行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※※※
※ **寬頻分碼多重進接無線通訊之加解密系統** ※
※ Cryptosystems for Wide-band CDMA wireless ※
※ communications ※
※※※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：□**個別型計畫** □**整合型計畫**

計畫編號：NSC－89－2219－E－009－032

執行期間：89 **年** 8 **月** 1 **日至** 90 **年** 7 **月** 31 **日**

計畫主持人：王聖智

共同主持人：林大衛

本成果報告包括以下應繳交之附件：

□**赴國外出差或研習心得報告一份**

□**赴大陸地區出差或研習心得報告一份**

□**出席國際學術會議心得報告及發表之論文各一份**

□**國際合作研究計畫國外研究報告書一份**

執行單位： 國立交通大學電子研究所

中 華 民 國 九 十 年 十 月 十七 日

行政院國家科學委員會專題研究計畫成果報告
寬頻分碼多重進接無線通訊之加解密系統

Cryptosystems for Wide-band CDMA wireless communications

計畫編號：NSC-89-2219-E-009-032

執行期限：89 **年** 8 **月** 1 **日至** 90 **年** 7 **月** 31 **日**

主持人：林大衛 (交通大學電子工程系教授)

共同主持人：王聖智 (交通大學電子工程系副教授)

計畫參與人員：陳信嘉、郭倫嘉、黃日良 (交通大學電子所研究生)

一、中文摘要

這次的進度報告包含兩個部分：DSP **系統模擬實現** RSA **演算法的結果報告，以及提出一個新的加解密演算法，試著結合公匙密碼系統和私匙密碼系統，以提供視訊資料傳輸上的保密要求。在這新的演算法中，我們提出了利用修改可變長度編碼表以進行視訊資料加解密之演算法，目的是希望能夠一方面加速加密解密的過程以達到即時處理傳輸的要求，一方面也能夠保持加密資料足夠的安全性。**

關鍵詞：不完全公匙密碼系統，有限域的乘法冪運算，可變長度編碼表

Abstract

This report includes two major parts: the implementation of RSA algorithm over DSP systems, and the development of a partial-encryption cryptosystem. In our partial-encryption cryptosystem, we introduce the en/decryption of video data via the modification of VLC table. With this cryptosystem, we may speed up the en/decryption process without sacrificing the security of the encrypted data.

Keywords：Partial Encryption Cryptosystem, Finite Field Multiplication, VLC table

二、進度報告

(1) DSP 系統模擬實現 RSA 架構的成果

在之前的報告中提到在 RSA **加解密演算法中乘法冪為主要的運算。在** DSP **系統中，最大的字元長度**(word length)**為 32 bits，而在** RSA **密碼系統中，以** 512 bits **長度的** key **加密可以有足夠的保密性，所以對於乘法冪的演算法，我們討論了兩種用來實現的架構，分別是** bit-wise **和** long-integer **的乘法架構。**

乘法冪

Bit-wise multiplication:

採用這個架構，對於 32 bits 的私鑰，對於 512 bits 長度的資料做加密，我們估計約需要 51,000,000 cycles 數，而 bit rate 約為 2.01 Kbits/sec 。

Long-integer multiplication:

同樣使用 32 bits 的私鑰，採用這個架構加密 512 bits 的資料，我們估計約需要 35,300,000 cycles，而 bit rate 約為 2.9 Kbits/sec 。

對於 RSA 公鑰密碼系統，無論採用那一個架構，也都無法符合即時處理傳輸的要求。減少公匙的長度，縮短處理資料的長度等方法雖然可以加速加解密的過程，但是其保密性也會大大的降低。如何在符合即時處理傳輸的條件下，增加資料的保密程度是我們的下一個課題。

(2)不完全公匙密碼系統的構想

公匙密碼系統的保密性高，而私匙密碼系統則有較高的加解密速度，我們往往依據使用的場合和所需求的保密程度，採用其中的一種系統當做加解密的方法。

在論文 [3] 中，針對影像內容的重要性，作者提出了對於內容重要但少量的部分，採用保密性較高的公匙密碼系統來加密，而對於其他部分則用加密速度快的私匙系統來加密，以增加資料處理的速度。依此想法，在影像編碼的過程中，我們可以針對不同重要程度的資料做不同的處理。

