建立在以量化為基嵌入技術上之數位影像藏密法

楊士鋒

環球科技大學資訊管理系

摘要

藏密法(steganography)為資訊隱藏(information hiding)技術的一種應用，希望藉由將機密訊息藏入掩護媒體(cover medium)中不被發現，來達到秘密通訊之目的。本文提出了利用量化為基嵌入技術(quantization-based embedding technique)所設計出，以數位影像做為掩護媒體之藏密法。在使用量化為基嵌入技術所設計出之數位影像資訊隱藏法來隱藏機密訊息時，使用之量化步距(quantization step size)越小，掩護影像(cover image)之失真程度越低。而本文所提出之方法，在原本之量化步距外，額外再導入一個可調整控制之參數，以進一步降低掩護影像之失真程度。實驗結果顯示，藉由此新導入之參數，的確可在選定量化步距後，進一步降低掩護影像之失真程度。惟需注意的是，偽裝影像之直方圖，可能會因為此新導入參數數值之不同，而出現不同程度之尖刺狀圖形，導致偽裝影像較難以抵抗以直方圖為工具所進行之偵測攻擊。

關鍵詞：資訊隱藏、藏密法、量化為基嵌入技術、數位影像

A Digital Image Steganographic Scheme Based on Quantization-Based Embedding Technique

Shih-Feng Yang

Department of Information Management, Transworld University

Abstract

Steganography is one of the applications of information hiding techniques. The purpose of steganography is to transfer messages secretly by embedding messages into cover media to conceal the very existence of the messages. In this paper, a digital image steganographic scheme is presented. The steganographic scheme is based on quantization-based embedding technique and uses digital images as the cover medium. In using digital image information hiding schemes based on quantization-based embedding technique to hide secret messages, the distortion of cover images will be smaller if a smaller quantization step size is used. Besides the quantization step size, the scheme presented in this paper incorporates an additional adjustable parameter to further decrease the distortion of cover images. Experimental results show that the new incorporated parameter can indeed further decrease the distortion of cover images under a selected quantization step size. However, it should be noted that because of the selection of different values of the new incorporated parameter, different types of spikes may appear in the histograms of stego-images leading to a decrease of the ability of stego-images against detection attacks based on histogram analysis.

Keywords: information hiding, steganography, quantization-based embedding technique, digital image

壹、前言

近年來，與資訊安全相關之資訊隱藏(information hiding)技術越來越受到重視，吸引了許多學者投入研究，開發出許多相關之技術，而藏密學(steganography)即為資訊隱藏技術的一種應用(Cheddad, Condell, Curran, & Mc Kevitt, 2010; Petitcolas, Anderson, & Kuhn, 1999)。

藏密學技術之目的在於秘密通訊，希望機密訊息能在不被察覺的情況下，安全地傳送給接收者。藏密學技術的做法，在於將機密訊息藏入掩護媒體(cover medium)中以得到偽裝媒體(stego-medium)，並盡力使偽裝媒體在外觀上與掩護媒體完全相同，然後將偽裝媒體傳送給接收方。當接收方收到偽裝媒體後，以適當之演算法，即可將機密訊息自偽裝媒體中取出。在傳送偽裝媒體的過程中，由於偽裝媒體在外觀上與掩護媒體幾近相同，故即使有心竊密者能看到偽裝媒體，亦無法察覺機密訊息之存在，從而達到秘密通訊之目的。

評估藏密學技術之優劣有兩個衡量標準(李榮三、張真誠，民 98)：其一是機密訊息的藏入量；另外則是機密訊息是否容易被偵測察覺。當掩護媒體被藏入機密訊息後，會造成一定程度的失真，而機密訊息的藏入量通常會與掩護媒體的失真程度成正比。因此，雖然我們希望藏入量越大越好，但卻不能造成掩護媒體失真程度過大，而使得有心竊密者能察覺偽裝媒體藏有機密訊息。除了失真程度的考量外，另一需考量的問題是，當掩護媒體被藏入機密訊息後，是否會改變其特性，而被偵測出其內藏有機密訊息。例如，做為掩護媒體之數位影像被藏入機密訊息後，其直方圖(histogram)是否會有特殊之模式產生，因而使得有心竊密者，能藉由偵測此類模式來判斷數位影像內是否藏有機密訊息。

