家用電話詐欺預警機制之研究

A Study on Home Phone Fraud Prevention

顏志平
中央警察大學總務處
桃園市龜山區大崗里樹人路56號
peter@mail.cpu.edu.tw

董正談
中央警察大學資訊管理所
桃園市龜山區大崗里樹人路56號
tung@mail.cpu.edu.tw

陳芳逸
中央警察大學資訊管理所
桃園市龜山區大崗里樹人路56號
im1033084@mail.cpu.edu.tw

摘要

隨著資訊通訊科技的發展，電信業者所能提供給消費者的電信服務較以往更多元及低成本，而電信詐欺的犯罪型態及手法亦與時俱進。犯罪集團亦透過各種通訊管道，包括電子郵件、通訊軟體、智慧型手機、傳統市話等來接觸被害人，使用電信業者所提供的電信服務來達到躲避偵查、節省通訊成本及竄改主叫號碼等目的，並以精心設計的詐騙劇本與情境詐騙，由詐騙人員在電話另一端以其逼真的聲音、語調與情境來取得被害對象的信任，典型的內容包括慈善詐欺、緊急救援詐欺、拍賣詐欺、恐嚇詐欺、退稅詐欺、台灣的篡改主叫號碼、猜猜我是誰詐欺等，這些詐欺手法往往利用人性弱點來實現。政府與民間為了減緩詐騙案件所造成的人民財產與社會經濟損失，除透過宣導與教育來提升民眾反詐騙意識外，也利用智慧型手機所提供的功能與服務發展詐騙防制與預警 APP，如 Whoscall、APP 防駭通等，因此智慧型手機上的反詐騙預警機制可以說是發展相當成熟，包括來電黑名單過濾、簡訊詐騙關鍵詞偵測等。反觀傳統家用電話尚無相關防制機制，儘管傳統家用電話已逐漸式微，但大多數家庭仍有配置家用電話，且有相當大比例之使用者為年齡層偏高之民眾，其接觸反詐騙資訊的管道也相對較少，因此為詐騙被害者之高危險群。有鑑於此，本研究利用嵌入式系統 － 以 Raspberry Pi 為例，結合語音辨識與關鍵詞偵測等相關技術提出有效的防制措施與解決方案，建構傳統電話詐騙預警系統，期能有效防制傳統家用電話之詐騙犯罪。

關鍵詞:電信詐欺、嵌入式系統、語音辨識、關鍵詞偵測。

Abstract

Due to the development of information and communication technology, telecom service providers can provide consumers telecom service with more variety and lower cost. But the criminal types and method of telecom fraud also advance with times. Criminal organizations also use all kinds of communication channels to contact with victims, including emails, communication softwares, smart phones and traditional home phones. They use the telecom service provided by telecom service providers to avoid investigation, save communication cost and tamper the caller ID. And they try to gain the victim's trust through well-designed script and lifelike voice and intonation on the phone. Typical cases include charitable fraud, emergency fraud, online auction fraud, intimidation fraud, tax fraud, and so on, these fraud techniques often exploit human weaknesses to achieve. In order to mitigate the loss of civil property and socio-economic from fraud, the official and private try to elevate the civil anti-fraud awareness through propaganda and education, they also use functions and services provided by smartphones to develop the fraud prevention and warning app, such as whoscall, so the anti-fraud prevention schemes on smartphones are literally mature, including caller ID blacklist filter and SMS fraud keywords detection. Conversely, there are no any relevant prevention schemes on traditional home phone, even it has become gradually declined, a large proportion of families still have it, and most of the users are elderly, they are regarded as high risk population. Therefore, this study tries to combine relevant techniques, such as speech recognition and keywords detection, and using the Raspberry Pi, to propose an effective method and construct a home phone fraud prevention scheme, wishing to prevent the home phone fraud crime effectively.

Keywords: telecom fraud, embedded system, speech recognition, keywords detection.

