具有抗頻道雜訊特性加密動態影像之無線寬頻多碼式分碼多工傳送架構研究

Design of Wideband Multicode Spread-Signature CDMA Transport Architecture for Wireless Error-Resilient Secure Motion Image Communications

計畫編號：NSC-89-2213-E-009-159

執行期間：89 年 8 月 1 日至 90 年 7 月 31 日

計畫主持人：張柏榮 國立交通大學電信系教授

一、 中文摘要

本計畫乃是延續八十八年度國科會計畫:無線 JPEG-2000 靜態影像通訊研究內容。本期計畫研究標的則著重在 MPEG-4 動態影像無線寬頻分碼多工(Wideband CDMA)傳送加密機制的研發。然而寬頻分碼多工系統所產生多人干擾(multi-user interference)將會使得加密影像產生相當大的位元錯誤率 (BER)，由於一般加密程序均具有相當高度非線性特性，因此加密影像的位元錯誤率雖然不大，但仍會造成極差的解密影像 (decrypted image)品質。所以本計畫希望同時考慮抗頻道雜訊及干擾，降低錯誤更正碼所增加位元數與加密三種功能並且整合應用在寬頻分碼多工影像傳送。為了提高抗頻道雜訊及干擾能力與影像資料壓縮效能，本計畫將 MPEG-4 動態影像編碼中的視訊物體元件分離(video object plane, VOP Segementation)機制與移動補償式小波多重解析度編碼(motion-compensated wavelet multi-resolution coding)技術整合。同時該新的編碼機制極適於寬頻多碼式分碼多工通訊系統(Wideband multicode CDMA system)。接著我們再針對不同預估誤差次影像依其重要性進行不同程度之抗頻道雜訊與保密機制。本計畫研發一全新的二維混沌亂碼(2D Chaotic random codes)加密機制以便產生具有極高保密程度的加密影像。接著採用輸入信號為高斯機率分佈並且可以隨著 SNIR(Signal-to-Noise/Interference ratio)強度大小調整其參數之適應式最佳化頻道純量量化器(SNIR-based adaptive Gaussian Channel Optimized Scalar Quantizer COSQ)及最佳量化值編碼器(optimal codeword encoder)以期提高抗頻道雜訊及干擾的效能。不過適應式最佳化純量頻道量化器有一極大的缺失是其祇針對二位元對稱頻道所設計，卻無法直接應用在無多重路徑 Rayleigh 衰落頻道。因此本計畫採用 MIT Wornell 教授所提出的 Spread-Signature CDMA 技術整合至寬頻多碼式分碼多工通訊系統。Spread-Signature CDMA 可以將多重路徑 Rayleigh 衰落頻道轉化成可加性高斯白色雜訊頻道(AWGN)。如此此一全新的 CDMA 整合系統不但可以提高位元傳輸速率同時降低多重路徑 Rayleigh 衰落頻道對傳輸品質的傷害。

關鍵詞：二維混沌動態影像加密機制，第四代動態影像編碼，寬頻多碼式 Spread-Signature 分碼多工

英文摘要

This research project is aimed at developing a new cryptographic method for encrypting the 4th generation MPEG-4-like motion images which are the important component of wireless multimedia communications, and then provides the secure transmission of image information via wireless WCDMA networks. Meanwhile, since the encryption process is highly nonlinear, both the multipath fading and multi-user interference on WCDMA radio channels tend to cause significant transmission error, and the encrypted MPEG-4 motion images are very vulnerable to these errors. To tackle this difficulty, our new encoding mechanism has been developed based on a combination of both the MPEG-4 video object plane (VOP) segmentation and the motion-compensated wavelet multiresolution wavelet encoding. For the MPEG-4 motion-image encoding, each picture frame of an input video is segmented into a number of arbitrarily shape image regions (video object plane) and each of the regions may possibly cover particular image or video content of interest ,i.e., describing physical objects or content within scenes. Each VOP is further encoded using the motion-compensated wavelet multiresolution wavelet encoding. This would lead to one most-important low resolution

