適用於可逆式資訊隱藏技術之藏密分析法
Steganalyses of Reversible Data Hiding Techniques

婁德權
長庚大學資訊工程學系
Email: dclouprof@gmail.com

周兆龍
國防大學理工學院電機電子工程學系
Email: chaolung.chou@gmail.com

瞿忠正
國防大學理工學院電機電子工程學系
Email: david.cc.chiu@gmail.com

***摘要*—可逆式資訊隱藏是一種能夠允許掩護媒體嵌入秘密訊息後，仍能有效萃取秘密訊息並將掩護媒體無失真還原的技術。在各種可逆式資訊隱藏演算法之中，Ni等學者在2006年提出了利用影像直方圖中的零點及峰點來進行資訊隱藏的技術。這個技術具有計算簡單與良好影像品質的優點，但藏密之後的影像直方圖卻會出現明顯的統計特徵。本文利用此統計特徵，對藏密前、後的直方圖特徵進行統計分析，提出一種簡單、快速的藏密分析方法，並提出直方圖偏差度作為檢測影像是否藏有秘密訊息的依據。經實驗證明，本文所提出之藏密分析方法對於一般自然影像有良好的偵測效果。**

***關鍵詞*—可逆式資訊隱藏、直方圖、統計分析、藏密分析。**

Abstract—Reversible data hiding is the technique that allows extracting embedding message meanwhile the cover-media can be recovered without any distortion. In 2006, Ni et al. proposed a reversible data hiding algorithm which utilizes zero point and peak point of image histogram to embed data. The advantages of this method are simple and providing good image quality. However, some statistical patterns were easy to be found during the embedding procedure. In this paper, we proposed a simple and quick steganalysis algorithm utilizing the measurement of histogram variation and the statistical analysis techniques. Experiment results shows that our method provide a good performance on natural images.

Keywords: reversible data hiding, histogram, statistical analysis, steganalysis.

一、前言

資訊隱藏(Data Hiding)是一種透過隱藏通道(Covert Channel)將訊息秘密安全的傳送出去而不引起他人懷疑的技術。隨著數位化程度的提昇，現今秘密訊息可以輕易的以數位化形式隱藏在各種多媒體(文字、聲音、影像、視訊...等等)之中，並且透過網際網路進行快速的傳輸，使其不易被人們所發覺。

從隱私權的角度來看，資訊隱藏技術提供了人們在密碼技術(Cryptography)之外另一種安全通訊的選擇。但是藏密技術一旦遭到有心人士的濫用，無形之中可能會對個人、團體甚至國家造成危害。因此，發展能夠偵測數位多媒體中是否藏有秘密訊息的藏密分析技術(Steganalysis)實有其必要性。

簡單來說，藏密分析就是對待測目標進行偵測或分析，看看其中是否藏有秘密資訊。藏密分析與破密(Cryptanalysis)的不同在於破密必須將密文完整解譯出來才算破解成功，而藏密分析只要能判別是否存在隱藏資訊的事實就算成功。一般常見的藏密分析技術可以區分為針對型(Target-based)與通用型(Universal)兩大類[2]。針對型藏密分析法通常會針對藏密演算法本身的特性進行分析，例如針對空間域的 LSB 最低位元取代法有 Westfield 等學者提出之 x^2(Chi-Square)偵測法[10]及 Fridrich 等學者提出之 RS 偵測法[3]；針對離散餘弦轉換(Discrete Cosine Transform；DCT)藏密法，則有 Fridrich

等學者提出的 JPEG 影像分析法[4]。

通用型藏密分析法是主要利用統計分析(Statistical Analysis)方法，歸納出統計上的變化特徵，再藉由樣式辨識(Pattern Recognition)的方式來判斷是否藏有秘密資訊，例如 Avcibas 等學者提出之影像品質矩陣(Image Quality Metrics：IQM) [1]；Lyu 等學者提出之機率密度函數(Probability Density Function；PDF) [6]；Harmsen 等學者提出之直方圖特徵函數(Histogram Characteristic Function；HCF) [5]等。通用型藏密分析法具備偵測未知藏密演算法的能力，較符合實務上的需求，不過由於運用統計的特性，在某些情況下仍可能發生高誤判率的缺點。

