

行政院國家科學委員會專題研究計畫 成果報告

發展醫學影像遭竄改時之偵測及還原系統

計畫類別：個別型計畫

計畫編號：NSC92-2314-B-039-010-

執行期間：92年08月01日至93年07月31日

執行單位：中國醫藥大學醫學系

計畫主持人：陳中和

共同主持人：王清林

報告類型：精簡報告

處理方式：本計畫可公開查詢

中 華 民 國 93 年 11 月 2 日

中文摘要

關鍵詞：數位影像、竄改、編碼、加密、偵測、還原

在台灣的醫療環境中，病人在不同醫院之間就診的情況極為常見，因此，病人常需要在醫療院所取得檢查的影像資料，到另外一個院所做為就診的參考。由於目前 PACS 在台灣已逐漸盛行，故這種醫院與醫院之間影像的傳遞，已由一般的拷貝影像的傳遞漸漸轉變為數位影像的方式，而不管是那一種方式，這些影像資料都極容易經由一般的影像軟體做竄改，這種竄改不外乎是在既有影像上做病灶的塗抹或加上新的病灶，以達到其領取保險金、帶病投保，或其他不法的索賠。這些事件雖然在目前尚不多見，但在將來數位化影像更普及的情況之下，將逐漸浮現。為了防止醫療影像在院與院之間傳遞時，遭到任意的竄改以達到不法的目的，對於這些數位影像資料加以管理、監控，並確保影像資料的真實性是很重要的事情。基於這種潛在的需要，本計劃小組在既有的基礎之下，對於數位影像及一般的拷貝影像做編碼加密以偵測及還原受竄改的影像。

英文摘要

關鍵詞：digital image, PACS, watermarking, Block Truncation Coding, Discrete Wavelet Transformation, Inverse Discrete Wavelet Transformation, tampered image, stego image

In Taiwan, patients searching for help in different hospitals are common. Diagnostic images are usually transferred between medical institutions. Due to the global trend of establishing PACS in recent years, the conventional transfer of hard copy is now added with these digital images. These two forms of images, once going outside of hospitals, are loss of control and easily tampered by various kinds of commercially or personally developed imaging software. The artificial images are usually for illegal purposes in health insurance. Assuring the originality of these medical images will therefore become a vital issue in the near future. Based on this potential demand, how to set up an effective verifying system for detecting distorted images is increasingly needed.

In this project, we attempt to build up a reliable and efficient system for authentication of medical images including digital images and the printed-and-scanned images. Our method is not the visible watermarking; rather, it is a hidden one. We use Block Truncation Coding (BTC) technique to acquire features of the raw data of original image, which we intend to manipulate. Then, by Discrete Wavelet Transformation (DWT), the spatial domain of the raw data was transferred to frequency domain image. The “In-Encryption Features” we choose are inserted into the medium and high frequency regions. Finally, by Inverse Discrete Wavelet Transformation (IDWT), these frequency domain data are converted into spatial domain images, which is called “stego Image”. Once the stego images are distorted either by erasing or by addition, the inserted “secret key” in the encryption features will help for decryption and find out where the image has been changed. Moreover, the tampered image can also be restored to its original one.

報告內容

前言、研究目的及文獻探討

目前對於數位影像的保護大多利用浮水印(Watermark)嵌入原始影像來達成，而浮水印的技術依照其特性可分為可視 (visible) 及不可視 (invisible) 兩類，可視的浮水印是一種從肉眼就可以辨別出來的浮水印，所以通常都是將有意義的圖示嵌入影像來達到影像權益保障的目的，例如公司的標記或是特別的標誌；而不可視的浮水印則是無法利用肉眼辨別，需透過某些特定的演算法之後，才能將浮水印藏入與取出，將來發生權益糾紛的時候我們可以從原始影像中取出預先藏入的浮水印來做驗證。由於可視的浮水印對於影像的美觀上的影響較大，而且可視的浮水印很容易就會遭受到竄改，為了不影響影像的美觀且在原始影像破壞最小的情況下藏入浮水印，所以在本計畫中我們採用不可視的浮水印方式將特徵值藏入影像之中，將來我們就以藏入的特徵值當做判斷影像是否遭竄改的依據。

