植基於人類視覺靈敏度之可適應性偽裝學技術
A novel adaptive steganography based on human vision sensitivity

盧宏文
中興大學 資訊科學與工程研究所
Email:lu4523@ms1.hinet.net

吳男益
中興大學 資訊科學與工程研究所
Email:rocjfk2000@yahoo.com.tw

王宗銘
中興大學資訊科學與工程研究所
Email: cmwang@cs.nchu.edu.tw

中文摘要

本篇研究論文針對灰階影像提出一個可適應性的影像偽裝學技術。其主要的研究貢獻是在嵌入大量的秘密訊息之後，同時也可以產生一張高品質的偽裝影像。本研究技術嵌入訊息容量的多寡，取決於原始影像的區域性複雜度的高低，在我們的方法中，一個影像內容的複雜度將被分成五個等級，等級愈低代表該區域影像紋理變化愈單調，因此嵌入較少的資料量，以免引起明顯地視覺失真;相對地，等級愈高則代表區域影像紋理變化愈複雜，因此將會嵌入較多的訊息。其所引起的失真度對於人類視覺仍然是不可視的。由於區域等級在嵌入完訊息之後，其等級大小仍然可被維持一致性，因此在訊息擷取時是不需要原圖的。最後，在實驗結果中，我們也將和現存可適應性偽裝學技術比較，証明本研究技術所產生的失真會比較少。

關鍵詞：偽裝學、可適應性、人類視覺靈敏度。

Abstract

This paper presents a novel adaptive steganography for digital grayscale image based on the human visual sensitivity so as to reduce the visual quality degradation after the data are hidden. The payload of each pixel is possible different in an image and the size of payload is assessed by its local image complexity. Basically, we hide more data into more busy area than the smooth area in which the original image feature can be maintained. The proposed scheme is blind since the degree of block complexity is hold before and after embedding data. The experimental results demonstrate the visual quality produced by our scheme is better than the existing technique.

Keywords: Steganography, adaptive, human visual sensitivity

1. 簡介

資訊隱藏技術(information hiding)是近年來是一門熱門的研究課題，它的主要應用包含了--浮水印技術(watermarking)、資料藏密學技術(steganography)與可逆資料隱藏技術(reversible data hiding)等等[1-4]。基本上，這三種技術的性質是類似地，其共同點是改變原始數位多媒體的內容來達到嵌入重要訊息的目的。但是，他們之間的研究需求與應用層面是不太一樣的。如浮水印技術必需追求強韌性(robustness)，以求資料在嵌入多媒體之後，即使多媒體遭受惡意破壞攻擊，其所嵌入的資料尚能存活。而資料藏密學技術(又稱偽裝學技術)通常是追求高隱藏量與高品質的偽裝圖，因此，強韌性不是主要的研究需求。可逆式資料隱藏技術除了具有資料藏密學的功能外，尚具有能力可以在取回所隱藏的資料後，能重建原始影像。但是，可逆式資料隱藏技術其隱藏量是很少的，更甚者，其所產生的失真性是很高的。通常浮水印技術是應用在智慧財產保護，偽裝學技術是應用在秘密通訊上，而可逆式資料隱藏技術是應用在軍事影像、醫療影像或是衛星遙測影像上。本篇論文著重於灰階影像偽裝學技術的研究，更進一步地提出一個高品質，且符合人類視覺靈敏度的可適應性灰階影像偽裝學技術。

影像偽裝學技術最主要是利用一張數位影像來掩護秘密訊息。由於數位影像的外表通常是屬於有意義的圖案，因此當敵人截取到它時，由於外表看不出來有任何的異樣，所以不會懷疑它是一張傳輸秘密訊息的媒介。傳統上，若用現代密碼學系統如 DES 或 RSA 加密技術，其所產生的訊息是屬於毫無意義的亂碼，雖然它很難被破解，但是卻會引起敵人的注意進而遭受攻擊破壞，如此一來，接收的那一方就無法正確還

