像素值差異偵密技術應用於彩色影像集之研究

李東岳、陳奕君、吳坤熹
國立暨南國際大學資訊工程學系

摘要

由於資訊科技的發展以及網際網路的便利性，使得資料得以快速傳輸。為了避免機密資料輕易被竊取，資料加密及資訊隱藏的技術成為了重要的研究課題。傳統的資訊隱藏使用最低位元替換藏密法（LSB），優點是很難被人類視覺系統察覺，但是藏密量不多。像素值差異藏密法（PVD）將祕密訊息透過更改兩兩相鄰之像素值差異，按規則藏入影像中，大幅增加藏密量。在進行PVD偵密時，基本假設為原始影像之像素差值直方圖呈常態分布（鐘型曲線），而經像素值差異藏密法（PVD）處理後之影像檔，像素差值直方圖會有不正常分布，呈階梯狀。過去之PVD偵密技術均以灰階圖片進行研究，本論文以不同特性之彩色影像集，驗證PVD偵密技術實行之基本假設，並提出特殊反例，說明具何種特性之影像集易令傳統PVD偵密技術形成誤判。

關鍵字：PVD偵密，RS偵密，直方圖，資訊隱藏。

On The Study of Anti-steganalysis on Pixel Value Differencing (PVD) for True Color Image Files

Dong-Yue Li, Yi-Jun Chen, Quincy Wu
Department of Computer Science and Information Engineering
National Chi Nan University

Abstract

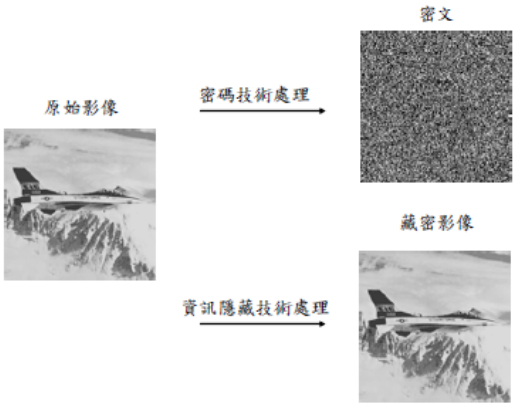
Sensitive data could be transmitted quickly and conveniently, with the development of information technology and the ubiquitous deployment of the Internet. In order to prevent sensitive data from being intercepted, the researches on data encryption and information hiding techniques become important. The advantage of least significant bit (LSB) steganography is that secret data would be difficult to detect by human visual systems, but its capacity of hiding is not large. Pixel value differencing (PVD) steganography hides data into the difference between pixel pairs, which significantly enlarge its hiding capacity. In detecting whether PVD is applied in hiding data in image files, previous literature focuses on grey-scale image files, and assumes that the histogram of original images should show a normal distribution (bell curve). This paper verified the assumption with several sets of image files, and pointed out some counterexamples violating that assumption, which will easily confuse current PVD steganalysis algorithms.

Keywords: Histogram, Information Hiding, Pixel Value Differencing, Regular-Singular Steganalysis.

1. 前言

由於網際網路與資訊科技的蓬勃發展，在軍事情報上，人們不再仰賴飛鴿傳書或快馬傳令這種傳統情報傳輸方式；取而代之的是運用方便又快速的網路媒介來增強雙方接收及傳送訊息的互通性。然而，資訊傳遞的過程中很容易被攔截或破壞，造成許多後勤或戰術的謀略因此失敗。因此，迎面而來的挑戰使得兩大新技術應運而生——資料加密（data encryption）及資訊隱藏（information hiding）[1][2]。