目前已有一些學者針對數位影像的保護技術作探討，這些方法皆是偵測影像是否遭受竄改之技術。不過這些方法只能偵測出被保護的影像所遭受竄改之處，並未提供將竄改處還原之功能。因此，我們提出一個新的方法，此方法不但能夠指出影像遭竄改之處，亦能將遭竄改的影像加以還原。目前對於影像的認證方面已經有許多的研究，由於這些方法大部分討論的範圍都在電腦中進行，並沒有考慮影像需要做列印輸出，為了讓列印後的影像也能受到保護是目前相當重要的研究方向，因此在本計畫中，我們別一個重點是針對列印輸出影像的權益保障問題提出一套解決方案。

對於影像列印前的影像保護，本計畫所提的方法，使用區塊截斷編碼 (Block Truncation Coding, BTC) 技術已獲取欲保護影像之特徵資料，同時也利用離散小波轉換 (Discrete Wavelet Transformation, DWT) 方式，將一張欲被保護的影像由空間域轉換成頻率域，然後再將特徵值加密並打散後隱藏到頻率域影像的中高頻處。最後再以反離散小波轉換方式將其轉回可被公開的空間域影像，我們稱此影像為偽裝影像。在偵測影像是否遭受竄改時，只須取出被藏入在偽裝影像中的特徵值，並以同樣方式計算偽裝影像的特徵值。若所得結果與原始藏入的特徵值不相同時，則可確認偽裝影像已遭竄改。此時可利用被隱藏的特徵值，將其影像還原。

對於影像列印後的影像保護，亦是本計畫的另一重點，我們所提的方法，利用邊緣 (Edge) 資料當作特徵值，將特徵值做 Reed-Solomon Code

(RS Code), 使得藏入的特徵值能夠有錯誤更正的能力, 再利用離散餘弦轉換 (DCT) 將特徵值藏入頻率域的中頻區域, 將來在偵測影像是否遭受到竄改的時候, 根據藏入的特徵值以及鏈碼 (Chain Code) 的技術, 就可以指出影像遭受到竄改的部分。一般的浮水印技術討論的範圍皆是在電腦中做處理, 而忽略影像列印後的保護, 若是一張數位影像需要做列印輸出時, 藏入的浮水印必須要能夠抵抗列印及掃描的嚴重失真, 因此浮水印的強韌性就受到很大的考驗, 本計畫著重在列印後掃描影像竄改之偵測, 所以我們藏入的浮水印除了要能夠抵抗列印及掃描的嚴重失真之外, 藏入的浮水印更需具備容錯及錯誤更正的能力才能夠提昇資料的正確性, 為了讓藏入的特徵值能有錯誤更正的能力, 我們利用 RS Code 的編碼技術對特徵值進行編碼, 為了讓藏入的特徵值具有強韌的特性, 我們使用離散餘弦轉換 (DCT) 將影像由空間域轉換至頻率域並將邊緣特徵藏入中頻區域, 竄改偵測是以藏入的邊緣特徵當做依據並利用 Chain Code 將影像中連續的區域圈選出來, 根據所圈選的區域判斷該影像是否遭竄改。

根據我們的初步實驗結果顯示, 無論竄改的動作是在影像列印前或是列印後, 我們的方法都可正確地指出影像遭竄改的部位, 這對於智慧財產權的保障有著非常卓越的貢獻。

竄改偵測與還原的方法與程序

偽裝影像產生程序

圖 1 為偽裝影像產生的程序。本計劃使用區塊截斷編碼 (Block Truncation Coding, BTC) 技術, 將欲保護之影像切割成數個不重複的區塊, 同時也求出每一區塊的位元圖及重建階, 再以此位元圖及重建階作為影像的特徵值。此方法結合離散小波轉換 (Discrete Wavelet Transformation, DWT) 方式, 將一張欲被保護的空間域影像轉換成頻率域影像。然後將特徵值加密並打散後, 再隱藏到頻率域影像中的中高頻處。最後, 再以反離散小波轉換方式將其轉回可被公開的空間域影像(偽裝影像)。