原資料。如果我們將加密完後的亂碼隱藏在一張有意義的數位多媒體中，則在傳輸的過程其安全性會更高[5]。

由於灰階影像的像素值可以容忍較大的修改幅度，其修改之後所呈現的色彩變化很難被人類視覺所察覺，因此許多關於偽裝學技術的研究大量的著重在灰階影像上。近年來有關影像偽裝學研究技術，由嵌入的過程中是否有考慮人類視覺靈敏度的變化分為二個類型，第一個類型是使用最低位元直接嵌入法(LSBs 技術)，此種類型技術在嵌入時並不考慮人類視覺靈敏度，所以影像中每一個地方的隱藏量都是一樣的。假設使用的是 3-LSBs 技術，則每一個像素值都將攜入 3 個位元的資料。此類型的研究方法目前都著重於如何在相同的隱藏量之下，來提昇偽裝圖的影像品質。LSBs 技術最早是由 Tanaka 等人所提出來的[6]，基於 LSBs 嵌入的技術，學者 Wang 等人提出了一套基於基因演算法以改善偽裝圖影像品質的技術[7]。目前，有關 LSBs 嵌入技術的研究[8-10]，其影像品質與[6,7]相比較，其 PSNR 值約可再提高 3dB。

另外一種類型是可適應性偽裝學技術，此種技術其影像中的訊息隱藏量並非是固定的[11-13]。一張影像以人類視覺靈敏而言，影像邊緣區與影像平滑區的隱藏量並非是相同的。實際上我們可以在較邊緣區塊(即紋理變化較複雜)的位置藏入較多的秘密訊息，其所引發的顏色變化對於人類視覺的感知也不會太大;相對地，在平滑區塊的位置藏入大量的秘密訊息時，就容易就會被肉眼所發覺。因此可適應偽裝學的隱藏量會隨著影像紋理的變化而增加或減少，故影像原始特性是可以被保持的，即邊緣的地方在嵌入資料後，仍然保持邊緣的特性，而平滑的區域在嵌入訊息之後，也可以保留平滑的特性。

可適應技術的研究發展，可依照嵌入的數學式不同產生不一樣的效果。如學者 Wu and Tsai 兩人[11]提出一種以二個連續像素值為主的 PVD(pixel-value differencing)技術，區域複雜度的高低可以用二個連續像素值的差值來判斷，若差值愈大則表示該對像素位於比較邊緣的地方，因此資料量就會嵌入愈多。相反地差值愈小，則表示該對像素位於比較平滑的地方，因此就嵌入較小量的訊息，以免破壞太大引起明顯的視覺上失真。接著，Chang and Tseng 兩人發展出一種類似 PVD 的 SM(side match)技術[12]，在他們的技術中，影像複雜度有參考二個以上相鄰像素值，至多可以使用週遭四個相鄰的像素值來估測影像複雜度。基本上，PVD 與 SM 技術其秘密訊息都是記錄在像素值之間的差值。

有別於PVD與SM的差值嵌入技術，在2005年，Zhang和Wang 兩位學者提出一種符合人類視覺的多樣基底偽裝學技術，簡稱MBNS技術[13]。此種偽裝學技術是利用一個像素值的左邊、左上角與上方等三個緊鄰的像素值的複雜性，來評估像素值的隱藏量。其方法為：計算三個相鄰像素值的標準差，再以標準差的大小來決定秘密訊息的基底(傳統的秘密訊息型態，皆是以二進制居多)，因此此種方式比起一般使用單一性的基底而言，安全性高了許多，且又符合人類視覺的靈敏度。

但是MBNS技術在評估區域複雜性時，所使用的像素值並非是原始的，原因在於MBNS是採用raster scanning來對每一個像素值進行評估的。當原始像素藏完訊息之後，即變成一個已失真且藏有訊息的像素，它會變成下一個像素值的參考值，也就是說前面已失真調整過的像素值，將會被後面的像素值當作計算標準差的參考數值來做運算，這樣可能導致後面所求出的標準差正確性愈來愈低，到最後產生了嚴重的累積性誤差。

從上述三個目前知名的可適應偽裝學技術裡，我們可以得到幾個共同的特性：(1)秘密訊息的藏入量可以是動態的，即依照影像特性的不同而有所改變。(2)整張影像在藏完訊息後，其外表比起LSBs嵌入技術更難察覺有任何失真性。(3)每個像素值的隱藏量估測都有基於人類視覺靈敏度的考慮，因此區域性的隱藏量多寡與區域性的影像紋理成正比。 (4)最重要一點是這些技術在擷取資料時，是不需要原始影像的。

