適用於中華衛星 1 號通道之保密傳真機之研製

The Study and Implementation of Secure Facsimile Machine for ROCSAT-1 Channel

吳錫堯　　張宗福　　賴溪松
Shee Yau Wu　　Chung Fu Chang　　Chi Sung Laih
南榮技術學院電子系　吳鳳技術學院電機系　成功大學電機系
henrywu@mail.njtc.edu.tw　ccf.ccu@msa.hinet.net laihcs@eembox.ee.ncku.edu.tw

摘要

本論文主要描述適用於中華衛星一號(ROCSAT-Ⅰ)通訊酬載實驗計畫之「保密傳真機」的系統功能，設計考量因素，以及用單晶片（Single-Chip Computer ）89C52 製作保密傳真機之原理，並敘述此成品利用中華衛星一號通道，以低速率傳送保密傳真資訊之實際經驗及數據。

關鍵字：保密傳真機，秘密通信，中華衛星 1 號（ROCSAT-1），改良式霍夫曼碼，IDEA 加密器。

一．前言

民國 80 年 10 月行政院院會通過「國家太空科技發展長程計畫」，同時成立「國家太空計畫室籌備處」，以作為我國十五年太空計畫的執行單位。太空計畫室成立以來，規劃了三個衛星計畫：中華衛星一號計畫（執行科學實驗任務），中華衛星二號計畫（進行遙測衛星任務規劃），及中華衛星三號計畫（進行氣象觀測任務規劃）。太空計畫室於台南縣歸仁鄉成大航太實驗場，提供固定通訊實驗地面站台（ECPGS），除可支援中華衛星一號，亦支援往後發展的其他實用性衛星。

中華衛星一號為一枚低軌道的科學實驗衛星[1]，其以距地球表面 600 公里、並與赤道傾斜 35 度的低軌道飛行。繞行地球一周約 97 分鐘，每日約六次通過。以 89 年 11 月 23 日至 12 月 8 日為例，16 天總共 106 次通過台灣上空，平均每日 6.6 次通過；其中，24 次（平均每日 1.5 次）仰角超過 50 度，30 次（平均每日 1.8 次）仰角小於 20 度。其餘 56 次通過的仰角，介於 20 度至 50 度之間，則宜於做實驗，亦為本保密傳真機實驗的主要依據。

中華衛星一號主要任務為科技研究，可進行海洋水色照相、電離層電漿電動效應及通訊實驗等三項科學及技術實驗。通訊實驗酬載為一可進行各種衛星通訊實驗的微波衛星通訊系統，分成空中部份及地面部份。「語音／數據／傳真及低速率視訊傳輸系統」是屬於地面部份之系統，利用中華衛星一號 ECP（Experimental Communication Payload）之固定通信台 RGT（Remote Ground Terminal）作語音、視訊及傳真等之即時且有效之通信。圖 1 為其系統架構，圖 2 是分系統方塊圖，圖中