實驗將原始影像(如圖 3(a)、圖 4(a)、圖 5(a) 及圖 6(a))利用離散小波轉換將其由空間域轉換成頻率域的影像, 並將中低頻帶的每一係數之低位元資料設為 0, 接著再以反離散小波轉換將其轉換成一張空間域的影像。將此空間域影像縮小成原始大小的四分之一後, 得到一張大小為 256x256 個像素的縮小影像。並將該縮小影像切成 64x64 個不重複的區塊, 即每一區塊由 4x4 個像素所組成。然後再以區塊截斷編碼方式, 計算出每一區塊的位元圖與重建階 a 、 b 。由此可知, 特徵值大小為 $64 \times 64 \times 32 = 131072$ 個位元。複製三份後的特徵值共佔 393216 個位元, 剛好與可藏入資料的空間大小相同。接著, 對特徵值作加密處理後, 並將其分散地藏入頻率域影像的中低頻係數中, 再將此頻率域影像轉回空間域影像, 即可獲得如圖 3(b)、圖 4(b)、圖 5(b)及圖 6(b)的偽裝影像。

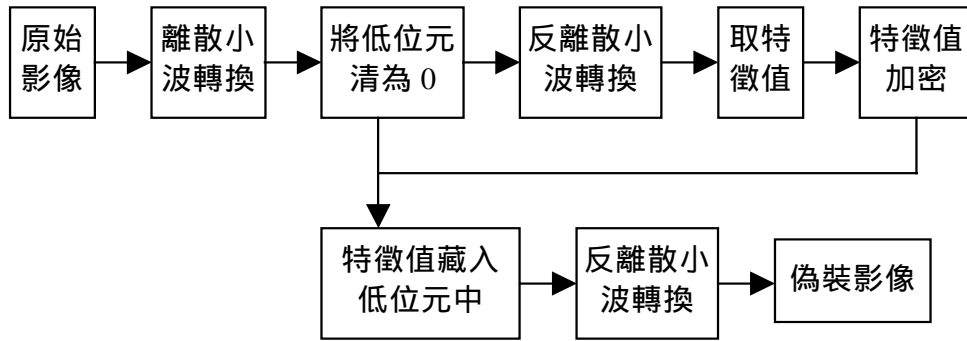


圖 1：特徵值藏入流程圖

竊改偵測與還原程序

圖 2 為偵測竊改及還原的程序。在偵測影像是否遭受竊改時，只需取出被藏入在該影像中的特徵值，並以同樣方式計算此影像的特徵值。若影像未遭竊改，則竊改前後所取得的特徵值，應完全相同。否則意味著該偽裝影像必已遭竊改。此時可利用被隱藏的特徵值(每一區塊的位元圖及重建階 a、b 值)來修補該遭竊改的區塊，將其恢復成原始影像。

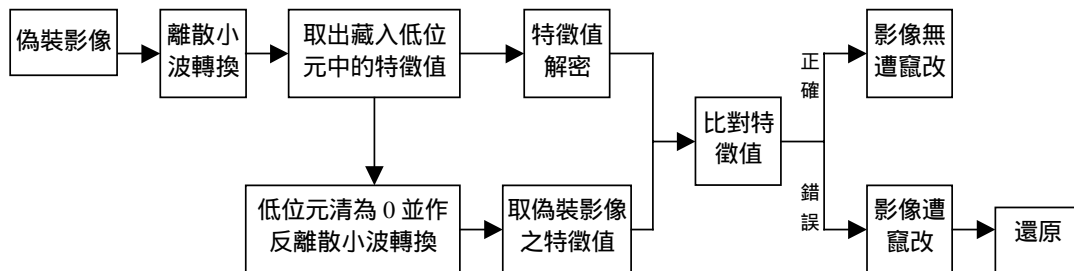


圖 2：偵測竊改及還原流程

實驗結果

此實驗使用圖 3(a) “Saiboat”、圖 4(a) “Airplane”、圖 5(a) “Lena”及圖 6(a) “Liver”的原始數據(.raw data)做為測試影像，此四張影像皆為含有 512×512 個像素的灰階影像。