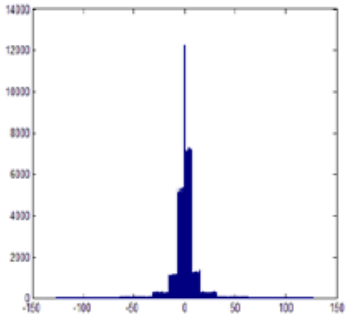
加解密系統可分為兩大類：秘密金鑰系統（對稱式加解密系統）及公開金鑰系統（非對稱式加解密系統）[3][4]。假設有n位使用者彼此間欲進行資料傳遞，前者系統之每位使用者就必須管理n-1個金鑰進行加解密，後者則每位使用者只需要保管好一個私有金鑰進行解密即可。公開公鑰可透過Certificate Authority（CA）、網頁WWW等方式公告週知，有效地簡化金鑰管理問題。但如同保險箱一樣，利用加密技術保護的資料，等於是宣告此筆資料非比尋常，極易吸引有心人士用盡各種方式來破解其加解密系統。為了避免這種「欲蓋彌彰」的窘境，資訊隱藏（information hiding）的技術應運而生。



圖一 密碼技術與資訊隱藏技術之比較[5]

以圖形檔為例，資料隱藏是將所要傳送的秘密資料藏入一張掩護影像(cover image)中，由於掩護影像與藏密前的原影像差異非常微小，所以第三方不容易察覺掩護影像是可疑的，如此就能提高傳遞秘密訊息的安全性。相形之下，資料加密會形成無意義亂碼，容易使人察覺影像的改變。圖一顯示資料加密與資訊隱藏不同之處。

Bender等學者於1996年所提出的最低位元替換藏密法（Least Significant Bit, LSB）[6]，優點是藏密後很難被人類視覺系統察覺異狀，缺點是藏密量最多僅1bpp（bit per pixel）。此外，此LSB藏密技術容易被 Regular-Singular（RS）偵密技術[7]所察覺。Wu與Tsai學者於2003年提出的像素值差異演算法(Pixel Value Differencing, PVD)[8]，將祕密訊息透過更改兩兩相鄰之像素值差異，按規則藏入影像中，此方法不但增加藏密量，並且可避免被RS偵密技術所察覺。然而PVD藏密法亦有其缺點。原始影像經PVD藏密後之像素差值直方圖會呈現不自然階梯狀分布，如圖二所示。依此原理所發展出的PVD偵測技術便能按此特性分辨出那些經由PVD藏密技術的影像，進行偵密[9][10]。



圖二 影像經PVD藏密之像素差值直方圖[10]

本論文之目的是探討PVD偵密技術實行之基本假設。由於PVD偵密技術是透過分析可疑影像之像素差值直方圖是否為不自然階梯狀之分布，來對一幅待評估之影像檔進行分類。其假設未藏密影像之像素差值直方圖是呈現常態分布（鐘型曲線）。本論文將利用夜景、海灘、人工符號等影像集，進行像素差值資料分析來驗證PVD偵密技術之常態曲線基本假設，並提出未來應如何改善此偵密技術以避免系統誤判。

本論文共分為四節：第1節為前言，說明本研究之目的及方法；第2節為RS及PVD偵密技術之基本介紹，並說明PVD偵密技術之疑慮；第3節說明本論文之資料分析方法及結果；第4節是結論及未來展望。

2. 相關文獻探討

2.1 Regular-Singular（RS）偵密技術

RS偵密技術是由Fridrich等學者[7]於2001年提出。假設掩護影像為I × J個像素，將其切割成長度為n個連續像素的群組$P=(x_1,\ldots,x_n)$，群組之間交集須為空集合。為了計算影像檔中的雜訊（藏入訊息就會令雜訊增加），這裡定義了鑑別函數（Discrimination Function）來計算混亂的程度：

$$f(P) = f(x_1,x_2,x_3,\ldots,x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i| \quad (1)$$

為了偵測是否有LSB隱藏的特性，定義了三種翻轉函數(Flipping Function)，。：

$$F_1(x) = x + 1, \text{ if } x \text{ is even};\quad x - 1, \text{ if } x \text{ is odd} \quad (2)$$

$$F_{-1}(x) = F_1(x+1) - 1, \quad \forall\, x \in P \quad (3)$$

$$F_0(x) = x, \forall\, x \in P \quad (4)$$

F_1（正翻轉）,F_{-1}（負翻轉）,F_0（不翻轉） 是三種翻轉函數，以八位元灰階圖形為例，像素值集合為P = {0, …, 255}。翻轉函數即是對灰階值進行微調。LSB隱藏相當於F_1翻轉。以像素值4為例，並選擇做正翻轉，則會4 → 5。以二進位表示就是00000100→00000101。同理，負翻轉及不翻轉之操作依公式(3)(4)可分別得到結果值。

