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 (3/3)　　※
※　　Cryptosystems for Wide-band CDMA wireless　　※
※　　communications　(3/3)　　※
※※※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：□個別型計畫　　✓整合型計畫

計畫編號：NSC－90－2219－E－009－005

執行期間：90 年 8 月 1 日至 91 年 7 月 31 日

計畫主持人：王聖智

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 一 年 十 月 十六日

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 (3/3)

計畫編號：NSC-90-2219-E-009-005

執行期限：90 年 8 月 1 日至 91 年 7 月 31 日

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、 駱昭隆、戴郁文 (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:以 DSP 系統模擬實現 RSA 演算法的結果報告，以及提出一個針對視訊資料加解密的新方法。在這新方法中，我們利用影像編碼方法中的兩個特性來達到視訊資料的保密，一是利用可變長度編碼表的特性，一個是利用時間預估及空間預估動作的特性。基本上，我們的方式省略了傳統加密的運算，而只需要在視訊的傳送前，根據金鑰來設定相關的可變長度編碼表，之後便只是一般性的視訊編碼過程，因此不管傳輸率多高，都一樣可以達到即時加密的效果。

關鍵詞：不完全公匙密碼系統，可變長度編碼表

Abstract

This report includes two parts: the DSP implementation of RSA algorithm and the development of a new partial encryption system. In the proposed method, we use two major properties of current coding techniques: the inherent property of VLC (variable length coding) tables and the property of temproal prediction and spatial prediction. In our method, all we need to do is to modify the contents of VLC tables before the initialization of coding process. Then, the remaining process is just the usual video coding procedure. Even for a high transmission rate, our approach may still achieve real-time computations.

Keywords：Partial Encryption Cryptosystem, VLC table

二、進度報告

(1) DSP 系統模擬實現 RSA 架構的成果

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

$T = AB \pmod{n}$;

Both A and B are 512-bit;

n is 513-bit;

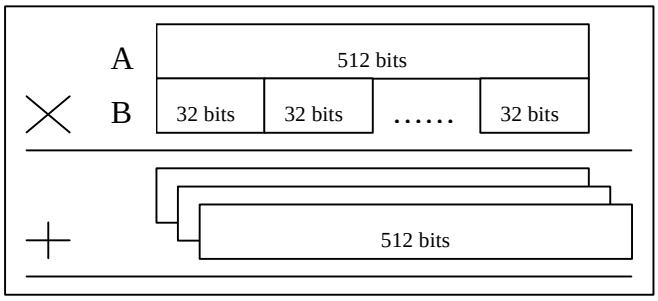
T is 512-bit;

Both A and B are put in 16 long-integer array;

T is assigned as 32 long-integer arrays;

n is put in 17 long-integer array;

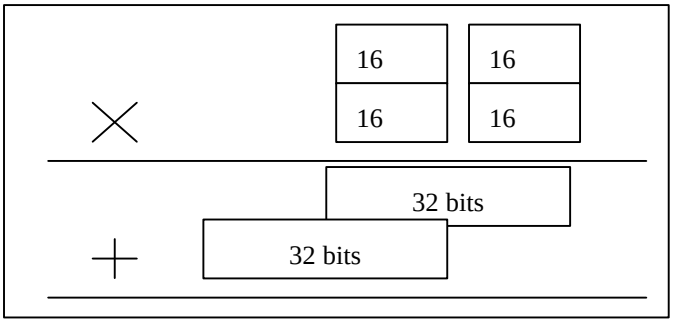
Bit-wise multiplication:



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:

512bits = 32 (bits/long-integer) *16 (long integers)



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 。

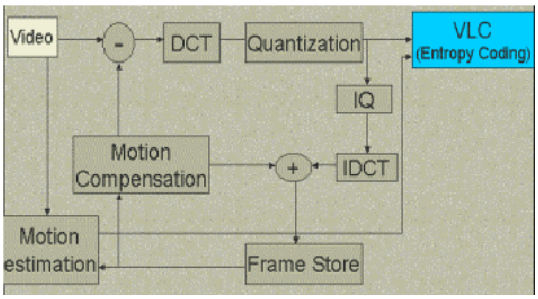
對於 RSA 公鑰密碼系統，無論採用那一個架構，也都無法符合即時處理傳輸的要求。減少公匙的長度，縮短處理資料的長度等方法雖然可以加速加解密的過程，但是其保密性也會大大的降低。

除此之外，為了符合 WCDMA 系統整合需求，我們亦針對 3GPP 中所採用的 F8 加密演算法在德州儀器的數位訊號處理晶片(TI TMSC6201)上實現，根據實測的結果，加密處理速度可達 5M bps(bits per second) 。