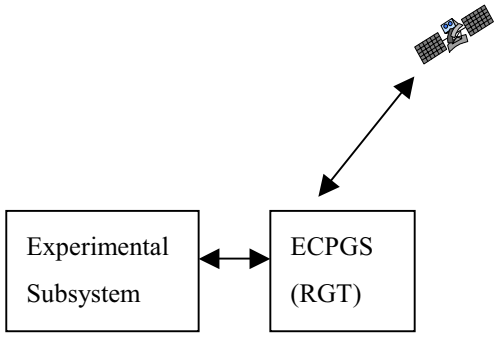


圖 1.華衛一號通訊酬載系統架構

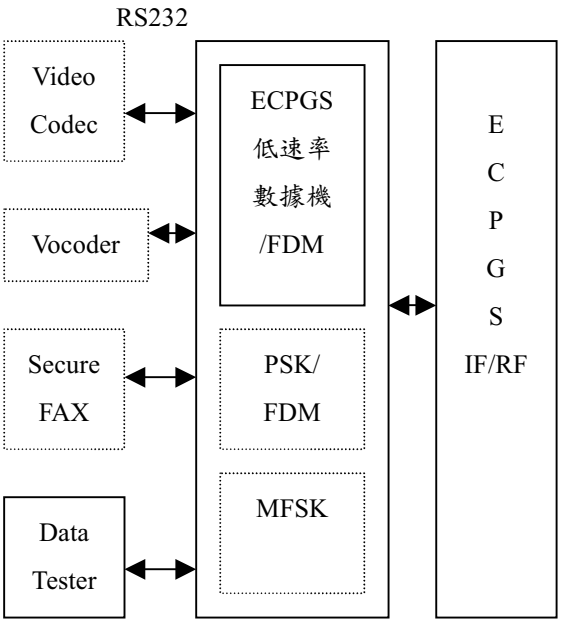


圖 2．華衛一號通訊酬載分系統方塊圖

虛線部分是由成功大學研製，Secure FAX（保密傳真機）之研製即本論文所探討之主題，其餘為向外採購。

二．研製背景與系統簡介

適用於中華衛星 1 號通訊實驗酬載之保密傳真機，以 RS-232 介面連接地面站台之低速率數據機（Low-Rate Modem）。當衛星通過地面站上空，衛星從地平線此端升起，至地平線彼端落下，衛星在天空停留時間大約 5 至 9 分鐘，停留時間之長短，依衛星所經路徑之仰角不同而異。衛星在天空逗留期間，在地面站台之發送傳真機讀取資料後，經 RS-232 傳送給數據機，數據機發射微波，經由衛星反射回地面站，經另一台數據機接收，由數據機介面 RS-232 端，將資料傳給另一台接收傳真機，接收傳真機接收到資料後，將資料印出。本系統所需用到的傳真機，必需具有以下幾個特性：（１）具有 RS-232 介面。傳送訊號必須透過 RS-232 傳送數位訊號，而非一般傳真機傳送的聲頻調變訊號；（２）單向傳輸。傳送訊號與接收訊號是在兩地進行，兩者之間只是單向傳輸，傳送系統與接收系統之間，完全沒有任何交握（Handshaking） 訊號可用，接收傳真機只能被動式作業；（３）可配合數據機作資料通訊。地面站低速率數據機之介面為 RS-232，採同步通訊，最高速率達 38.4 K 鮑（Baud），最低 9.6 K 鮑。系統最好也能作非同步通訊，因為系統若具非同步通訊，測試時可以跟個人電腦連線，利用個人電腦作輔助測試工具，或是直接藉市售數據機連線測試；（４）具加密／解密功能。衛星訊號任何人都可接收，若不經加密處理，毫無安全性可言；（５）可作資料壓縮／解壓縮。這是任何傳真機必有的功能，可節省資料傳輸時間。圖 3 是適用於中華衛星 1 號通訊實驗酬載之保密傳真機系統示意圖。

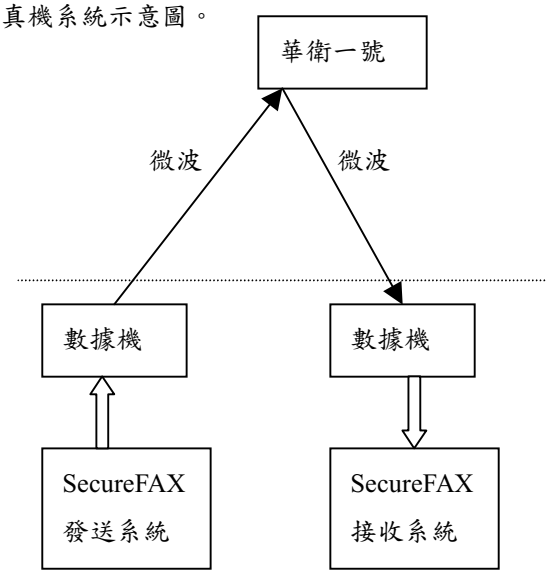


圖 3．適用於華衛一號通訊酬載之保密傳真機系統示意圖

傳統的傳真機，包含三個主要組件：CIS（密著式影像感測器，Contact Image Sensor）影像掃描器、印表頭 TPH（熱感測列印頭，Thermal Printer Head）、以及傳真控制電路。市售傳真機，大多是使用 Rockhill 晶片組 R96xx，當傳真控制電路的核心元件，晶片組包含兩顆 IC，一顆充當數據機，另一顆是資料唧筒（Data Pump）。我們以聲寶 SAMPO FT-12A 型傳真機來瞭解傳真機的工作原理，

圖 4 為 FT-12 型傳真機之方塊圖。在本傳真機中，R96FE（中央處理器）之控制程式係由 EPROM 27512 儲存。

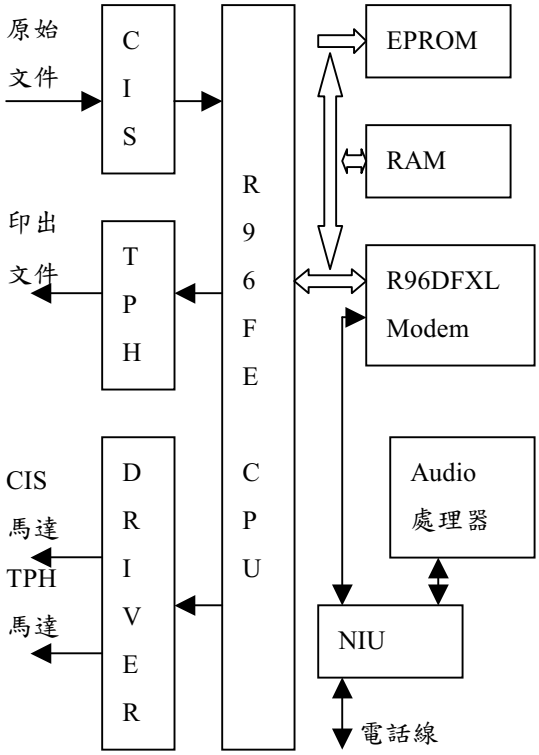
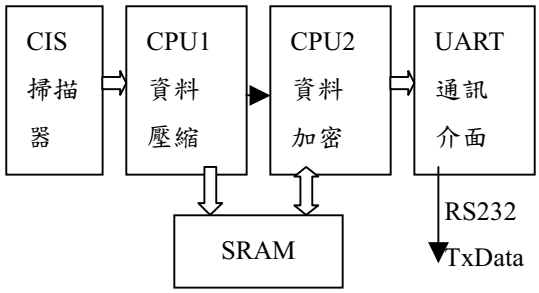


圖 4．FT-12 型傳真機之方塊圖

發送傳真時，文件經 CIS 掃描將影像轉成電子信號，經 R96FE 壓縮編碼後，存入 RAM 28257，R96FE 再透過 R96DFXL MODEM，經介面 NCU 由電話線傳送出去。接收時，文件（電子信號）經 NCU 介面由 R96DFXL MODEM 進入 RAM 儲存，再經 R96FE 解壓縮碼後，由 TPH 印出。影像資料以改良式霍夫曼碼（MHC，Modified Huffman Code）[6]壓縮（依據 CCITT T.4 建議標準壓縮編碼[7-13]）。

市面上現有之傳真機以音頻調變傳輸，係依據電話網路而設計，並不適於中華衛星一號之數位鍊路。除了必須將音頻調變部分取消，還需加入密碼加解密，符合上述特性之傳真機，實不容易用 R96xx 晶片組製成；由於國內廠商並沒有修改 R96FE FAX Engine 之技術，本製作小組因此決定自行研製保密傳真機。