對圖 3(b)、圖 4(b)、圖 5(b)及圖 6(b)做竊改，圖 3(c)、圖 4(c)、圖 5(c)及圖 6(c)為竊改後的影像。再依據偵測竊改方法，從圖 3(c)、圖 4(c)、圖 5(c)及圖 6(c)中萃取出藏入之特徵值，並重新計算圖 3(c)、圖 4(c)、圖 5(c)及圖 6(c)之特徵值。比較這些特徵值後，得知圖 3(b)、圖 4(b)、圖 5(b)及圖 6(b)已遭竊改，遭竊改區域如圖 3(d)、圖 4(d)、圖 5(d)及圖 6(d)所示。找到竊改處後，再根據還原方法，將其還原成如圖 3(e)、圖 4(e)、圖 5(e)及圖 6(e)所示的影像。



(a) 原始影像

(b) 偽裝影像

(c) 遭竄改影像



(d) 偵測影像遭竄改之位置

(e) 還原影像

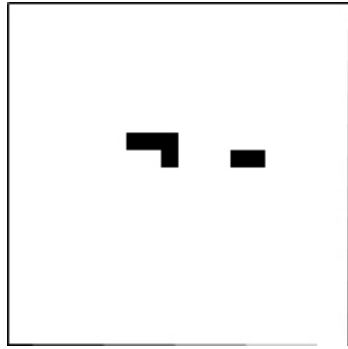
圖 3：“Saiboat”影像



(a) 原始影像

(b) 偽裝影像

(c) 遭竄改影像



(d) 遭竄改位置



(e) 還原影像

圖 4：“Airplane”影像



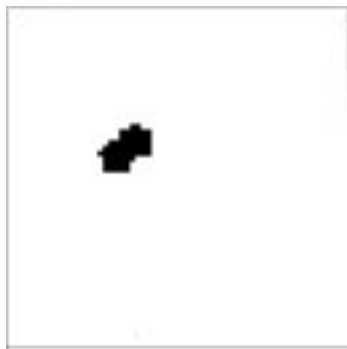
(a) 原始影像



(b) 偽裝影像



(c) 遭竄改影像

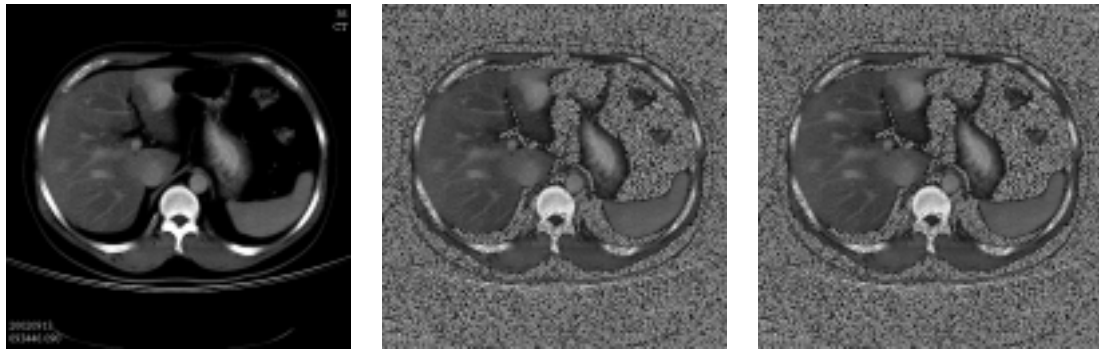


(d) 遭竄改位置



(e) 還原影像

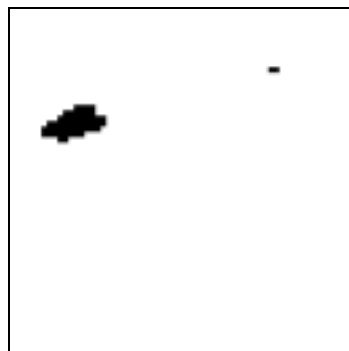
圖 5：“Lena”圖



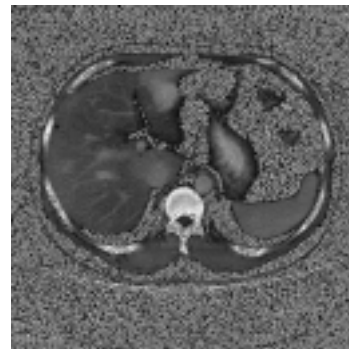
(a) 原始影像

(b) 偽裝影像

(c) 遭竄改影像



(d) 遭竄改位置



(e) 還原影像

圖 6 : "Liver"圖

此實驗亦計算偽裝影像、還原影像與原始影像比較之 PSNR 值，表格 1 列出其結果。

表格 1：與原始影像比較之 PSNR 值

項目 影像名稱	偽裝影像之 PSNR (dB)	還原影像之 PSNR (dB)
Saiboat	33.89	31.65
Airplane	32.68	32.58
Lena	33.48	33.36
Liver	5.96	5.96

由圖 3(d)、圖 4(d)、圖 5(d)及圖 6(d)所顯示的實驗結果可看出，我們的系統都能有效偵測出影像遭竄改的區域。由圖 3(e)、圖 4(e)、圖 5(e)及表格 1 的 PSNR 值可看出，此方法亦有不錯的還原效果。