單一翻轉函數所造成混亂的程度不大，但是如果經過兩次不同的翻轉函數則會有極大的差異。LSB偵密的原理即是，比較翻轉後的混亂程度。沒藏訊息之影像經一次翻轉與原影像比較後，其差異值不大；有藏訊息之影像經一次F_{-1}翻轉與原影像比較後，其差異較大，因為實際上該影像共被翻轉了兩次。

翻轉後利用鑑別函數f來衡量，依照下列關係分成三大群組：

正規組(Regular Groups)：

$$P \in R \Leftrightarrow f(F(P)) > f(P) \quad (5)$$

奇異組(Singular Groups)：

$$P \in S \Leftrightarrow f(F(P)) < f(P) \quad (6)$$

不變組(Unusable Groups)：

$$P \in U \Leftrightarrow f(F(P)) = f(P) \quad (7)$$

如果用一個遮罩向量M來表示進行哪些翻轉動作，例如n=4時，M=(1,0,0,1)代表對(x_1,x_2,x_3,x_4)依序進行F_1,F_0,F_0與F_1翻轉。R_M為依遮罩向量M作用下正規組占所有像素的比例，S_M為依遮罩向量M作用下奇異組占所有像素的比例。R_{-M}為依遮罩向量-M（若M表示進行F_1,F_0,F_0,F_1翻轉，則-M表示進行F_{-1},F_0,F_0,F_{-1}翻轉）作用下正規組占所有像素的比例；S_{-M}為依遮罩向量-M作用下奇異組占所有像素的比例。正常圖片下，

$$R_M \fallingdotseq R_{-M} \quad \text{and} \quad S_M \fallingdotseq S_{-M} \quad (8)$$

此外正常群組數應當大於異常群組數。亦即：

$$R_M > S_M \quad (9)$$

經過LSB藏密後，隨著藏密量的增加，R_M和S_M的差距會減少，而R_{-M}和S_{-M}的差距會變大。亦即：

$$R_M \fallingdotseq S_M \quad (10)$$

如果不符合上述(8)(9)條件，那麼就能判定該圖為經

由LSB方法隱藏的圖片。

2.2 PVD偵密技術[9][10]

由於PVD在藏入時是按照像素差值所座落的區間來分類，新的像素差值直接取決於訊息加上該區間的下限值，這樣會使分類好的區間內每個像素值出現的頻率一致，利用此一特性便能夠偵測到PVD隱藏技術。

差值直方圖是表示一張圖的相鄰兩像素差值出現次數的狀況。在正常的圖片差值直方圖顯示出來的會是常態分布，而經由PVD隱藏過後的圖片差值直方圖則會出現階梯狀分布，這是因為PVD這種特殊藏法導致而成的，當每個區間內每個像素差值出現次數差不多時，在差值直方圖上區間與區間就會形成類似階梯的形狀，斷層的地方就是區間的界線。

假設有一圖共有m*n個像素，兩相鄰像素為一組，總共會有m*n/2個像素組，其差值為 $x_1, x_2, \cdots, x_d$，其中d = m*n/2。在只有考慮灰階的情況下，由於每個像素的值介於0至255間，像素差值的可能範圍為-255到255。令H_k為像素差值k出現次數， H_k算法如下：

$$H_k = | \{ x_i | x_i = k, \forall\ i=1, 2, 3, \ldots, d \} |$$

由於一般使用者傳送的圖片皆為彩色，傳統研究中，以相鄰兩灰階像素取差值，本論文採類似的手法，取出像素值後細分成RGB三個相對應的值，再分別從RGB三個不同方向去抓相鄰兩像素來計算差值，故本論文在進行差值直方圖分析時，每張圖都會有三張差值直方圖。