為達成中華衛星 1 號保密傳真機所需之規範，本文描述用單晶片 89C52 自製一低成本傳真控制電路，所有的零件都可以在零件市場購得，再配合國產品 CIS 掃描器，以及日製 TPH 熱感應印表頭，即可完成一台自製傳真機。由於，系統是單向傳輸，因此將傳真機分成 FAX 發送子系統及 FAX 接收子系統兩部分，分別連接兩台低速率數據機，一組發送資料，另一組接收資料，其方塊圖如圖 5 及圖 6。由於單晶片的運算功能有限，系統設計時，將系統幾個主要功能，壓縮、加密、解密，以及解壓縮，設計由 4 個 CPU 分別擔任，既可避免 CPU 運算負荷太重，程式也較易模組化。



5．保密傳真發送子系統方塊圖

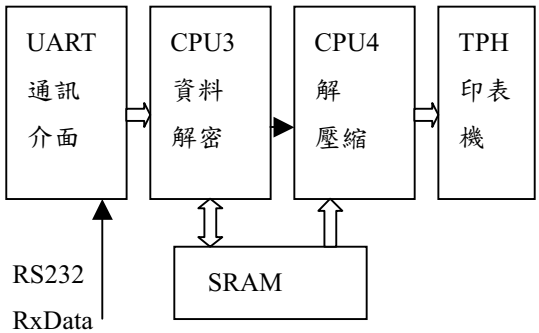


圖 6．保密傳真接收子系統方塊圖

三．CIS 掃描與資料壓縮

CIS 是線型掃描元件，一般傳真機以傳送 A4 尺寸之文件為主，所用之 CIS 掃描器每行掃描 1728 點，一張 A4 之文件大約需 2300 行掃描。這種掃描精密度大約是以普通書寫用之油性原子筆，在紙上輕輕畫一直線，此線寬經 CIS 掃描，大約可得到 3 點的線寬。自 CIS 掃描取得的資料，如果不經壓縮處理，一張

A4 文件之資料量為 1728 乘 2300 位元，將是一筆龐大的資訊。

資料壓縮方法有很多種，大約可分為：無失真（Lossless）壓縮法，與有失真（Lossy）壓縮法。無失真壓縮法要求資料經壓縮／解壓縮後，資料可以完全還原無誤; 這種壓縮法的壓縮率比較低，一般數據／資料大多採用這種壓縮法。常見的無失真壓縮法，有霍夫曼壓縮法、LZW 壓縮法等 [5]。有失真壓縮法，資料經壓縮／解壓縮後，資料即無法完全還原為原始資料，但仍可為人類感官所接受；有失真壓縮法的壓縮率比較高，常見於聲音及影像壓縮; 由於，人類的聽覺及視覺器官，都有其頻寬限制，適當的有失真壓縮，並不影響人們的視聽效果。常見的有失真壓縮法，有 JPEG 及 MPEG 等壓縮法 [5]。傳真機傳送文件，雖然是屬於影像傳輸，卻採無失真壓縮法，可能因素是：（１）制定傳真機規格時，有失真壓縮法技術尚不成熟；（２） 成本考量。

一般傳真機，採用改良式霍夫曼碼壓縮法，並以'行'（Line）為單位來壓縮資料及傳送資料，亦以'行'為單位來接收／解壓縮／印出資料。原始資料一行為 1728 點，以一點對應一個位元（Bit），以 8 個位元為一個位元組（Byte），一'行'未經壓縮的原始資料為 216 位元組，經霍夫曼碼壓縮後（以附錄資料為範本），每行資料位元組數之分佈情況為：

（１）介於 1 至 15 之間：約 1%
（２）介於 16 至 31 之間：約 35%
（３）介於 32 至 47 之間：約 19%
（４）介於 48 至 63 之間：約 27%
（５）介於 64 至 79 之間：約 12%
（６）介於 80 至 95 之間：約 6%

其中，整行全白壓縮後，剩 4 位元組，整行全黑壓縮後，剩 8 位元組。整頁的平均壓縮率約為 21%（大約壓縮 5 倍）。傳真機若有良好的壓縮比，可大量節省資料傳輸時間。

圖 7 流程圖說明了資料壓縮程式的工作原理。資料壓縮程式，內建一 MHC 碼表格，程式偵測到點資料變色（由黑變白，或由白變黑），即計算累計的位元數，然後呼叫壓縮副程式（查 MHC 碼表格，求得壓縮轉換碼，並儲存之），若累計的位元組總數已達 216 值，即停止程式，若否，則繼續讀取下一個位元組。

