出國報告（出國類別：國際會議）

參加 ICCVE2013 國際會議及發表論文

服務機關：國立虎尾科技大學
姓名職稱：謝仕杰 副教授
派赴國家：美國
出國期間：102 年 12 月 2 日至 102 年 12 月 9 日
報告日期：103 年 3 月 5 日

摘要

此次前往美國參加第二屆 International Conference on Connected Vehicles & Expo的主要目的爲發表論文及蒐集與Connected Vehicles研究領域相關的知識與研究方向。該國際研討會是由IEEE多個(包含Computer、Communications、Intelligent Transportation Systems、Vehicular Technology、Power and Energy、Product Safety Engineering以及RFID等)協會所支持與支援的一種整合不同研究領域之新創辦的研討會。只要是與Connected Vehicles相關的研究主題或發展趨勢都包含在該國際研討會的徵稿範圍內。個人所投稿的論文題目爲 “A Reversible Image Steganographic Scheme Based on SMVQ and Huffman Coding”，是一種可以應用於隱密通訊上的策略及方法，在該研討會的議程中被歸類在“Mobile Internet, Spatial and Social Systems, Internet of Things”研究領域。此研究領域總共有三場次的口頭論文發表時段。在論文發表的過程中，來自新加坡與加拿大的兩位學者表達對此研究題目的興趣。會後，兩位學者與個人進一步討論此研究未來在Connected Vehicles上實現的可行性，個人覺得獲益良多。

目次

本文

目的：

ICCVE2013 國際研討會是由IEEE多個組織支持辦理之研討會。參與的IEEE組織包含Standards Association、Computer Society、Communications Society、Consumer Electronics Society、Industrial Electronics Society、Intelligent Transportation Systems Society、Vehicular Technology Society、Power and Energy Society、Power Electronics Society、Electromagnetic Compatibility Society 、Product Safety Engineering Society以及RFID Committee等等。ICCVE是一種整合不同研究領域之新創立的研討會，第一屆於中國北京舉辦，個人此次前往美國內華達州參加的爲第二屆，第三屆將於 2014 年在歐洲奧地利維也納舉辦。

此次前往美國參加 2013 International Conference on Connected Vehicles & Expo (ICCVE2013) 的主要目的爲發表論文及蒐集與Connected Vehicles研究領域相關的知識與研究方向。在會議過程中，個人口頭發表了一篇研究報告，論文題目爲 “A Reversible Image Steganographic Scheme Based on SMVQ and Huffman Coding”。此論文所展示的研究成果是一種可以應用於隱密通訊上的策略及方法。此篇論文在該研討會的議程中被歸類在“Mobile Internet, Spatial and Social Systems, Internet of Things”研究領域。值得一提的是，被ICCVE2013所接受且出席報告的論文將收錄於IEL電子全文資訊系統以及Engineering Village – Compendex資料庫。因此，個人所發表的論文將歸類爲EI論文。

過程：

此次參加 ICCVE2013 國際會議最主要之目的爲口頭發表論文。由於 ICCVE 是一種整合不同研究領域之新創立的國際會議，此國際會議更規劃了五種不同形式的議程內容，包括專題演講與 Summits、工業論壇(Industry Forums)、技術會議(Technical Sessions)、課程(Tutorials)以及展覽(Exhibition)。在技術會議(技術論文)方面，涵蓋的研究主題包含以下六大領域。

(1) Wireless Communications and Vehicular Networking

(2) Cooperative Driving, Intelligent and Autonomous Vehicles

(3) Transportation and Connected Vehicles

(4) Electric Vehicle and Transportation Electrification

(5) Automotive Electronics and Automatic Control

(6) Mobile Internet, Spatial and Social Systems, Internet of Things

ICCVE2013 技術會議議程總共安排了四天，個人的論文發表時間被安排在第二天下午，所發表之內容摘要如下敘述。

影像藏密技術(image steganography)是一種可行的隱密通訊(covert communication)機制。此技術已經成功地實作在各種數位媒體之上，尤其是數位影像。影像藏密技術除了可以直接地實作於數位影像的空間域(spatial domain)與頻率域(frequency domain)之外，亦可以實作於數位影像的壓縮域(compression domain)。相較於在空間域或頻率域上實作之藏密技術，在壓縮域上實作之藏密技術面臨了更多的挑戰。在資料隱藏量(payload)方面，由於影像壓縮去除了原始影像大部分的重複資訊(redundancy)，因此可用來作爲藏密的空間將會大大地減少。在影像的視覺品質方面，由於影像壓縮與資料藏入的效應，在取密端獲得之掩護影像的視覺品質將會明顯地降低。此外，就掩護影像之壓縮碼本身而言，其位元率(bit rate)亦可能因爲機密資料的藏入而增加。然而，在影像的壓縮域上實作藏密技術亦有其優點。此類型之藏密技術不但可以增加機密資訊在傳遞時的便利性；同時，藉由數位影像壓縮碼的掩護，機密資訊的安全性更可以獲得提升。