在 WCDMA 編碼的架構中，如何針對資料加密以增加其保密性而又不失其加密速度，是目前我們所研究討論的課題。

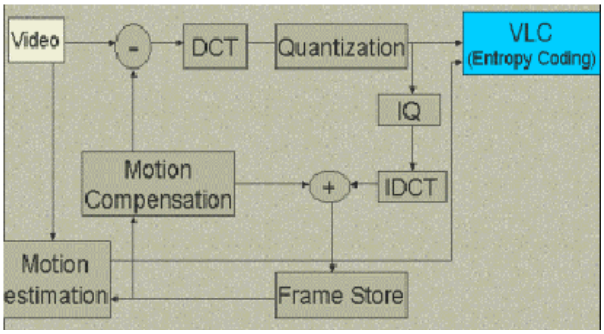

圖 1. 訊源編碼架構圖

一般視訊壓縮的標準都採取了以 DCT 為主的方法，以 8*8 區塊為基本單位來處理， 圖 1 是訊源編碼的架構圖。如果我們更進一步來看整個編碼過程，一個 8*8 的區塊經過 DCT 的處理, 之後經由量化及 zigzag scanning order 轉成一個低精準度但可高壓縮的一維陣列值，而其編碼採用了 Run length coding 的方式來表示 AC 係數之間的關係，再用 VLC (variable length coding)來傳送這些關係及係數值。

視訊資料中，大量的 AC 資訊與 VLC 表密切相關，當 VLC 表發生變動時，整個 AC 資訊的資料將隨之大幅地改變。變動 VLC 表並不會花大多時間，但卻會導致 AC 資訊的大幅改變。下面將討論如何運用這個特性來提供我們資料保密的特性。

根據一些想法與實驗, 我們將 VLC 表的變動對加密好處分成兩部分，第一個是 VLC 更動造成的影響，表示我們變動了 VLC 表後，第三者在不知道我們的表的情況下，即使拿到資料也會因為不知道 VLC 的對應關係而無法解回資料。第二個則是因為影像編碼中採用了預測的方式, 使得影像因 VLC 更動產生的保密效果可以繼續不斷擴散下去。

為了方便我們對 AC 可變長度編碼表的修正，我們將 VLC 表轉成圖 2 的 Huffman 樹架構，依照由上至下、由左而右的次序，我們將它們依序編號。

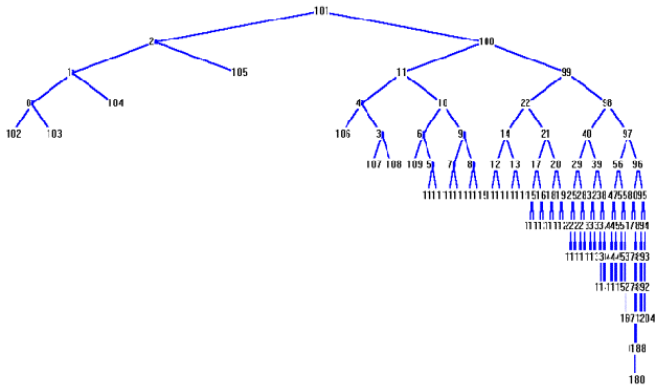

圖 2. H.263 內建 AC 可變長度編碼表對應之 Huffman 樹

下面是我們對 VLC 表進行調整，分成四種狀況來分別討論這四種狀況對影像解碼的影響，並分析變動 VLC 表時對於還原訊號所造成的影響。

(狀況 1).變動成相同長度的 codeword，而其中所代表的內容是 last 部分相同且 run 所表示的零值個數相差不大的情況：當這種變動產生時，別人在不知道表經過修改的情況下，就會解回如圖 3 的影像。可以發現這樣的錯誤影像就如受到雜訊的干擾影響一般，並不會造成太大的影像影響。

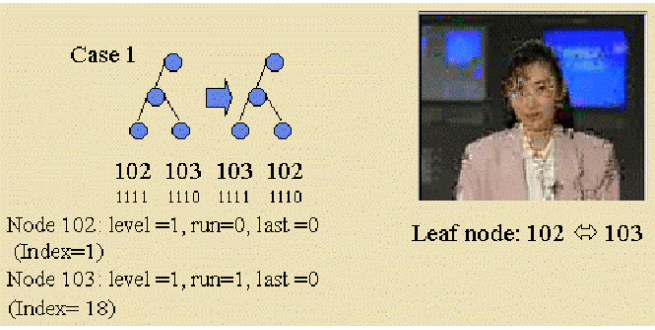

圖 3. 交換樹節點-狀況 1

(狀況 2). 變動成長度相同的 codeword，但其中所代表的內容是 last 相同但 run 的值相差很大時：這錯誤的影響可能如狀況 1 只是雜訊的干擾，但也可能如圖 4 的情況，因 run 的錯誤而造成後續資料的嚴重錯誤而全數捨去。這是一種我們可以充分利用的特性。