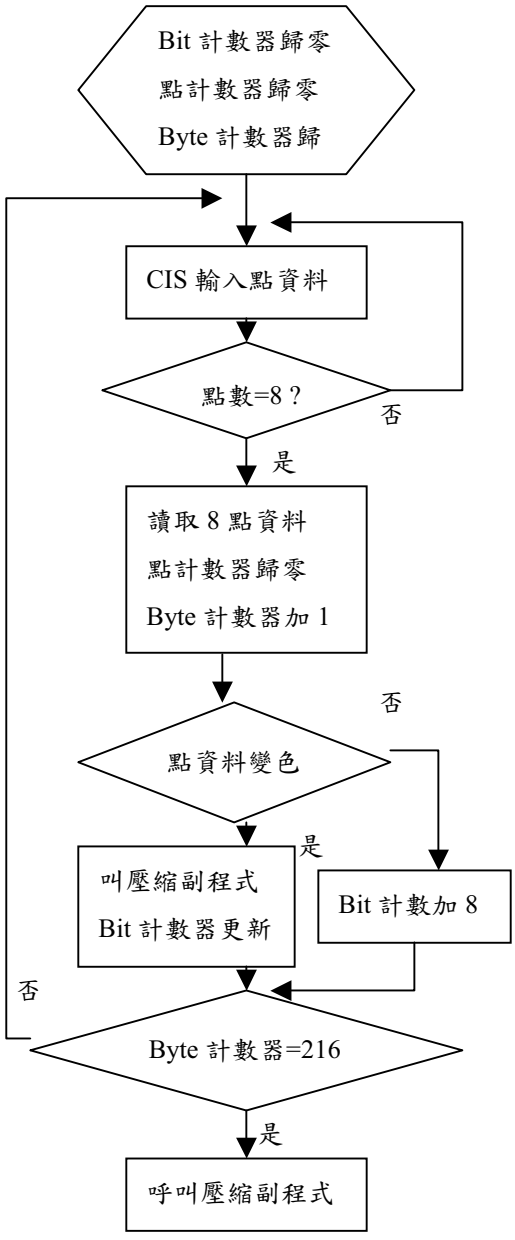


圖 7 ・資料壓縮流程圖

資料解壓縮程式的工作原理如圖 8 流程圖所示。資料解壓縮程式，是將壓縮碼還原成原始資料，其原理是：利用二元樹（Bit-Tree）

分裂法，依序將輸入資料分割，匹配成合適的 MHC 壓縮碼，此 MHC 壓縮碼經查表後，還原成原始資料。

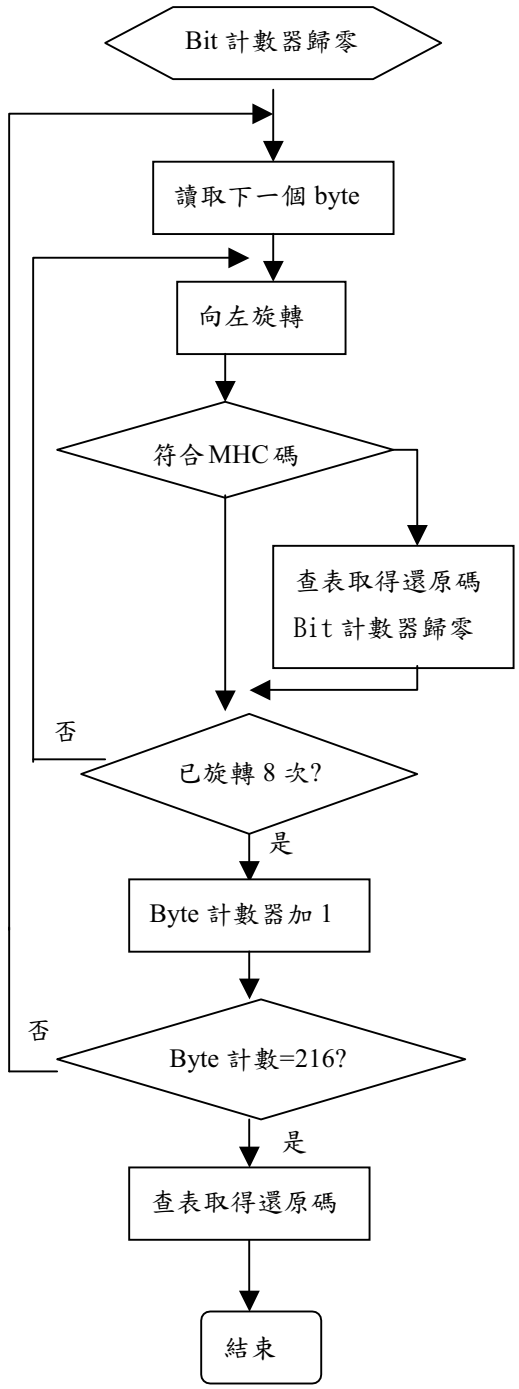


圖 8 ・資料解壓縮流程圖

四・資料壓縮與通訊協定

改良式霍夫曼碼是一種不定長度編碼（Run-Length Coding）方式，自 CIS 掃描得到的一行資料為 216 位元組，經 MFC 碼壓縮後，一行的資料長度為不定。如前所述，我們的傳真系統，完全沒有交握訊號可用，這種不定長度的行資料，若無適當定義的通訊協定輔助，將無法順利地將資料經由通訊媒體傳輸。因此，我們定義其通訊協定如下：

（１）以一行資料為一個資料包（a data package）。

（２）一次傳送一個資料包，每傳送一個資料包，有若干長度的休息時間。

（３）資料包的格式定義如下：

（55H）（AAH）（長度值）（…行資料…）（檢查和）。

其中，（55H）（AAH）為啟始辨識值。長度值為介於 0 至 216 之值。檢查和（Checksum）為 55 加 AA 加長度值，再加上所有的資料值，並附加於整行資料之後。

根據上述的通訊協定，我們設計一個狀態轉移表（State Transition Table, 如表一[6]），作為通訊流程的控制，依此狀態轉移表，可以很容易地完成通訊程式。此通訊程式經測試，結果相當理想，在無雜訊干擾下，錯誤率是零。

表一. 狀態轉移表（新旗幟值與原旗幟值／新接收字元之關係）

接收字 旗幟值	55	AA	長度	資料	檢查和
FF	00	00	FF	FF	FF
01	00	01	FF	FF	FF
02	02	02	02	02	02
03	03	03	03	03	03

（註）：

新旗幟值 FF：接收終止

新旗幟值 00：接收第一字元 55;