向量量化(vector quantization, VQ)技術是一種可以有效達成低位元率壓縮的影像編碼技術。邊緣匹配向量量化(side-match vector quantization, SMVQ)技術改良了向量量化技術在影像壓縮方面的效能。近年來，研究學者將向量量化技術與影像藏密技術結合，多種以 VQ 壓縮技術或 SMVQ 壓縮技術爲基礎之影像藏密技術已經被提出來。Chang 與 Lin 學者於 2006 年提出一種以預測機制爲基礎之針對 VQ 與 SMVQ 壓縮影像之可還原的(reversible)藏密技術。同年，Chang，Tai 與 Lin 學者提出另外一種植基於 SMVQ 之可還原資料隱藏技術。Chang 與 Lin 學者在 2007 年基於分解叢聚(declustering)策略與利用影像的空間域特色提出一個可還原的以 SMVQ 影像壓縮方法爲基礎的藏密技術。Shie 與 Lin 學者在 2009 年提出一種植基於 VQ 索引值之搜尋順序編碼(search-order-coding, SOC)的藏密技術。Chen 與 Chang 學者於 2010 年發表一篇植基於 SMVQ 與利用適應性索引(adaptive index)之高容量藏密技術。同年，Lee，Chiou 與 Guo 學者提出另一種植基於 SMVQ 索引值直方圖修改之可還原的藏密技術。

此論文提出一種植基於邊緣匹配向量量化壓縮技術之高隱藏量且可還原的影像藏密方法。提出的方法是一種在數位影像壓縮域上實行之藏密法。藉由此藏密法，機密資訊可以間

接地被隱藏於數位影像的壓縮碼之中而不是直接地藏入於數位影像本身。此藏密法的主要設計構想爲利用向量量化編碼本(codebook)內的編碼字(codeword)與編碼字之間的特性，在藏密端(傳送端)將機密資料藏入於影像的壓縮碼以及在取密端(接收端)將機密資料從影像的壓縮碼中取出。由於邊緣匹配向量量化影像壓縮技術可在傳送端與接收端同步地建構狀態編碼本(state codebook)。此外，該狀態編碼本具有適應性地產生(adaptively generated)與已排序的(sorted)的特性。因此，此研究利用此特性，在藏密端與取密端同步地產生一個部份排序的(partially sorted)編碼本作爲所提出之藏密方法的主要參考依據。此外，本方法利用霍夫曼編碼進一步降低整體必須傳遞至接收端的資料量。整體的效能分析結果顯示提出的方法在傳送端可以提升機密資料之藏入量、在傳輸通道上(communication channel)可以維持影像壓縮碼之位元率以及在接收端可以完整地取出機密資料並且無失真地重建(losslessly restore)壓縮影像。

ICCVE2013 國際會議同一時間至少有五個會議室(Session room)同時進行。因此，在個人發表論文的會議室內，人數沒有想像中的多。在論文發表的過程中，來自新加坡的 Ali Oran 與加拿大的兩位學者主動表達對此研究題目的興趣。此外，Ali Oran 在此 Session 中臨時被指定擔任此 Session 的主席。會後，兩位學者與個人進一步討論此研究未來在 Connected Vehicles 上實現的可行性，個人覺得獲益良多。在參加其他 Session 的過程中，個人聽了不少與個人研究有關的論文報告，也與部分論文作者交換了意見。在溝通過程中，個人獲得不少在研究上的新觀念。在此國際會議中所接觸到的討論與報告經驗令個人覺得相當寶貴。

心得及建議事項：

本次參與之 ICCVE2013 國際會議主題爲 Connected Vehicles 相關之研究與應用趨勢。由於 Connected Vehicles 之研究與應用涵蓋了多種不同學門與不同專長領域之研究課題，是一種整合且應用各學門相關研究於車輛平台上的新領域。因此，在此次國際會議中能見識到許多不同研究領域之研究成果與未來的研究趨勢及應用。建議國內相關單位關注 Connected Vehicles 領域之發展趨勢。由主辦單位所邀請之專題講座、議程委員以及參與會議之研究學者得知，此國際會議廣受世界各國相關研究領域之學者所重視。也因此個人發現，在會議中被宣讀論文之研究題目差異性頗大，由此可知 Connected Vehicles 這個研究領域範圍之浩翰。個人在論文報告過程中，曾有學者根據個人所提出論文之方法討論其在不同環境下之應用。個人覺得這是一個很好的意見交流，個人將在未來的研究中參考他國學者的意見，這也是個人認爲參與此次國際會議收穫最大的部分。

