

國立交通大學
電機與控制工程學系

碩士論文

自動鐵捲門監控系統之研究

A Study of Shutter Monitoring System



研究生：吳見晉

指導教授：廖德誠 博士

中華民國九十五年七月

自動捲門監控系統之研究

A Study of Shutter Monitoring System

研究生：吳見晉

Student : Jian-Jin Wu

指導教授：廖德誠 博士

Advisor : Dr. Der-Cherng Liaw

國立交通大學

電機與控制工程學系



Submitted to Department of Electrical and Control Engineering

College of Electrical Engineering and Computer Science

National Chiao Tung University

In Partial Fulfillment of the Requirements

For the Degree of Master

in

Electrical and Control Engineering

July 2006

Hsinchu, Taiwan, Republic of China.

中華民國九十五年七月

自動鐵捲門監控系統之研究

研究生：吳 見 晉

指導教授：廖 德 誠 博士

國立交通大學電機與控制工程學系



本文結合遙控自動捲門二態編碼及滾動碼技術，架構出一套整合性的自動鐵捲門監控系統，並利用單晶片實現之。傳統的二態捲門遙控系統有著密碼單調易被破解的風險，而滾動碼系統彈性低，無法隨使用者自定規格。綜合以上問題，本論文提出了一整合性的自動捲門監控系統，結合二態編碼的使用便利性及滾動碼技術的安全性，並應用無鑰進入系統之概念，且增加了可由使用者自定的變數，提高了此一自動捲門監控系統的彈性。

在人身安全部分，在系統中加入了紅外線偵測機制，可有效判斷當捲門落下時是否有人，避免造成人員傷亡，亦可有效監控是否有人闖入，增加了使用上的安全性。

關鍵字：門禁系統、自動捲門、無鑰進入系統。

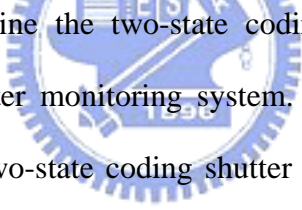
A Study of Shutter Monitoring System

Student : Jian-Jin Wu

Adivisor : Dr.Der-Cherng Liaw

Department of Electrical and Control Engineerong
National Chiao Tung University

Abstract



In this thesis, we combine the two-state coding shutter and Keelog coding technique to establish a shutter monitoring system. There is a drawback of being monotone in the traditional two-state coding shutter system, and the Keelog shutter system is short of elasticity. To address these issue, we propose a new scheme in shutter monitoring system, it combine the facilitation of use in traditional two-state coding shutter system and the safety in the Keelog shutter system. We also apply the aspect of no-key entrance system on it, and add a function that user could decide the variable in coding to prove the flexibility of the shutter monitoring system.

In the safety work, we add the infrared ray detecting system to decrease the unexpected events. It could recognize if people stand below the shutter when if falls.It could also increase the safety by detecing if someone barge in through the shutter.

Keyword : shutter monitoring system 、 no-key entrance system

致 謝

在這兩年期間，我要感謝我的指導老師廖德誠教授，經由他的教導讓我體會不同的思考模式以及求學該有的態度，並培育學生對求知的耐心；另外要謝謝王宜楷老師，他觸類旁通的頭腦以及認真積極的教學態度讓人佩服不已，任他的助教讓我在實驗課程中培養電子電路的實力，也讓我看到身為一個敬業的授業者所採取的態度。

同時要感謝實驗室所有成員，讓我在這兩年的研究充滿歡樂充實回憶：頭腦清楚理論超強體力充沛的成哥、搞笑愛錢幣的文敬學長、電路實作功力一流的翁學長、帥氣有型、任勞任怨銘祺的學長、硬底子的佳勳學長、第一射手的重訓男鎮綸學長、流行最前線的韋翰學長、認真憨厚的大大、出手不手軟的阿蠻、號稱神之手的強者小剛、做事踏實的月半、實驗室女高音烏賊。

在職專班的學長們，像是裕昌學長、思齊學長、通達學長、仁華學長、富貴學長、朝源學長，還有去年畢業的緯評學長，除了給我課業上的幫助之外，也用他們豐富的人生歷練，讓我在實驗室中能順利度過低潮。

此外也要感謝我的家人，總是站在我這邊支持我，無論是在我低潮時，或是在我陷入抉擇的時候，總是提供各方面的看法，讓我容易看清楚整個局面，以及我可愛的姪子昌泰，每次回台北都會想找他出來玩，因為他很可愛。有家人的照顧，讓我每次回家都能從疲憊的狀態中馬上恢復。最後補充的是我女朋友侑貞，總是在我的背後支持我，又會賺錢，又會買便宜又好看的鞋，也知道拿坡里內用的價錢跟外帶的優惠價是一樣的，讓我在專心準備唸書之外，其他生活上的細節，幾乎都不用操心。

目 錄

摘 要.....	i
Abstract.....	ii
致 謝.....	iii
目 錄.....	iv
圖目錄.....	vi
表目錄.....	viii
第 1 章 序論	1
1.1 研究動機與背景	1
1.2 論文主題	2
1.3 論文結構	2
第 2 章 相關研究與技術探討	3
2.1 數位門禁系統	3
2.2 無線收發模組	5
2.2.1 幅移鍵控調變(ASK)	8
2.2.2 頻移鍵控調變(FSK)	9
2.3 編解碼 IC	10
2.4 KEELOG 演算法	11
2.5 單相交流馬達	13
2.5.1 單相交流馬達的特性	13
2.5.2 單相交流馬達的啟動	13
2.5.3 單相交流馬達的轉向	16
2.5.4 單相交流馬達的應用	16
第 3 章 自動捲門監控系統	20
3.1 系統架構	20

3.2 系統規格	22
3.2.1 半雙工通訊機制	22
3.2.2 認證機制	25
3.2.3 隨機數產生機制	26
3.2.4 加密機制	26
3.2.5 自動捲門馬達控制	26
3.2.6 紅外線感測功能	27
3.3 功能實現	27
3.3.1 半雙工通訊功能實現	27
3.3.2 認證功能實現	30
3.3.3 隨機數功能實現	31
3.3.4 加密機制功能實現	31
3.3.5 紅外線感測功能實現	32
3.4 系統整合	33
第 4 章 自動捲門監控系統驗證	38
4.1 資料傳輸	38
4.2 認證機制	40
4.3 隨機碼	41
4.4 驗證碼與認證金鑰	42
4.5 紅外線監控系統	44
4.6 電磁開關與馬達驅動	45
第 5 章 未來展望	47
5.1 結論	47
5.2 未來展望	47
參考文獻.....	48

圖目錄

圖 2-1	數位監控系統.....	4
圖 2-2	門禁系統架構.....	4
圖 2-3	無線通信網路示意圖.....	6
圖 2-4	單工通訊示意圖.....	6
圖 2-5	半雙工通訊示意圖.....	6
圖 2-6	全雙工通訊示意圖.....	7
圖 2-7	類比調變技術與數位調變技術.....	7
圖 2-8	曼徹斯特編碼範例.....	8
圖 2-9	ASK 基本調變波形.....	8
圖 2-10	ASK 方塊圖及波形關係圖.....	9
圖 2-11	BFSK 基本調變波形.....	9
圖 2-12	利用二態碼的 HT-12E 組成的遙控器.....	10
圖 2-13	單相交流電源。.....	13
圖 2-14	分相交流馬達電阻啟動.....	15
圖 2-15	分相交流馬達反動啟動。.....	15
圖 2-16	分相交流馬達電容啟動.....	15
圖 2-17	電容啟動單相交流馬達.....	16
圖 2-18	單向交流馬達轉向控制.....	16
圖 2-19	自動捲門與馬達電磁開關配線圖.....	17
圖 2-20	東元馬達 DS30、DS70、DS100.....	19
圖 3-1	自動捲門監控系統架構.....	21
圖 3-2	發射模組外觀與接腳說明.....	23
圖 3-3	接收模組外觀與接腳說明.....	23
圖 3-4	HT-12E 編碼 IC 接腳圖.....	24

圖 3-5	HT-12D 解碼 IC 接腳圖	24
圖 3-6	認證機制流程圖	25
圖 3-7	脈衝信號寬度	27
圖 3-8	發射模組電路圖	28
圖 3-9	接收模組電路圖	29
圖 3-10	HT12E 資料傳送格式.....	29
圖 3-11	資料編碼示意圖.....	29
圖 3-12	操作時間示意圖	30
圖 3-13	認證機制工作流程圖	31
圖 3-14	4 位元轉 8 位元資料格式	32
圖 3-15	識別碼與認證金鑰運算示意圖	32
圖 3-16	紅外線偵測機制流程圖	33
圖 3-17	遙控器工作方塊圖	34
圖 3-18	捲門主機工作方塊圖	35
圖 3-19	MPLAB 整合式的發展平台.....	37
圖 3-20	MPLAB 開發環境。.....	37
圖 4-1	自動捲門監控系統	38
圖 4-2	資料傳輸波形週期	39
圖 4-3	資料傳輸內容圖	39
圖 4-4	送出的認證資料波形圖	40
圖 4-5	認證通過介面：LED 燈號.....	41
圖 4-6	捲門可遙控時間與計數機制示意圖	41
圖 4-7	紅外線感測系統	44
圖 4-8	電磁開關關閉，馬達不運作	45
圖 4-9	電磁開關運作使得馬達正轉	45
圖 4-10	電磁開關運作使得馬達反轉.....	46

表目錄

表 2-1 東元捲門機性能規格表.....	18
表 4-1 連續 8 次操作的識別碼變化.....	43
表 4-2 修正規則後，連續 8 次操作的識別碼變化.....	43
表 4-3 連續 4 次操作的認證金鑰變化.....	44



第1章 序論

1.1 研究動機與背景

隨著時代的進步，現代社會交流的複雜化使得犯罪問題日益嚴重，因此，居家安全的觀念越來越受到重視。目前台灣許多大樓社區都有專屬的保全系統，不過大部分都是屬於舊式的類比式監控系統，即以人員搭配錄影監控的方式進行安全維護，其監控方式較為被動，對於入侵者無法主動的告知，而且需要定期更換錄影帶。此外，長時間以人力監看容易造成人員的疲勞而影響到監視效率。

為了改善上述缺失，因而有了數位式監控系統[1]的發展。數位式監控系統主要是以數位影像搭配電腦硬體平台達成及時自動監控及數位儲存影像的功能，搭配網路技術甚至還能進行遠端監控[2]。此類系統在進行人員身份辨識時，常使用影像技術或語音處理技術作為判斷準則。但目前絕大多數的數位式錄影監控系統卻大多用於發生事故後的“調閱錄影紀錄”，很少做到我們所期望的“即時性警告與嚇阻”作用。

現行門禁系統在人員的辨別上大致可分為非遙控式和遙控式兩種類型。非遙控式大都採用接觸式或感應式的方式開啟門禁之管制。在接觸式門禁系統中，使用者須先透過刷卡機刷卡或者以輸入密碼的方式開啟門禁。而在感應式門禁系統，使用者須要使用識別感應卡片開啟門禁。而遙控式類型則為較單純的門禁系統，透過紅外線或 RF 射頻遙控器操控以開啟門禁之管制。在人員及車輛進出入的管制上，自動捲門已普遍應用在門禁系統上，不論是一般家庭或者是社區的地下停車場及大門，自動捲門搭配門禁系統可有效解決管制人員出入的需求，然而在科技進步的同時，也衍生了許多安全性上的問題。例如一般市面紅外線與 RF 射頻遙控器容易因為遙控器遺失所導致易於被拷貝，或者是密碼破解的風險，使得在門禁系統上出現漏洞，並對使用者的居家安全造成風險。

1.2 論文主題

在本篇論文中，針對遙控式門禁系統提出一綜合傳統二態及滾動碼的優點並利用單晶片實現的自動鐵捲門監控系統，改善傳統自動捲門在門禁系統使用上所出現的安全性漏洞，並建立一使用者認證機制，增加安全性，同時利用 EEPROM 做資料的存取，使系統可提供給多人使用，利用使用者遙控器上所儲存的專屬安全密碼進行認證，並在每次完成動作後，隨機產生一新密碼，有效改善了遙控門禁系統的安全問題，希望能對門禁系統的安全性改善上有所貢獻。

1.3 論文結構

本論文共分為五章，第一章為序論，簡敘了研究的動機與背景；第二章則介紹了自動捲門在門禁系統的應用及遙控器的工作原理。在第三章中則說明吾人所提出之自動捲門監控系統並實現之；第四章為系統的驗證；第五章則為結論與未來展望。



第2章 相關研究與技術探討

2.1 數位門禁系統

傳統的監控系統多為類比式系統，多台攝影機與分割器連接，然後將分割好的畫面送到監視器與錄影機內儲存，缺點在於必需依賴現場管理人員的操控，容易因為人員體力問題或者分心而發生疏失，且無法對於特定目標或時間點作出自發性的錄影及因應警告的信號；加上重複利用錄影帶，容易降低影像品質。

現行的數位監控系統可便利警衛做中央控管，也能夠提供所有的社區用戶遠端即時的畫面，因此數位化的錄影監視系統逐漸取代了類比式監控系統成為社區保全的主流。

門禁系統主要利用數位監控系統，搭配其他軟硬體共同實現居民的出入管理，並可隨時掌握社區的安全狀況。其架構係利用一部或多部以上的數位攝影機在不同的角度或不同的地區做監控，舉例來說，設置於大門的攝影系統可使住戶清楚的看到來訪者以決定是否請警衛放行；停車場的監控畫面可讓住戶隨時掌握愛車的狀況。影像處理方面，作為伺服器的電腦利用影像擷取卡獲得所監視影像資料，並利用區域網路〔LAN〕或 INTERNET 將影像資料傳送到影像伺服器作儲存，當使用者需要查閱特定的影像時，便可向影像伺服器送出要求。所獲得的影像經過處理之後，判斷是否有異狀[3]，達到主動預警的功能。若搭配遠端監控系統，使用者只須透過瀏覽器連結至伺服器端之互動式網頁，即可利用網際網路監控遠端之受控系統裝置 [4]；搭配無線感測器，當監測區域發生意外如火險時，便可快速且有效率的指引民眾往安全出口前進，減少傷亡[5]。

數位門禁系統的最終目的在於提供一無人操控且能依照預設工作模式自發性運作，並且能及時反應異常狀況並做出回應的，以保障使用者的人身安全。自動捲門現今已普遍應用在門禁系統上，不論是一般家庭或者是社區的地下停車

場，自動捲門在門禁上的使用解決了人員出入的需求，然而在科技進步的同時，也衍生了許多安全性的問題。例如加強自動捲門在使用上的安全性，減少壓傷人員的意外發生機率，並考慮一般市面紅外線或 RF 射頻遙控器，因為遙控器遺失所導致易被盜拷，或者是遙控器密碼過於單調，容易有密碼被破解的風險，使得住民的生命財產受到損害。