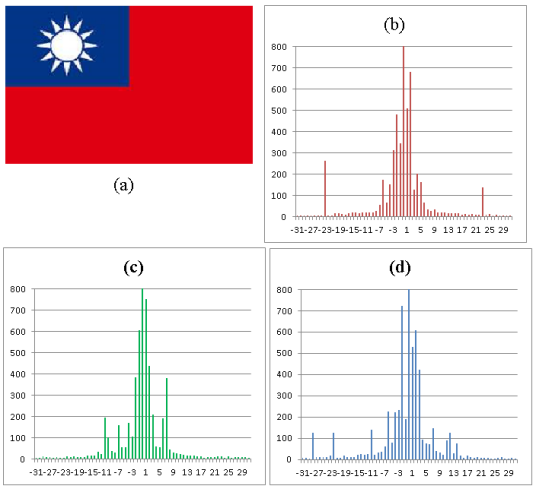
2.3 對於偵測 PVD 特徵值的疑慮

由於[9][10]中所用於偵測PVD之演算法，將會利用到圖形檔像素之特性，也就是「原始影像之像素差值直方圖呈常態分佈；經PVD藏密後之像素差值直方圖則呈現不自然階梯狀分布」。為了降低演算法應用在彩色圖片時的誤判率，本文希望透過實際的影像集，檢驗以下兩個假設：第一是原始影像之像素差值直方圖是否均呈常態分布。第二是未來進行PVD偵密時，系統將藉由分析是否為不自然階梯狀分布之直方圖，此一規格之誤判（false alarm）比率將會是多少。

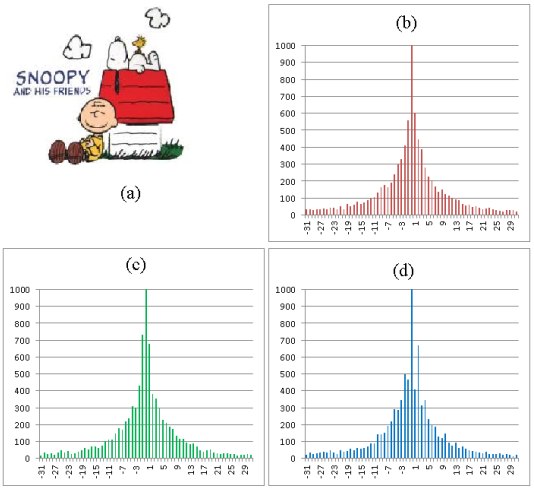
3. 資料分析與結果

3.1 掩護影像之特殊反例

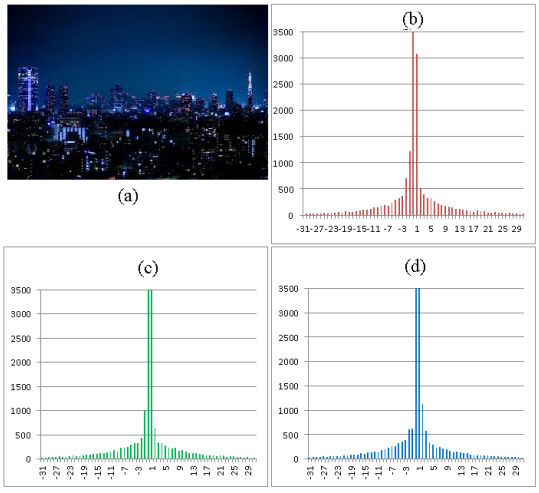
對於2.3節提出的疑慮，我們針對夜景、海灘、人工符號等影像集做像素差值直方圖分析。這些影像集的特性是相鄰色彩差異度不高，分析後所呈現之像素差值直方圖近似於不自然階梯狀分布。影像集如圖三至圖八。