A Reversible Image Steganographic Scheme Based on SMVQ and Huffman Coding

Ji-Han Jiang, Shih-Chieh Shie, WeiDer Chung, and Wei-Jyun Syu

Abstract — *A reversible image steganographic scheme implemented in the SMVQ compression domain of image is proposed. The goal of this scheme is to hide secret data into the compression codes of image by applying the SMVQ state codebook. In addition to reversibility and high-payload, the bit rate of the compressed cover image is another consideration in the proposed scheme since the secret data are delivered through the compression codes of cover image. To compact the volume of the overall data needed to be transmitted, the Huffman coding technique is applied. By the proposed scheme, the original VQ-compressed cover image can be restored losslessly at the receiver. Simulation results demonstrate the feasibility of the proposed scheme.*

Index Terms — Reversible image steganography, data hiding, side-match vector quantization, Huffman coding.

I. Introduction

The techniques of image steganography have been widely studied during the last decade [1]-[10]. Image steganography involves embedding data secretly into another cover image at the transmitter. Then, the cover image convoying the secret data is transmitted to the receiver through the communication channel. Finally the receiver extracts the secret data from the received cover image based on the designed extraction procedure. Image compression has been studied in the last decades. Among the various image compression techniques, vector quantization (VQ) technique [11] is an efficient one and is easy to implement. One feature of VQ is that, with relatively small block sizes, high compression ratios and good visual quality can be achieved. The ordinary VQ only exploits the statistical redundancy among neighboring pixels within a block. However, it totally ignores the correlation among neighboring blocks. Fortunately, side-match finite-state vector quantization (SMVQ) [12] overcomes this problem.

Recently, several VQ-based or SMVQ-based image steganographic schemes have been proposed in the literature [3]-[10]. Hu proposed a high-capacity scheme for hiding several secret images into one image based on VQ [3]. Chang *et al*. proposed an SMVQ-based data hiding scheme which focuses on the reversibility of the compressed cover images [4]. Later, Chang and Lin proposed another reversible scheme by declustering the codewords of codebook [5]. Shie and Lin proposed a VQ-based data hiding scheme [6]. This scheme was implemented on the compression codes of VQ indexes of cover image. The receiver can efficiently and simultaneously receive the compressed cover image and the secret data at low bit rate. In 2010, Chen and Chang proposed an SMVQ-based and high-capacity data hiding scheme [7]. This scheme uses a modified Euclidean distance measure criterion and an adaptive index assignment strategy to increase the probability of SMVQ in the image compression procedure and, therefore, more hiding capacity can be obtained. Shie *et al*. proposed a scheme to transmit a set of good-quality images via one image by embedding the VQ indexes and codebook into the cover image [8]. Lee *et al*. proposed a reversible scheme by transforming the VQ-compressed image into SMVQ-compressed one to achieve high hiding capacity and low bit rate [9]. In 2012, Shie and Jiang proposed another SMVQ-based scheme which focuses on the payload, reversibility, computational efficiency, and compression rate [10].

Ji-Han Jiang is with the Department of Computer Science and Information Engineering, National Formosa University, Taiwan, R.O.C. (e-mail: jhjiang@nfu.edu.tw).

Shih-Chieh Shie is with the Department of Computer Science and Information Engineering, National Formosa University, Taiwan, R.O.C. (e-mail: scshie@nfu.edu.tw).

WeiDer Chung is with the Mechanical and System Research Laboratory, Industrial Technology Research Institute, Taiwan, R.O.C. (e-mail: weider@itri.org.tw).

Wei-Jyun Syu is with the Department of Computer Science and Information Engineering, National Formosa University, Taiwan, R.O.C. (e-mail: 10063102@gm.nfu.edu.tw).

II. Proposed Reversible Steganographic Scheme

In the SMVQ compression domain, finding redundant space for hiding secret data is difficult. Besides, restoring the original VQ-compressed image is another challenge since the compression codes are altered by the hidden data.

A. Hiding Algorithm at the Transmitter

The input of transmitter includes a cover image $\boldsymbol{I}$, a main codebook $\boldsymbol{C}$, the secret data $\boldsymbol{S}$, and parameters, and the output of transmitter includes the modified compression codes of cover image, the Huffman table $\boldsymbol{HT}$ and Huffman codes $\boldsymbol{HC}$.