在本篇論文中，我們提出一個高品質的可適應性影像偽裝學的技術，同時具備之前提到的四種特性。為了要準確的判斷影像區域的紋理結構，以致能正確地分辨該區域是屬於平滑區或是邊緣區，本篇論文採

用了獨立區塊式的估測方式，分別分析影像區域的複雜度。我們的新方法將至少使用16個像素(即最小子影像的區塊大小為4×4)來分析影像區域的複雜性，比起上述三種方法(至多只使用4個)，新方法對於影像特性變化的評估更為精準、完善。在我們的新技術中，每一個子影像都將求得它的標準差(一個子影像有一個標準差)，然後統計所有子影像標準差的直方圖。依據直方圖的分佈特性進行容量大小的分配。新方法將子影像複雜度分成五個等級，也就是說，一張影像將有五種大小不一樣的隱藏量。愈高等級的藏愈多資料、而等級較低的即隱藏較小。每一個子影像依照它的標準差將對應一個等級，而它的等級在藏完資料後若有溢位發生，將會被進行校正工作。因此，每一個子影像標準差的等級在資料嵌入前或嵌入後，都將維持一致性。此外，新方法也能維持影像的原始特徵值，所產生的偽裝圖的影像品質是非常好的。

接下來，將詳細介紹本論文的訊息嵌入與取出方法，之後是實驗結果與分析比較，最後是結論與建議。

2. 本論文研究方法

我們的嵌入程序分為三個部份，第一個部份(2.1節)是計算出子影像(即區塊)複雜度之標準差的統計直方圖，接著觀察直方圖的分佈特性設定四個等級的門檻值，以便將直方圖上的區塊標準差分為五個等級，門檻值的設定是符合人類視覺靈敏度且兼具容量與品質的最佳比例配置。第二個部份(2.2節)是資料嵌入的步驟，每一個像素所攜帶的訊息依照它所在的區塊所對應的等級。第三部份(2.3節)確認區塊內所有像素在嵌入完秘密訊息後，判斷原本所屬之等級是否有改變，如果改變的話，可利用本文所提供的方法調整回原等級。

2.1 影像區塊之直方圖統計

首先將整張影像分成若干個 $n\times n$ 且不重疊的子影像(區塊)，其區塊內成員為 $A_{i,j}$ 其中 i=1,2, ...,n. j=1,2, ...,n。每一個子影像的標準差定義為 s，其值可由下列公式推導

$$s=\sqrt{\frac{1}{(n\times n)-1}\sum_{i=1}^{n}\sum_{j=1}^{n}(A_{i,j}-\bar{x})^2} \qquad (1)$$

其中 $\bar{x}$ 指的是該區塊的平均值。

計算所有區塊的塊標準差，假設共有t個區塊，則 s_i, i=1,2, ...,t. 得到所有的標準差之後，我們可以使用統計學的方法，求得所有標準差的直方圖。進一步地在本程序中需要給予四個門檻值，以便將直方圖上所分佈的標準差劃分成五個等級。假設四個門檻值為 th_1、th_2、th_3和th_4，而d_i代表s_i所對應的等級，其等級分類規則如下所示：

$$d_i=\begin{cases}1, if\ \ 0\le s_i < th_1;\\ 2, if\ \ th_1\le s_i < th_2;\\ 3, if\ \ th_2\le s_i < th_3;\\ 4, if\ \ th_3\le s_i < th_4;\\ 5, if\ \ s_i \ge th_4,\end{cases} \qquad (2)$$

如果d_i=1的話，則代表該區塊內每一個的成員只會被嵌入1個位元的訊息，以此類推，若等級為5的話(即d_i=5)，則表示該區塊內的每一個像素值都將被嵌入5個位元的秘密訊息。在下一節中，將介紹資料嵌入的方法，其中參數d_i是很重的參考值。