截至目前為止，已有許多資訊隱藏法被提出，請參閱 Cheddad et al. (2010)、Petitcolas et al. (1999)、李榮三與張真誠(民 98)，以及其內所列出之參考文獻。在眾多資訊隱藏技術中，量化為基嵌入技術(quantization-based embedding technique)受到了許多學者的重視，提出了不少以該技術所設計出之資訊隱藏法(Chen & Wornell 2001; Eggers, Bäuml, Tzschoppe, & Girod, 2003; Lu, Chang, and Liu (2009); Wu, 2003; Wu & Liu, 2003)。在這些以量化為基嵌入技術所設計出之資訊隱藏法中，Lu et al. (2009)提出了利用量化為基嵌入技術所設計出，以數位影像做為掩護媒體之資訊隱藏法。該方法是先將機密訊息加密，並轉換成位元流(bit stream)，接著再利用選定之量化步距(quantization step size)，將掩護影像(cover image)像素值(pixel value)所在之區間，如[0,255]，分成數個子區間，然後依據欲藏入之機密訊息位元值(bit value)，以及掩護影像像素之像素值落於第偶數個或第奇數個子區間內，計算出偽裝影像(stego-image)像素之像素值，以此來將機密訊息藏入掩護影像中。在 Lu et al. (2009)所提出之資訊隱藏法中，量化步距之選擇佔有相當重要之地位。量化步距越小，掩護影像藏入機密資訊後之失真程度越小，而量化

步距越大，則藏入之機密訊息越不容易因遭受破壞而無法取出。

本文之目的，在於提出一利用量化為基嵌入技術所設計出之藏密法。此方法在量化步距外，額外再導入一個可調控之參數。藉由此新導入之參數，可在同一量化步距下，減少掩護影像藏入機密訊息後之失真程度，以降低有心竊密者察覺偽裝影像藏有機密訊息之風險。

本文之其餘部分組織如下：第貳節介紹本文所提出之數位影像藏密法；在第參節中，我們以常見之標準測試影像來進行實驗，並討論其結果；第肆節則為結論部分。

貳、提出之方法

令$P=\{p_1,p_2,\dots,p_{N\times N}\}$，其中$p_i$為第 i 個像素且$p_i\in[0,255]$，為大小為$N\times N$之掩護影像，而$D=\{d_1,d_2,\dots,d_M\}$，其中 $d_i\in\{0,1\}$，為欲隱藏機密訊息之位元流。為了強化其秘密性，我們不直接將D藏入P中，而先以密鑰 SK 將D加密成為$S=\{s_1,s_2,\dots,s_M\}$，其中$s_i\in\{0,1\}$，然後再將加密後之資料，即序列S，藏入P中。以密鑰 SK 將D加密成S，其做法為，先以密鑰 SK 產生序列$E=\{e_1,e_2,\dots,e_M\}$，其中$e_i\in\{0,1\}$，然後以下式將D加密成S：

$$S=D\otimes E=(d_1\otimes e_1,d_2\otimes e_2,\dots,d_M\otimes e_M) \tag{1}$$

其中⊗表互斥或(exclusive or, XOR)運算。

在將S藏入P時，設整數q為選定之量化步距，並令

$$\begin{aligned}\alpha(p_i)&=\left\lfloor\frac{p_i}{q}\right\rfloor+1\\ n&=\left\lceil\frac{256}{q}\right\rceil\\ \beta&=256-(n-1)q\end{aligned} \tag{2}$$

其中⌈·⌉為天花板函數(ceiling function)。在選定整數 k，且滿足$k<\beta$後，利用下式將S藏入P中，以產生偽裝影像$\hat{P}=\{\hat{p}_1,\hat{p}_2,\dots,\hat{p}_{N\times N}\}$，

$$\hat{p}_i=\begin{cases}p_i+\left\lfloor(\alpha q-p_i)\dfrac{k}{q}\right\rfloor, & \text{若}\alpha(p_i)\neq n\text{且}\alpha(p_i)\bmod 2=s_i \quad (3a)\\ \alpha q+k+\left\lfloor(p_i-\alpha q)\dfrac{k}{q}\right\rfloor, & \text{若}\alpha(p_i)\neq n\text{且}\alpha(p_i)\bmod 2\neq s_i \quad (3b)\\ p_i+\left\lfloor(256-p_i)\dfrac{k}{\beta}\right\rfloor, & \text{若}\alpha(p_i)=n\text{且}\alpha(p_i)\bmod 2=s_i \quad (3c)\\ (n-1)q+\left\lfloor(p_i-256)\dfrac{k}{\beta}\right\rfloor, & \text{若}\alpha(p_i)=n\text{且}\alpha(p_i)\bmod 2\neq s_i \quad (3d)\end{cases}$$