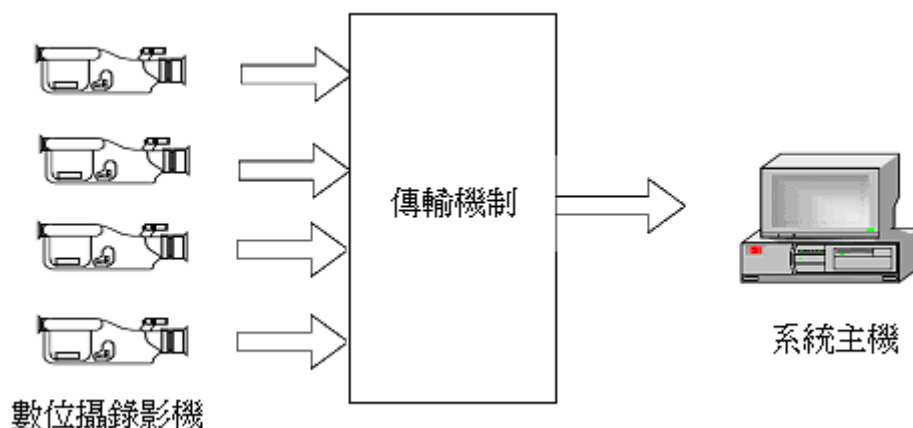


圖 2-1 數位監控系統

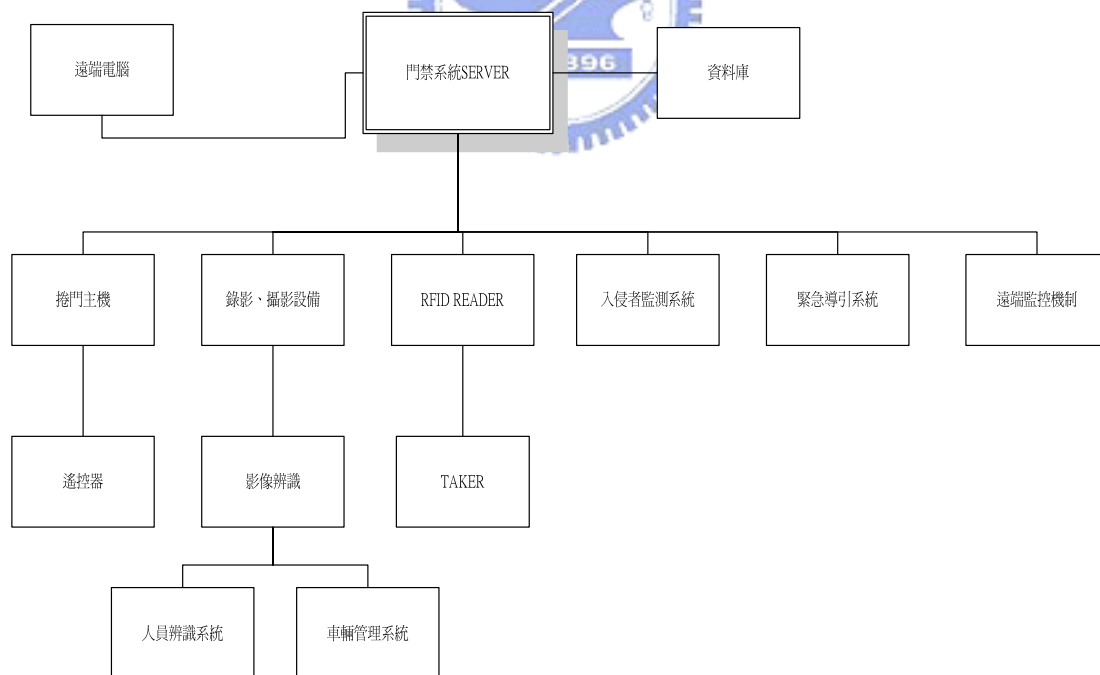


圖 2-2 門禁系統架構

2.2 無線收發模組

在傳統自動捲門的操作上，使用者利用遙控器以無線通信的方式送出指令到捲門主機。所謂無線通信是指傳輸媒介無實體結構，訊息由發射設備或天線將電磁波發射至遠端，再由接收端藉接收天線及設備感應電磁波，將接收信號放大與還原，天線通訊方式有無線電、紅外線、微波等多種方式[6]。手機便是無線通訊最常見的例子，見圖 2-3。無線通信的方式有單工通訊、半雙工通訊、全雙工通訊。單工通訊時，發射機只能發射訊號；接收機只能接收訊號。採用半雙工通訊通訊模式時，兩組發射接收設備彼此可互相發射與接收信號，然而同一時間、同一設備只能發射或接收無法同時發射與接收，傳統的無線電便是如此。全雙工通訊則發射與接收設備可同時工作，可以同時發射與接收，但為避免發射器與接收器互相干擾，發射與接收頻率不同但同時傳輸資料時，可能會有互調現象 (Intermodulation) 發生[7]。當多種信號在非線性 (Non Linear) 設備同時相互作用，有可能產生一種或多種不同交調頻率信號，此一交調信號會影響收訊，甚至導致收訊故障。

在資料的傳輸上，則使用調變技術先將資料轉換成適合在傳播媒介傳送的格式，在接受器端再將所收到的信號轉換成原本的資料格式。比如說人與人對話的時候是一種通訊。說話的人把資訊透過空氣這一傳播媒介傳達到收話人的耳朵。因為聲波不適合在空氣中傳播，所以說話聲音無法傳播到遠處。若要把人聲傳播得遠，我們便先將人聲轉換成電流訊號，調變技術能將電流訊號與高頻率的載波信號結合，結合後的信號能在傳播媒介的空氣中傳送得更遠。輸入信號頻率為低頻信號，載波信號頻率則為高頻信號，調變後的輸出信號則為高頻信號。

調變技術可以分成兩大類：類比信號調變技術與數位信號調變技術。類比信號調變技術有振幅(AM)調變、頻率(FM)變、相位(SK)調變等方式；數位信號調變技術有幅移鍵控調變(ASK)、頻移鍵控調變(FSK)等[8]。

當發射器透過無線通信傳送一個位元的數位信號時，將在一定的週期內，假

定為 T ，產生一個持續的信號。一個預設的定時器負責計時。接收設備必須知道 T 時間的長度及信號的週期，這樣才能在每個 T 時間單元內對收到的信號進行採樣。就像指揮家確保演奏者的同步一樣，通信設備也需要某種機制以使發射器及接受器同步，不變的信號不具備同步機制。但如果信號有一規則性的變化，便可利用此改變來保持設備的同步。有些強制信號改變的編碼方案就是基於這個原因，如最常見的曼徹斯特編碼(Manchester Code)[9]。

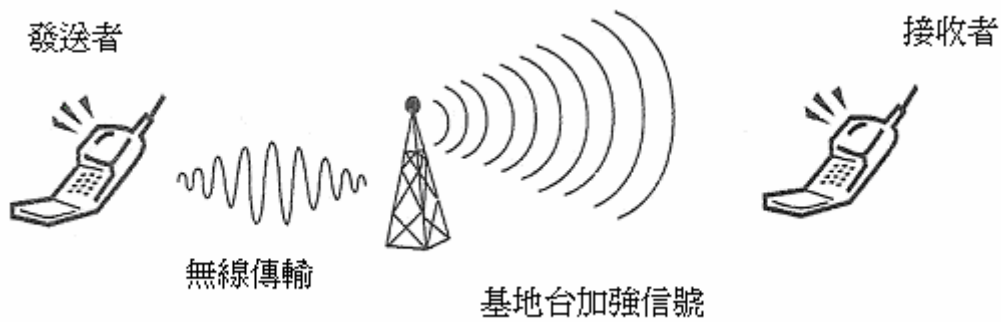


圖 2-3 無線通信網路示意圖

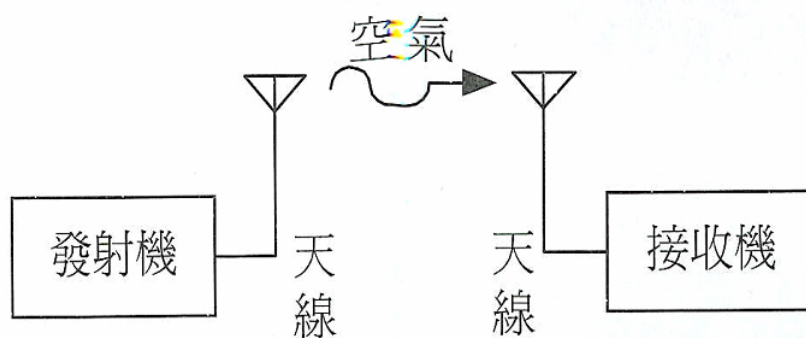


圖 2-4 單工通訊示意圖

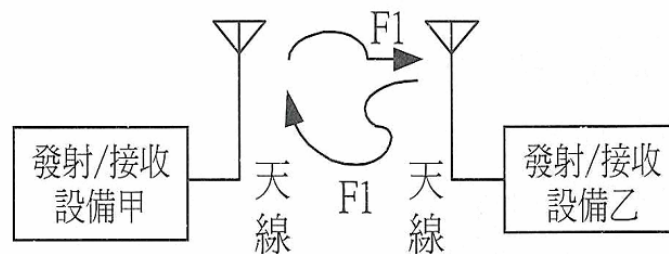


圖 2-5 半雙工通訊示意圖

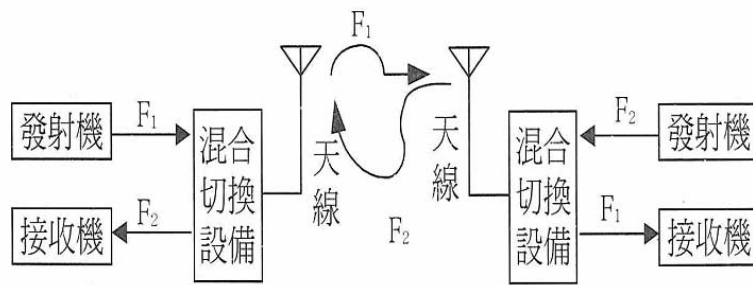


圖 2-6 全雙工通訊示意圖

自動捲門主機與遙控器資料的傳輸多用 RF 通訊作傳輸媒介，資料的調變則利用數位信號調變技術如 ASK 或 FSK，而為了減少雜訊干擾及確定發射器送出的數位信號與接收器所收到的信號完全無誤，則常利用編解碼 IC 來確保收到的指令是正確的。

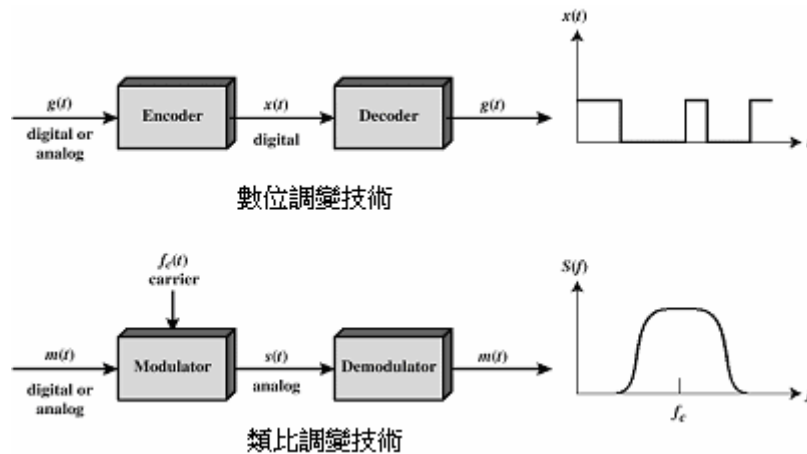


圖 2-7 類比調變技術與數位調變技術

曼徹斯特編碼利用判斷信號的變化來保持發送設備與接受設備的同步，也有人稱之為自同步碼(Self-Synchronizing Code)，主要利用電壓的變化來分辨 0 和 1，它明確規定從高電壓到低電壓的跳變代表 0，而從低電壓到高電壓的跳變代表 1。圖顯示了位元串 01011001 的曼徹斯特編碼。如圖所示，信號的保持不會超過一個位元的時間間隔。即便是 0 或 1 的序列，信號也將在每個工作時脈間隔的中間發生跳變。這種跳變將允許接受器的時脈與發射器的時脈保持一致。但其缺點便是相較於原信號需要兩倍的頻寬如圖 2-8 所示。

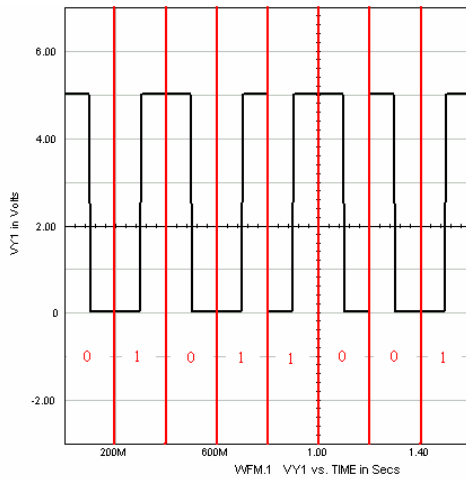


圖 2-8 曼徹斯特編碼範例

2.2.1 幅移鍵控調變(ASK)

幅移鍵控調變是最常被人們所利用的調變技術，利用輸入數位信號振幅的有無即 0 或 1，作為載波信號傳送與否的依據，當固定振幅的載波出現時表示一個二進數值，沒有載波信號表示另一個二進數值。

$$s(t) = \begin{cases} A \cos(2\pi \cdot f_c \cdot t) & \text{二進制 1} \\ 0 & \text{二進制 0} \end{cases}$$

其中 $A \cos(2\pi \cdot f_c \cdot t)$ 為載波信號。然而因為 ASK 調變中載波信號振幅會瞬間變化，易受雜訊干擾，並不是一個有效率的調變技巧。

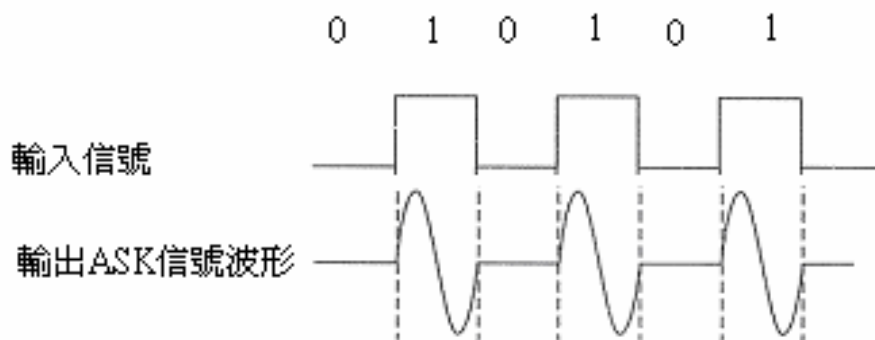


圖 2-9 ASK 基本調變波形

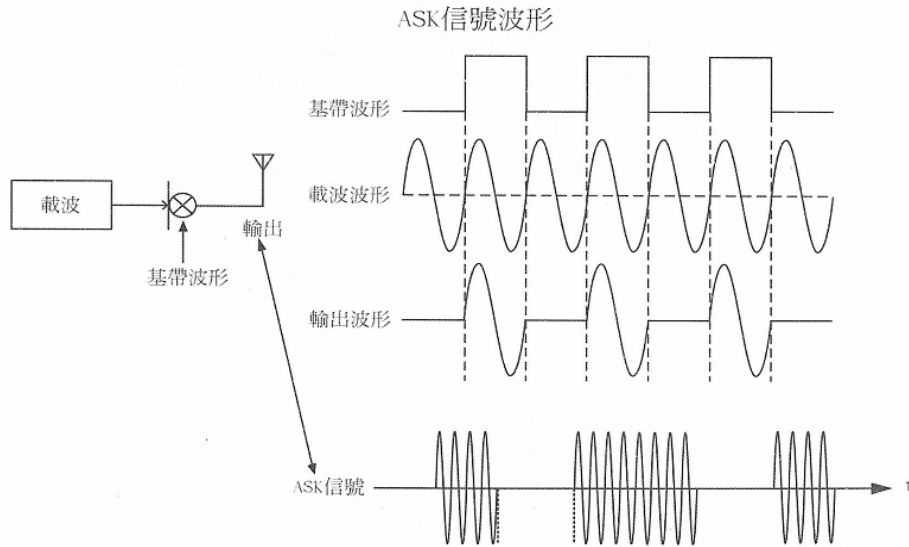


圖 2-10 ASK 方塊圖及波形關係圖

2.2.2 頻移鍵控調變(FSK)