通常掩護媒體(Cover-Media)在嵌入秘密訊息之後會破壞原本載體的品質，造成一定程度的失真，這對需要高解析度及精確性的醫學影像、軍事影像、衛星影像及藝術影像是一種限制。為了滿足這類的應用需求，近年來學者提出可逆式資訊隱藏(Reversible Data Hiding)技術，利用影像的特性嵌入秘密訊息，在萃取階段除了能取出秘密訊息之外，還能將原始影像無失真的還原，因此可逆式資訊隱藏又被稱作無失真式資訊隱藏(Loseless Data Hiding 或 Distortion-free Data Hiding)。

常見的可逆式資訊隱藏方法有 Vleeschouwer 及 Marq 等學者提出利用環形內插(Circular Interpretation) 及模運算 (Modular Operation)之方法[9]；Xuan 等學者提出利用整數小波轉換(Integer Wavelet Transform)之方法[11]；Tian 等學者提出利用差值擴張(Difference Expansion)之方法[8]及 Ni 等學者提出利用直方圖(Histogram)位移之方法[7]。

其中 Ni 等學者提出的可逆式資訊隱藏方法利用影像直方圖中的特性來進行藏密，其演算法簡單且可以維持藏密影像良好的視覺品質。本文針對 Ni 等學者所提出之方法，提出一種快速、簡易的藏密分析方法，利用其藏密後產生之直方圖特徵，分析其直方圖統計關係，並定義直方圖偏差度作為藏密分析之判別基礎。

二、可逆式資訊隱藏技術

2006 年 Ni 等學者在提出一種利用影像直方圖的可逆式資訊隱藏技術[7]，該方法主要選取影像直方圖中最大值位置及其相鄰位置來藏密，以提高藏密量。一般而言，影像峰值雜訊比(Peak Signal-to-Noise Ratio；PSNR)超過 30 dB 以上，人眼不容易感受影像品質上的明顯變化。此方法在最差的情況下(Worst Case)每個像素值最多變動量為 1，因此可以確保藏密後的影像 PSNR 值維持在 48 dB 以上。

Ni 所提出之方法藏密程序說明如下：

步驟 1：計算影像直方圖，並找出其中出現次數最多與出現次數為零的最大值及最小值，分別稱之為峰點(Peak Point)及零點(Zero Point)。若找不到次數為零的位置，則以出現次數最少的點作為零點。

步驟 2：假設選取的零點位置在峰點的右側，以循序方式掃瞄影像，將大於峰點的像素值均加 1。此作法等同於將峰點右側的位置全部向右位移一個位置。此時峰點的下一個位置會被清空，預備作為藏密之用。

步驟 3：以相同的順序掃瞄影像，遇到峰點所代表的像素值時，與欲藏入之秘密訊息比對。若秘密訊息為 0，則不作任何改變；若秘密訊息為 1，則將該像素值加 1。

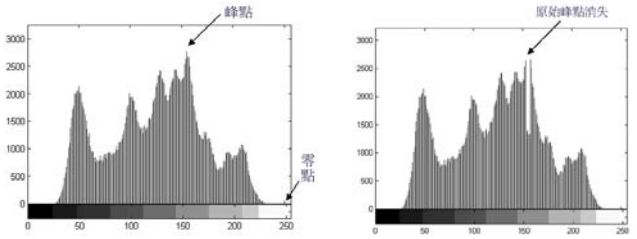
還原時，必需知道原始峰點的位置，再以相同的方式循序掃瞄影像，將原始峰點及其下一個位置取出，分別對應成位元 0 與位元 1，萃取出秘密訊息。接著將原本右移一個位置的直方圖像素值均減 1，即可以無失真的將原始影像還原。

Ni 等學者所提出的方法其最大藏密量(Capacity)即為峰點的數值，經過藏密程序之

後，秘密訊息的位元 0 與 1 被分別藏在峰點及其相鄰位置，因此會造成原始峰點及其相鄰位置數值下降。

舉圖 1(a) Lena 影像為例，圖 1(b)為計算出之原始直方圖，當採用上述方法藏密時，先在圖 1(b)中找到峰點為 154，右側零點為 237。接著將峰點右側所對應的像素值依序加一，如 155→156、156→157、…、237→238，則峰點右側相鄰的位置 155 即會被清空。藏密時依照上述步驟 3 的方式將秘密訊息位元分別嵌入在位置 154 及 155，完成嵌入後原始的峰點會消失，並出現明顯的缺口，如圖 1(c)所示。