當接收方收到偽裝影像後，若欲取得隱藏在偽裝影像內之機密訊息，則先以下式取出S

$$s_i = \alpha(\hat{p}_i) \bmod 2 \tag{4}$$

然後再以密鑰 SK 所產生之序列E，利用下式來取得機密訊息

$$D = S \otimes E = (s_1 \otimes e_1, s_2 \otimes e_2, \ldots, s_M \otimes e_M) \tag{5}$$

上述(2)、(3)式藏入機密訊息之做法，是以量化步距q將區間[0,255]區分為n個子區間。像素值位於奇數子區間內之像素藏入 1，而像素值位於偶數子區間內之像素，則藏入 0，如圖 1 所示。由於每一個像素可藏入一個位元之資料，故本文所提出之藏密法，其酬載(payload)為 1 bbp (bit per pixel)。在藏入機密訊息時，依據像素可藏入之值是否與欲藏入之s_i相同，而將像素之像素值由 $[(\alpha(p_i)-1)q, \alpha(p_i)q)$映射(map)至$[(\alpha(p_i)-1)q+k, \alpha(p_i)q)$或$[\alpha(p_i)q, \alpha(p_i)q+k)$，以得到掩護影像對應像素之像素值，如圖 2 所示。需注意的是，經映射後所得之像素值，有可能會超出允許之範圍而造成溢位(overflow)，故需進行調整。式(3d)之作用，即是在針對映射後產生溢位之像素，將其像素值減少$\beta + k$，以避免溢位。

參、實驗結果與討論

我們以圖 3 中之 Airplane、Baboon、Lena、Peppers 等四張常見之標準測試影像做為掩護影像，以本文所提出之藏密法，將圖 4 中之機密影像藏入其中，來進行實驗。圖 3 中之掩護影像，皆為512×512之 8 位元灰階影像，至於圖 4 中之機密影像，則為512×512之黑白影像。藏入機密影像後之掩護影像，其失真程度，是以尖峰信號雜訊比(peak signal-to-noise ratio, PSNR)來評估，其計算方式為(Yu, Chang, & Lin 2007)