prediction error subimage and a number of least-important detail prediction error subimages. The MPEG-4 video is particularly suitable for the multicode CDMA system in order to achieve the high data transmission rate via the bandlimted wireless channel since each VOP generated from the MPEG-4 video may be assigned to a orthogonal variable spreading factor (OSVF) whereas the MPEG-4 itself is assigned to a specified scrambling code. In other words, it is creates more than one virtual channel for transmitting the VOPs of the MPEG-4 video parallelly. Furthermore, a two-layer highest security protection mechanism is applied to the most-important low resolution prediction error subimage. This two-layer security protetion mechanism includes (1) 2D Chaotic phase scrambler and (2) Chaotic image pixel scanning order encryption. To increase the error resilience for those encrypted prediction error subimages via the wireless CDMA channel, an adaptive channel optimized scalar quantizer(COSQ) and optimal codeword encoder is developed for the encrypted subimages according to the value of signal-to-noise/interference(SNIR). Unfortunately, there is a major drawback in the SNIR-based adaptive COSQ. It is only suitable for the binary symmetric channel(BSC). To overcome this difficulty, this research project applies Wornell's Spread-signature CDMA-based Rayleigh-to-Gaussian channel transformation technique to our multicode CDMA system. Thus, from the perspective of the coded symbol stream, the Rayleigh fading channel looks in effect like an ideal additive white Gaussian noise channel.

Keywords: 2D chaotic motion encryption, MPEG-4, wideband multicode spread-signature CDMA system

二、 計畫緣由及目的

為了因應電子化政府和電子商務時代來臨，行政院於民國八十八年十二月二十三日通過電子簽章法草案，明定電子文件和電子簽章具有法律效力。該法案將「電子文件」定位為：文字，聲音，圖片，影像，符號或其他以人之知覺無法直接認識之方式，所製成足以表示其用意之記錄，而供處理之用者。「電子簽章」指依附於電子文件上，用以辨識及確認電子文件簽署人身份及電子文件真偽者。並以簽署人之私密金鑰對其加密，形成所謂「數位電子簽章」。對於一般低頻道雜訊干擾之有線網路上加密及數位電子簽章的研究及商業成品相當多。但是對於無空間地形限制的無線網路加密系統研發則比較有限。由於無線通訊頻道是公開的，如此對私人信息傳送實在無任何私密及安全性可言。所以目前 GSM 採用基於線性回饋位移暫存器(Linear Feedback Shift Registers)加密方式(encryption)。並且採用用戶身份識別(SIM)卡來識別用戶身份。SIM 卡上燒錄有行動電話用戶私密金鑰及用戶身份碼，並且可以儲存暫時用戶身份碼。但是該加密方式保密程度卻不高，極易被人所破解。目前 ERICSSON，MOTOROLA，NOKIA 及 UNWIRED PLANET 等四家廠商，針對未來無線網路的加值服務所共同成立的一個業界聯盟稱之為無線應用協定論壇(WAP Forum)。WAP 協定將採用橢圓曲線密碼系統(ECC)。因為 ECC 密碼系統祇需 160 位元數，便與需 1024 位元數的 RSA 或 EIGamal 密碼系統，具有同等的安全等級，所以極適於有頻道容量限制的無線傳輸。另外展頻分碼多工系統保密系統涵括有行動使用者與基地台之間認證保密(cryptographic authentication protocols)及語音保密(voice privacy)[1]。認證加密方式採用基於美國官方使用的數據加密標準(Data Encryption Standard,DES)的改良架構。語音加密方式則採用私密長 PN 亂數展頻碼。該私密 PN 碼為私人獨有並不屬於 TIA/ELA/IS-95 展頻碼中。Simon,Omura,Scholtz 與 Levitt[2]指出 m-sequences 及 Gold sequence PN 展頻的保密程度均很有限，易為人破解。不久的將來第三代行動通訊的寬頻分碼多工 (Wideband CDMA)如 IMT-2000 及 FRLMTS 將提供無線寬頻多媒體傳送的服務。因此本計畫將著重研發具有抗干擾特性加密多媒體電子文件在寬頻分碼多工系統上傳送的機制。在八十八年上一期計畫我們從事在靜態影像如 JPEG -2000 加密機制的研究。本期計畫將延續上一期計畫研究成果著重在研發動態影像加密系統。目前加密靜態與動態影像的研究均侷限在無頻道雜訊及干擾環境(Channel noise-free and interference-free)上[3][4][5]。然而寬頻分碼多工系統所產生多人干擾(multi-user interference)將會使得加密影像產生相當大的位元錯誤率(BER)。由於一般加密程序均具有高度非線性，因此加密影像的位元錯誤率雖然不大但仍會造成極差的解密影像(decrypted images) 品質。當然利用錯誤更正碼來保護加密影像是一可行的辦法。可是錯誤更正碼所附帶多餘位元資料同時也造成無線傳輸上的負擔及占用過多有限無線頻道容量。尤其針對本身就具有極大位元資料量的影像而言，錯誤更正碼所產生多餘的位元資料就更多了。有關動態影像部份，最值得注意的是 MPEG-4 動態影像抗頻道雜訊的機制。R. Talluri [7] 則針對 MPEG-4 動態影像提出抗無線頻道雜訊的機制。包括有四種基本方法。(1)影像資料依其重要性作分割並且給予不同程度的保護(2)可回復式可變長度編碼(Reversible VLC), (3)視訊包封重新同步機制(Video packet resynchronization)，及(4)Header extension code。但也同樣未考慮到加密影像的應用。本計畫則希望將抗干擾與雜訊，保密及降低錯誤更正碼所增加位元數同時考慮並且整合為一。首先我們將 MPEG-4 動態影像編碼中的視訊物體元件分離(Video object plane, VOP Segmentation) 機制與移動補償式小波多重解析