新旗幟值 01：接收第二字元 AA

新旗幟值 02：接收第三字元：長度值

新旗幟值 03：接收資料

狀態轉移表是以封包為單位，啟始位元 55 被接收到時，設定一新旗標值 00，若不是字元 55 被接收到，則終止接收（新旗幟值

FF)；新旗幟值為 00 時，下一接收到的字元必為 AA，若是 AA 被接收到，則更新旗幟值為 01，否則接收終止（新旗幟值 FF)；新旗幟值為 01 時，下一被接收字元是長度值，此值可能是 00 至 FF 之間的任何值，設新旗幟值為 02；新旗幟值為 02 時，下一被接收字元是資料，此值可能是 00 至 FF 之間的任何值，設新旗幟值設為 03；新旗幟值為 03 表示正在接收資料或檢查碼（和)。當接收字元數，滿足"長度值"，新旗幟值設為 00，以便進行下一封包之接收。

五．資料加密／解密

加解密是採用歐洲廣泛使用的 IDEA（International Data Encryption Algorithm）[4]。此演算法是由瑞士學者 Lai 及 Massey 在 1990 年所提的 PES（Proposed Encryption Standard）所改良而成的對稱式加密器（Symmetric Cryptosystem）[4]。所謂的對稱式加密器是指發送方與接收方均擁有一把相同的的秘密金鑰，這種加密法加密與解密使用同一運算法則，加密端與解密端所負擔的運算時間大致相同，常見的對稱式加密法有 DES、IDEA 及 Skipjack 等。所謂非對稱式加密法，是指發送方與接收方各自擁有一把不同的秘密金鑰，加密與解密使用不同的運算法則，加密端與解密端所負擔的運算時間，各自不同，常見的非對稱式加密法，有 RSA 及 Rabin 等。

我們選擇 IDEA 做為本系統之加密器而不採用 DES 的原因有下列幾點：

(1)金鑰長度：IDEA 之金鑰長度為 128 位元而 DES 只有 56 位元，由其金鑰長度觀點而言，IDEA 比 DES 更為安全。事實上，自 IDEA 由 1992 年發表以來，並沒有任何明顯的證據顯示 IDEA 存有其他致命的安全上弱點。

(2)設計原理：IDEA 是由學術界人士所設計，其設計原理完全公開，而 DES 是由美國國安局所設計。雖然 DES 之演算法亦完全公開，但其一些重要的設計原理，如 S-盒子，並未公開。因此，許多人士懷疑 DES 可能存有某些暗門(但無法證實)。由此觀點言，IDEA 之安全性應更能讓人信服。

(3)實現的容易度：IDEA 是由三個基本運算所組成，即模 2^{16} 之加法，XOR 及模 $2^{16}+1$ 之乘法，非常適合於 DSP 或單晶片來實現。事實上，我們以單晶片實現 DES 及 IDEA，在速度上 IDEA 亦比 DES 更為快速。

本保密傳真機實現初期（85 年 2 月），IDEA 仍是很新的加密器，如今下一代加密器 AES（Advanced Encryption Standard）[3]將於今（2001）年底前制訂為標準，未來若以此加密器取代 IDEA 模組，則得到安全性更高的保密傳真機。

IDEA 是一種塊狀密碼器（Block Cipher），利用 128 位元的密鑰對 64 位元的明文塊（Message Block）加密，經過連續加密運算，產生 64 位元的密文塊。塊狀密碼器是資訊安全中，一個非常重要的密碼元件，它的特點是加解密的速度非常快，它可達成資訊的隱私性，完整性與鑑別性。其工作原理可參考[4]。特別強調的是 IDEA 之加密與解密過程，都只用到互斥 XOR 運算，模加法及模乘法運算，這兩種運算，用單晶片 89C52 來運算，雖然有些耗時，但是，由於資料量不大（已經壓縮過)，而且系統裡尚有其他更慢速的元件，例如 TPH 印表機，相對地，加密與解密過程所耗時間，對整個系統的執行效能負擔很小，並不致影響本系統傳輸時間。

六．資料加密與通訊協定之修正

要將資料加密處理，需考慮：(1) 每行的長度值最好經加密處理，而啟始辨識值不需加密；(2) Block 加密法，需自動將不足一個 Block 的資料補齊，即不足 8-Bytes 的尾數，需自動補滿 8 個 Bytes，所以長度值會變動，這種變

動，會影響原先編寫好的通訊程式及解壓縮程式，為了程式的最小異動，我們將通訊協定修正如下：

（55）（AA）（長度 2）（5A）（A5）（長度 1）（…資料… ）（檢查和 1）（…）（檢查和 2）

其中（5A）（A5）是第二個啟始辨識值。（5A）至（檢查和 2）之前的資料，是要經加密處理的，其長度是 8 的倍數。（長度 1）是原來未加密前的長度值，而（長度 2）是加密後的長度值，所以（長度 2）必為 8 的整數倍之值。（檢查和 1）是未加密前的檢查和，而（檢查和 2）是資料加密後的檢查和。經過如此通訊協定的安排，壓縮後的（長度 1）（資料）與（檢查和 1），都籠罩在密碼保護之下，而（長度 2）及（檢查和 2）是以明文傳訊，使通訊軟體能依狀態轉移表，迅速而準確地處理接收進來的資料。

七．系統程式流程

傳真傳送子系統與接收子系統，每個子系統各有兩顆 CPU，CPU 與 CPU 之間的聯繫，是採鬆散耦合（Loose Coupling）。CPU1 與 CPU2 之間的耦合關係如圖 9 所述，CPU3 與 CPU4 之間的耦合關係如圖 10 所述。這兩個子系統的兩個 CPU 之間的切換時間，不僅關係全系統的穩定，也決定全系統的效能，將於下一節一併討論。

八．系統傳送時間預估與實測

依據圖 3 系統示意圖，系統分三階段進行：（1）於 RS-232 端利用 Null-modem[11]連線，作傳送／接收測試；（2）經由通訊酬載實驗的另一成員，成大蘇賜麟教授研發小組製作的“RF Modem”連線測試，此 RF Modem 功能相當於圖 2 裡的 Low-Rate Modem，於 RF 端迴接（Loop-Back）測試；（3）經由太空計畫室提供的 Low-Rate Modem，於 RF 端迴接測試，之後再經由衛星連線測試。