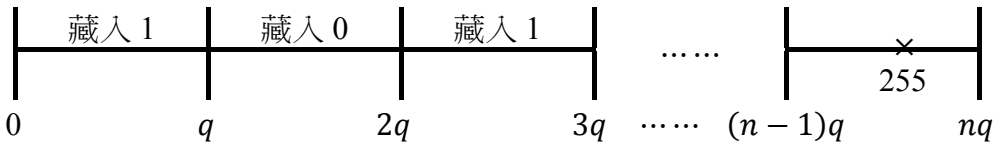


圖 1 子區間之可藏入值

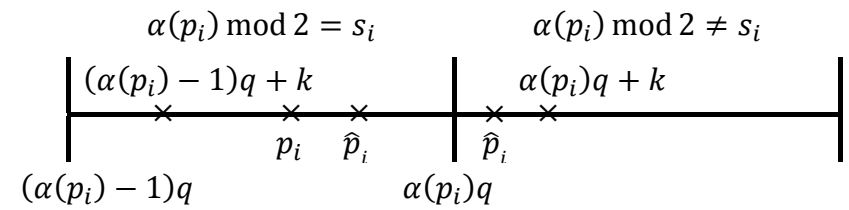
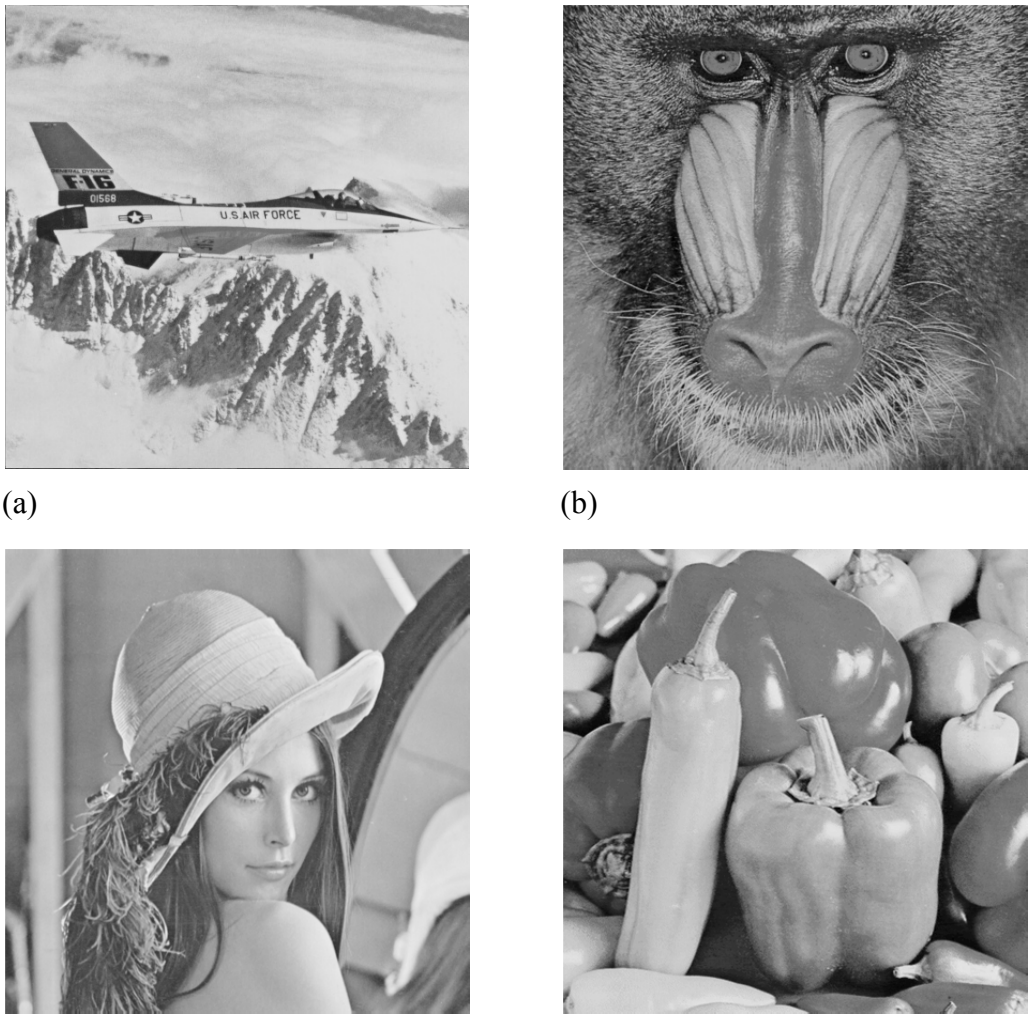


圖 2 藏入機密訊息之做法



(a) (b)

(c) (d)

圖 3 掩護影像 (a) Airplane (b) Baboon (C) Lena (D) Peppers

圖 4 機密影像

$$\text{PSNR} = 10 \times \log_{10}\left(\frac{255^2}{\text{MSE}}\right) \tag{6}$$

式中之 MSE 為均方誤差(mean squared error)，其定義為

$$\text{MSE} = \frac{1}{N_p}\sum_{i=1}^{N_p}(p_i - \hat{p}_i)^2 \tag{7}$$

其中N_p為像素個數，而p_i與$\hat{p}_i$則分別為掩護影像與偽裝影像，其第 i 個像素之像素值。PSNR 之單位為分貝(dB)，其值越大，則影像失真程度越低，越不容易以肉眼察覺偽裝影像內藏有機密訊息。

利用本文所提出之藏密法，以不同之q值及k值，將圖 4 中之機密影像，藏入圖 3 之掩護影像中，所得到之偽裝影像，其 PSNR 如表 1 所示。由表 1 可看出，q或k越小，則偽裝影像之 PSNR 越大，其與掩護影像間之差異越小，亦即掩護影像被藏入機密影像後，其失真程度越低。之所以會有此結果，其原因在於，藏入機密資訊時，是將像素之像素值由 $[(\alpha(p_i)-1)q, \alpha(p_i)q)$映射至$[(\alpha(p_i)-1)q+k, \alpha(p_i)q)$或$[\alpha(p_i)q, \alpha(p_i)q+k)$，$q$或$k$越小，則映射後所得到之像素值，與原來之像素值間之差距越小，故偽裝影像會有較大之 PSNR。由表 1 亦可看出，在相同之q值下，k越小，則 PSNR 越大。換句話說，當選定量化步距q後，可藉由選擇較小之k值，進一步提升偽裝影像之 PSNR，而達到降低失真程度之目的。