度編碼(motion-compensated wavelet multi-resolution coding)技術[10]整合，如此不但可以提高抗頻道雜訊的能力及影像資料壓縮效能，同時該編碼機制極適於多碼式分碼多工通訊系統(multi-code CDMA Communications)[11]。每一個視訊物體元件將經由移動補償式小波多重解析度編碼機制分解成一重要性最高的低解析度預估誤差次影像(low-resolution prediction error subimage)與若干重要性較低的詳細預估誤差次影像(detail prediction error subimages)。接著我們再針對不同預估誤差次影像依其重要性進行不同程度之抗頻道雜訊與保密機制。例如重要性最高的低解析度預估誤差次影像採用兩層保密措施(i)二維混沌加密相位機制及(ii)混沌影像掃描取樣次序機制。由於原低解析度預估誤差次影像的機率分析會隨著影像內容不同而改變，因此我們採用 Popat與Zeger及 Chen與 Fischer 的設計理念將低解析度預估誤差次影像轉化成具有高斯機率分佈的信號。接著採用輸入信號為高斯機率分佈並且可以隨著 SNIR 強度大小調整其參數之適應式最佳化頻道純量量化器(SNIR-based adaptive Gaussian COSQ)及最佳量化值編碼器(optimal codeward encoder)以期提高抗頻道雜訊及干擾的效能。至於詳細預估誤差次影像是為固定的廣義高斯機率分佈 (shape parameter=0.7)同時不隨著影像內容不同而有很大的變化。因此我們祇需採用廣義高斯機率分佈(shape parameter=0.7)之適應式最佳化頻道純量量化器及最佳量化值編碼器即可。