頻移鍵控調變則是利用接近載波頻率的兩個不同頻率載波信號分別表示二進制數值 (BFSK)，當輸入數位信號波形的振幅為 1，則傳送載波 1 的訊息；當基帶波形的振幅為 0，則傳送載波 2 的訊息，載波 1 與載波 2 的頻率不同。

$$s(t) = \begin{cases} A \cos(2\pi \cdot f_1 \cdot t) & \text{代表二進制 1} \\ A \cos(2\pi \cdot f_2 \cdot t) & \text{代表二進制 0} \end{cases}$$

其中 f_1 和 f_2 分佈在載波頻率的兩側，且與載波頻率的差相等。BFSK 抗雜訊能力比 ASK 好，其錯誤率較低比 ASK 好，在圖 2-11 則以 $f_1 = 2f_2$ 為例。

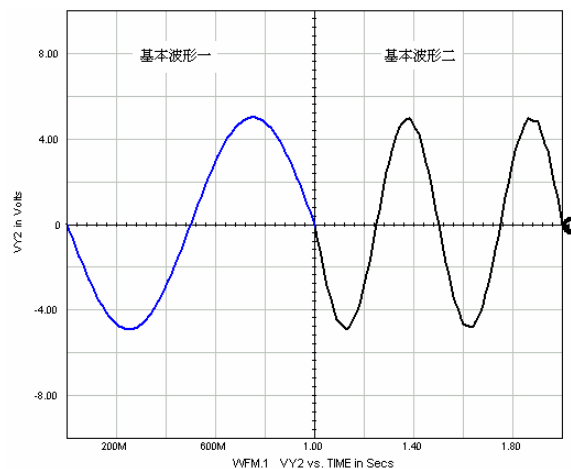


圖 2-11 BFSK 基本調變波形

2.3 編解碼 IC

在自動捲門的使用上，為了確保無線通訊所收到的信號正確無誤，常搭配編解碼 IC 使用，常見的編解碼 IC 依工作方式可分為二態、三態及滾動碼形式。以下將分別介紹其工作模式[10]。2 態的基本模式如下：XXXXXXXXAAAA，X 是 0 或 1，作為辨識碼，若遙控器與接收器的辨識碼不同，則視為密碼錯誤，將不會工作；A 是 0 或 1，稱為控制碼，當遙控器與接收器的辨識碼相同時，接收器便會將控制碼讀入，並根據所對應的指令內容作出相對應的動作。



圖 2-12 利用二態碼的 HT-12E 組成的遙控器

三態的基本模式跟二態的類似，只是 X 或 A 變成 0、1 或 F。滾動碼的基本模式如下：

- (1) XXXXXXXXXXXAAAA
- (2) XXXXXXXXXXXXXXXXXXXX

在(1)的部分，X 跟 3 態的變化一樣，但是每按一次遙控器會有不一樣的排列，即當編碼器及解碼器完成一次工作時，便會改變辨識碼一次。(2)的部分跟上述的都不一樣，X 是 16 位元，第 1 碼是按鍵碼，第 2 到 5 碼是主機碼，6 到 8 碼是出廠碼，9 到 16 碼是變動辨識碼，每按一次按鍵 9 到 16 碼都不一樣，利用獨特的演算法達到每完成一次工作便改變辨識碼。

二態或三態的編解碼形式使用簡單，成本低，但在使用上卻有極高的風險，因為其辨識碼單調而變化少。二態或三態的編解碼方式因為固定編碼及解碼格

式，使得辨識碼固定，而且可以變化的密碼組數很少，以 2 態為例，密碼長度為一 8BIT 的位元組 XXXXXXXX，而 X 只有 0 或 1 的變化，因此從 00000000 到 11111111 總共只有 256 組密碼。三態與二態類似，參數 X 有 3 種變化 0、1、F，但是算起來也只有 6561 種變化。而滾碼型的遙控器，安全性極高，密碼不易重複，可避免密碼被破解的風險，但因無法拷貝，當遙控器遺失時，便需更換整個主機及遙控器，大大減低了其方便性

2.4 KEELOQ 演算法

目前滾動碼系統專用晶片系列中，HCS300[11]是其中較典型的一款，由 Microchip 公司以 KEELOQ 技術為基礎所開發。它是一塊 8 接腳的編碼 IC 晶片，裏面內建 KEELOQ 演算法和其他一些功能，帶有四個按鍵介面，可實現 15 種對應的功能。內建 192bits (12×16bit words) EEPROM，用來存放 EN_KEY (加密金鑰)、SN (使用者序號)、SYNC (同步碼)、SEED (認證碼) 等。序列號用來標識不同的對象；加密金鑰用來對所發送的數據進行加密，增加破譯的難度，不會直接發送出去；同步計數器用來抗截獲，每次發送數據時，同步計數器的值，即同步碼都被更新，所以每次發送的數據都不一樣。認證碼用於參與加密密鑰的生成。接收方必須先通過認證來獲得並紀錄發送方的序列號、加解密密鑰和同步計數器的值。主機在接收到信號後，首先比對序列號，然後利用認證過程中得到並紀錄的加密密鑰對接收的數據進行解密；接著檢查解密後的同步計數器是否匹配，在確認其匹配後，再去處理接收到的控制碼，並根據接收到的按鍵指令作出相應的動作反應。HCS300 的系統使每次發送的密文都不相同，有效防止了空中截獲法和數據重傳帶來的安全隱患。

KEELOQ 技術的核心思想是用 64bit 的 EN_KEY[64:0] (加密密鑰) 去加密 32bit 的 CSR[31:0] (校驗碼) 得到 32bit 的 CRYP 密文。其加密機制為：首先定義一個非線性加密機制，這個非線性表有 5 位輸入 NLF_IN[4:0]，一位輸出 NLF_OUT。它在 CSR [31:0] 中間隔均勻地取固定 5 位：I0、I1、I2、I3、I4，

通過非線性加密產生一個輸出碼 NLF_OUT；這一位輸出碼 NLF_OUT 再與 EN_KEY 中的 15 位、CSR 中的 2 位進行 XOR 運算後輸出第一位輸出碼 CRYP[0]；每輸出一位後，EN_KEY、CSR 分別進行移位，EN_KEY 作迴圈移位，CRYP[0]作為 CSR 移位的輸入；重復上述步驟直到輸出 32 位 CRYP[0:31]。依此法，即使 32bit 的校驗碼 CSR 中只有一位發生變化，用 KEELOQ 加密演算法得到的 CRYP 密文也會有 50%以上的數據位（16bit）發生變化。

儘管 KEELOQ 技術有上述獨特的優點，但是經過深入分析不難發現 KEELOQ 演算法及其硬體實現技術也存在一些不足：

(1) 利用固定的出廠碼和認證碼產生加密金鑰。在 HCS300 晶片中，加密密鑰 EN_KEY 是由出廠碼、序列號 SN 和認證碼生成的。而 SN 和認證碼在發送數據的過程中未經加密，是可截獲的。且出廠密鑰一經確定便無法更改，內建於晶片中，使用者無法依情況自行更改，缺乏使用彈性。此一做法，雖可有效的防止拷貝，但也無法依使用者要求進行複製，一旦遺失，則需更換整套系統，且若出廠碼外流，後果極其嚴重。

(2) 傳輸效率較低。在發送的數據中，其有用資訊（如序列號、功能碼）全部在固定碼中，功能碼只作為一種加密用的附加數據，這樣不但降低了安全性，而且傳輸效率不高。以 HCS300 為例，發送的 66 位數據中只有 32 位為有用資訊，傳輸效率低。

(3) 缺乏偵錯機制，且利用 RF 作傳輸時，須先經過調變，在這一過程中，容易受雜訊而影響資料的正確性，在傳輸過程中，功能碼代表所要實現的功能，如上轉、下轉、關閉等。若發生錯誤，例如發送的數據是 0010，而接收的數據為 0100，其後果非常嚴重。

(4) 受硬體設計限制，靈活性差，成本較高，由於不擁有核心技術，容易受制於人。

2.5 單相交流馬達

自動捲門主機接收到使用者的指令之後，利用控制單相交流馬達的轉向來完成使用者對捲門的上下捲動要求，考慮到所需的扭力，大多選用單相交流馬達。

2.5.1 單相交流馬達的特性

由於交流電的電壓和電流隨時間而變動，因此交流電通過馬達的定子線圈而產生的磁場並不是一個固定的磁場，而是隨時間而變化極性的變動磁場，利用此特性，可經設計使得周圍磁場在不同時間、不同的位置推動轉子，使其持續運轉，就如同周圍站了一圈的同學，大家順序伸手去推中間那一位同學轉動一樣，大家推的時間不一樣，使得轉子的合力不等於零，因此若要轉子持續旋轉，我們必須讓周圍的磁場在不同的時間來產生 N 極或 S 極，所以周圍磁場的線圈常分為幾組，通以不同相位的交流電。在實作上，馬達常在一組周圍磁場線圈串接一個電容器，稱為分相電容，以使與其他組線圈產生相位差，如電風扇、家庭用水加壓機等。

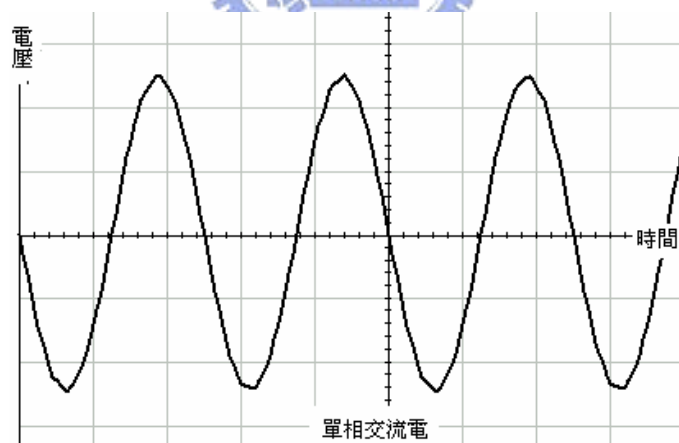


圖 2-13 單相交流電源。

2.5.2 單相交流馬達的啟動

單一定子繞組設計的單相感應電動機因無法產生起動轉矩，為使電動機能夠起動，定子繞組必須做某種特殊的安排方法才能產生起動轉矩。單相感應電動機起動最簡單的方法，就是在主要的定子繞組之外再加上一組輔助的繞組或稱啟動

繞組，而將此電動機當作二相電動機起動。這兩組繞組的軸在定子中空間上相差 90° 相位角。若我們使兩組繞組的阻抗不相同，則兩組繞組之間的電流相位亦不同。這樣，此電動機就可以等效於不平衡的二相電動機，產生一不為零的合力，結果使定子的旋轉場能夠產生出起動轉矩。這兩組繞組經過適當設計，也可以使電動機像平衡的二相電動機一樣地運轉。

單一定子繞組的單相感應電動機若在運轉中便可產生起動轉矩，因此當電動機起動後，啟動繞組便可以由電路中去除。要達到這一點，我們可以在輔助電路中接上一個離心開關。當轉速達到額定值 75% 的時候，離心開關就會打開，使輔助繞組由電路中切開減少能源浪費[13]。

啟動繞線(start winding)從啟動電路斷開後，其磁極不是超前就是落後轉動繞線極性的改變，造成一合力帶動馬達轉動。若啟動繞線及轉動繞線分別自馬達帶出，則轉動方向可由其中一組繞線或兩者同時與電源之反相連接而改變。

單相交流馬達啟動的方式及轉動方向有以下幾種方式：

- (1) 電阻啟動：啟動繞線比轉動繞線少，有較少的感應，磁極改變較轉動繞線早，致使磁場轉動方向由啟動繞線轉到轉動繞線。
- (2) 反動啟動：附加於轉動繞線之感應線圈使其磁極改變慢於啟動繞線磁極之改變。磁場有效轉動方向是由啟動到轉動繞線。
- (3) 電容啟動：有與啟動繞線串連之電容器，使啟動繞線之極性變換早於轉動繞線。磁場有效轉動方向是由啟繞線動到轉動繞線。達到應有轉速後，電容及啟動電路未切閉，稱為電容轉動馬達或永久電容馬達。

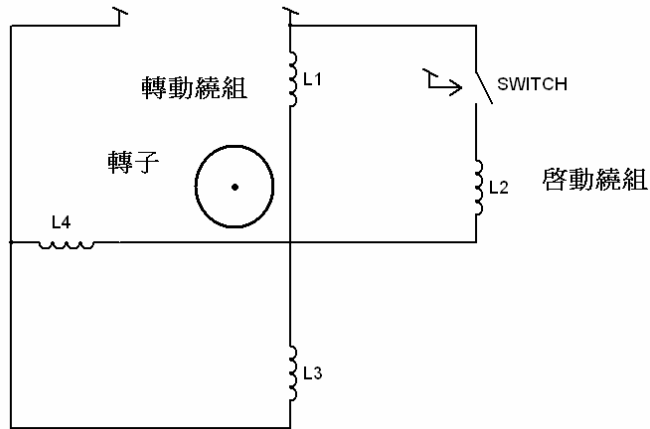


圖 2-14 分相交流馬達電阻啟動

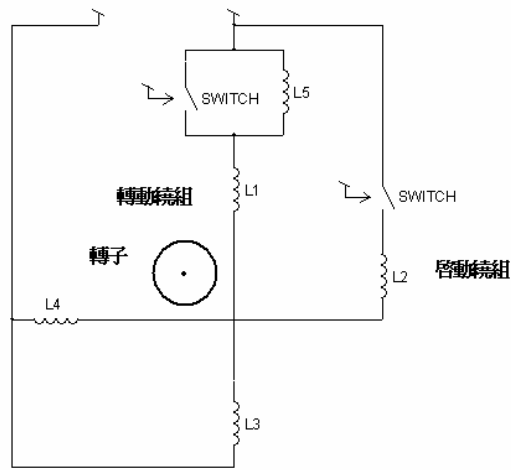


圖 2-15 分相交流馬達反動啟動。

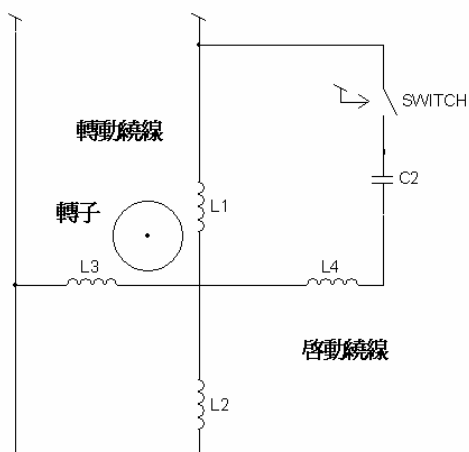


圖 2-16 分相交流馬達電容啟動

2.5.3 單相交流馬達的轉向

以電容啟動單相交流馬達做範例，基本轉向控制的原理是改變啟動繞線所接的交流電壓接線，利用一電磁接觸器來作為控制馬達運轉的開關，若欲加入一轉向控制，則電路則為圖 2-18 所示，利用 MCF 及 MCR 兩個開關便可達成轉向的控制，常見的方法則為送出一脈衝信號來控制 MCF 及 MCR 的開關與否。