表 1

不同之q值及k值下所得到之偽裝影像 PSNR

q	k	PSNR (dB)			
		Airplane	Baboon	Lena	Peppers
4	1	42.24	42.26	24.22	42.26
	2	40.72	40.73	40.71	40.77
	3	39.60	39.58	39.59	39.57
8	1	36.99	37.21	37.05	37.26
	2	36.39	36.56	36.43	36.61
	3	35.80	35.95	35.83	35.98
	4	34.77	34.89	34.80	34.94
	5	34.29	34.39	34.31	34.41
	6	33.45	33.52	33.46	33.53
	7	32.78	32.84	32.78	32.84

表 2

Lu et al. (2009)之方法在不同之q值下所得到偽裝影像之 PSNR

q	PSNR (dB)			
	Airplane	Baboon	Lena	Peppers
4	40.72	40.73	40.71	40.77
8	34.77	34.89	34.80	34.94

為了與 Lu et al. (2009)所提出之方法相比較，我們亦將圖 4 中之機密影像，以 Lu et al. (2009)所提出之方法藏入圖 3 之掩護影像中。藏入機密影像後所得到之偽裝影像，其 PSNR 如表 2 所示。由表 1 與表 2 可看出，本文所提出之藏密法，在$k = q/2$時，藏入機密訊息後所得到之偽裝影像，其 PSNR 與 Lu et al. (2009) 所提出之方法相同。事實上，若將$k = q/2$代入(3a)及(3b)式中，經簡單之運算後，即可得到與 Lu et al. (2009)所提出方法相同之結果。惟需注意的是，在 Lu et al. (2009)所提出之方法中，並無防止溢位之機制存在。

圖 5 為 Lena 影像於$q = 4$時，以不同之k值將圖 4 之機密影像藏入後所得到之偽裝影像。比較圖 3 中之掩護影像與圖 5 中之偽裝影像可發現，兩者很難以肉眼區分其差異，由此可知，本文所提出之藏密法，其藏密效果相當良好。事實上，眾所週知的是，當影像之 PSNR 大於 30 dB 時，人類之眼睛便不易察覺其是否失真，而由表 1 可知，利用本文所提出之藏密法，以不同之q值及k值，將圖 4 中之機密影像藏入圖 3 之掩護影像中，所有得到之偽裝影像，其 PSNR 均大於 30 dB，故肉眼無法察覺偽裝影像與掩護影像之間有何不同。

圖 6 為 Lena 影像，以及其在$q = 4$時，不同之k值下所得到偽裝影像之直方圖。由圖 6 可看出，$k = 2$時所得到之偽裝影像，其直方圖與原影像之直方圖最接近。事實上，當$k = q/2$時，藏入機密影像後所得到之偽裝影像，其直方圖與原影像之直方圖最接近。換句話說，當$k = q/2$時所得到之偽裝影像，最能抵抗以直方圖為工具之偵測攻擊。當$k = q/2$時所得到之偽裝影像，其直方圖之所以會最接近原影像之直方圖，原因在於藏入機密影像時，是將像素值由$[(\alpha(p_i) - 1)q, \alpha(p_i)q)$映射至$[\alpha(p_i) - q/2\,, \alpha(p_i)q)$或$[\alpha(p_i)q, \alpha(p_i)q + q/2)$，而不管是$[\alpha(p_i) - q/2\,, \alpha(p_i)q)$或$[\alpha(p_i)q, \alpha(p_i)q + q/2)$，其寬度皆為$q/2$。換句話說，藏入機密訊息後所得到之像素值，其在由量化步距q所區分出之相鄰的兩個子區間$[(\alpha(p_i) - 1)q, \alpha(p_i)q)$及$[\alpha(p_i)q, (\alpha(p_i) + 1)q)$中之分佈會較為平均，而不易造成偽裝影像之直方圖出現如圖 6 (b)、圖 6(d)中之尖刺狀圖形。當$k \neq q/2$時，以$k = 1$為例，若$\alpha(p_i) \neq n$且$\alpha(p_i) \bmod 2 \neq s_i$，則在藏入機密資訊時，會將位於區間$[(\alpha(p_i) - 1)q, \alpha(p_i)q)$之像素值，映射至區間$[\alpha(p_i)q, \alpha(p_i)q + 1)$中，而此區