一、前言

(一)研究動機

近年來，為了快速致富以獲得優渥的物質享受，使不少人懷著懶惰及投機的心態，願意冒著被司法制裁的風險，試圖以詐欺手法取得不法利益，對於社會治安影響甚鉅。隨著資訊通訊科技的發展，詐騙集團的詐騙手法也日新月異，不斷精進其技術及組織，調整其經營模式以順應時代潮流。為了保障人民的財產安全，內政部警政署於 93 年 4 月 26 日成立「165 反詐騙諮詢專線」，由專責員警負責受理民眾的詐騙案件及提供諮詢服務。同時不斷更新詐騙集團所使用的科技工具及辦案手法，並定期將最新的詐騙案例發佈於網路上供民眾參考。而各縣市警察局也配合警政署，利用各種廣告媒體針對詐騙案件進行宣導，甚至在金融機構的 ATM 提款機張貼反詐騙海報，目的就是為了使民眾了解最新的詐騙資訊。同時也編排派出所員警至各大郵局、銀行等金融機構執行守望勤務，向民眾實施反詐騙宣導，這些措施都是為了避免讓民眾成為詐騙被害者，讓詐騙集團有機可乘。

據 165 反詐騙諮詢專線統計，詐欺案例類型多達 35 種，包括：假退費(稅)真詐財、假綁架真詐財、假借親友出事勒索、假借銀行貸款詐財、假冒公務機關詐財、假借信用卡遭盜刷詐財、假借個人資料外洩詐財、中獎通知、假借郵局招領、假借催討欠款、刮刮樂、互助會詐財、色情應召詐財、拍賣詐財、芭樂票騙貨、金光黨、假瓦斯安檢、假交友、假快遞、假投資、假求職、假車禍、假廣告、假推銷、假催收信用卡費、假慈善機構、假預付型詐財、假算命、猜猜我是誰、騙取個人資料、擄車勒贖、觀光區鏢客詐財、六合彩等等。

依據警政署公布資訊及 165 反詐騙諮詢專線的統計資料，早期是傳統的郵寄刮刮樂中獎詐騙，而在 2002 年行動電話逐漸普及以後，詐騙集團開始利用網路電話及行動電話進行詐騙，典型的案例包括假冒檢察官、猜猜我是誰、網路購物詐欺等等，以精心設計的詐騙劇本詐騙民眾，因而詐騙案件數急劇上升，造成許多被害人財產上的損失。政府為了遏制詐欺犯罪，於 2004 年起陸續頒佈新的相關法規及措施，包括「金融電信人頭帳戶及電話犯罪案件處理執行規定」、「詐騙電話快速停話平臺」、「靖頻專案」、「警示帳戶聯防機制」等；另外將刑法的連續犯以一罪一罰的方式取代，以提高詐欺犯罪之刑責。同時成立「165 反詐騙諮詢專線」，接受民眾報案、諮詢，並隨時提供最新詐騙手法，降低民眾受騙被害的機會。2009 年簽署之「海峽兩岸共同打擊犯罪及司法互助協議」也有效控制了詐欺案件數；且於 2010 年將「電腦處理個人資料保護法」修正更名為「個人資料保護法」，以合理規範個人資料之蒐集、處理及利用，並避免個人權利受到侵害及促進個人資料之合理利用，並明訂罰則以督促使用個人資料之機關善盡保護責任。

圖一：2007 年至 2015 年詐欺犯罪案件統計表
(資料來源：內政部警政統計年報)

隨著資訊通訊科技的發展，詐騙集團的詐騙手法亦日新月異，不斷精進其技術與組織，調整其經營模式以順應時代潮流。經由相關文獻探討可得知，新興詐欺犯罪均須仰賴詐欺訊息的傳遞與被害對象的互動以實現其詐騙手法，並利用人性弱點來實現，其中電信詐欺犯罪更透過資通訊媒介及設備來向被害對象傳遞詐騙訊息，並藉由金融機構所提供的轉帳、匯款等服務使其交付財物，進而獲得不法利益。因此，電信詐欺犯罪已不容忽視，有必要就電信詐欺犯罪的手法與模式等層面來分析，並找出解決之道。