圖 6(b)為加入特徵資料後的偽裝肝臟圖,此圖和原始影像差異甚大,其 PSNR 值為 5.96,此乃因進行 DWT 轉換時,像素值超出 0 至 255 範圍之故,本方法將對此處之 DWT 轉換稍加以改善,相信可克服此處圖像品質之不良。圖 6(c) 為遭竄改後的影像。依據偵測竄改方法,從圖 6(c)中萃取出藏入之特徵值,並重新計算圖 6(c)之特徵值。比較這些特徵值後,證明圖 6(c)已遭竄改,遭竄改區域如圖 6(d)所示。找到竄改處後,再根據還原方法,將其還原成如圖 6(e)所示的影像。雖然圖 6(e)和原始影像比對之 PSNR 值為 5.96,但此和前述之 DWT 轉換像素值超出 0 至 255 範圍是相同原故。事實上,還原影像(圖 6(e))和偽裝影像(圖 6(b))比對之 PSNR 值為 37.88,此已說明所還原之影像和所公佈之偽裝影像間之相似程度,當然在醫療影像上,對於影像品質之要求更高,因此本方法將進一步為滿足此影像品質之要求而努力。

結論

實驗顯示,在無原始影像可比對的情況之下,本方法的確能由遭到竄改的偽裝影像將遭竄改之區塊有效偵測出來並加以還原,而且還原影像與原圖比較皆可得到不錯的效果。雖然本系統仍存在一些瑕疵,但本方法在影像遭竄改之偵測及還原上仍值得採用。

計畫成果自評部份

台灣大部分的醫院已漸漸進入數位影像傳輸的無片時代,由於數位影像在院際間頻繁的傳遞,影像的防偽技術開發日漸重要。

本計劃原本預計在一年的期間達成數位影像防偽編碼技術,偵測竄改,及影像還原的目的。前兩項技術已完成目標,後一項目標則仍未臻完善,有待更進一步的努力。針對這點,計劃主持人已另外尋找國立中興大學工學院的專家繼續努力中,成果當指日可期。

參考文獻

- [1] W. Bendar, D. Gruhl, N. Morimoto, & A. Lu, "Techniques for Data Hiding," *IBM System Journal*, Vol. 35(3/4), pp. 313-337, 1996.
- [2] B. B. Chai, J. Vass, and X. Zhuang, "Significance-linked connected component analysis for wavelet image coding," *IEEE Transactions on Image Processing*, Vol. 8, No. 6, Jun. 1999, pp. 774 -784.
- [3] Y. K. Chan, and C. C. Chang, "Concealing a Secret Image Using the Breadth First Traversal Linear Quadtree Structure," *The Proceedings of the Third International Symposium on Cooperative Database Systems for Advanced Applications*