Step 1. Divide cover image into non-overlapping blocks. Encode the blocks in the first row and first column by VQ.

Step 2. Process the residual blocks according to the Zigzag scan order and let the currently processed block be $\boldsymbol{X}$.

Step 3. Generate SMVQ state codebook $\boldsymbol{SC}$ for $\boldsymbol{X}$. Note that the state codebook size equals the main codebook size. Find the most similar codeword to $\boldsymbol{X}$ in $\boldsymbol{SC}$. Let the index value of this codeword be iv.

Step 4. If ($iv = 0$), get ($\lfloor \log_2(a) \rfloor$-$\lfloor \log_2(iv+1) \rfloor$-1) secret bits from $\boldsymbol{S}$ and set the indicator value for $\boldsymbol{X}$ be $\lfloor \log_2(iv+1) \rfloor$; else if ($0 < iv < 2^{\lfloor \log_2(a) \rfloor - 1}$), get ($\lfloor \log_2(a) \rfloor$-$\lfloor \log_2(iv) \rfloor$-1) bits and

set the indicator value be $\lfloor \log_2(iv) \rfloor$; else get no secret bit and set the indicator value be $\lfloor \log_2(iv) \rfloor$. Let the secret bits be $\boldsymbol{D}$.

Step 5. Concatenate $\boldsymbol{D}$ with the binary value of iv to generate the modified compression code for $\boldsymbol{X}$. Put the indicator value into the indicator table. If there exists unprocessed block, goto *Step 2*.

Step 6. Encode the indicator table by Huffman coding and output the Huffman table $\boldsymbol{HT}$ and the Huffman codes $\boldsymbol{HC}$. Collect the modified compression codes of image blocks and output the modified compression codes of cover image $\boldsymbol{O}$.

B. Extracting and Restoring Algorithm at the Receiver

The input of receiver includes the main codebook, parameters, the modified compression codes, the Huffman table and Huffman codes, and the output of receiver includes the secret data and the original VQ-compressed cover image.

Step 1. Decode the blocks in the first row and first column by VQ. Based on the Huffman table $\boldsymbol{HT}$, generate the original indicator table by decoding the received Huffman codes $\boldsymbol{HC}$.

Step 2. Process the residual blocks according to the Zigzag scan order and let the currently processed block be $\boldsymbol{X}$. Get $\boldsymbol{K}$ ($\boldsymbol{K} = \lceil \log_2(a) \rceil$) bits from the received compression codes $\boldsymbol{O}$. Let the $\boldsymbol{K}$ bits be represented as $\boldsymbol{Y} = (y_{\boldsymbol{K}-1} y_{\boldsymbol{K}-2} \ldots y_1 y_0)_2$.

Step 3. Find the indicator value iv of $\boldsymbol{X}$ from the indicator table. Generate candidate index values $\boldsymbol{P}$ based on $\boldsymbol{Y}$, $\boldsymbol{P} = \{(\boldsymbol{p}_0)_{10}, (\boldsymbol{p}_1)_{10}, \ldots, (\boldsymbol{p}_{\boldsymbol{K}-1})_{10}\} = \{(y_0)_2, (y_1 y_0)_2, \ldots, (y_{\boldsymbol{K}-1} y_{\boldsymbol{K}-2} \ldots y_1 y_0)_2\}$.

Step 4. Generate SMVQ state codebook $\boldsymbol{SC}$ for $\boldsymbol{X}$. Restore the VQ-compressed block of $\boldsymbol{X}$ by decoding $(\boldsymbol{p}_{iv})_{10}$ with $\boldsymbol{SC}$.

Step 5. Extract the hidden bits $\boldsymbol{D}$ by getting ($\boldsymbol{K}$-iv-1) bits from $\boldsymbol{Y}$. That is $\boldsymbol{D} = (y_{\boldsymbol{K}-1} y_{\boldsymbol{K}-2} \ldots y_{iv+2} y_{iv+1})_2$. If there exists unprocessed block, goto *Step 2*.

Step 6. Collect all the hidden bits $\boldsymbol{D}$ to make the secret data $\boldsymbol{S}$. Rebuild the original VQ-compressed cover image $\boldsymbol{RI}$ by merging the restored VQ-compressed image blocks.

III. Experimental Results

In computer simulations, the proposed scheme has been conducted on a set of test images. For VQ and SMVQ compression, the images are divided into blocks with 4×4 pixels. The main codebooks with different sizes are generated from the test images by the LBG algorithm, respectively. The secret data are obtained by composing randomly generated bits.

