Wu [4], and Jiang-Lung Liu[3]

[1]Department of Computer and Information Science, ROC Military Academy

[2]Department of Electrical Engineering, ROC Military Academy

[3]Department of Electrical Engineering, Institute of Technology, National Defense University

[4]Department of Aviation & Communication Electronics, Chinese Air Force Institute of Technology

Abstract

Due to rapid development of the Internet and computer techniques, duplication and distribution of digital information has become easier and quicker than before. How to protect the security of secret information has become an important researching issue. In recent years, information hiding has become an attractive topic in protecting the secret information and has widely discussed in multidisciplinary fields.

A good technique of information hiding can be estimated by several aspects, including robustness, imperceptibility, capacity, and security. However, these characteristics are mutual conflicting. For example, increasing embedding capacity will degrade the imperceptibility and robustness. Hence, developing a technique that meets above requirements at the same time is a challenge for many researchers. .

The paper will discuss some information hiding techniques that have published to provide some new directions for designing algorithm of information hiding.

Key words：Information hiding, robustness, imperceptibility.