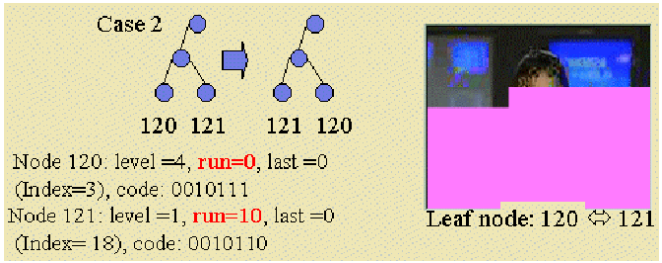

圖 4. 交換樹節點-狀況 2

(狀況 3) 變動為長度相同的 codeword，但表示內容中的 last 由 0 變 1 或是由 1 變 0：可以想見當這種狀況發生時，可能會造成這個區塊的資料流入下一個區塊內，因而造成區塊內的係數個數超過 64 個個數；產生一些沒有對應的 Huffman codeword；或是因為誤抓後續區塊的資料而產生解碼資料的嚴重錯誤。圖 5 右下側則是顯示一些這類情形發生的狀況，可以看到雖然只更換了兩個 codeword，就造成了影像資訊嚴重的失真。

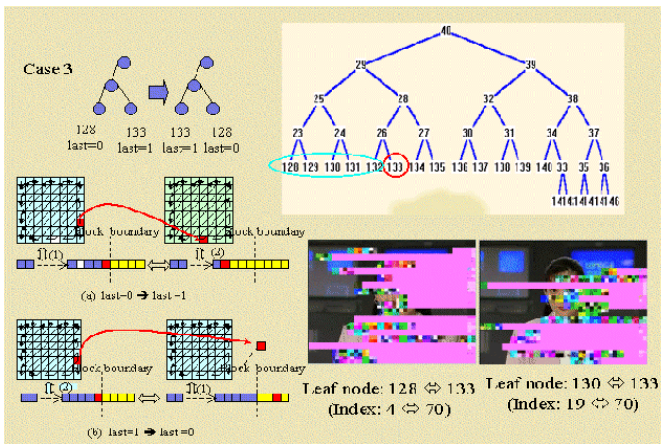

圖 5. 交換樹節點-狀況 3

(狀況 4). 這個狀況不在於改變 codeword 的內容，而是造成原先的一些 codeword 消失，並產生新的一種 codeword。這類的錯誤發生時會一直連續錯誤下去直到被解碼端判別成捨去資料為止，一旦發生錯誤解碼就無

法取得原始影像的內容，如圖 6 所示。

運用這後面三種狀況，我們可以利用 VLC 的特性使影像加密，別人如果不知道我們的表，就無法解回我們的影像。此外，除了改變 VLC 表的順序之外，我們也可以改變 CBPY (MB header codebook) 的檔頭 (header)，進而提高保密性。

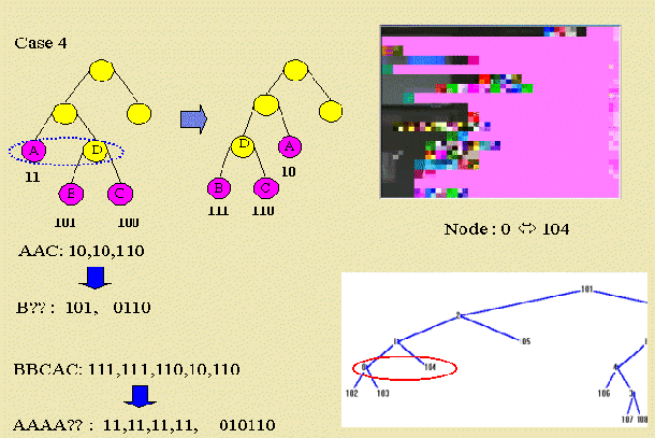

圖 6. 交換樹節點-狀況 4

圖 7 就是我們所提議的架構圖，透過 VLC 表的變動，我們的架構可以提供即時加密的傳送，而加密所需要的額外時間只有一開始更換 VLC 表所需要的時間(模擬結果約 0.15 秒)。

四、參考文獻

[1] I. Agi, L. Gong," An empirical study of secure MPEG video transmissions," Network and Distributed System Security, 1996., Proceedings of the Symposium on , 1996 Page(s): 137 –144

[2] G.A. Spanos, T.B. Maples," Security for real-time MPEG compressed video in distributed multimedia applications," Computers and Communications, 1996., Conference Proceedings of the 1996 IEEE Fifteenth Annual International Phoenix Conference on , 1996 Page(s): 72 –78

[3] H. Cheng, Li Xiaobo, "Partial encryption of compressed images and videos," Signal Processing, IEEE Transactions on , Volume: 48 Issue: 8 , Aug. 2000 Page(s): 2439 –2451

[4] ITU T Rec. H.263, Version 2," Video Coding for Low Bit Rates Communication," Jan. 1998

[5] G. Gote, B. Erol, M. Gallant, and F. Kossentini," H.263+ : Video Coding at Low Bit Rates", IEEE Transactions on circuits and systems for video technology, vol. 8. no. 7, Nov. 1998