三、 研究方法與成果

本研究計畫進行步驟依圖(一)所示可以分成以下七個階段：(1)將 MPEG-4 動態影像編碼中的視訊物體元件分離(Video object plane, VOP segmentation)機制與移動補償式小波多重解析度編碼 (motion-compensated wavelet multiresolution coding)技術整合成一具有影像資料重要程度排序特性(data priority partition)的新編碼機制將有助於抗頻道雜訊的能力，(2)由於 MPEG-4 動態影像編碼所採用的可逆式可變長度編碼(Reversible variable-length code, VLC)抗頻道雜訊能力仍十分有限，為了避免使用錯誤更正碼中附帶多餘位元資料所造成無線傳輸上的負擔，因此我們將針對每一視訊物體元件經由移動補償式小波多重解析度編碼機制所產生不同解析度及重要程度的預估誤差次影像(detail prediction error subimages)進行抗頻道干擾及雜訊與加密機制設計，(3)為了同時達到保密及抗頻道干擾與雜訊的要求，我們對於重要性最高的低解析度預估次影像(low-resolution prediction error subimage)擬採用二維混沌相位加密機制及混沌影像單元掃描取樣次序加密機制兩層保護以便達到較高的保密等級。然而對於比較不重要的詳細預估誤差次影像(detail prediction error subimages)則採用單層的混沌影像單元掃描取樣次序加密機制，(4)由於詳細預估誤差次影像的統計機率函數經由實驗證實為廣義高斯機率分佈(Generalized Gaussian distribution with shape parameter=0.7)同時不隨輸入影像不同而改變，因此我們將採用輸入信號為廣義高斯機率分佈(shape parameter=0.7)同時可以依照頻道信號雜訊及干擾強度比(Signal to noise and interference ratio, SNIR)大小不同調整其參數之適應式最佳化頻道純量量化器(Generalized Gaussian Channel Optimized Scalar quantization, COSQ)。接著再依據 SNIR 強度不同將量化值經由最佳化編碼器轉化成抗頻道雜訊的數位碼。但是低解析度預估次影像的機率密度函數則與前者截然不同會隨影像內容不同而改變，因此我們採用 Popat與 Zeger所提出利用全通濾波器即僅有相位變化之濾波器的方法將原低解析度預估次影像轉化為具有高斯機率分佈的信號。同時利用二維混沌相位加密機制改良原先 Chen 與 Fischer[16]所採用的基於 m-sequence PN 亂碼相位變化技術並且同時提高其保密效能。接著再採用輸入信號為高斯機率分佈並且可以隨著 SNIR 強度大小調整其參數之適應式最佳化頻道純量量化器(Gaussian COSQ)與最佳量化值編碼器(Optimal Codeword encoder)以便提高抗頻道雜訊及干擾的效能。(5) 適應式最佳化頻道純量量化器與最佳量化編碼器有一極大缺失是其祇針對二位元對稱頻道(Binary Symmetric Channel)所設計的，卻無法直接應用在無線多重路徑 Rayleigh 衰落頻道。因此我們採用 M.I.T. Worell 教授所提出的 Spread-Signature CDMA 碼多工系統[22]可以將多重路徑 Rayleigh 衰落頻道轉化成可加性高斯白色雜訊 (AWGN) 頻道 (Rayleigh-to-Gaussian channel transformation)。此舉相當類似 Popat 與 Zeger[15]的全通濾波器可將任一機率分佈之輸入信號轉化成具有高斯機率分佈的信號。Spread-Signature CDMA 係將多頻率信號處理及濾波器集組(Multirate signal processing and filter bank)理論融入分碼多工通訊系統設計架構，其中每一個多頻率濾波器脈衝響應均可視為一特定用戶展頻碼。經由濾波器多相位分離(filter polyphase decomposition)及最佳化處理可得到 maximally spread signature 展頻碼並且其數值為二位元(binary-valued)。為了進一步提高 MPEG-4 動態影像傳輸速率及品質，本計畫將多碼式分碼多工機制與 Spread-Signature CDMA 整合以期提供其擁有多於一個展頻碼。換言之，該整合系統可以使得每一 MPEG-4 在同一頻寬的通訊頻道上產生多於一個虛擬通道(Virtual Channel) 如此將可提高位元傳輸速率，並且可以同時避免多重路徑 Rayleigh 衰落干擾對傳輸品質所造成的傷害。為了進一步消除 MPEG-4 本身所產生的自身干擾(Self-Interference)，本計畫採用直交多變展頻因子通道化碼(orthogonal variable spreading factor, OVSF channelization code)代表 MPEG-4 中一特定視訊物體元件(VOP)。OVSF 直交碼的數目將隨著 MPEG-4 所分離出之視訊物體元件數目而改變。(6)利用具有即時處理能力之排線式遞迴類神經網路預估 SNIR 值以便提供適應式最佳

化純量量化器中參數調整機制。(7)利用 Xilinx 新開發具有數位信號處理功能的 XCV600-4HQ2400C FPGA 嵌入式晶片與 MDX-VIRTEX-FSH 平台製作二維混沌信號產生硬體平台。

混沌信號具有相當於亂碼雜訊的特性，同時不受到長度上的限制。然而傳統的 Gold codes 及 m-sequences 不但受到長度上的限制，同時數量也很有限。因此保密程度均不太高。混沌信號產生機制主要由起始點 (Starting points)及混沌地圖 (Chaotic map) 及其相關參數所控制。其中起始點，混沌地圖及相關參數的選擇範圍相當大不受到數量上的限制可以提供相當多人使用而無人數上的限制。在接收端，祇要行動使用者(mobile user)掌握傳送端(transmitter) 的混沌加密信號的起始點，混沌地圖及相關參數即可重建該具有無窮長度的混沌信號而無需浪費極大記憶體儲存該混沌信號。若他人欲破解該混沌信號，但是祇要起始點，混沌地圖及相關參數猜測預估有輕微錯誤時將導至預估混沌信號誤差以指數函數快速加大(exponentially increasing errors)。因此起始點，混沌地圖及相關參數可以當做加密系統中的鑰匙(key)。針對二維混沌相位加密機制如圖(二)所示，本計畫採用三種不同的混沌地圖產生二維混沌加密信號。首先使用者自行約定起始點與第一個混沌地圖及相關參數產生一序列起始點以便啟動 MPEG-4 所分離出之視訊物體元件中的低解析度預估誤差次影像二維相位加密機制所擁有的特定混沌地圖模組產生混沌二維相位信號。該地圖模組包含另外兩種不同混沌地圖。其中由第一個混沌地圖所產生混沌序列中的第一個點將當作第二個混沌地圖的起始點以便產生二維混沌信號的第一行。依此類推，序列中的第 k 個點將經由第二個混沌地圖產生第 k 行。當然序列中點的排序並無需相對於行的排序。排序的對應關係可以經由自行約定的混亂洗牌過程(Scrambling)進一步提高保密的能力。相同地，視訊物體元件中的低解析度預估誤差次影像二維混沌相位加密機制的起始點排序也無需固定。首先我們使用原先第一種混沌地圖產生數量相當大的候選起始點(Starting point candidate)，接著增加第四種混沌地圖以便任意產生視訊物體元件中之低解析度預估誤差次影像對應於候選起始點的相對位址。換言之，以上機制可以將原先起始點次序重新洗牌打亂。本計畫的第二種加密方法為混沌影像單元掃描取樣次序加密機制如圖(二)所示。該加密機制可以同時應用在低解析度與詳細預估誤差次影像。其中每一個預估誤差次影像均擁有相同的混沌地圖但起始點卻不同。至於起始點的產生與二維混沌相位加密機制類似。首先需要兩種不同混沌地圖以便提供每一視訊物體元件所需起始點同時其次序也已經由混亂洗牌程序打亂。接著再採用另外兩種不同混沌地圖經由以上相同程序所產生的視訊物體元件起始點以便產生其低解析度及詳細預估誤差次影像所需的起始點。該起始點將可經由每一特定預估誤差次影像所擁有的混沌地圖產生其掃描取樣次序。本計畫採用著名"Akiyo"視訊樣本進行測試。圖(四)顯示在 SNIR=10.09dB(BER=0.005) 傳送條件下接收端解密 Akiyo 視訊 PSNR 效能變化。