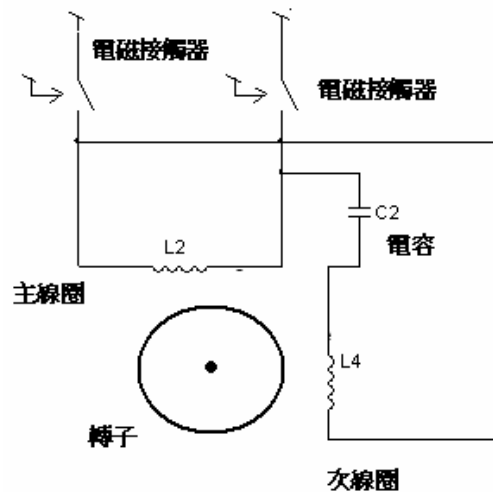


圖 2-17 電容啟動單相交流馬達

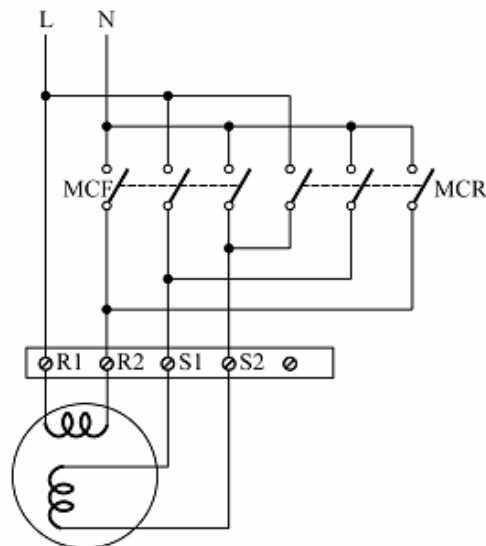


圖 2-18 單相交流馬達轉向控制

2.5.4 單相交流馬達的應用

將單相交流馬達應用在自動捲門上時，不同設計的馬達有不同的啟動方式和

動力特性，而適用於不同用途的機械中，例如有些馬達有高轉矩和扭力，而有些馬達則能定速旋轉，或者轉幾分之一圈，一般而言驅動機器的能力以輸出的功率來計算，馬達輸出功率的單位為「馬力」，Horse power，簡稱 HP，1 馬力 (HP) = 746 瓦特 (W)，馬力愈高在單位時間裡輸出的功也愈大，在機械中主要的驅動馬達，都需要比較大的動力，而作為控制用途如定位、定速…等的馬達，則輸出功率較小。

通常鐵捲門所用的馬達則因為扭力的要求所需，大多選用單相交流馬達 [14][15]。而根據需求的不同，例如捲門的捲升速度、捲門的重量、馬達的體積等，可依上表選擇最適合的馬達來帶動捲門，表一中可明顯看到各種不同規格的馬達，一般市面上的捲門馬達透過一電磁開關與捲門控制器相連結，其配線圖可見圖 2-19。

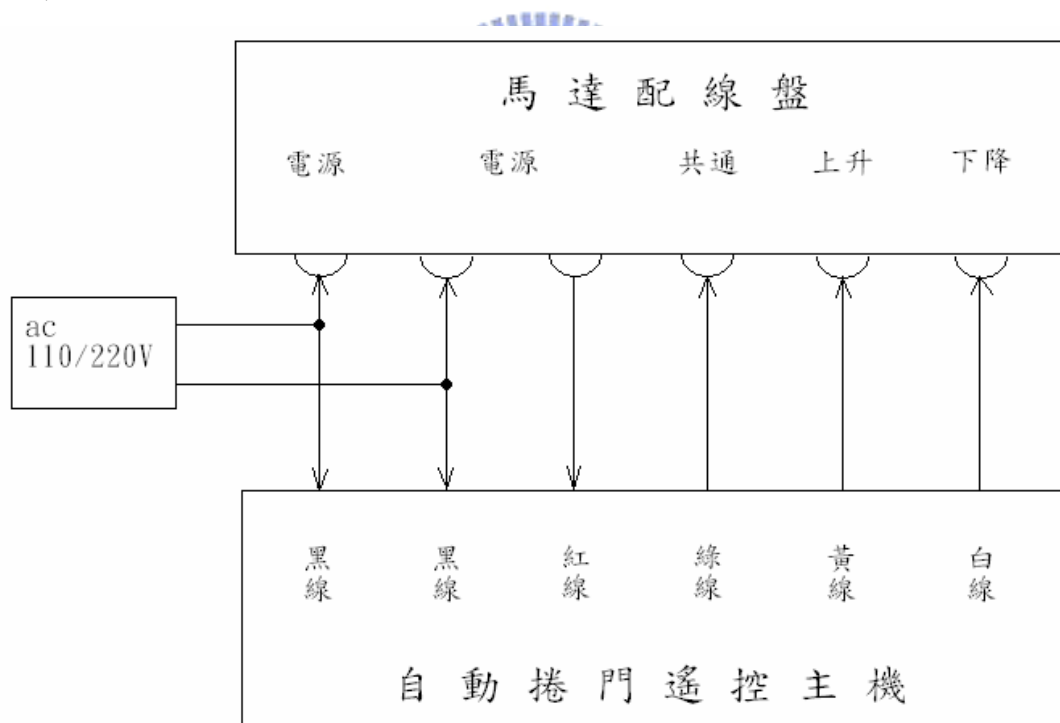


圖 2-19 自動捲門與馬達電磁開關配線圖

表 2-1 東元捲門機性能規格表

捲門機性能規格表					
型號	DS-30	DS-40	DS-50	DS-70	DS-100
輸出功率	150 W	220 W	350 W	550 W	750 W
出力輪轉速(r. p. m.)	35	35	35	28	17.5
架板:					
A. 規格	40	40	45	-	-
B. 齒輪(捲軸/馬達)	T50/T9	T50/T9	T50/T9	T50/T9	T52/T11
C. 鏈條	#530	#530	#530	#640	#640
D. 捲軸轉速:	5.2/6.3	5.2/6.3r	5.2/6.3r	4.5/5.3r	3.0/3.7
50/60HZ(R. P. M)	rpm	pm	pm	pm	rpm
最大捲揚能力	300 kg	400 kg	500 kg	700 kg	1000 kg
	4"	4"	5"	5"	6"
	(114Φ)	(114Φ)	(140 Φ)	(140Φ)	(165Φ)
	捲軸	捲軸	捲軸	捲軸	捲軸
最大高度	6.0M	6.0M	6.8M	7.5M	8.6M
馬達重量	12 kg	13 kg	15 kg	17 kg	40 kg



圖 2-20 東元馬達 DS30、DS70、DS100



第3章 自動捲門監控系統

現行的自動捲門遙控器工作形式大致上可分為二態、三態及滾動碼形式，各有優缺點，本文提出一綜合其優點並改善其缺點的自動捲門監控系統，及可用單晶片實行的技術，並實際應用在自動捲門上，本章將針對其內容進行介紹。

3.1 系統架構

在建購系統之前，我們必須要先了解系統的需求，才能針對希望解決的問題進行系統功能上的設計。在 2.4 節中提到了傳統的二態、三態編碼及基於 KEELOG 的滾動碼晶片 HCS300，根據之前的分析以及結合單晶片的特性，提出一具有滾動碼特性且使用上更具彈性及安全性的系統。

(1) 用一使用者自定碼取代出廠密鑰，功能相同，但可由使用者自行決定和更改，提升其使用上的靈活性。

(2) 加入一隨機數，此一參數在自動捲門監控系統每次完成動作後便自行產生，再透過無線通訊傳送到遙控器，再分別在遙控器及主機利用各項參數產生任證所需要識別碼及認證金鑰，彼此只透過無線傳輸傳送隨機數，可有效防止出廠碼和認證碼的外洩。

(3) 改進數據傳輸的方式，提高傳輸效率，利用半雙工的無線傳輸機制，使遙控器與捲門主機在數據傳輸上可更具安全性。

根據以上三點，主機產生的辨別碼不再受限於生產廠家和出廠碼的限制，可依使用者自行改變自定碼，增加了安全性及靈活性，考慮系統的升級和功能的擴展，故利用單晶片搭配其他軟硬體來實現整個系統。其中出廠密鑰、序列號、加密密鑰、隨機數均可按需要進行位元數的增加或減少。

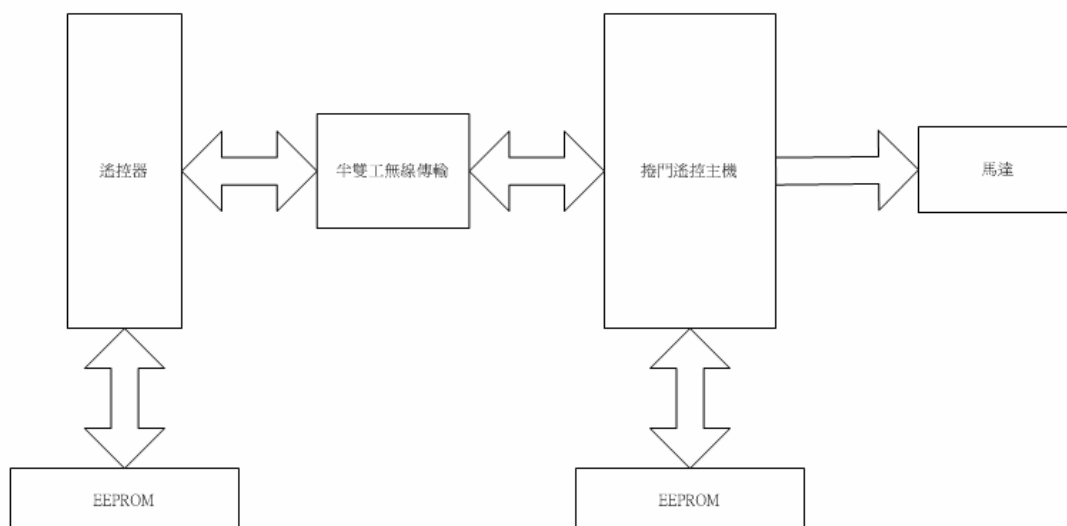


圖 3-1 自動捲門監控系統架構

整個系統分為用戶端（CLIENT）和主機端（SERVER），可見圖 3-1。當用戶端欲使用捲門功能時，須先透過遙控器送出認證要求，主機端收到認證要求後，根據所傳來的用戶序列號作判斷，通過認證後，主機端便開放權限供用戶端使用捲門之各項功能，在此段固定時間內，用戶端可自由送出指令來控制捲門的上下運作，到達指定的時間後，便視為一次的認證與遙控結束，此時主機端會送出一信號告知用戶端停止送出指令，並準備接收主機端所傳送的隨機碼，之後主機端與用戶端各自根據隨機碼執行新密碼的產生。

在使用者與捲門主機中，欲完成一次的認證及遙控捲門動作，必須通過兩次的識別碼認證比對及一次的認證金鑰比對，此舉可有效減少利用掃描密碼的方法使得門禁系統被破解的風險，認證金鑰則用來辨別是否為合法的使用者，且因用來產生新識別碼的計數器計數值、用戶識別碼均內建於捲門主機及遙控器上，並引進一隨機數，使得新識別碼的產生不易預測其編碼規則，當遙控器收到主機回傳的隨機碼後，便產生新的識別碼及認證金鑰，故無法在傳輸過程中攔截到新的識別碼及認證金鑰，但是透過半雙工無線通訊傳送有隨機碼被攔截的風險，考慮到這點，故再加上適當的無線通訊編碼機制，增加其傳輸位元長度，增加攔截及破解的難度。

3.2 系統規格

根據上一節的系統架構，我們瞭解了自動鐵捲門監控系統所需達到的要求，接下來，我們將針對這些要求提出實現的方法，茲對其內容介紹如下：

3.2.1 半雙工通訊機制

本系統中，一次完整的工作流程需要用戶端與主機端透過無線傳輸來作資料上的傳輸及溝通。用戶端利用無線傳輸來傳送認證過程中所需的兩組識別碼、用戶序列碼及專屬認證金鑰；主機端則利用無線傳輸來傳送認證是否通過之訊息，以及工作完成後傳送用來產生新識別碼及認證金鑰的隨機碼。

常見的無線傳輸模組可分為紅外線與無線電遙控兩種，紅外線遙控有空間上的限制，一般適用於家電產品控制上，例如電視、冷氣機等；無線電的使用距離較遠，應用範圍較廣，從遊戲用遙控賽車、汽機車遙控到防盜保全等不同領域都有廣泛應用。為了確保用戶端與主機端傳輸資料的準確性，吾人選用 TG-11 無線傳輸模組搭配 HT-12 編解碼晶片建立起無線通訊之機制以確保資料傳輸的正確性。為了避免互調現象產生，本系統所使用的兩組無線傳輸模組為半雙工模式，即同一時間內僅有一組發射器作用，且使用頻率不同。

TG-11 是組由發射器和接收器所組成的模組，若在沒有阻隔的情況之下，此發射接收電路可以發送超過 30 公尺以上的距離，但由於建築物的阻擋，使得無線電波並不如預期理想地傳送，且實際空間中充滿各式各樣的電磁信號，接收模組所收到的序列信號便容易受到雜訊干擾，為了確保收到信號的正確性，常搭配編解碼 IC 使用。其中 TG-11 系統特性如下[17]：

- (1) 具備 UHF 發射接收電路，可做無線電傳輸及控制等相關應用。
- (2) 搭配編解碼 IC，不易受外界雜訊干擾。
- (3) 可搭配 DIP 開關裝置或單晶片輸出接腳來調整密碼設定。
- (4) 頻率範圍從 300MHz 到 434MHz。