2.2 資料嵌入的方法

在資料嵌入的過程中採用最佳化 LSBs 嵌入技術[8]。假設一個灰階像素值為 $A_{i,j}$ ，其所要嵌入的訊息量為 d_i 個位元。其嵌入的程序為：先將十進制的灰階值 $A_{i,j}$ 轉換成為 8 個位元的二進制值，再選取 8 個位元的最右邊 d_i 個位元(即 d_i 個最低位元)來藏入的秘密訊息。所謂「嵌入」是指直接將訊息覆蓋過去即可，之後再還原成十進制的灰階值，即成為一個有攜帶訊息的偽裝像素值 $A'_{i,j}$。為了使嵌入的訊息所產生的品質失真能減到最低，我們使用下列公式來找到一個最接近原始像素值的偽裝值 $A''_{i,j}$，其中 $A''_{i,j}$ 所攜帶的訊息是與 $A'_{i,j}$ 一樣的。

$$A''_{i,j}=\begin{cases}A'_{i,j}, if\ |A_{i,j}-A'_{i,j}|\le|A_{i,j}-A'_{i,j(-)}|\le|A_{i,j}-A'_{i,j(+)}|;\\ A'_{i,j(-)}, if\ |A_{i,j}-A'_{i,j(-)}|\le|A_{i,j}-A'_{i,j}|\le|A_{i,j}-A'_{i,j(+)}|;\\ A'_{i,j(+)}, if\ |A_{i,j}-A'_{i,j(+)}|\le|A_{i,j}-A'_{i,j}|\le|A_{i,j}-A'_{i,j(-)}|.\end{cases}$$

其中 $A'_{i,j(-)}=A'_{i,j}-2^{d_i}$ 以及 $A'_{i,j(+)}=A'_{i,j}+2^{d_i}$。加 2^{d_i} 或減 2^{d_i} 實際上是修改的第 d_i+1 位元，這兩個操作並不會影響嵌入在 d_i 個位元中的訊息。故無論是 $A'_{i,j}$、$A'_{i,j(-)}$或 $A'_{i,j(+)}$其二進制中的 d_i 個最低位元所隱藏的訊息都是一樣的，但這三個數值中，有一個是最接近原始像

素值 $A_{i,j}$ 的，因此利用上面的公式，我們可以輕易找到一個失真性最低的數值。

2.3 子影像複雜度等級的一致性校正

當區塊中每一個像素值都嵌入完秘密訊息後，必須再次確認該區塊的等級與原本未嵌入前的等級必須一致。在嵌入完訊息後有可能會發生等級溢位的狀況，即等級上昇與下降等兩種狀況，等級不一致將導致訊息在擷取的過程中會發生錯誤。接下來我們提出等級一致性的檢查與校正步驟。

(1) 首先，定義一個偽裝子影像的標準差、平均數與所對應的等級各自為 s'_i 、 d'_i 及 $\overline{x}'$。標準差 s'_i 可使用 Eq.(1)求得。而所對應的等級 d'_i，必須使用嵌入時的 4 個相同的門檻值與 Eq.(2)來推導。

(2) 其次，判斷該偽裝子影像區塊的等級 d'_i 是否與原本未嵌入前的等級 d_i 是否一致;如果是相同的話，則整個嵌入程序完成，往下讀取下一個子影像區塊繼續做處理。如果等級不一致的話 ($d'_i \neq d_i$)，則必須執行下一步驟(3)，然後再次修改偽裝值 $A''_{i,j}$ 直到 $d_i = d'_i$ 為止。

(3) 在資料嵌入後，會有兩種溢位產生，即 overflow(等級上昇)與 underflow(等級下降)。針對這兩種溢位，我們分別提出兩種校正的技術 --OVERFLOW-REVISED( )程式與 UNDERFLOW-REVISED( )程式。基本上，只要比較 d_i 與 d'_i，就可知道發生那一種溢位了。若 $d'_i > d_i$，則表示發生了 overflow，那就使用 OVERFLOW-REVISED( )程式進行校正動作。相反地，若 $d'_i < d_i$，則使用 UNDERFLOW-REVISED( )程式進行校正。

OVERFLOW-REVISED(th ,d_i)