間之寬度僅為 1，故會造成偽裝影像中，像素值為$\alpha(p_i)q$之像素，其數量偏高，而導致直方圖中，出現尖刺狀之圖形。

在結束本節前，值得一提的是，為了強化欲隱藏機密訊息之秘密性，在藏入機密訊息前，會以密鑰將機密訊息加密，然後再將加密所得之資料藏入掩護影像中。此步驟除了可強化欲隱藏機密訊息之秘密性外，亦可減少偽裝影像直方圖中尖刺狀圖形之產生。例如，圖 7 所示即為在$q = 4, k = 2$之設定下，不事先以密鑰加密，而直接將圖 4 中之機密影像藏入 Lena 影像中，所得到偽裝影像之直方圖。比較圖 6 (c)與圖 7 可發現，藏入密鑰加密後之資料所得到之偽裝影像，其直方圖中之尖刺狀圖形較不明顯。

(a) (b)

(c)

圖 5 Lena 影像在$q = 4$及不同之k值下，藏入機密影像後所得到之偽裝影像 (a) $k = 1$ (b) $k = 2$ (c) $k = 3$

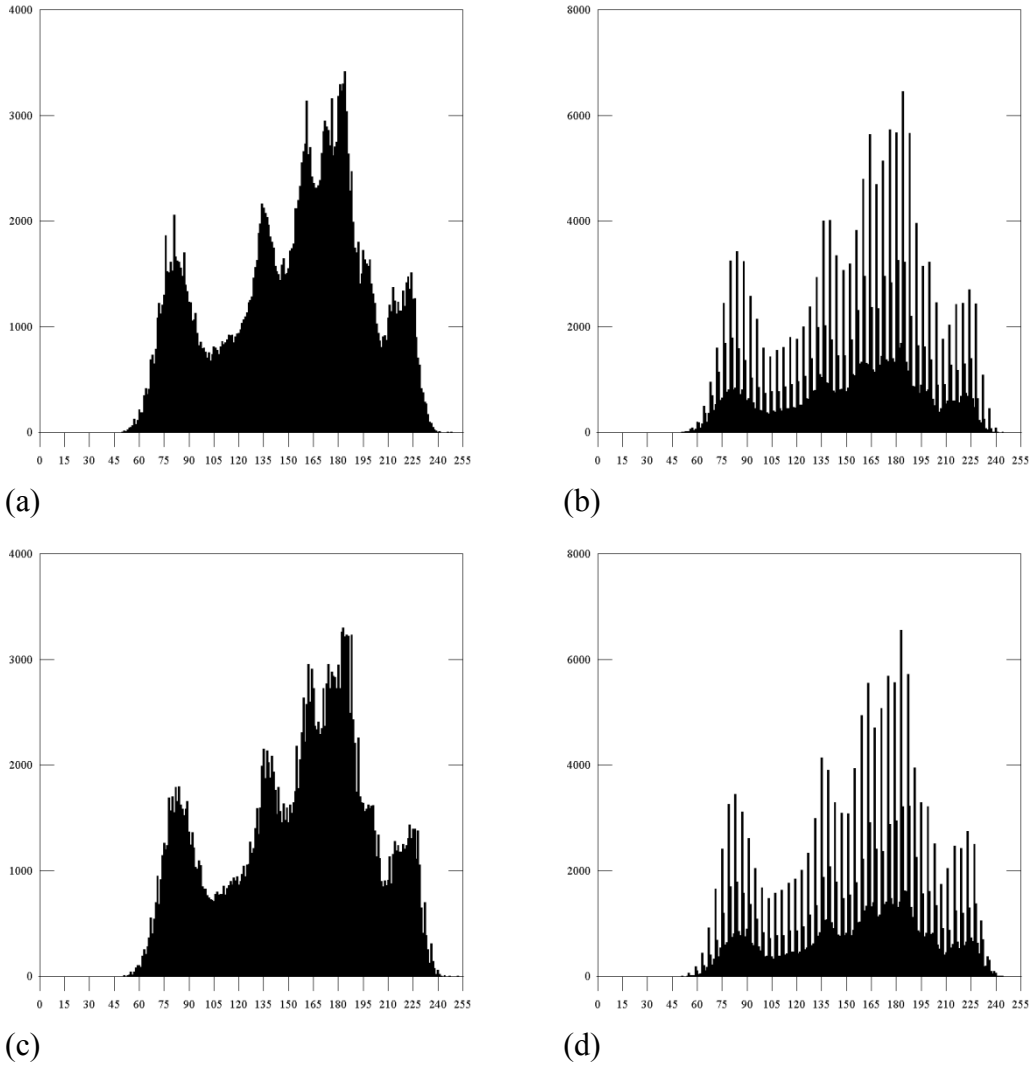


圖 6 Lena 影像在$q = 4$及不同之k值下，藏入機密影像後所得到之偽裝影像直方圖 (a) 原影像 (b) $k = 1$ (c) $k = 2$ (d) $k = 3$

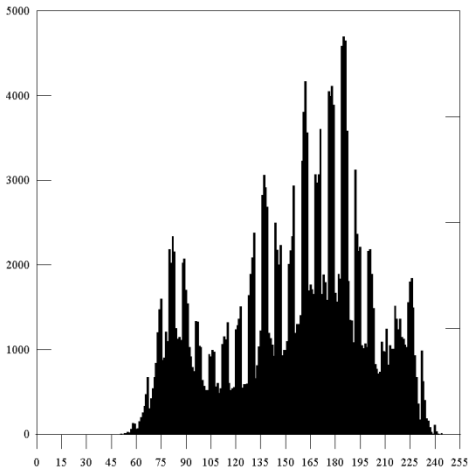


圖 7 在$q = 4, k = 2$之設定下，不先以密鑰加密，而直接將機密影像藏入 Lena 影像中，所得到偽裝影像之直方圖

肆、結論

在本文中，我們提出了利用量化為基嵌入技術所設計出，以數位影像做為掩護媒體之藏密法。此方法在原本以量化為基嵌入技術中之量化步距外，額外再導入一個可調整控制之參數。在使用以量化為基嵌入技術所設計出之數位影像資訊隱藏法藏入機密訊息時，所用之量化步距越小，則掩護影像在藏入機密訊息時，其失真程度越小。而藉由此新導入之參數，可在選定量化步距後，進一步降低掩護影像藏入機密訊息時之失真程度。由實驗結果可知，此新導入之參數，的確可在選定之量化步距下，進一步降低掩護影像在藏入機密訊息時之失真程度。惟需注意的是，雖然掩護影像在藏入機密訊息時之失真程度較低，但所得到之偽裝影像直方圖，卻容易出現尖刺狀之圖形，因而較難以抵抗以直方圖為工具所進行之偵測攻擊。

參考文獻

Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: survey and analysis of current methods. *Signal Processing, 90,* 727-752.