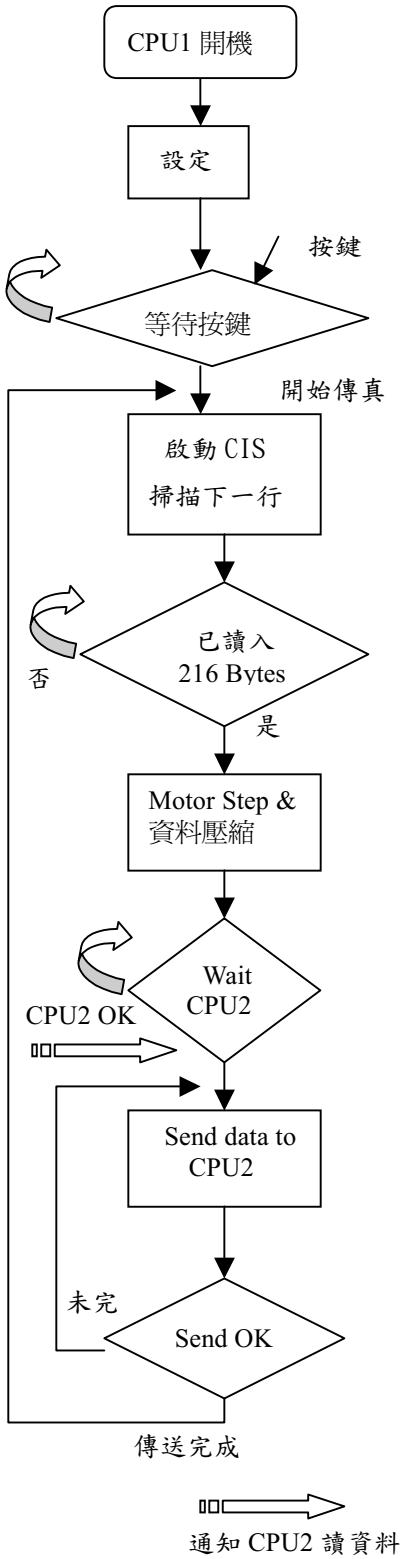


圖 9．CPU1 與 CPU2 之間的耦合

(A) CPU1 系統流程

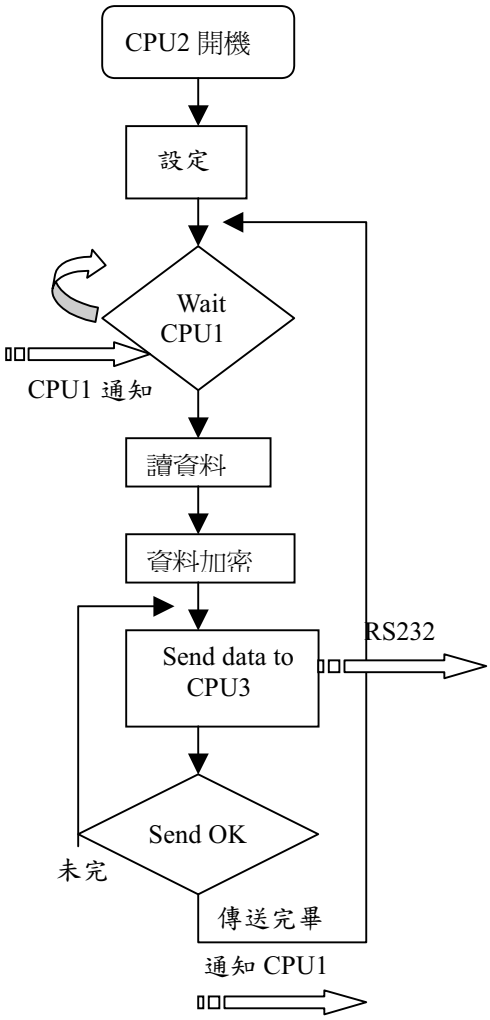


圖 9・(B) CPU2 系統流程

一張 A4 尺寸的文件（以附頁資料為範本），經整個系統以原始資料傳送／接收而不採取任何型式之壓縮，以 9.6 K 鮑，非同步通訊方式傳送時，約需 11 分鐘；以 19.2 K 鮑，非同步通訊，則約需 6 分鐘。同一文件，資料經壓縮，同步通訊傳送，在不同時脈速率之下，其傳送時間（利用 Null-modem 及外接同步時脈產生器）如表二所示。測試所用之製具（Test Fixture），包含（１）Null Modem 配線；（２）同步時脈產生器。由於 RS-232 於同步模式時，需由外界提供同步時脈，此時脈由振盪電路提供即可，但需具 RS-232 位準。我們觀察到表二的數據裡，傳送時間並不與傳送速率呈比例關係。這種因素我們推測，可能是