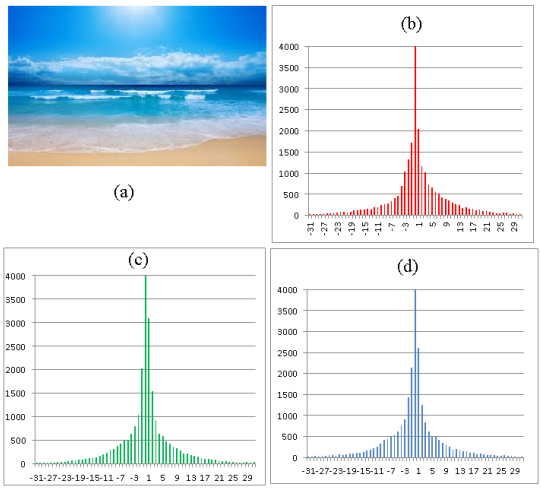
圖三 (a)中華民國國旗[11]
(b)紅像素 (c)綠像素 (d)藍像素



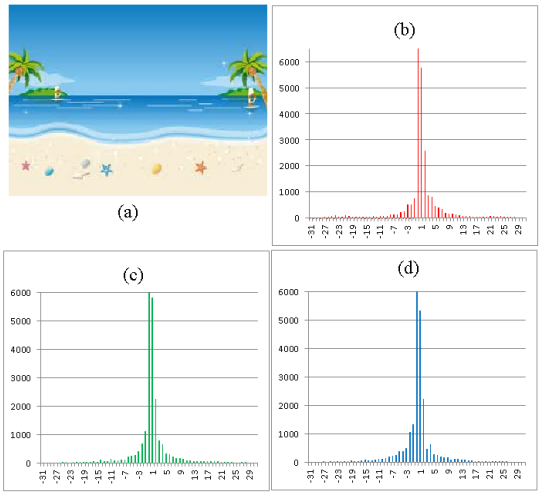
圖四 (a)史奴比[12]
(b)紅像素 (c)綠像素 (d)藍像素



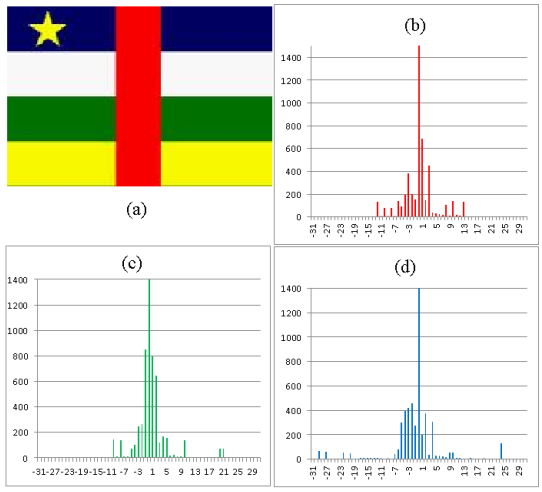
圖五 (a)夜景[13]
(b)紅像素 (c)綠像素 (d)藍像素



圖六 (a)海灘一 [14]
(b)紅像素 (c)綠像素 (d)藍像素



圖七 (a)海灘二 [15]
(b)紅像素 (c)綠像素 (d)藍像素



圖八 (a)中非國旗[16]
(b)紅像素 (c)綠像素(d)藍像素

3.2 實驗結果

運用本論文2.2節提及之計算相鄰像素中RGB差值的方法對未經PVD藏密之特殊反例作資料分析，並且把計算結果用直方圖呈現，其分布呈近似不自然階梯狀之分布。但此圖形檔其實未經PVD藏密，故知此類圖形易令現有之PVD偵密法造成誤判。

4. 結論與未來展望

本研究目前對於影像檔繪出直方圖後，仍需仰賴人工判讀其分佈是否呈近似鐘型曲線之常態分佈。未來擬進一步利用貝式網路（Bayesian network）[17]、模糊理論（fuzzy logic）[18]、類神經網路（neural network）[19]、以及基因演算法（genetic algorithm）[20]發展自動偵密之工具。屆時將可對各種演算法之命中率（hit ratio）與誤判率（false alarm）有更精確之統計數字。

5. 誌謝

本論文由國科會編號NSC 101-3113-P-033 -003計畫所支持。由於國科會的支持，使本計畫得以順利進行，特此致上感謝之意。

6. 參考文獻

[1] Huaiqing Wang, “Cyber warfare: steganography vs. Steganalysis,” Communications of the ACM, Volume 47 Issue 10, Pages 76-82, October 2004.