- (CODAS'1), 2000, pp. 194-199.
- [4] C.C. Chang, D. C. Lin, and T. S. Chen, "An Improved VQ Codebook Search Algorithm Using Principal Component Analysis," *Journal of Visual Communication and Image Representation*, Vol. 8, No.1, pp. 27-37, 1997.
- [5] C. C. Chang, K. F. Hwang, & M. S. Hwang, "A Block Based Digital Watermarks for Copy Protection of Images," *Communications, 1999. APCC/OECC '99. and Fourth Optoelectronics and Communications Conference*, Vol. 2, pp. 977- 980, 1999.
- [6] C. C. Chang, C. S. Tsai, and T. S. Chen, "A new scheme for sharing secret color images in computer network," *Image Processing, 2000*, Proceedings. 2000 International Conference on, Vol. 1, pp. 601-604, 2000.
- [7] C. C. Chang, H. C. Hsia, and T. S. Chen, "Reliable information hiding for printed images," in *Proceedings of 2000 International Symposium on Information Theory and Its Applications*, November 2000, Vol. 1, pp. 97-100.
- [8] C. W. Chao, C. H. Hsieh, P. C. Lu, and T. A. Cheng, "Modified block truncation coding for image compression," *Pattern Recognition Letters* 17, 1996, pp.1499-1506.
- [9] T. S. Chen, C. C. Chang, and M. S. Hwang, "A Virtual Image Cryptosystem Based upon Vector Quantization," *IEEE Transactions on Image Processing*, Vol. 7, No. 10, October 1998, pp. 905-910, 1998.
- [10] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia", *IEEE Transactions on Image Processing*, 1997, Vol. 6, No. 12, pp. 1673-1687.
- [11] M. Craizer, E. A. B. D. Sulva, and E. G. Ramos, "Convergent Algorithms for Successive Approximation Vector Quantization with Applications to Wavelet Image Compression," *IEE Proceedings- Vision Image and Signal Processing*, Vol. 146, No. 3, June 1999, pp. 159-164.
- [12] L. Z. Chuang, and C. C. Chang, "The Study of Image Tampering Detection," *Master Thesis*, National Chung Cheng University, Chiayi, Taiwan, R.O.C., 2000.
- [13] P. P. Dang, and P. M. Chau, "Image Encryption for Secure Internet Multimedia Applications," *IEEE Transactions on Consumer Electronics*, Vol. 46, Issue: 3, August 2000, pp. 395-403.
- [14] E. J. Delp and O. R. Mitchell, "Image compression using block truncation coding," *IEEE Trans. Commun.* 27, 1979, pp.1335-1342.
- [15] M. Feil, M., R. Kutil, P. Meerwald, and A. Uhl, "Wavelet Image and Video Coding on Parallel Architectures," *The 2nd International Symposium on Image and Signal Processing and Analysis (ISPA'1)*, 2001, pp. 24-35.
- [16] A. Gersho, R. Gray, "Vector Quantization and Signal Compression," *Kluwer Academic Publishers*, Dordrecht, 1992.