Chen, B. and Wornell, G. W. (2001). Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. *IEEE Transaction on Information Theory, 47*(4), 1423-1443.

Eggers, J. J., Bäuml, R., Tzschoppe, R., & Girod, B. (2003). Scalar Costa scheme for information embedding. *IEEE Transactions on Signal Processing, 51*(4), 1003-1019.

Lu, T.-C., Chang, C.-C., & Liu, Y.-L. (2009). An information-hiding scheme based on quantization-based embedding technique. *Fundamenta Informaticae, 91,* 597-610.

Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding—a survey. *Proceedings of the IEEE, 87*(7), 1062-1078.

Wu, M. (2003). Joint security and robustness enhancement for quantization based data embedding. *IEEE Transactions on Circuits and System for Video Technology, 13*(8), 831-841.

Wu, M. & Liu, B. (2003). Data hiding in image and video: part-I—fundamental issues and *solutions*. *IEEE Transactions on Image Processing, 12,* 685-695.

Yu, Y.-H., Chang, C.-C., & Lin, I.-C. (2007). A new steganographic method for color and grayscale image hiding. *Computer Vision and Image Understanding, 107,* 183-194.

李榮三、張真誠 (民 98)。多媒體安全技術之最新發展。載於國家實驗研究院科技政策研究與資訊中心(主編)，**資通安全專論彙編之一**(1-38 頁)。台北市：國家實驗研究院。