TG-11 無線收發模組的外觀與相關接腳說明可見圖 3-2 與圖 3-3。詳細特性則

請參閱製造廠商所提供的產品資料手冊[18]。

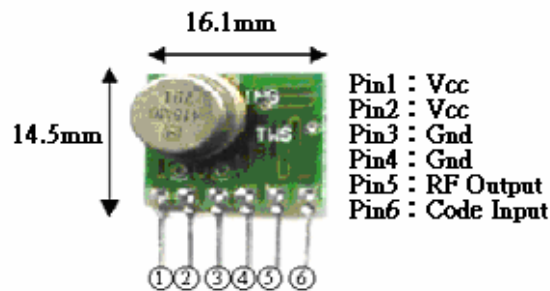


圖 3-2 發射模組外觀與接腳說明

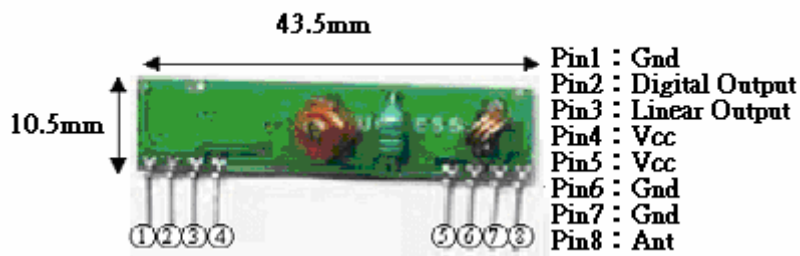


圖 3-3 接收模組外觀與接腳說明

而 HT-12[19] 為一系列編解碼 IC，吾人選用 HT-12D 作為解碼 IC，而 HT-12E 作為編碼 IC，HT-12D 與 HT-12E 的主要特性如下：

- (1) 應用 CMOS 技術，具有省電、防雜訊等優點。
- (2) 工作電壓在 2V~12V。
- (3) 內含振盪電路，只需外加一只電阻即可提供工作頻率。
- (4) HT-12E 編碼 IC 可以有 $2^8 = 256$ 組密碼設定，並可傳送 4 個位元資料。
- (5) HT-12D 解碼 IC 具有 4 位元資料輸出，8 位元密碼設定，輸出資料具有拴鎖功能。

HT-12E 編碼 IC 的接腳說明如圖 3-4 所示，A0~A7 是 8 位元的密碼設定，總共有 256 種不同的組合；D0~D3 是資料輸入位元；DATA OUT 是資料發送端。

**8-Address
4-Address/Data**

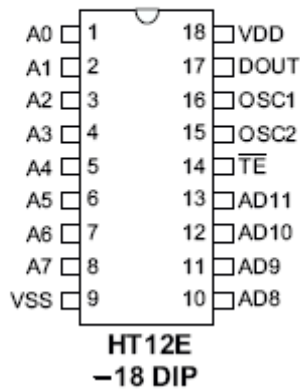


圖 3-4 HT-12E 編碼 IC 接腳圖

HT-12D 解碼 IC 的接腳說明如圖 3-5 所示，A0~A7 是 8 位元的密碼設定，總共有 256 種不同的組合；D0~D3 是資料輸出位元；DATA IN 是資料接收端。當 HT-12D 與 HT-12E 搭配使用時，使用單晶片的輸出接腳來動態設定 A0~A7 所須輸入的密碼，當兩者密碼一致時，HT-12E 所傳送的 4 位元資料會出現在 HT-12D 的 D0~D3 接腳上。



**8-Address
4-Data**

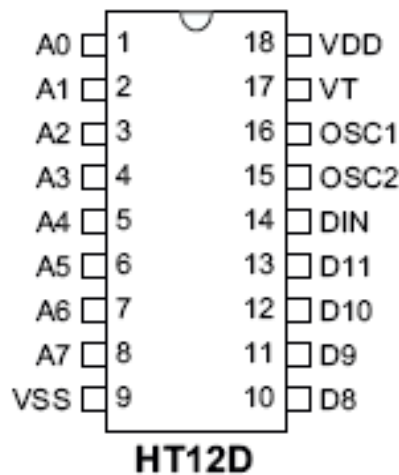


圖 3-5 HT-12D 解碼 IC 接腳圖

3.2.2 認證機制

認證流程為使用者先送出認證的要求，透過無線傳輸機制送出共一十六BITS的訊號，前八BITS為辨別碼，後八BITS則為4BITS的使用者序列碼及認證金鑰，若辨別碼正確，則捲門主機將根據所收到的使用者序列碼，作認證金鑰比對的查驗，若正確，視為認證通過，則在一定時間內開放使用者權限以控制捲門的運作，稱為可操作時間，其長度可由使用者依需求自行設定，由數十秒到數分鐘不等，透過一LED作為輸出介面。

進行認證時，主機端先根據所傳來的使用者序列碼從EEPROM中取出相對應的使用者認證金鑰，再與所收到的認證金鑰作比對，若正確，便送出一認證通過信號回傳用戶端，之後主機端便根據所收到的功能碼去執行使用者的要求，完成動作後，若主機端在接受指令的時間內，發現有辨別碼不正確的情形則有系統故障或遭密碼掃描之風險，便送出警告信號。

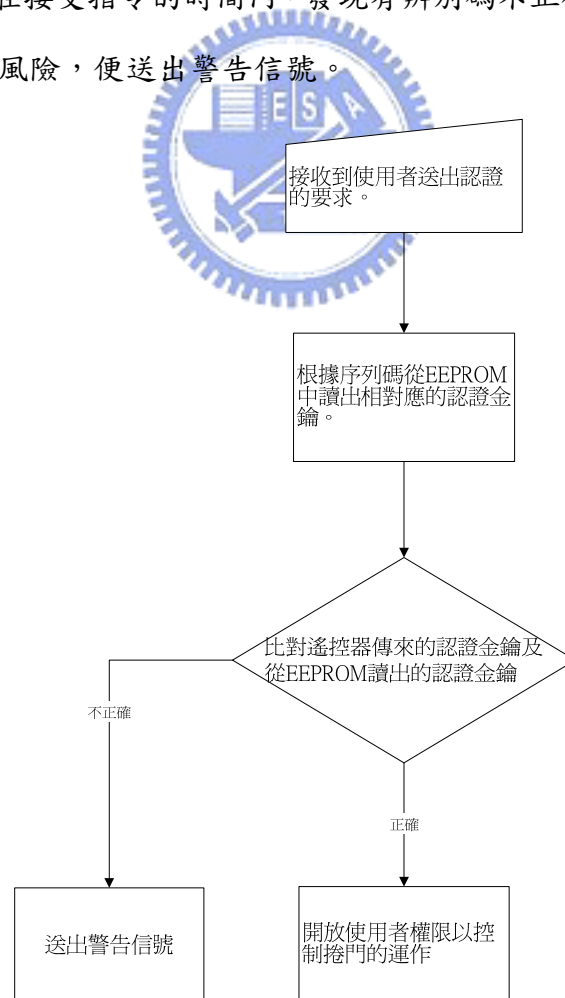


圖 3-6 認證機制流程圖

3.2.3 隨機數產生機制

隨機數是利用單晶片的計數機制產生，有兩種方法供選用：第一種為當單次操作完畢後，計數器一直不停地計數，在外界對它進行再次操作或者要發送數據時停止計數。因為外界的操作或發送的時間是不定的，所以計數暫存器裡面的數是隨機的；第二種方法則為對按鍵或操作時間進行計時。用戶每次按鍵或操作的時間都是不定的，並且按鍵從抖動到穩定的時間也是不定的，對它進行計時，如果把間隔的時間取得合適，即可得到近似隨機數。

3.2.4 加密機制

在本文所提出系統中，主要利用一用戶自定碼(8bit)配合使用者序列碼(4 bit)及隨機碼(8bit)作運算產生兩組識別碼(8BIT)及認證金鑰(4BIT)。主機端再將隨機產生的隨機碼，透過半雙工無線傳輸將產生的隨機碼傳到遙控器上作密碼的同步更新；利用主機內部的計數器、用戶碼及隨機碼產生兩組識別碼(8BIT)及一組認證金鑰(4BIT)，其中一組識別碼及認證金鑰使用在下次的認證程序上，另一組識別碼則使用在下次認證通過後，用來送出動作指令的識別碼。

透過適當的運算及搭配隨機數，可以確保每次工作完成後，密碼會自動變化，且不與前次工作之識別碼及認證金鑰重複，可有效降低因為掃描密碼而帶來的安全性風險；加入了用戶自定碼，使用者可透過修改用戶自定碼來改變識別碼及認證碼產生的規則，搭配隨機碼，可使每次產生的識別碼及認證金鑰不易觀察出其規則，增加了破解的難度。

3.2.5 自動捲門馬達控制

在 2.5 節中，吾人知道，若要控制自動捲門馬達的轉向，只需利用控制電磁開關即可，常見的方法則為送出一脈衝信號來控制 MCF 及 MCR 的開關與否，根據各電磁開關規格不同，脈衝信號長度也有不同限制，本文所送出的信號則為 450ms，見圖 3-7。

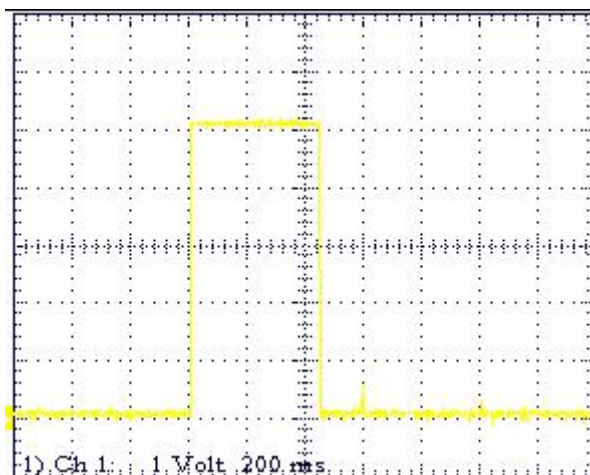


圖 3-7 脈衝信號寬度

3.2.6 紅外線感測功能

吾人利用紅外線發射器及紅外線接受器 TSOP4838 在自動捲門前後兩側實現感測功能，設定為當捲門落下時，便自動偵測是否有異物在捲門下方，或者是有人意圖在捲門落下時潛入，若有異常情況時，便送出警告信號，並停止捲門運作以策安全。



3.3 功能實現

根據在 3.2 節中所提出系統各功能，我們瞭解了自動鐵捲門監控系統所需具備的功能，接下來，我們將針對這些系統功能做更深入的介紹並實際實現之，茲對其內容介紹如下：

3.3.1 半雙工通訊功能實現

本文是在單晶片上裝設五個按鈕開關，一個為認證要求開關，另四個則為捲門動作指令。當認證通過後，主機允許使用者送出要求，此時先將所輸入的信號透過單晶片的編碼，在控制信號之外加入 START BIT 及 END BIT，再傳到 HT-12E 的 AD8~AD11 上，之後透過無線收發模組來控制 HT-12D 的資料腳位輸出 (Pin10~Pin13)，呈現高低電位信號，每次傳送 4 位元的控制信號，加上其他應用電路，便可達到無線遙控功能。而在用戶端與主機端的資料互傳方面，則建立一同步機制，以確保資料的傳輸正確。

本文以單晶片搭配無線電收發模組電路之基本工作原理來實現半雙工的無線傳輸機制。在發射端，利用單晶片控制編碼 IC 的 \overline{TE} 腳位狀態，決定何時將 8 位元密碼與 4 位元資料進行編碼組合後一起以串列方式傳送出去；在接收端，單晶片判斷解碼 IC 的 VT 腳位何時為高電位或低電位，高電位時，表示前 8 位元的密碼正確，接著讀取後 4 位元資料，低電位時表示密碼錯誤，並將前一次 4 位元資料拴鎖住，等待下一次動作。搭配單晶片與程式判斷，一次資料的發射與接收便能有 $2^4=16$ 組訊號。加入了編碼機制後，更可以程式實現傳送多組資料。

發射模組電路圖可見圖 3-8，由於本系統使用了兩組 TG-11 來實現遙控器與遙控主機的半雙工無線通信，為了避免出現交調現象，分別使用 315MHz 及 405MHz 頻率的發射模組。HT-12E 為編碼 IC，其 Pin1~Pin8 可連接 DIP 開關，調整 JUMP 來設定密碼，在本系統中則是連結到單晶片的輸出接腳，在每次完成動作之後，由單晶片設定密碼，當發射模組與接收模組的密碼設定相同時才能進行收發動作；HT-12E 編碼 IC 的 Pin10~Pin13 是控制訊號輸入腳位，接收外部 ON/OFF 訊號。

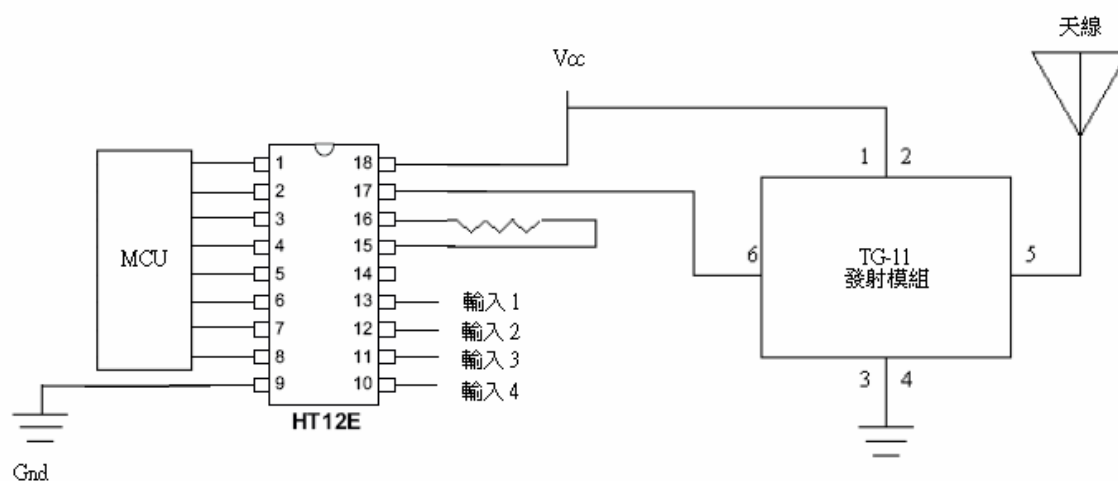


圖 3-8 發射模組電路圖

接收模組電路圖可見圖 3-9，遙控器與遙控主機分別使用 315MHz 及 405MHz 頻率的接收模組，搭配 HT-12D 為解碼 IC，其 Pin1~Pin8 連接到單晶片的輸出接腳，當發射模組與接收模組的密碼設定相同時才能進行收發動作；HT-12D 解碼