（a）



（b）　　（c）

圖1. 影像直方圖變化示意圖 (a)Lena影像(b)原始直方圖(c)藏密後直方圖

Ni 等學者方法的優點是演算法簡單，毋須進行複雜運算或各種頻率域轉換(Frequency Domain Transform)，因此計算快速；此外影像 PSNR 值可以維持在 48dB 以上，具有較佳之影像品質及不可見性(Imperceptibility)。至於缺點的部分是藏密量依據不同影像類型而有差異，因此必要時需選擇一組以上的峰點與零點作為藏密的選擇；另外的缺點是會產生如的圖 1(c)之特徵，這種特徵透過一般人眼不易察覺，但經由電腦則仍可明顯判別其差異。本文提出之方法，即依據此特徵來進行藏密分析。

三、本文所提出之方法

本文以 8 位元灰階自然影像為例，假設 Ni 等學者方法採用一組峰點及零點，其最大藏密量為峰點的數值，並且零點位於峰點右側。令 h(p)代表影像直方圖中的各點，其中 p=0~255；假設 H_p 代表峰點數值，H_{p-1} 代表峰點的前一個位置數值，H_{p+1} 代表峰點的下一個位置數值，以此類推。在一般情況下，訊息位元 0 與位元 1 的比例大多呈現常態分佈，可以假設秘密訊息的位元 0 與位元 1 比例接近。這表示 Ni 方法藏密後峰點 H_p 及其下一個位置 H_{p+1} 的數值應該接近，令 θ 代表其數值比例，如式(1)所示。

$$\theta = \frac{H_{p+1}}{H_p} \approx 1 \pm \omega \ , \qquad (1)$$

其中 ω 代表秘密訊息的位元 0 與位元 1 數量差異所產生的誤差，一般 ω 近似於 0.05。

另外，一般自然影像的相鄰直方圖數值分佈較接近，這表示藏密前峰點 H_p 與前後相鄰各點(H_{p-1} 及 H_{p+1})的數值應接近；而藏密之後，原本峰點的 H_p 數值將明顯降低約一半左右，而且原本的 H_{p+1} 向右位移一個位置成為 H_{p+2}，因此藏密後峰點 H_p 與原本相鄰兩點的數值比例會產生明顯的差異。在此以 α 及 β 分別代表相鄰位置藏密後其數值比例，如式(2)所示。

$$\alpha = \frac{H_{p-1}}{H_p}, \beta = \frac{H_{p+2}}{H_p} \ , \ \alpha > \theta \ \text{ and } \ \beta > \theta \ 。 \qquad (2)$$

由於最大藏密量即為峰值的數值，被分散

嵌入在峰點及其下一個位置，因此藏密後 H_p 與 H_{p+1} 的總和應該分別大於原本左右相鄰的數值，此關係如式(3)所示。

$$\begin{cases} H_p + H_{p+1} > H_{p-1} \\ H_p + H_{p+1} > H_{p+2} \end{cases} 。 \quad (3)$$

上述式(1)至式(3)即為針對 Ni 等學者方法產生的直方圖特徵基本判別方式，本文參考上述各種統計特性提出藏密分析演算法，其程序說明如下：

步驟 1：計算影像直方圖，並依式(4)計算影像平均值，以作為藏密分析之門檻值。

$$m = \sum_{p=0}^{255} \frac{h(p) \cdot H_p}{256} 。 \quad (4)$$

步驟 2：為了提升計算效能，僅針對高於影像平均值的位置進行檢測。直方圖採由左至右的順序進行掃瞄，若 H_p 低於門檻值則不作任何動作；若 H_p 高於門檻值，則分別代入式(1)、式(2)及式(3)檢驗之，如式(5)所示。

$$if \begin{cases} H_p > m, \text{ check Eq.(1-3)} \\ H_p < m, \text{ do nothing} \end{cases}, p \in \{0 \sim 255\} 。 \quad (5)$$

步驟 3：定義直方圖偏差度 Δ_p 如式(6)所示。若 H_p 在步驟 2 中低於門檻值或經過式(1)至式(3)檢測後有任何一項不符合者，其 Δ_p 一律為 0；其餘符合的位置則繼續依式(6)完成直方圖偏差度 Δ_p 之計算。

$$\Delta_p = \left\{ \left(\frac{\alpha}{\theta} \right)^2 + \left(\frac{\beta}{\theta} \right)^2 \right\}^2, p \in \{0 \sim 255\} 。 \quad (6)$$