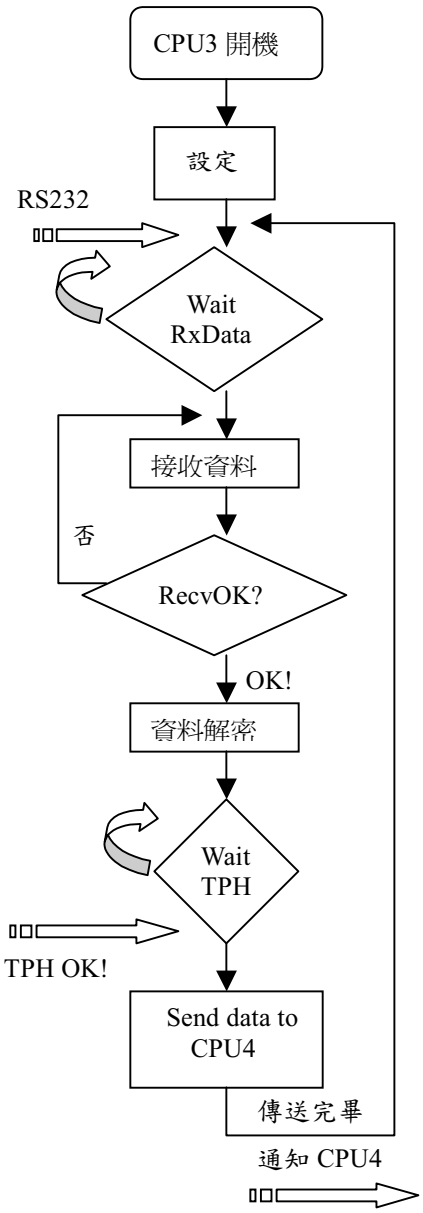


圖 10・CPU3 與 CPU4 之間的耦合

(A) CPU3 系統流程

CPU1（負責壓縮工作）與 CPU 4（負責解壓縮工作）的系統頻率太低，只有 6MHz。我們假設系統處理壓縮／解壓縮時間為 T 秒，而通訊時間為 t 秒（以 38.4K 鮑而言），由表二的數據轉成表三。通訊時間與傳送速率成比例關係，t：2t：4t，我們簡約得到 T＝51 秒，t＝7 秒。換句話說，如果我們將 CPU1 與 CPU4 系

統頻率提高為 12MHz，則系統壓縮/解縮時間將降為 T/2，即 26 秒，預估可得表四之改進結

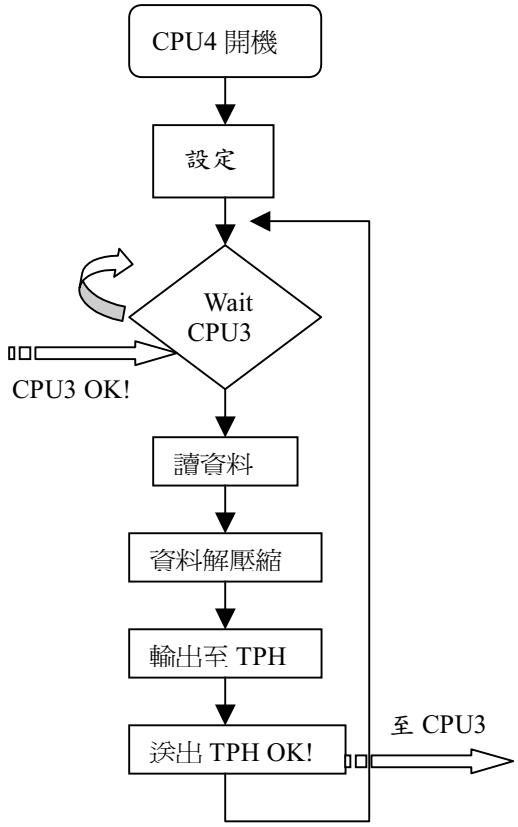


圖 10・(B) CPU4 系統流程

表二・經 Null Modem 外接同步時脈產生器測試結果

傳送速率	傳送時間
9.6KHz	1 分 14 秒
19.2KHz	1 分 5 秒
38.4KHz	58 秒

表三・由表二的數據轉成，各種傳送速率傳送時間之評估

傳送速率	傳送時間
9.6KHz	74 秒=T+4t
19.2KHz	65 秒=T+2t
38.4KHz	58 秒=T+t

(註):T＝壓縮/解壓縮時間

nt＝通訊時間

果。但是經實作結果顯示，因為：（１）TPH 是個慢速元件，其印字原理是依靠 TPH 上面的電阻加熱，使感應紙受熱而印字，感應紙受熱的最少時間就是印字的最短時間，無法再減少；（２）資料壓縮／解壓縮時間，由 CPU 系

表四・系統時脈採用 12MHz 時預估傳送時間

傳送速率	傳送時間
9.6KHz	54 秒
19.2KHz	40 秒
38.4KHz	33 秒

統時脈快慢決定，但是提高 CPU 時脈會造成 UART 元件 8251 無法被 CPU 讀取，因為 8251 通訊處理器是一顆慢速元件；（３）CIS 掃描時間。以上三個因素，以第一個 TPH 熱感應輸出時間緩慢，為最主要因素。若我們要提高傳真速率，可以考慮不用 TPH，而改用 CRT 顯示器直接顯示，或用個人電腦存檔後再印出。

為了讓 CPU 工作切換時，能掌握較佳的時程，圖 11 是用 9600 鮑同步通訊時，系統傳

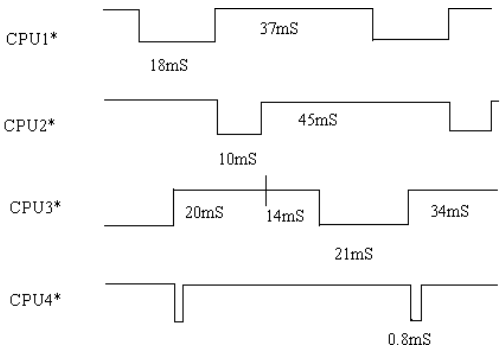


圖１１・CPU 與 CPU 之間的連動時序

送一行資料時，CPU 1 至 CPU 4 之連動時序圖。CIS 掃描與資料壓縮時間 18ms（CPU１*，星字代表低位啟動），資料加密時間 10ms（CPU2*），資料解密時間 10ms（CPU3*之部分時間，CPU3*時間 21ms = 11ms +10ms，11ms 是傳傳輸時間），同步 9600 鮑，資料傳輸時間 14ms+11ms=25ms，資料解壓縮時間 0.8ms（CPU4*），TPH 印出時間約 40ms（CPU4）；若改用 19200 鮑，則傳輸時間降為 13ms；38.4k