1 For $j \leftarrow 1$ to $n \times$ n

2 If $s'_i \geq th$ and $A''_{i,j} \geq \overline{x}'_i$ and $A''_{i,j} - 2^{di} \geq 0$

3 Then $A''_{i,j} \leftarrow A''_{i,j} - 2^{di}$

4 Elseif $s'_i \geq th$ and $A''_{i,j} < \overline{x}'_i$ and $A''_{i,j} + 2^{di} \leq 255$

5 Then $A''_{i,j} \leftarrow A''_{i,j} + 2^{di}$

UNDERFLOW-REVISED(th ,d_i)

1 For $j \leftarrow 1$ to $n \times$ n

2 If $s'_i < th$ and $A''_{i,j} \geq \overline{x}'_i$ and $A''_{i,j} - 2^{di} \geq 255$

3 Then $A''_{i,j} \leftarrow A''_{i,j} + 2^{di}$

4 Elseif $s'_i < th$ and $A''_{i,j} < \overline{x}'_i$ and $A''_{i,j} + 2^{di} \geq 0$

5 Then $A''_{i,j} \leftarrow A''_{i,j} - 2^{di}$

在程序OVERFLOW-REVISED( )中的th參數是指子影像原始等級的上邊界(upper boundary)的門檻值，舉例來說，如果子影像是屬於第一級的話，那它的上邊界為門檻值th_1；若子影像屬於第二級的話，那它的上邊界為門檻值th_2，以此類推。而在程序UNDERFLOW-REVISED( )中的th參數是指子影像原始等級的下邊界(low boundary)的門檻值，舉例來說，如果子影像屬於第二級的話，則它的下邊界門檻值為th_1，如果是第三級的話，則它的下邊界門檻值為th_2。

必須注意的是在OVERFLOW-REVISED( )與UNDERFLOW-REVISED( )這兩個程序中，每一次for迴圈結束之後(即程式碼1至5行執行一遍)，代表已經校正完了一個像素值。每校正完一個像素值則必須重新計算子影像的標準差與平均數。因此每一次for迴圈結束，必須更新參數s'_i與$\overline{x}'$。這樣做的原因是因為在等級校正的過程中，並非要校正所有像素值，每校正一個像素值之後就判斷等級是否已經維持一致性了，如果已經相等了，則不用再校正其它像素。相反的如果校正一個不夠的話，就得校正二個、三，甚至全部(此狀況幾乎不存)，直到等級相同為止。

2.3 資料取出的方法

在這一節，將介紹如何取出秘密訊息。首先將整張偽裝圖切割成與嵌入時一樣大小的子影像。接著，使用 Eq.(1)計算所有子影像的標準差，與 Eq.(2)將所有子影像進行等級分類(必須使用當初嵌入時的 4 個

門檻值)。由於當初在嵌入資料時，我們有維持等級的一致性，因此在擷取過程時所求得的等級，必然與嵌入時一樣。有了子影像的等級之後，我們即可判斷該子影像的每一個像素值的隱藏量，如若等級為 1，則代表該子影像內的每一個像素值的隱藏量為 1 個位元，如等級為 2，則表示像素值的隱藏量為 2 個位元，以此類推。最後我們只要將十進制的像素值轉換成 8 位元的二進制，依照其等級的大小，從最低位元的地方依順取出訊息即可。

3.1 實驗結果與分析比較

在實驗的過程中，我們使用了大量的影像來測試新方法，而所有產生的偽裝影像的外表，即使與原始影像放置在一起，也是非常難以察覺有失真性的。在此，我們臚列四張(大小皆列 512×512)比較有代表性測試影像—“Lena”、“Baboon”、“Man”和“Peppers” (如圖一(a)、(b)、(c)與(d)所示)。而使用的子影像大小為 4×4 來進行影像切割動作。圖二是這四張影像的標準差直方圖，很明顯地，從標準差直方圖可以觀察一張影像的原始特性。如圖二(b)，擁有大量的高階子影像標準差，因此我們可以判定這張影像是屬於高複雜度的影像。反之如圖二(d)，大多數的子影像標準差皆落在低階位置，因此可以判斷這張影像是由非常多的平滑區所組合而成的。