(2)不完全公匙密碼系統的構想

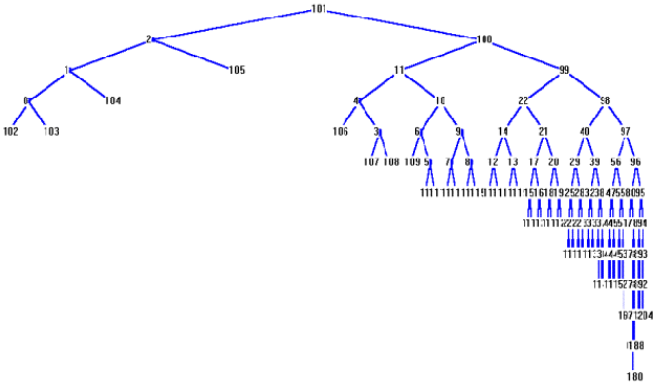
在本年度計畫中，我們針對無線傳輸過程中的視訊資料，討論如何針對資料特性進行加密而又不失其處理及傳輸速度。

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， 圖一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 的處理後轉成一維的陣列，再經過量化得到一個低精準度但可高壓縮的陣列值，而其編碼先採用 Run length coding 的方式來表示 AC 之間的關係，再採用 VLC(variable length coding)來傳送這些關係。我們可以看到大量的 AC 資訊都與 VLC 表密切相關，當 VLC 表發生變動時，整個 AC 資訊的資料將大幅的改變。然而，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。



圖一. 訊源編碼架構圖

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 錯誤，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，即使他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 error 產生的保密效果可以繼續延續下去。



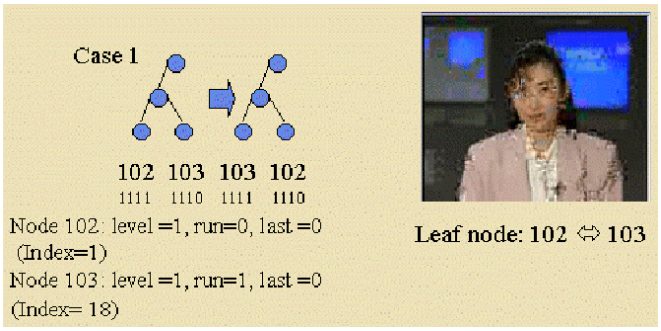
圖二. H.263 內建 AC 可變長度編碼表對應之 Huffman 樹

為了方便我們對 AC 可變長度編碼表的修正，我們將 VLC 表轉成圖二的 Huffman 樹架構，由上至下，由左而右我們將它們依序編號。

下面是我們對 VLC 表進行調整，分成四種狀況

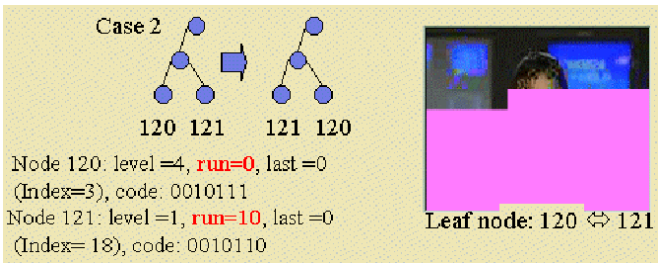
來分別討論這四種狀況對影像解碼的影響，分析變動 VLC 表對於還原訊號所造成的影響。

狀況 1. 相同長度的 codeword，所代表的內容為 RLC 參數 last 相同且 run 所表示的零值個數相差不大的情況：當錯誤產生，這兩個節點交換時。別人在不知道表經過修改的情況下，就會解回如圖三的影像。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。



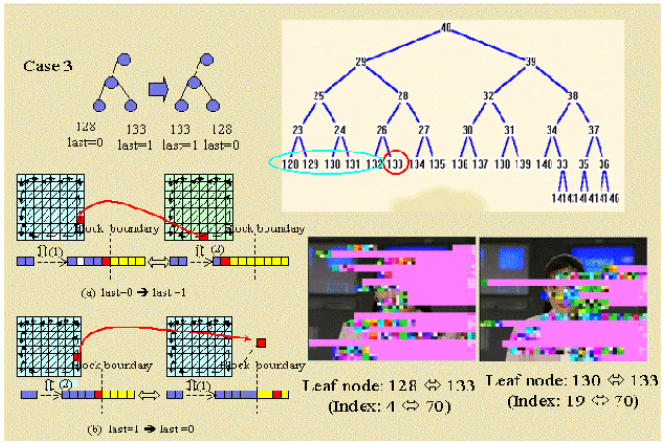
圖三. 交換樹節點-狀況 1

狀況 2. 若是搬動相同長度的 codeword 但 codeword 所代表的內容是 last 相同但 run 的值相差很大時：而這錯誤的影響可能如狀況 1 只是雜訊的干擾，但也可能如圖四，發生錯誤造成後續資料的捨去，被捨去後成了粉紅色的區域，而無半點原始影像的資訊。所以這是一種我們可以充分利用的特性。