四、 結論與討論

本計畫完成工作項目及具體成果主要包括以下數點：1.完成整合 MPEG-4 動態影像編碼中的視訊物體元件分離機制及小波多重解析度技術的新編碼機制軟體設計。2.完成一全新二維混沌相位加密機制及混沌影像單元掃描取樣次序加密機制軟體設計。3.完成輸入信號為高斯機率分佈與廣義高斯機率分佈(shape parameter=0.7)同時可以依照頻道信號雜訊及干擾強度比大小不同調整其參數之適應式最佳頻道純量量化器及最佳化編碼器軟體設計。4.完成排線式遞迴類神經網路 SNIR 值預估子系統軟體設計。5.完成無線多碼式 Spread-Signature 分碼多工通訊系統軟體設計。本計畫所發展出具有抗頻道多人干擾及雜訊特性加密靜態影像之無線寬頻分碼多工傳送機制並未在其他文獻出現過類似研究成果。目前本計畫已經延伸至新一代動態影像 MPEG-7 抗頻道干擾及雜訊加密機制研究並且有初步的研究成果。

五、 參考文獻

[1] M. Y. Rhee, CDMA and Network Security, Prentice-Hall 1998.

[2] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, Spread Spectrum Communications, Handbook, New York:McGraw-Hill, 1994.

[3] N. Bourbakis and C. Alexopoulos, "Picture data encryption using SCAN patterns," *Patt. Recog.* **25**(6) (1992).

[4] C. J. Kuo, "Novel image encryption technique and its application in progressive transmission," ***J.*** *Electron. Imaging* **2**(4), 345-351(1993).

[5] B. M. Macq and J. –J. Quisquater, "Cryptology for digital TV broadcasting," *Proc. IEEE* **83**(6), 994-957 (1995).

[6] A. C. Popat and K. Zeger, "Robust quantization of memoryless sources using dispersive FIR filters," IEEE Trans. Commun. , Vol. 40 , pp. 1670-1674, Nov. 1992.

[7] Q. Chen and T. R. Fischer, Image coding using robust quantization for noisy digital transmission, Ph. D thesis, Washington State University, Pullman,

Jan. 1998.

[8]M. Gotz, K. Kelber, and W. Schwarz, “Discrete-time chaotic encryption system,” IEEE Trans. Circuits and Systems-I, vol44, no10, pp.963-970, Oct., 1997.

[9] R. Talluri, “Error-resilient video coding in the ISO MPEG-4 Standard,” IEEE Communications Magazine, Vol.36 , no.6, pp112-119, June 1998.

[10]Y. Q. Zhang and S. Zafar, “ Motion-compensated wavelet transform for color video compression,” IEEE Trans. Circuits and Systems, Vol.2 , no.3, pp285-296, Sept. 1992.

[11]P. R. Chang and C. F. Lin, “ Wireless ATM-based multicode CDMA transport architecture for MPEG-2 Video transmission, ” Proceedings of IEEE, Vol.87 , no.10, pp1807-1824, Oct. 1999.

[12]G. W. Wornell , “ Spread-Signature CDMA: efficient multiuser Communication in presence of fading,” IEEE Trans. Information Theory, Vol.41 , no.5, Sept. 1995.