步驟 4：依序完成整張影像之直方圖偏差度 Δ_p 計算。最後若所有 Δ_p 出現明顯峰值之位置，即代表影像經過藏密且該位置即為原始峰點位置。

經過本文提出之直方圖偏差度 Δ_p 計算方法，未經藏密之影像不會有明顯之峰值；而經藏密後之影像則會在原始直方圖峰點位置會出現明顯的峰值。例如圖 2 為 Lena 影像藏密前、後之直方圖偏差度計算結果，藏密影像經過檢測後可以在峰點 154 位置發現明顯之峰值。

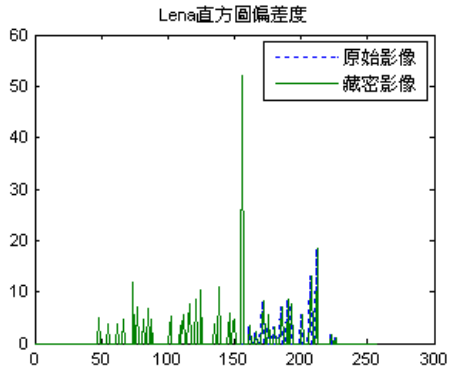
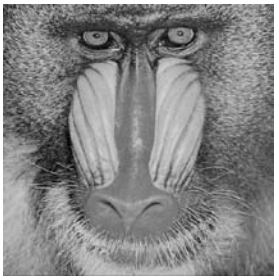


圖 2. Lena 影像直方圖偏差度示意圖

四、實驗結果分析

（a）Lena

（b）Peppers



（c）Baboon

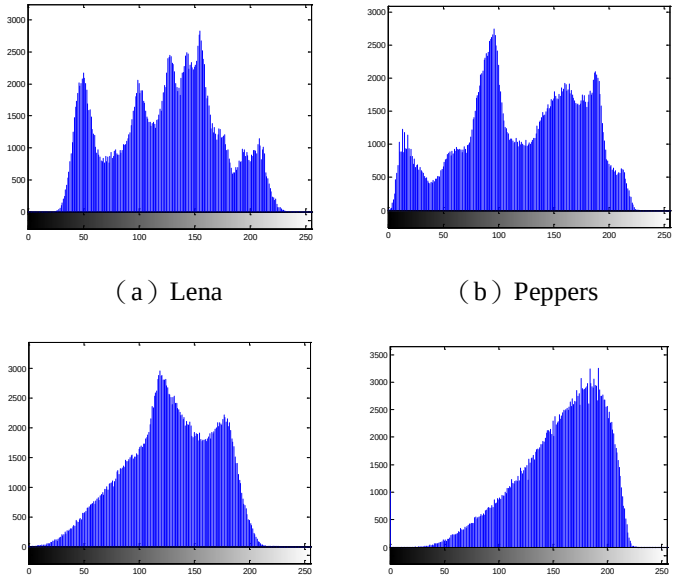
（d）Straw

圖3. 實驗影像

本實驗軟體採用 Matlab 7 版本，實驗影像使用 TIFF 格式之 8 位元灰階影像，影像大小均為 512x512，如圖 3 所示。實驗影像之直方圖如圖 4 所示。為了計算方便，秘密訊息係以隨機方式產生的 0 與 1 位元序列，秘密訊息容量為各影像直方圖之峰值。

實驗先將各影像以本文提出之藏密分析演算法進行計算，得出原始影像直方圖偏差度。接著再利用 Ni 等學者提出之可逆式資訊隱藏方法對各實驗影像進行藏密，各藏密後之影像再分別以本文提出之藏密分析法計算其直方圖偏差度。