由於每一張的標準差直方圖的分佈皆不一樣，我們必須基於每張影像的原始特性來設定四個門檻值，故這四張的門檻值都不會相同。基本上，為了提供高容量同時為了擁有高品質的偽裝圖，我們選擇了那些落在直方圖峰值附近的子影像來使用 2-LSBs 技術，即這些子影像內的每一個像素都將被嵌入 2 個位元的訊息。當然低於峰值的子影像，將只會被嵌入 1 個位元的訊息，而大於峰值的子影像，將被嵌入 3、4 或 5 個的訊息。實驗結果如圖二(e)、(f)、(g)與(h)所示，証明我們的方法不但可以嵌入大量的容量，也可以擁有一張高品質的偽裝圖影像。

最後，本論文的方法也與現存知名可適應性影像偽裝學技術[13]做比較。其比較結果如表一所示。在相同的容量之下我們的新技術可以擁有比較好的 PSNR 值。又如前面所提到的，MBNS 在容量估測方面會產生累積性的誤差，如表一中的 Baboon 與 Man 等兩張影像，由於他們是屬於比較高複雜度的影像，因此，MBNS 就會產生比較大的失真性，然而，我們的新方法在容量估測時是獨立運作且並不會互相影響，所以在這二張測試影像的比較結果上，我們的新方法可以大大地減少偽裝影像品質的失真(約提昇 PSNR 值 4dB)。至於比較平滑的影像，新方法仍然也可以改善 MBNS 的偽裝影像品質的失真(如表一所示)。

4. 結論

本篇論文提出一種基於人類視覺靈敏度的新型可適應性資訊隱藏方式。影像中的隱藏量會隨著區域性複雜度而改變，即遇到平滑的地方就藏少一點，遇到較複雜的地方就藏多一點。整張影像即使在嵌入大量的訊息之後依然可以保持原始影像屬性，因此偽裝影像的外表與原始影像相比較之下，是很難分辨出有任何明顯差的地方。此外，基於新方法所提的子影像等級一致性校正技術，訊息在擷取過程中是不需要原圖的。

參考文獻

[1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hiding – a survey,” Proceedings of the IEEE: Special Issue on Identification and Protection of Multimedia Content, vol. 87, pp. 1062–1078, July 1999.

[2] I. J. Cox and M. L. Miller, “Electronic watermarking: the first 50 years,” in 2001 IEEE Fourth Workshop on Multimedia Signal Processing, pp. 225–230, Oct. 2001.

[3] G. J. Simmons, “The prisoners’ problem and the subliminal channel,” in Proc. CRYPTO’83, pp. 51–67, 1983.

[4] M. U. Celik, G. S., A. M. Tekalp, and E. Saber, “Lossless generalized-LSB data embedding,” IEEE Transactions on Image Processing, vol. 14, pp. 253–266, Feb. 2005.

[5] N. W. and M. S. Hwang, “Data hiding: Current status and key issues,” International Journal of Network

Security, vol. 4, pp. 1–9, Jan. 2007.

[6] K. Tanaka, Y. Nakamura, and K. Matsui, “Embedding secret information into a dithered multi-level image,” Proc. IEEE Milcom, pp. 216–220, 1990.

[7] R. Z. Wang, C. F. Lin, and J. C. Lin, “Image hiding by optimal LSB substitution and genetic algorithm,” Pattern Recognition, vol. 34, pp. 671–683, Mar. 2001.

[8] C. C. Thien and J. C. Lin, “A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function,” Pattern Recognition, vol. 36, pp. 2875–2881, Dec. 2003.

[9] C. K. Chan and L. M. Cheng, “Hiding data in images by simple LSB substitution,” Pattern Recognition, vol. 37, pp. 469–474, Mar. 2004.

[10] S. J. Wang, “Steganography of capacity required using modulo operator for embedding secret image,” Applied Mathematics and Computation, vol. 164, pp. 99–116, Jan. 2005.

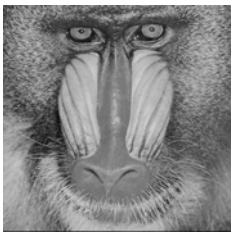
[11] D. C. Wu and W. H. Tsai, “A steganographic method for images by pixel-value differencing,” Pattern Recognition Letters, vol. 24, pp. 1613–1626, Jun. 2003.