IC 的 Pin10~Pin13 是控制訊號輸出腳位，隨著發射端的訊號產生不同的動作，如高或低電位。

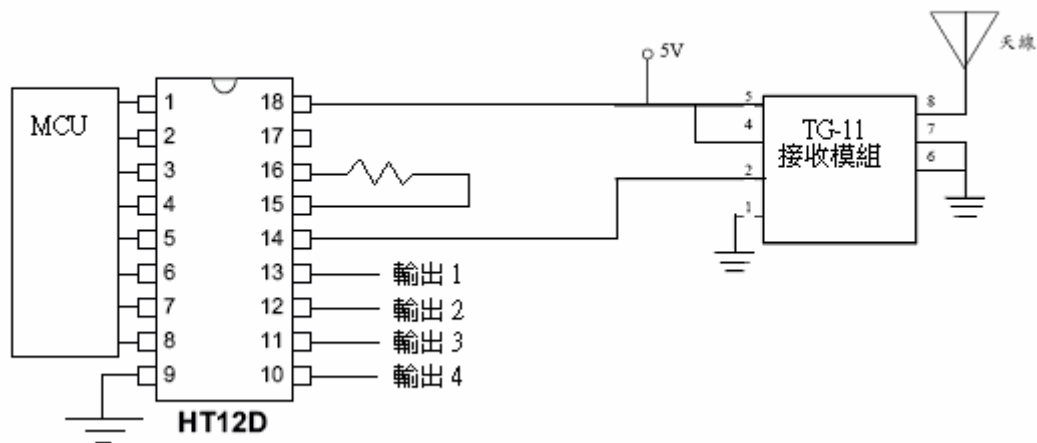


圖 3-9 接收模組電路圖

當吾人欲傳輸資料時，便將 \overline{TE} 腳位設為 LOW，使用 HT-12E 將欲送出的四位元資料連同所設定的辨別碼透過 TG-11 送出一筆共 12 位元長的序列資料，內容為前 8 位元的辨別碼加上後四位元的傳送碼，當接收端的 HT-12D 其辨別碼與收到的 8 位元辨別碼一致時，此時 HT-12D 的 VT 腳位為 HIGH，再將所收到的 4 位元輸出。但是在本系統中，一次完整的傳輸中，資料內容有 8 位元，所以加入了曼徹斯特編碼技術，在 4 位元傳送碼的部分，加入了起始位元及結束位元，利用軟體來判斷所收到的資料順序，便可實現傳輸 8 位元或以上的資料，見圖 3-10 及圖 3-11。

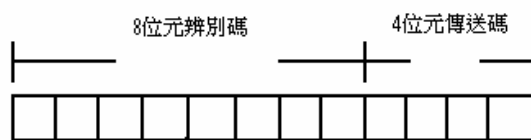


圖 3-10 HT12E 資料傳送格式

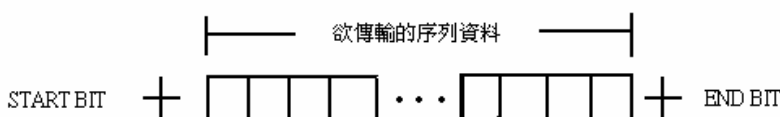


圖 3-11 資料編碼示意圖

3.3.2 認證功能實現

進行認證時，首先等待使用者按下認證指令，確認按下之後，便從 EEPROM 中讀出所需要的兩組識別碼、使用者序號、一組認證金鑰，之後透過半雙工的傳輸機制，傳送出〔識別碼 + 使用者序號〕及〔識別碼 + 認證金鑰〕，遙控器端送出認證所需的資料如使用者序列碼及認證金鑰，主機端再根據所傳來的使用者序列碼從 EEPROM 中取出相對應的使用者認證金鑰，再與所收到的認證金鑰作比對，若正確，便送出一認證通過信號回傳用戶端，之後主機端便根據所收到的功能碼去執行使用者的要求，其流程圖可見圖 3-13，完成動作後，若主機端在接受指令的時間內，發現有辨別碼不正確的情形則有系統故障或遭密碼掃描之風險，便送出警告信號。若認證通過則在一定時間內開放使用者權限以控制捲門的運作，稱為可操作時間，其長度可由使用者依需求自行設定，由數十秒到數分鐘不等，透過一 LED 作為介面，本文則設定為 35.8Sec。

為了避免同時按上或下時，造成電磁開關發生短路的情形，利用軟體偵錯，當馬達為停止狀態時，可接受往上或往下運轉的指令；但若已經往上或往下運轉時，則只能接受停止的指令，避免出現短路的情況。

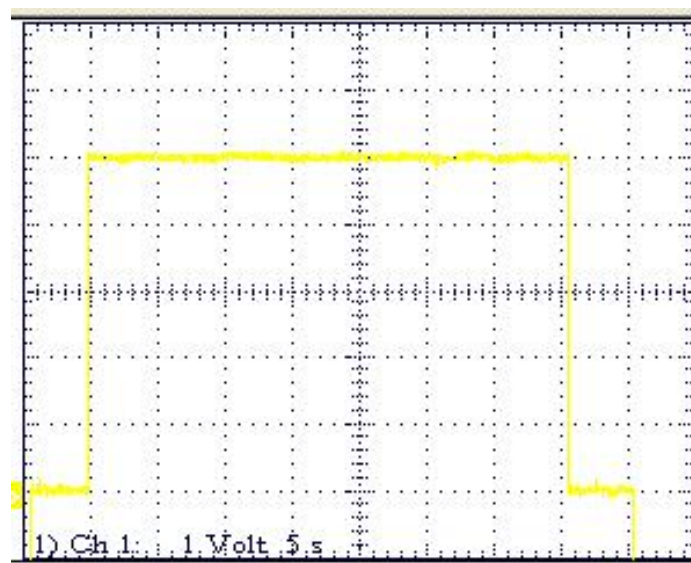


圖 3-12 操作時間示意圖

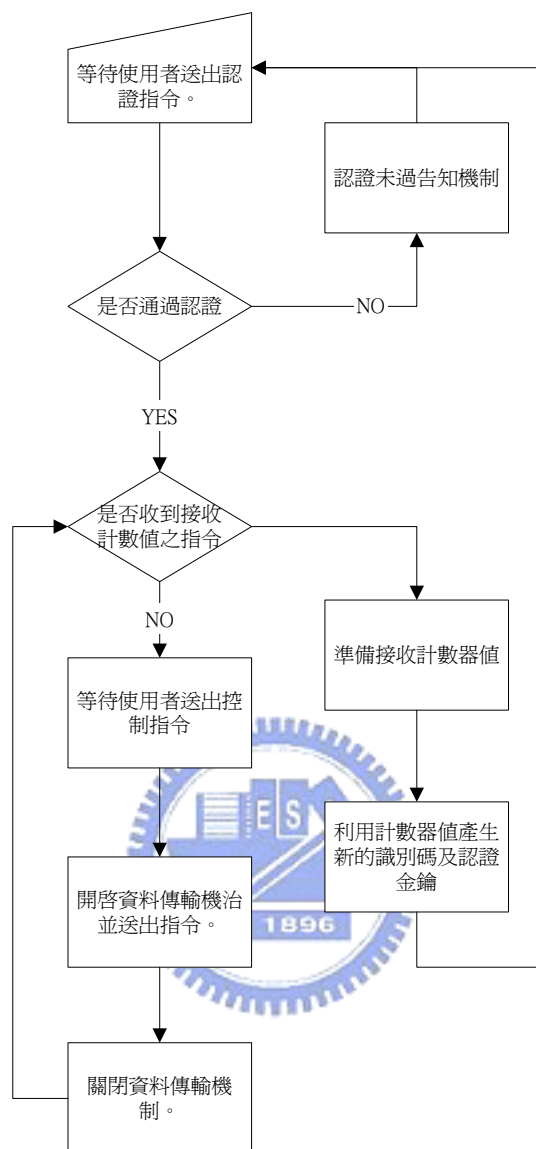


圖 3-13 認證機制工作流程圖

3.3.3 隨機數功能實現

本文選用之前所提到的第二種方式，選定適當的間隔時間作為時間單位，當使用者透過遙控器通過認證之後，捲門主機開放權限在操作時間之內，可任意輸入指令，此時便利用該時間單位來計數共收到幾次指令以作為一隨機數。

3.3.4 加密機制功能實現

本系統所使用的單晶片其內部暫存器為 8 位元架構，在運算時，需先將 4 位元的資料如認證金鑰化為 8 位元方便處理，見圖 3-14，在過程中，會多出四

Bit 的資料，則此四 BIT 分別寫入 0 或 1 亦會影響最後產生的新識別碼及認證金鑰，例如原資料為 AAAA，轉為 8 位元後可成為 0A0A0A0A 或 A1A1A1A1，透過簡單的 XOR 運算便可產生相當多的變化。之後再對所有的資料分次進行運算，產生出新的識別碼及認證金鑰，見圖 3-15。

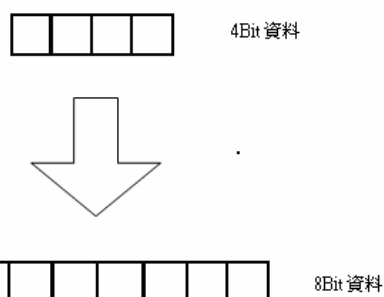


圖 3-14 4 位元轉 8 位元資料格式

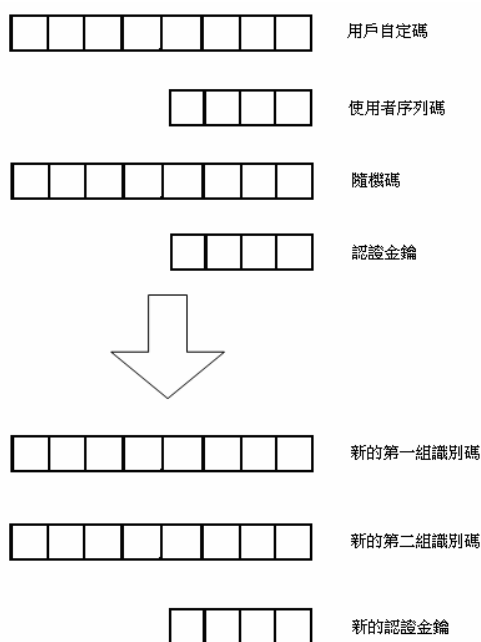


圖 3-15 識別碼與認證金鑰運算示意圖

3.3.5 紅外線感測功能實現

透過在自動捲門前後佈置兩組紅外線收發器，使得我們可判斷使用者之進出行為，亦可在自動捲門落下時，判斷是否有人或異物在捲門下方，以免造成意外；透過紅外線的偵測機制，亦可避免不肖歹徒趁捲門落下之空檔尾隨使用者進入，

成為一個使用上的盲點。

針對以上可能情形，利用軟體來判斷紅外線接受器所回傳信號，其流程圖如圖 3-16 所示，當捲門為落下狀態時，便自動開啟偵測機制，以達到吾人對於安全性的要求。

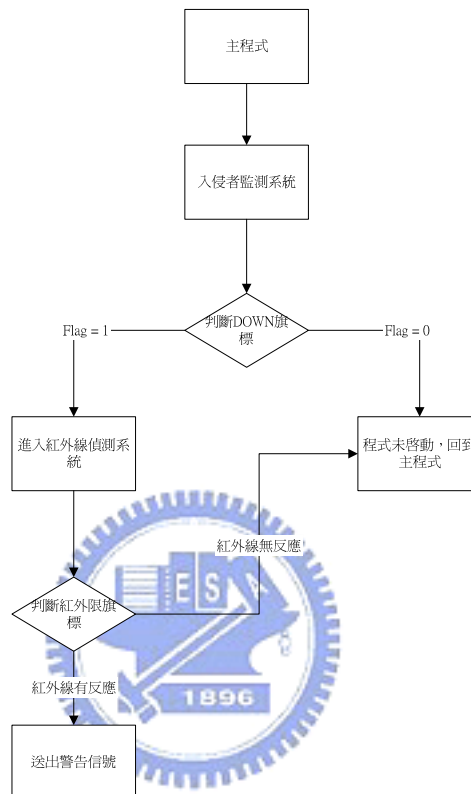


圖 3-16 紅外線偵測機制流程圖

3.4 系統整合

我們將對 3.3 中所提出的各項功能作一整合，並提出完整的系統工作流程圖。在確立了半雙工的資料傳輸機制後，配合所提出的結合二態及滾動碼的加密方式，以及軟體偵錯，提出了完整的遙控器與遙控主機的工作流程，見圖 3-17 及圖 3-18。