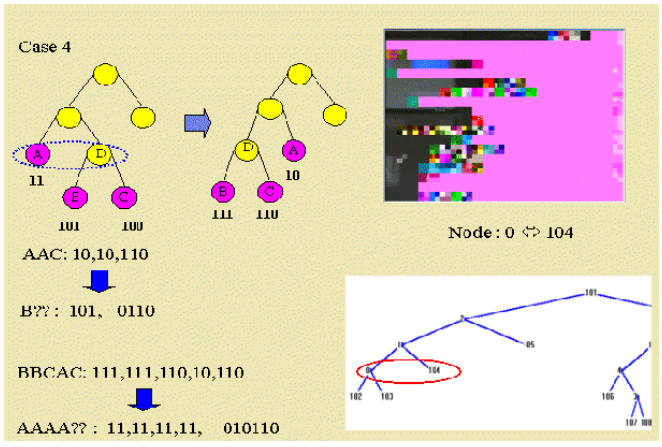
圖四. 交換樹節點-狀況 2

狀況 3. 當搬動長度相同的 codeword 但表示的內容是 last=0 與 last=1 兩種不同 last 的狀況時：可以想見當這種狀況發生時會造成這個區塊的資料將流入下一個區塊內而造成區塊內的係數個數超過 64 個個數、或一些沒有對應的 Huffman codeword 的錯誤產生。而反之則因為原先係數已滿的區塊將會去抓取下面區塊的資料而產生捨去。圖五右下側則是一些這種 case 發生的情況，可以看到只有兩個點的搬移，就造成影像資訊嚴重的失真。



圖五. 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，如圖六所示。



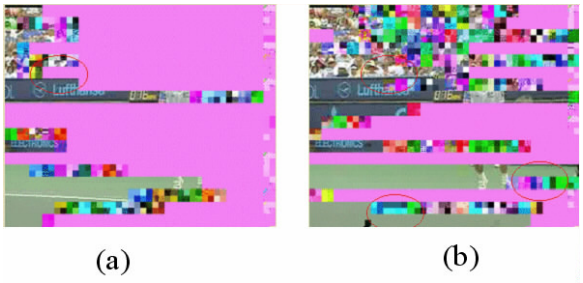
圖六. 交換樹節點-狀況 4

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。

若一些影像區塊只具有 DC 值(如均勻的背

景)，改變 AC 的 VLC 表將不具加密作用，為解決這個問題，我們觀察到在 CBPY (MB header codebook) 的檔頭 (header)中有包含 DC 的資訊，若交換 CBPY 檔頭的 VLC 表之節點，則可對 DC 影像區塊加密，進而提高保密性。

此外，在無線傳輸的過程中，雜訊的干擾對影像的品質會造成相當程度的影響。就本加密方式而言，除了一開始更改 VLC 表，之後的動作就如同一般壓縮過程，所以加密動作並不會使雜訊的干擾變嚴重，事實上在本方法中，加密資料受到雜訊的干擾的程度，與未經加密的資料受雜訊干擾的程度是一樣的。圖七顯示了區塊式加密與本方法在受到相同隨機錯誤干擾下所產生的結果，圖八則是對區塊式加密與在本方法在受到相同失同步錯誤干擾下作的比較。由這些例子可以看出到我們的加密方式在抗雜訊干擾上優於區塊加密的方式。至於與串流式加密比較上，我們的方法不需要像串流式加密一樣，必需加入同步訊號來防止失同步錯誤的產生，所以本加密方式不需增加額外的資料在防止雜訊干擾上。

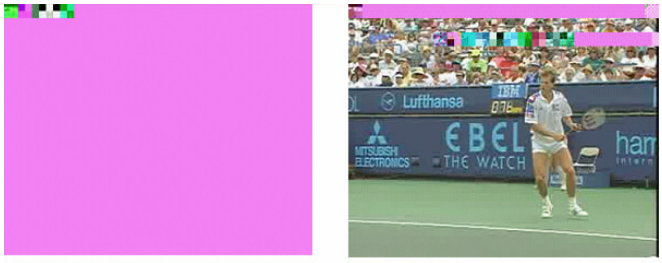


(a) (b)

圖七. 隨機錯誤的影響(a) 區塊式加密 (b) 改變 VLC 表

由於本方法是以改變 VLC 表的方式來加密，所以並不會破壞 MPEG 4 中原本具備的錯誤更正回復機制(Error Resilience)，如 RVLC 或 Resynchronization Marker 等，因此，更增加了本加密方法對於雜訊的免疫力。

在我們提議的架構中，主要是透過 VLC 表的變動來進行加密，這個架構在於任何視訊傳輸率要求下都能達到即時加密的傳送。而加密所需要的額外時間只有一開始建立 VLC 表所產生金鑰的時間(模擬結果約 0.15 秒)。綜合來說，本加密方式包含以下特點: (1)及時 (real time)加密。(2)運算複雜度低。(3)抗雜訊能力高。 (4)保密性佳。因此，本方法相當適合應用在影像訊號之無線傳輸上。



(a) (b)

圖八. 失同步錯誤的影響(a) 區塊式加密 (b) 改變 VLC 表

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