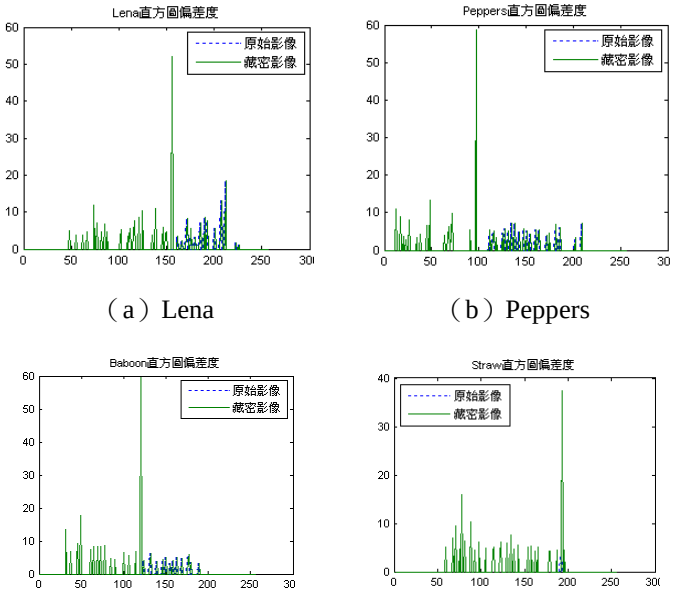
圖 5 為各影像藏密前、後所計算得出之直方圖偏差度，可以看出藏密影像在原始峰點位置會產生明顯之峰值。利用本文方法之實驗結果詳如表 1 所示，可以發現藏密後影像原始峰點位置可以被正確檢測出來，並且藏密影像的最大直方圖偏差度均明顯高於原始影像，約達 2.5 至 4.4 倍。



（a）Lena　（b）Peppers

（c）Baboon　（d）Straw

圖 4. 實驗影像直方圖



（a）Lena　（b）Peppers

（c）Baboon　（d）Straw

圖 5. 實驗影像直方圖偏差度

表 1：本文方法實驗結果

實驗影像	原始影像		藏密影像	
	峰點位置	最大直方圖偏差度	峰點位置	最大直方圖偏差度
Lena	154	18.56	154	52.16
Peppers	97	13.37	97	58.67
Baboon	120	17.68	120	59.61
Straw	193	15.86	193	37.35

五、結論

本文提出一種簡單、快速的藏密分析方法，針對 Ni 等學者提出之可逆式資訊隱藏方法，分析各種直方圖統計特性，並定義直方圖偏差度作為藏密分析的判斷依據。經實驗證明對於一般自然影像有良好之偵測效果。

未來本方法將朝向偵測多重嵌入(Multiple Embedding)的方向發展，並將針對自然、人物、醫學、紋理等不同類型之影像，區分直方圖特性加以分析，以提高藏密分析之準確率。

六、誌謝

本研究為中華民國行政院國家科學委員會專題研究計畫部分成果，計畫編號：NSC 98-2221-E-182-066-MY2。

七、參考文獻

[1] I. Avcibas, N. Memon, and B. Sankur, "Steganalysis using image quality metrics," *IEEE Transactions on Image Processing*, vol. 12, no. 2, pp. 221-229, Feb. 2003.

[2] R. Chandramouli, M. Kharrazzi, and N. Memon, "Image steganography and steganalysis: Concepts and practice," *Proceedings of International Workshop on Digital Watermarking*, Seoul, South Korea, Oct. 30 – Nov. 1, 2004, pp. 35-49.

[3] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color and gray-scale images," *Magazine of IEEE Multimedi*a, vol. 8, no. 4, pp. 22-28, Oct.-Dec. 2001.

[4] J. Fridrich, "Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes," *Proceedings of 6th Information Hiding Workshop*, Toronto, Canada, May 23-25, 2004, pp. 67-81.

[5] J. J. Harmsen, and W.A. Pearlman, "Steganalysis of additive noise modelable information hiding," *Proceedings of the SPIE, Security, Steganography, and Watermarking of Multimedia Contents V*, Santa Clara, CA, USA, Jan. 21, 2003, pp. 131-142.

[6] S. Lyu, and H. Farid, "Steganalysis using higher-order image statistics," *IEEE Transactions on Information Forensics Security*, vol. 1, no. 1, pp. 111-119, March 2006.

[7] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354-362, March 2006.

[8] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890-896, Aug. 2003.

[9] C. D. Vleeschouwer, J.-F. Delaigle, and B. M. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," *IEEE Transactions on Multimedia*, vol. 5, no.1, pp. 97-105, March 2003.

[10] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," *Proceedings of 3rd Information Hiding Workshop*, Dresden, Germany, Sept. 29 – Oct. 1, 1999, pp. 61-75.

[11] G. Xuan, J. Chen, J. Zhu, Y.Q. Shi, Z. Ni, and W. Su, "Lossless data hiding based on integer wavelet transform," *Proceedings of IEEE International Workshop on Multimedia Signal Processing*, St. Thomas, Virgin Islands, USA, Dec. 9-11, 2002, pp. 312-315.