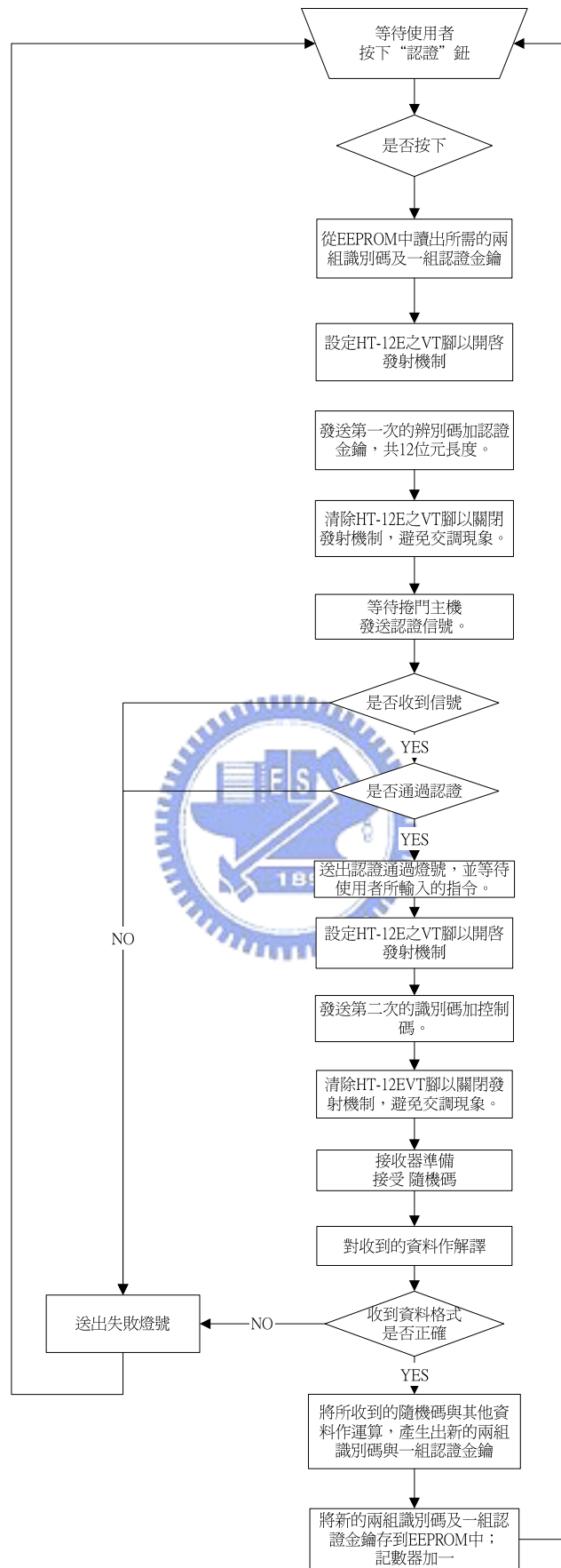


圖 3-17 遙控器工作方塊圖

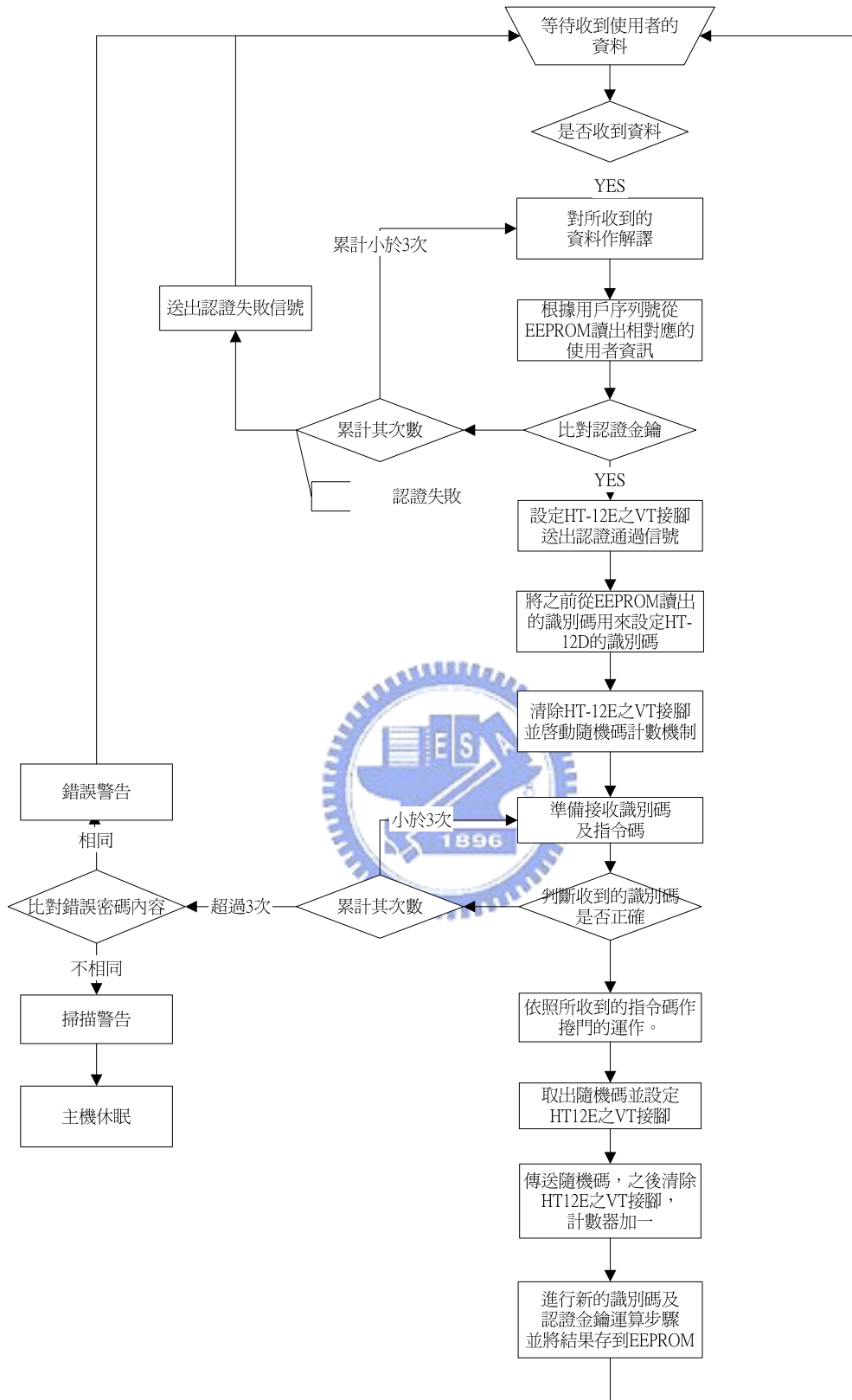


圖 3-18 捲門主機工作方塊圖

在單晶片的使用上，吾人所使用的微控制器系列是由美國 MICROCHIP 公司所開發生產的 8 位元單晶片微電腦。PIC 是一個採用精簡指令架構，易學易用輸入輸出介面功能強的 8 位元單晶片微電腦。基本上 PIC8 位元微控制器的分類根據指令位元數的大小可分為三類，基本型的指令為 12 位元(編號 PIC12CXX、16C5X)、中階型的指令為 14 位元(編號 PIC16C6X、16C7X、16F87X)以及高階型的指令為 16 位元(編號 PIC17CXX、18Cxx、18FXX2)。PIC 微控制器各個系列單晶片雖然在功能、記憶體大小及接腳個數上略有不同，其內部架構及指令集卻是大同小異[20][21]。

在本系統中，考慮功耗、週邊功能的擴展等需要，本系統選用 MICROCHIP 的 PIC18F452 單晶片，40-PIN DIP。PIC18F452 採用 HARVARD 電腦的架構，精簡指令集(RISC)，共有 75 個組合語言指令，且大部分的指令皆固定為 16 位元的字元(Word)以及少部分的指令為 2 個 16 位元字元，64K 的 EEPROM，工作時脈最快可到 40MHZ。

在程式的開發方面，吾人使用的工具是美國 Microchip Technology Inc. 所發展的一套微處理控制器軟體：MPLAB IDE 以研製作業平台，它架構於 Windows 的作業環境；對使用者而言，MPLAB IDE 展現出優越的多視窗的除錯環境，可協助使用者迅速找出程式錯誤之所在。

MPLAB IDE 是一套整合式的發展平台，在 MPLAB 的架構下它提供多視窗文字編輯功能，使用者可直接在 MPLAB 環境下直接撰寫、修改原始程式(Source Code)，同時使用者也可以直接啟動語言工具(Language Tools)進行 C 的編譯(Compiler)或組譯(Assembler)工作，產生微處理機可執行的 HEX 檔(INTEL' s HEX Format)。使用者可依實際的除錯環境來選擇使用何種硬體模擬或軟體模擬方式來除錯，最後使用者可直接啟動 MPLAB 的燒錄功能來燒錄 PICmicro，完成此設計案；以上為使用微處理架構的單晶片時不可欠缺的步驟，透過 MPLAB 的整合從最初的程式撰寫到最終的燒錄都可一氣呵成無須跳出 MPLAB 的視窗。



圖 3-19 MPLAB 整合式的發展平台

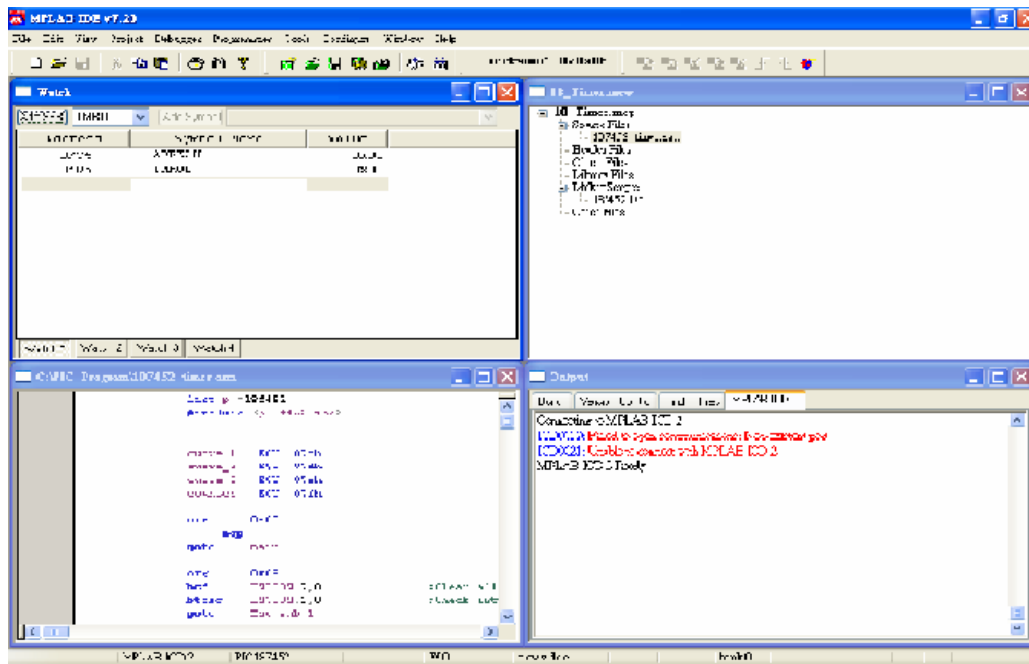


圖 3-20 MPLAB 開發環境。

第4章 自動捲門監控系統驗證

根據第三章所提出的架構，吾人實現了自動捲門監控系統，見圖 4-1，包含使用者端的遙控器及自動捲門監控系統主機，接下來將利用此一系統來作各項功能的驗證。

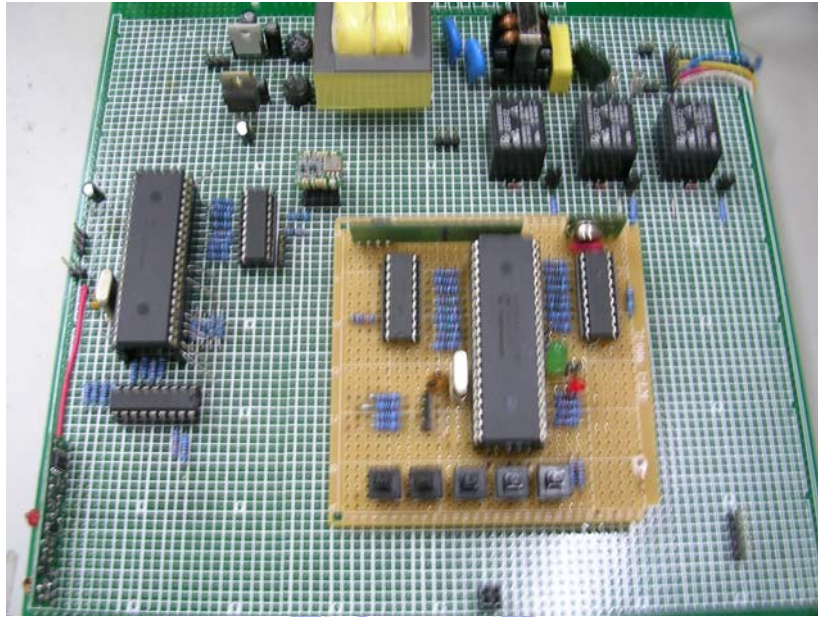


圖 4-1 自動捲門監控系統

4.1 資料傳輸

考慮到使用環境的問題，無線電波傳輸效率並不如預期理想，且實際空間中充滿各式各樣的電磁信號，接收模組所收到的序列信號便容易受到雜訊干擾，為了確保收到信號的正確性，本系統使用 HT-12D、HT12E 編解碼 IC 及 TG-11B 無線傳輸模組實現資料的傳輸，故在設計主機端與使用者端的通訊機制時，便需考慮到上述硬體之特性作設計。HT-12D 及 HT-12E 為了確定資料傳輸正確，且避免雜訊影響，對於一信號的處理需累積多次重複收到才視為一正確信號，故其信號之發送週期較長，見圖 4-2，其週期約為 20ms。了解這點後，在主机端與使用者端的通訊機制時，一次資料的傳送便必須大於 20ms 以符合 HT12 之硬體限制，無線收發模組才可順利工作，吾人在資料的發送時，以 200ms 為基本單位，

即每次發送單筆資料 10 次，在資料的接收端，則同步接收，且須接收到 3 次以上才視為正確的資料。其中每一筆的資料本身共 13 個位元，可見圖 4-3，一長時間連續 LOW 的信號與第一個信號組成起始位元，第 2 到第 9 位元則為辨別碼，第 10 到 13 位元則為指令碼。

而因發射端與接收端的信號傳遞必有一時間延遲，故吾人建立一同步機制，以確保不會誤判傳輸資料。首先在主機端與用戶端先定義一相同的傳送時間，當傳送資料時候，先送出起始位元，接收端收到起始位元後，則開始計數其長度，達到所定義傳送時間之 80%時，則判斷正確，之後便開始讀取所傳送的資料，當收到結束位元後，便回傳訊號告知發送端資料讀取已結束。

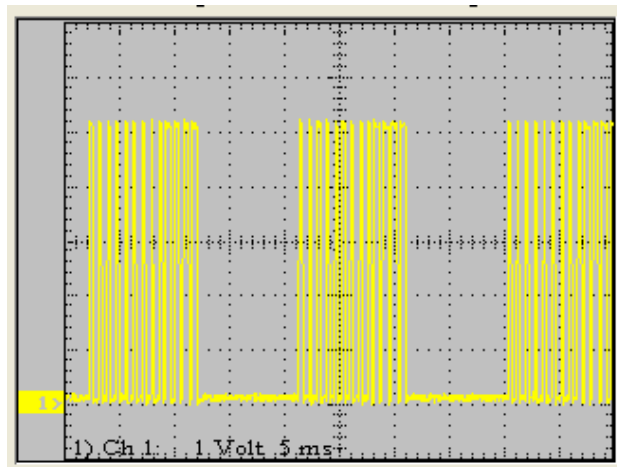


圖 4-2 資料傳輸波形週期

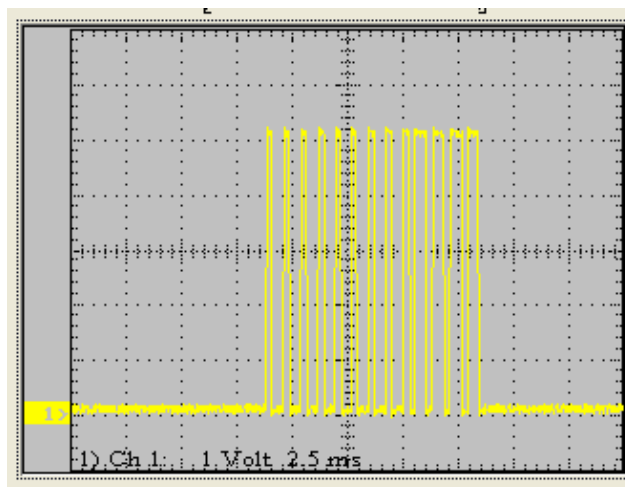


圖 4-3 資料傳輸內容圖

4.2 認證機制

當使用者按下認證鈕後，會送出兩筆資料，第一筆資料為 8 位元的識別碼及 4 位元的用戶序列碼，共送 10 次，再進行第二筆資料的發送，前 8 位元為與前筆資料相同的識別碼，後 4 位元則為認證金鑰，認證金鑰與辨別碼共同組成一 12 位元的資料可用來當作密碼識別，有效增加了辨別碼長度到 12 位元，共 4096 組。發送完畢後便等待主機端的回傳信號，根據認證成功與否，透過 LED 燈傳遞資訊給使用者，如圖 4-5。

主機端收到認證要求時，會根據所收到的使用者序列號從 EEPROM 中讀出所對應的認證金鑰，此時認證金鑰與辨別碼共同組成一 12 位元的資料，再與先前所收到使用者傳來之認證金鑰作比對，若正確，則視為認證通過，送出相對應的認證信號；若否，則送出認證失敗信號。