[12] C. C. Chang and H. W. Tseng, “A steganographic method for digital images using side match,” Pattern Recognition Letter, no. 25, pp. 1431–1437, 2004.

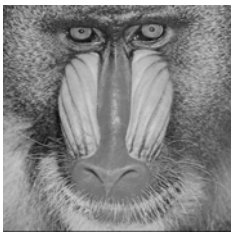
[13] X. Zhang and S. Wang, “Steganography using multiple-base notational system and human vision sensitivity,” IEEE Signal Processing Letters, vol. 12, pp. 67–70, Jan. 2005.

(a) Lena(原圖)

(e) Lena(偽裝圖)



(b) Baboon(原圖)



(f) Baboon (偽裝圖)

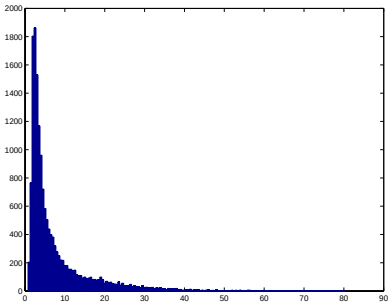
(c) Man(原圖)

(g) Man (偽裝圖)

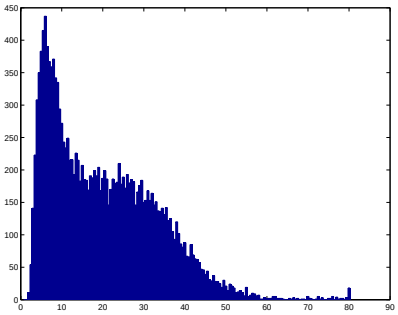
(d) Peppers(原圖)

(h)Peppers(偽裝圖)

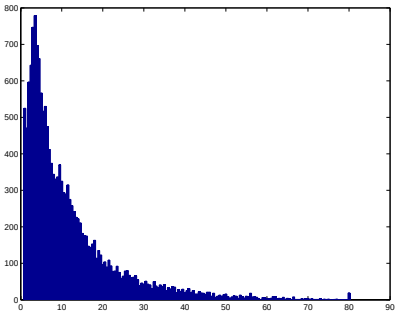
圖一、四張原始測試影像與所產生的偽裝圖影像。圖(e)的所使用的門檻值為[2,10,25,40]、整張隱藏量為 573072 bits、PSNR 值為 41.87dB。圖(f)的所使用的門檻值為[5,15,35,55]、整張隱藏量為 691376 bits、PSNR 值為 39.71dB。圖(g)的所使用的門檻值為[2,11,45,80]、整張隱藏量為 610673 bits、PSNR 值為 42.53dB。圖(h)的所使用的門檻值為[2,8,25,50]、整張隱藏量為 603632 bits、PSNR 值為 41.45dB。



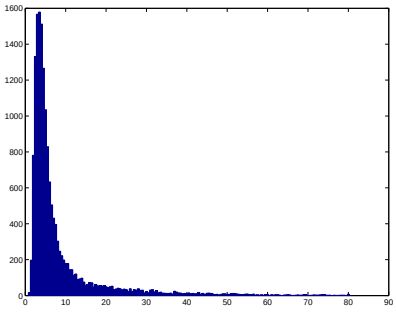
(a) Lena 影像的標準差直方圖



(b) Baboo 影像的標準差直方圖



(c) Man 影像的標準差直方圖



(d) Peppers 影像的標準差直方圖

圖二、四張測試影像的標準差直方圖，其所採用的子影像大小為 4×4。

表一、新方法與現存可適應技術，在相同的隱藏量之下，比較其偽裝圖所產生品質，PSNR 值愈高，代表失真愈少。

測試影像	MBNS[13]		我們的方法		
	容量 (bits)	PSNR (dB)	容量 (bits)	PSNR (dB)	4 個門檻值 [*th1*,*th2*,*th3*,*th4*]
Lena	440000	44.3	443408	47	[3,36,60,80]
Baboon	440000	41.4	444352	45.9	[15,36,60,85]
Man	520000	41.3	520256	45.08	[2,37,52,80]
Peppers	440000	45	440912	46.22	[4,30,50,85]