- [17] J. R. Hernández, J. M. Rodríguez, and F. Pérez-González, "Improving the Performance of Spatial Watermarking of Images Using Channel Coding," *Signal Processing*, Vol. 80, Issue: 7, July 2000, pp. 1261-1279.
- [18] C. T. Hsu and J. L. Wu, "Multiresolution watermarking for digital images," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, Vol. 45, No. 8, Aug. 1998, pp. 1097 –1101.
- [19] Y. C. Hu, C. C. Chang, "Low complexity index-compressed vector quantization for image compression," *Consumer Electronics, IEEE Transactions on*, Vol. 45, Issue: 1, pp. 219-224, Feb. 1999.
- [20] J. Huang, Y. Q. Shi, and Y. Shi, "Embedding Image Watermarks in DC Components," *IEEE Transactions on Circuits and Systems for Image Technology*, 2000, Vol. 10, No. 6, pp. 974-979.
- [21] H. Jiwu, and Y. Q. Shi, "Embedding Gray Level Images," *The IEEE International Symposium on Circuits and Systems (ISCAS'1)*, Vol. 5 , 2001, pp. 239 -242.
- [22] N. F. Johnson, and S. Jajodia, "Steganography: Seeing the Unseen", *IEEE Computer*, February 1998, pp. 26-34.
- [23] Y. K. Lee, and L. H. Chen, "An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement," *The Ninth National Conference on Information Security*, Taichung, Taiwan, R.O.C., May 1999, pp. 8-15.
- [24] E. T. Lin, C. I. Podilchuk and E. J. Delp, "Detection of image alterations using semi-fragile watermarks," in *Proceedings of Security and Watermarking of Multimedia Contents*, January 2000, pp. 152-163.
- [25] G. S. Lin, and W. N. Lie, "A Study on Detecting Image Hiding by Feature Analysis," *The IEEE International Symposium on Circuits and Systems (ISCAS'1)*, Vol. 2, 2001, pp. 149-152.
- [26] R. Y. Li, Jung Kim, and N. Al-Shamakh, "Image compression using transformed vector quantization," *Image and Vision Computing*, Vol. 20, Issue: 1, pp. 37-45, January 1, 2002.
- [27] M. L. Marvel, C. G. Jr. Bonchelet, and C. T. Retter, "Spread Spectrum Image Steganography," *IEEE Transactions on Image Processing*, Vol. 8, No. 8, 1999, pp. 1075-1083.
- [28] A. Munteanu, J. Cornelis, G. V. D. Auwera, and P. Cristea, "Wavelet Image Compression – the Quadtree Coding Approach," *The IEEE Transactions on Technology in Biomedicine*, Vol. 3, No. 3, September 1999, pp. 176-185.
- [29] F. Pérez-González, J. R. Hernández, and F. Balado, "Approaching the Capacity Limit in Image Watermarking: a Perspective on Coding Techniques for Data Hiding Applications," *Signal Processing*, Vol. 81, Issue. 6, June 2001, pp. 1215-1238.
- [30] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information Hiding - a Survey", *Proceeding of IEEE*, Vol. 87, No. 7, 1999, pp. 1062- 1078.

- [31] A. Said and W. A. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees," *IEEE Transactions on Circuits and System for Video Technology*, Vol. 6, No. 3, Jun. 1996, pp. 243 –250.
- [32] J. M. Shapiro, "Embedded image coding using zerotrees of wavelet coefficients," *IEEE Transactions on Signal Processing*, Vol. 41, No. 12, Dec. 1993, pp. 3445 –3462.
- [33] Shu Lin, Daniel J., and Costello Jr, "Error Control Coding: Fundamentals and Applications," Prentice-Hall, Englewood Cliffs, N. J., 1983.
- [34] A. Tefas and I. Pitas, "Image authentication and tamper proofing using mathematical morphology," in *Proceedings of EUSIPCO 2000*, European Signal Processing Conference, September 2000, Vol. 3, pp. 1681-1684.
- [35] H. J. Wang, and C. C. J. Huo, "A Multi-Threshold Wavelet Coder (MTWC) for High Fidelity Image Compression," *The IEEE International Conference on Image Processing*, Vol. 1, 1997, pp. 652-655.
- [36] R. Z. Wang, C. F. Lin, and J. C. Lin, "Image Hiding by Optimal LSB Substitution and Genetic Algorithm," *Pattern Recognition*, Vol. 34, Issue: 3, March 2001, pp. 671-683.
- [37] Z. H. Wei, P. Qin, & Y. Q. Fu, "Perceptual Digital Watermark of Image Using Wavelet transform," *IEEE Trans. On Consumer Electronics*, Vol. 44, Issue: 4, pp. 1267-1272, 1998.
- [38] C. R. Yang, M. S. Hwang and Y. L. Tang, "Tampering double detection algorithm," *Proceeding of the Eighth National Conference on Science and Technology of National Defense*, pp. 165-170, Tao-Yuan, Taiwan, November 1999.
- [39] W. H. Yeh, and J. J. Hwang, "Hiding Digital Information Using a Novel System Scheme," *Computers and Security*, Vol. 20, Issue: 6, September 2001, pp. 533-538.
- [40] 陳同孝、林泉成, "一種利用數位離散餘弦轉換及影像邊緣偵測技術設計之 列印後影像竄改防治系統", 台北科技大學 - 2000 年科技與管理學術研討會論文集, pp. 419-426。