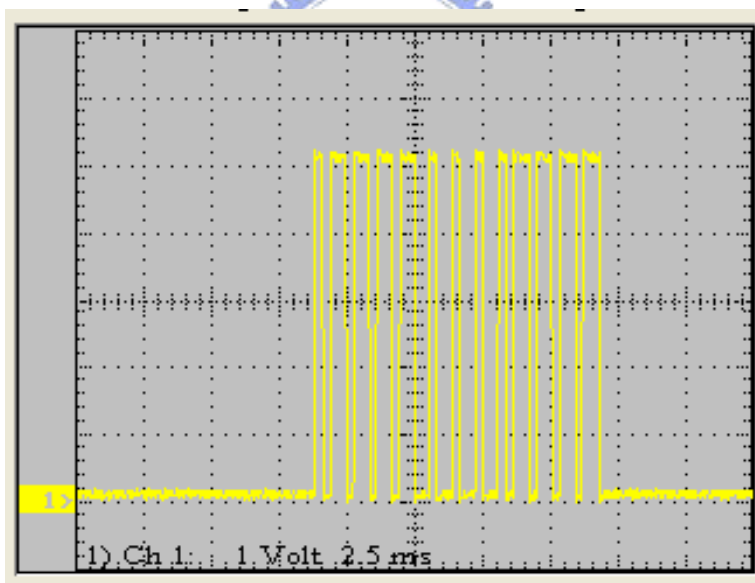


圖 4-4 送出的認證資料波形圖

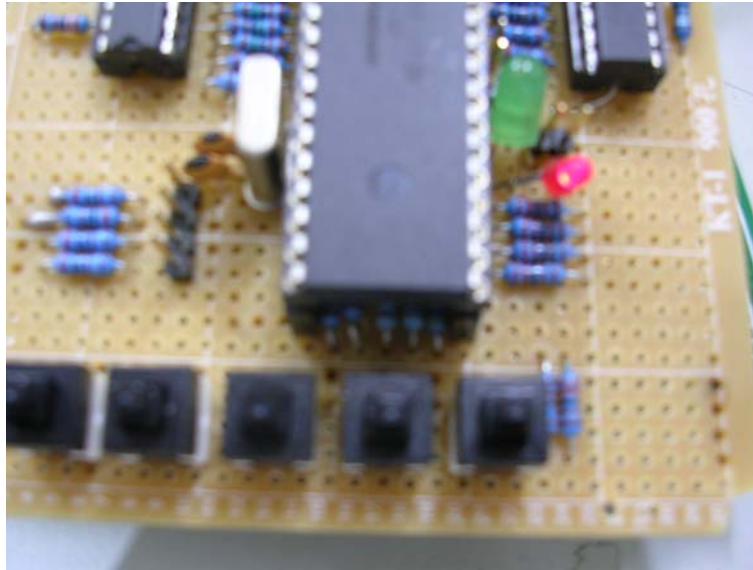


圖 4-5 認證通過介面：LED 燈號

4.3 隨機碼

認證通過後，遙控器上的 LED 會持續點亮，已告知使用者可在 LED 熄滅前的這段時間內，可任意送出捲門遙控要求。自動捲門主機根據使用者按下按鈕時間長短來作計數，其示意圖可見圖 4-6，不同時間長度的捲門遙控要求代表不同的計數值，當限定時間結束後，便會透過資料傳輸機制，將所計數之值回傳到遙控器上作各項資料之更新。

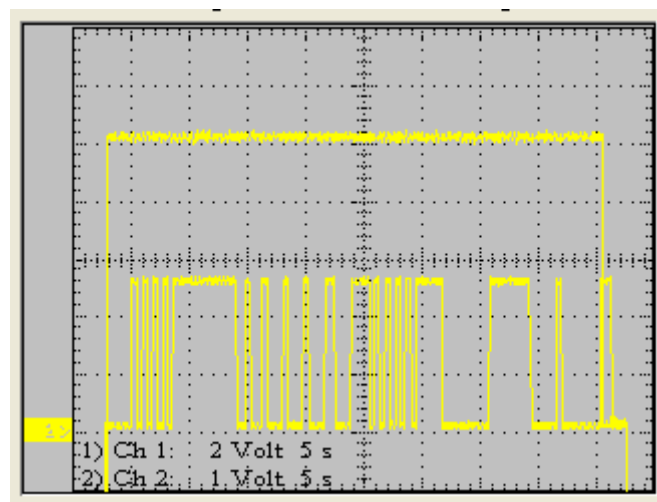


圖 4-6 捲門可遙控時間與計數機制示意圖

4.4 驗證碼與認證金鑰

在本文中，認證金鑰與驗證碼的產生是利用計數產生的隨機碼與相關資料作乘法的運算再透過位移及互斥或的作用而產生。認證碼的實際操作可見表 4-1，在同一使用者輸入同一指令，不同時間長度，連續八次使用下得到表 4-1 的結果，考慮到計數器為 8 位元，當計數值到達 255 時，便會回到 0，而 00000000 跟 11111111 在運算上相當單調，容易使得識別碼出現重複的情形，吾人針對此種情況再適當改正密碼產生的方式，見表 4-2。

產生新識別碼後，再與原識別碼作比較，若相等，則將新識別碼作往左一位的資料移動，若又相等，則再移動一次，務求新舊密碼不完全重複。若左移八次後，發現仍相等，則代表資料為 00000000 或 11111111，此時則針對特列作修正，得到表 4-2 之結果。

認證金鑰之產生亦如同識別碼產生之方式，但因為認證金鑰僅為 4 位元，重複率較高，見表 4-3。

雖然 8 位元單晶片限制了識別碼之長度，但透過每次正常工作需經過一次認證金鑰及兩次識別碼的檢驗，且每次工作完畢，便自動更新，提高了系統的安全性，使其不易因密碼掃描而遭人破解。為了不使加密規則外洩，加密流程利用兩 8 位元數相乘得到 16 位元長度的新識別碼或認證金鑰，如此便不易藉由紀錄識別碼而破解加密規則，因有 8 位元的資料是不外洩的。

當使用者感覺有加密規則外洩的疑慮時，便可藉由改變使用者自定碼與產生的隨機數作 XOR 的動作，以改變加密規則。

表 4-1 連續 8 次操作的識別碼變化

次數	識別碼	00001111	識別碼變化率
1		10110100	75%
2		11111111	50%
3		00000110	75%
4		10111101	75%
5		11010100	50%
6		01100111	62.5%
7		11111111	37.5%
8		00000111	62.5%

表 4-2 修正規則後，連續 8 次操作的識別碼變化

次數	識別碼	00001111	識別碼變化率
1		00110001	62.5%
2		00001010	62.5%
3		01111011	50%
4		11111111	25%
5		01001010	62.5%
6		00111110	50%
7		00001001	62.5%
8		11001000	37.5%

表 4-3 連續 4 次操作的認證金鑰變化

次數 \ 認證金鑰	0010	認證金鑰變化率
1	1010	25%
2	1110	25%
3	1000	50%
4	1010	25%

4.5 紅外線監控系統

利用在自動捲門之前後兩側設置一組紅外線感測系統，可有效判斷當捲門落下時，其正下方是否有人或異物，減少誤傷人員的機會，可見圖 4-7。

兩組紅外線分別連接到單晶片的接腳中斷，預設信號為 LOW，若有人經過紅外線感測區域時，則變為 HIGH，進而引發接腳中斷。吾人可知，若在鐵捲門落下時，若有人欲尾隨進入，則必將觸發兩組紅外線感測器所對應之接腳中斷，且有其先後順序，故可判斷是否有人尾隨進入。

實測時發現，紅外線收射器與接收器之距離會影響其判斷的正確性，且使用的紅外線無法判斷是人或動物，且只有兩組紅外線感測器的數目對於若同時有多人進出自動捲門，則會有誤判的情形發生。

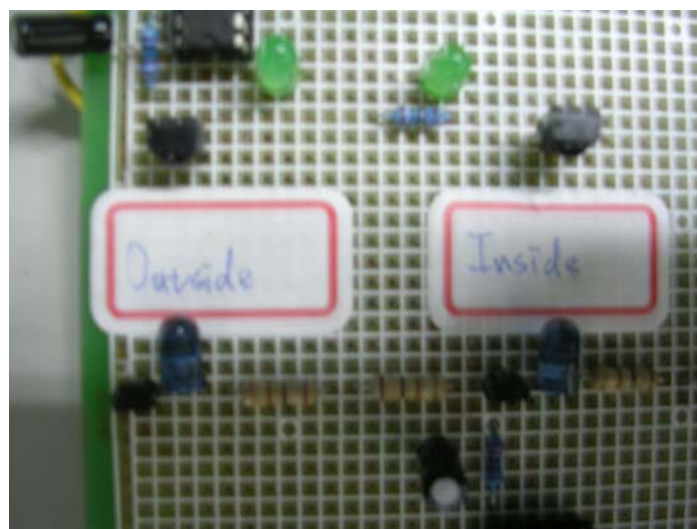


圖 4-7 紅外線感測系統

4.6 電磁開關與馬達驅動

當使用者通過認證並開始傳送捲門遙控指令時，主機端便根據所收到的指令作軟體偵錯，避免發生電磁開關的 MCR 及 MLR 同時導通，使得單相直流馬達發生短路之情況，嚴重時可能燒毀馬達並引發火災造成人員傷亡及財產的損失。

電磁開關工作之情形可見圖 4-8、圖 4-9 及圖 4-10



圖 4-8 電磁開關關閉，馬達不運作

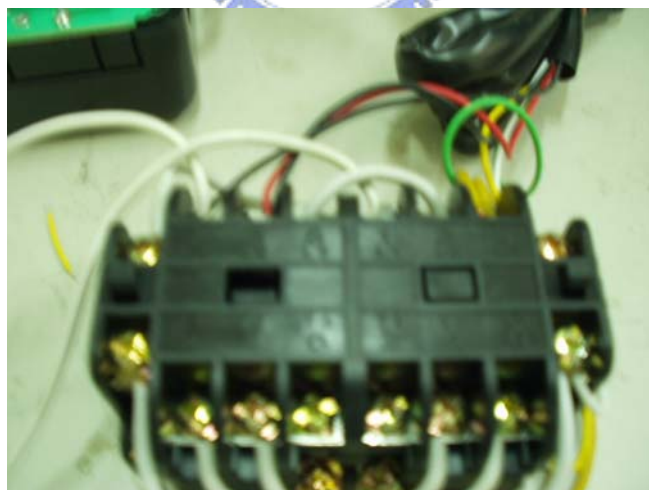


圖 4-9 電磁開關運作使得馬達正轉

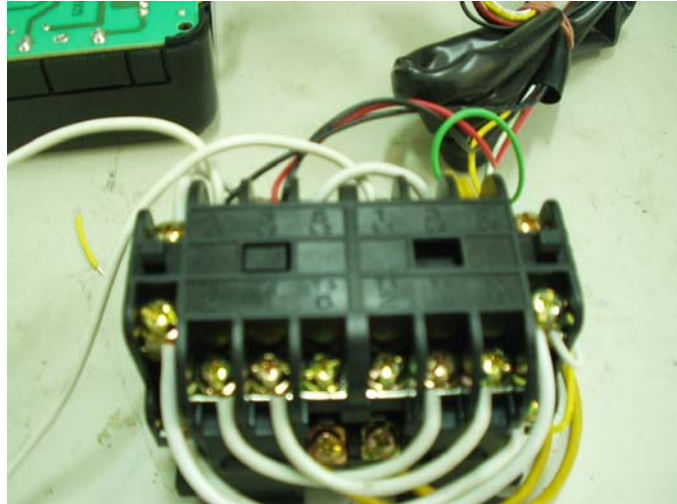


圖 4-10 電磁開關運作使得馬達反轉



第5章 未來展望

5.1 結論

本文提出一綜合傳統二態編解碼與滾動碼之系統，並用單晶片實現之，識別碼的變化每次工作結束後則有明顯的變化，對於自動捲門應用在門禁系統上的安全性，有一定程度的提升，然而受限於所使用的硬體，其密碼組數仍有過少的隱憂，之後可使用較高階的單晶片或者是嵌入式系統以改善此一問題。且由於使用的單晶片暫存器為 8 位元大小，識別碼的產生是 XOR、AND 或取補數等步驟而產生，運算過程較為簡單，雖能達到隨機改變識別碼的功能，但仍略嫌不足，若能搭配高階晶片及使用對稱加密或非對稱加密(RSA)作為加密方式，可使安全性更為完善。

在資料的傳輸上，透過 HT-12 需要一定的傳輸時間，在傳輸的效率上顯得過於耗時，且用 ASK 做調變，所以很容易受干擾，一般用編解碼 IC 大多是單純的啟動與停止，只傳送 4bits 的資料，而且它是傳送非常多的訊號，接收端才接收到，可見干擾之多，所以若要做有效率數據傳輸，須拿掉編解碼 IC，自己在程式中再做防干擾的動作，今後可在此方面加強，以提高系統之反應速度。

5.2 未來展望

本文提出的隨機加密系統概念亦可推廣在無鑰進入領域的應用，特別適合應用於無線傳輸領域的小型系統的數據加密，並與數位門禁系統作整合。

隨著射頻技術、無線技術和藍芽技術的發展，射頻卡身份證的實施，其應用領域可以擴展到身份識別、安全管理、防盜報警、考勤、收費、無線抄表、智慧監控、隨機檢測器、標識資訊等諸多領域。

參考文獻

- [1] 蘇峰儀，數位監控系統的設計，義守大學資訊工程研究所碩士論文，2003。
- [2] 黃泰祥，具備人臉追蹤與辨識功能的一個智慧型數位監視系統，中原大學電子工程研究所碩士論文，2004。
- [3] 藍嘉華，無線網路技術應用於門禁系統的研究與實作，中央大學資訊工程研究所碩士論文，2004。
- [4] 蔡博智，影像追蹤方法應用在監控系統的研究，中原大學機械工程研究所碩士論文，2002。
- [5] 簡健州，網際網路遠端監控系統之研究與開發，逢甲大學電機工程研究所碩士論文，2004。
- [6] 蔡岳洋，以無線感測器網路實作室內安全監控以及緊急逃生導引系統，國立交通大學資訊工程學系碩士論文，2005。
- [7] 許進富，廣播電波傳播之實測與模擬，台灣科技大學電機工程研究所碩士論文，2004。
- [8] 陳文杰，紅外線數據傳輸，國立交通大學光電研究所碩士論文，1999。
- [9] 陳秉瑜，交流伺服馬達驅動器與整合式旋轉編碼器之介面設計，南台科技大學電子工程研究所碩士論文，2004。
- [10] 如何選購鐵捲門遙控器，from web：
<http://e-shin.com.tw/cht/modules/news/article.php?storyid=5>。
- [11] HCS300 datasheet，from web：
http://ww1.microchip.com/downloads/cn/DeviceDoc/cn_21137f.pdf。
- [12] 王聖傑，電腦網路與資料通訊，知城數位科技數份有限公司，2005。

- [13]王璧超，馬達控制原理概論，儒林圖書公司，1988。
- [14]王佑仁，電機機械與電力電子學原理，五南圖書出版有限公司，2002。
- [15]東元交流馬達規格，from web：<http://www.teco.com.tw>。
- [16]東元捲門馬達規格，from web：
<http://www.tubular-motor.com.tw/c-09.htm>。
- [17]無線電收發模組電路製作介紹，from web：
<http://designer.mech.yzu.edu.tw/article/articles/technical.htm>。
- [18]TG-11 datasheet，from web：
http://www.100y.com.tw/pdf_file/TG11-315M.pdf。
- [19]ht-12 datasheet，from web：<http://www.holtek.com.tw>。
- [20]王聖弼、李魁才、林書弘及李育璿，微電腦人員追蹤控制系統，光武技術學院專案報告，2003。
- [21]施慶隆及劉宴維，PIC18FXX2 微控制器原理與實作，使用組合語言與 C 語言，宏友圖書開發股份有限公司，2004。