For performance evaluation, the simulation result of our scheme is compared with that of Lee *et al*.s' scheme [9]. Fig. 1 illustrates the comparison in $\boldsymbol{ER}$ (the embedding rate, the proportion of the secret data to the overall transmitted data to the receiver) over $\boldsymbol{BR}$ (the bit rate of compressed cover image) under codebook sizes 128, 256, 512 and 1024. Note that both of our scheme and [9] are reversible schemes. The original VQ-compressed cover image (with the best quality for a given main codebook in VQ or SMVQ system) at the transmitter can be losslessly restored at the receiver. Simulation results show that the proposed scheme outperforms Lee *et al*.s' scheme [9].

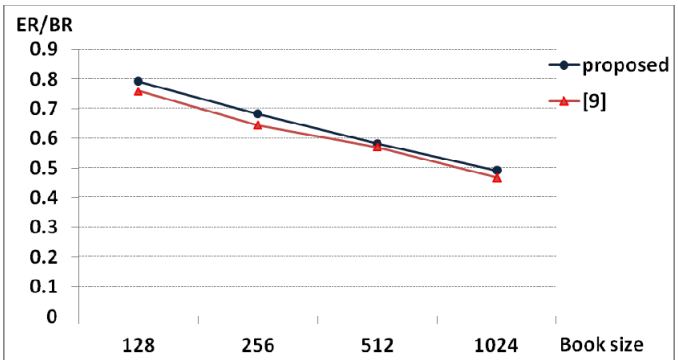

Fig. 1. Performance comparison in embedding rate (ER) over bit rate (BR) under different codebook sizes.

IV. Conclusions

A reversible image steganographic scheme capable of delivering secret data via the SMVQ compression codes of image is introduced. Based on the proposed scheme, not only the SMVQ-compressed cover image but also the original VQ-compressed one can be losslessly restored at the receiver. In addition, the visual quality for these reconstructed cover images is good. Therefore, we conclude that the proposed scheme is feasible for secret data transmission.

Acknowledgment

This work is supported by National Formosa University (Yunlin, Taiwan, R.O.C.) and National Science Council (Taiwan, R.O.C.) with project no. NSC 102-2221-E-150-064.

References

[1] T. S. Chen, C. C. Chang and M. S. Hwang, "A virtual image cryptosystem based upon vector quantization," *IEEE Trans. Image Proc.*, vol. 7, no. 10, pp. 1485-1488, 1998.

[2] S. D. Lin and S. C. Shie, "Secret image communication scheme based on vector quantization," *Electron. Lett.*, vol. 40, no. 14, pp. 859-861, 2004.

[3] Y. C. Hu, "High-capacity image hiding scheme based on vector quantization," *Pattern Recognition*, vol. 39, pp. 1715-1724, 2006.

[4] C. C. Chang, W. L. Tai, and C. C. Lin, "A reversible data hiding scheme based on side match vector quantization," *IEEE Trans. on Circuits and Systems for Video Tech.*, Vol. 16, No. 10, pp. 1301-1308, 2006.

[5] C. C. Chang and C. Y. Lin, "Reversible steganographic method using SMVQ approach based on declustering," *Infor. Sciences*, vol. 177, pp. 1796-1805, 2007.

[6] S. C. Shie and S. D. Lin, "Data hiding based on compressed VQ indices of images", *Computer Standards & Interfaces*, Vol. 31, No. 6, pp. 1143-1149, 2009.

[7] C. C. Chen and C. C. Chang, "High capacity SMVQ-based hiding scheme using adaptive index," *Signal Proc.*, vol. 90, pp. 2141-2149, 2010.

[8] S. C. Shie, J. H. Jiang, L. T. Chen and Z. H. Huang, "Secret image transmission scheme using secret codebook," *IEICE Trans. Infor. and Sys.*, vol. E93-D, pp. 399-402, 2010.

[9] J. D. Lee, Y. H. Chiou and J. M. Guo, "Reversible data hiding based on histogram modification of SMVQ indices," *IEEE Transactions on Information Forensics and Security,* vol. 5, pp. 638-648, 2010.

[10] S. C. Shie and J. H. Jiang, "Reversible and high-payload image steganographic scheme based on side-match vector quantization," *Signal Proc.*, vol. 92, no. 9, pp. 2332-2338, 2012.

[11] Y. Linde, A. Buzo and R. M. Gray, "An algorithm for vector quantizer design," *IEEE Trans. Commun.*, vol. 28, pp. 84-95, 1980.

[12] T. Kim, "Side match and overlap match vector quantizers for images," *IEEE Trans. Image Proc.*, vol. 1, pp. 170-185, 1992.