鮑，則降為 6.5ms。以 9600 鮑，處理一條線的時間是：20ms+25ms+10ms＝55ms。若改為 19200 鮑，則是 43ms；而 38.4k 鮑，則降為 36.5ms。綜合言之，不論傳輸速率多快，對於處理一張 A4 的時間，大約介於 2 分鐘至 1 分 10 秒之間。

系統完成上述測試後，再經 RF Modem 連線測試，結果如表五所示。表五的傳送時間略長於表二所述，可能因素為 RF Modem 內部產生的時脈，有若干延遲因素存在，例如

表五．經華衛一號實際測試結果

傳送速率	傳送時間
9.6KHz	1 分 29 秒
14.4KHz	1 分 18 秒
19.2KHz	1 分 12 秒
38.4KHz	1 分 7 秒

Preamble Clock，這種訊號不會出現在表二（因為測試所用之製具只是同步時脈模擬而已），而這訊號在兩台「真正」的 Modem 之間的「同步化」卻是必須的。

與 RF Modem 連線成功後，改與太空計畫室提供的低速率數據機連線，先以 RF 端迴接測試，成功後再經由衛星連線測試，除天候不良時會有雜訊，測試情況大致良好（參考附錄），傳送文件時間與表五差不多，於衛星通過期間大約可傳送 4 至 6 張 A4 圖稿。

圖 12 是保密傳真發射子系統與接收子系統實作圖。未加密前，傳送一張 A4 尺寸的文件，大需 1 分 10 秒。加密後，傳送同一張 A4 文件，大需 1 分 30 秒。操作者可自鍵盤輸入金鑰密碼，接收端之金鑰密碼與接收端之金鑰密碼符合，接收到的傳真資料才可還原，否則形成一片亂碼。

九．結論

傳統傳真機在傳真機的市場，趨近於飽和，而傳真機的功能，趨近於定型化。開發傳真機的新功能，以期開拓傳真機的新市場，其關鍵在於是否能掌握傳真機的技術。本文描述適合於中華衛星一號通道的保密傳真機製作方法，進一步開發 AES 或其他型式之傳真機，期再造傳真機的新市場。另外，加解密演算法驅近於簡單化，不僅有助於密碼安全性的驗證，也將進一步帶動密碼學，往生活上的各個層面滲透。密碼學往單晶片製作，將是一個不容忽視的領域。

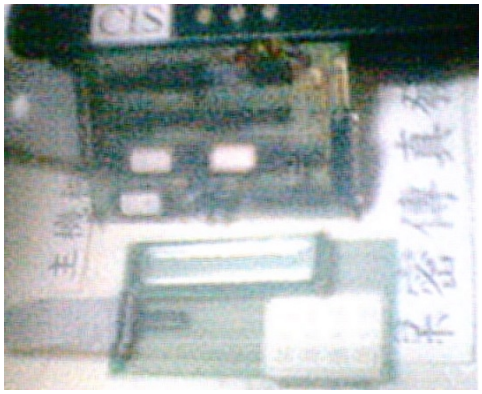


圖１２．(A)保密傳真發送子系統實作圖

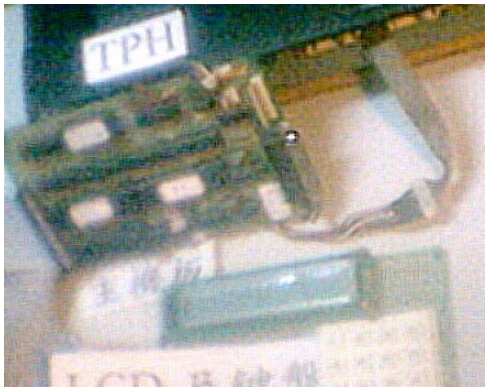


圖１２．(B)保密傳真接收子系統實作圖

十．致謝

本計畫發展期間，承聲寶公司提供傳真機資料；本文撰稿期間，承本計畫助理高嘉敏小姐提供協助，在此一併致謝。最後感謝國科會四年來經費上的補助（NSC-85-NSPO(A)-ECP-006-01）。

十一・參考文獻

[1] 太空計畫室網站，"http://www.nspo.gov.tw/"。

[2] 陳宗義，傳真機-FAX，1994， 3 月，全華圖書出版社。

[3] 國科會工程科技推展中心，"下一代 加密標準研究成果發表會論文集"，2000 年 11 月 21 日。

[4] 賴溪松、韓亮及張真誠，近代密碼學及其應用，第 5 章，1995 年 9 月，松崗出版社。

[5] Cibson，Berger，Lookabaugh，Baker，"Digital Compression for Multi-media"，Morgan Kaufmann。

[6] FRED HALSALL，"Data Communications，Computer Networks，and Open Systems"，ADDISON-WESLEY。

[7] ITu-T T.2 "Standardization of group 1 facsimile apparatus for document transmission", 1988 Blue Book. 。

[8] ITu-T T.3 "Standardization of group 2 facsimile apparatus for document transmission", 1988 Blue Book. 。

[9] ITu-T T.4 "Standardization of group 3 facsimile apparatus for document transmission", 1988 Blue Book. 。

[10] ITu-T T.6 "Facsimile coding schemes and coding control functions for group 4 facsimile apparatus" 1988 Blue Book。.

[11] ITu-T T.20 "Standardized charts for document facsimile transmission", 1988 Blue Book。

[12] ITu-T T.21 "Standardized test charts for document facsimile transmission" 1988 Blue Book。

[13] ITu-T T.30 "Procedures for document facsimile transmission in the global switched network", 1988 Blue Book。

十二・附錄

經中華衛星一號通訊酬載實驗保密傳真機接收之傳真稿件。