[2] Hal, Berghel, “Hiding data, forensics, and anti-forensics,” Communications of the ACM, Volume 50 Issue 4, Pages 15-20, April 2007.

[3] Mike Burmester, Yvo G. Desmedt, “Is hierarchical public-key certification the next target for hackers?” Communications of the ACM, Volume 47 Issue 8, Pages 68-74, August 2004.

[4] Craig Gentry, “Computing arbitrary functions of encrypted data,” Communications of the ACM, Volume 53 Issue 3, Page 97-105, March 2010.

[5] 左豪官、戴鑑廷、盧嘉鴻、婁德權、劉江龍、吳嘉龍，資訊隱藏技術之研究，黃埔學報，第五十二期，第 9-16 頁，2007。

[6] W. Bender, D. Gruhl, N. Morimoto, and Aiguo Lu, “Techniques for data hiding,” IBM Systems Journal, Vol. 35, No. 3-4, pp. 313-336, 1996.

[7] J. Fridrich, M. Goljan, and R. Du, “Detecting LSB Steganography in Color and Gray-scale Images,” IEEE Multimedia, Vol.8, No.4, pp. 22-28, Oct-Dec 2001.D. C.

[8] Wu, and W. H. Tsai, “A steganographic method for images by pixel-value differencing,” Pattern Recognition Letters, Vol. 24, No. 9-10, pp. 1613-1626, 2003.

[9] V. Sabeti, S. Samavi, M. Mahdavi, and S. Shirani, “Steganalysis and payload estimation of embedding in pixel differences using neural networks,” Pattern Recognition, Vol. 43, No. 1, pp. 405-415, 2010.

[10] 劉江龍、李翊豪、劉興漢，可偵測使用模數運算像素值差異藏密法之偵密技術，第 20 屆國防科技學術研討會論文集，桃園、台灣，第 631-637 頁，2011。

[11] Flag of Republic of China, http://www.president.gov.tw/Default.aspx?tabid=1031

[12] Snoopy Photo, http://ameblo.jp/asovinbar/entry-11567469937.html?frm_src=thumb_module

[13] Night View of Tokyo City, http://www.picstopin.com/3916/night-view-from-westin-tokyojpg-wikimedia-commons/http:%7C%7Cupload*wikimedia*org%7Cwikipedia%7Ccommons%7Cf%7Cf9%7CNight_view_from_Westin_Tokyo*jpg/

[14] Beach Photo, http://www.wallpaperok.biz/img/blue-ocean.html

[15] Beach Photo, http://www.ananedu.com/walltaper/w33.htm

[16] Flag of Central African Republic, http://www.wallpapergate.com/wallpaper11047.html

[17] Aruna Ambalavanan, Rajarathnam Chandramouli , “A Bayesian image steganalysis approach to estimate the embedded secret message,” MM&Sec '05: Proceedings of the 7th workshop on Multimedia and security, August 2005.

[18] Qingzhong Liu, Andrew H. Sung, “Feature mining and neuro-fuzzy inference system for steganalysis of LSB matching stegangoraphy in grayscale images,” IJCAI'07: Proceedings of the 20th international joint conference on Artifical intelligence, January 2007.

[19] Shaohui Liu, Hongxun Yao, Wen Gao, “Neural network based steganalysis in still images,” ICME '03: Proceedings of the 2003 International Conference on Multimedia and Expo - Volume 1 , Volume 1, , July 2003.

[20] Xiao Yi Yu, Aiming Wang, “An Investigation of Genetic Algorithm on Steganalysis Techniques,” IIH-MSP '09: Proceedings of the 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, September 2009.