嵌入式系統的技術與產品近年來已成為全球 IT 產業發展的重點。嵌入式系統產品強調硬體的功能必須要體積小、低耗能與高效能，軟體則要相容性高、開發容易及操作簡單。隨著產品提供各種多元化的應用，與人們生活周遭的食衣住行都有著密切相關；而語音辨識技術在科技快速發展亦日益成熟，搭配語句分析及資訊檢索等技術亦使準確率大幅提升，蘋果（Apple）公司的 Siri 軟體即是結合語音辨識、人工智慧及搜尋技術等機制應用於行動服務的範例，能自動搜尋相關資訊，並將最適切的答案提供給使用者。例如當使用者欲查詢氣象，Siri 便能自動回報氣象資訊，而非僅提供氣象網站的超連結供使用者自行查詢。

現行智慧型手機之防詐騙 APP 如 LINE whoscall、CM Security 等，均提供有效的反詐騙機制，包括黑名單來電號碼過濾、檢查簡訊內容及警示詐騙簡訊等，而僅管目前電信詐欺案件多發生於智慧型手機，但由於智慧型手機所提供之詐騙預警機制已相當成熟，反觀傳統家用電話尚無相關防制機制，因此傳統電話之詐騙預警機制仍有其重要性。

(二)研究目的

本於前述之研究動機與研究背景，本研究欲利用嵌入式系統所提供的各項優勢，結合語音辨識功能與關鍵詞偵測技術，發展出應用於傳統家用電話之詐騙預警系統，將通話中的語音轉換為文字，以實現詐騙關鍵詞辨識及警示的功能。當被害人接到詐騙集團的語音電話時，能透過嵌入式系統所提供的通話錄音、語音識別、警示提醒等功能來警告被害人，使其能在第一時間提高警覺，並對於詐騙集團所精心設計的詐騙劇本有所防

備。因此本研究藉由發展嵌入式系統應用於傳統家用電話，將詐騙集團的對話內容進行辨識，並識別可能的關鍵詞後警示被害人，本研究所研擬之系統期能達到以下目的：

1. 號碼過濾：詐騙集團常透過網路電話，利用竄改主叫號碼之方式，冒名為政府機關或拍賣網站，以各種名義向被害人進行詐騙，因此本研究將建立號碼過濾機制，對於符合條件之來電號碼實施預警機制。
2. 將通話內容進行錄音與辨識：當使用者接起警示之來電後，嵌入式系統即開始針對對方通話內容利用語音識別功能進行辨識，並將辨識結果的文字進行詐騙關鍵詞檢查，同時將通話內容進行錄製，可供警方進行後續案件偵查之用。
3. 針對疑似詐騙電話之通話內容進行警示：由於詐騙集團會以各種名義向被害人進行詐騙，使被害人陷入詐騙陷阱而不自覺，因此當嵌入式系統偵測到通話內容中的詐騙關鍵詞時，經過權重分析後，如判斷為高機率之詐騙電話將透過警示燈進行提醒或強制結束通話。

本研究希望由此方向出發，發展家用電話之詐騙防制預警系統，並與現有的智慧型手機防制詐騙機制互補，以減少民眾直接接觸詐騙集團之機會，期能有效防制電信詐騙案件之發生。

本研究在第二節文獻探討中，闡述嵌入式系統、語音辨識之機制與關鍵詞擷取等本研究所涉及之基礎背景知識，第三節說明電信詐欺之犯罪管道、內容與交付手法，並於第四節提出解決方案，介紹系統架構與模擬情境，最後於第五節說明本研究之結論與未來研究方向。

二、相關文獻與背景知識

本研究欲透過嵌入式系統，結合語音辨識功能與關鍵詞比對技術，發展出應用於傳統家用電話之詐騙預警系統，能夠將通話中的語音轉換為文字，以實現詐騙關鍵詞辨識及警示的功能，因此本研究需要「嵌入式系統」、「語音辨識」與「電信詐欺手法」做為基礎背景知識，相關整理如下：

(一) 嵌入式系統

1.嵌入式系統之軟硬體概述：

嵌入式系統(Embedded system) [6]專用於處理特定任務，以較小的體積和成本，發展可靠與效能高的產品，普遍應用於工業、醫療、自動化、商業及軍事等領域。Operating System (OS)作業系統則是管理電腦軟硬體資源的程式，提供資源的有效管理、人機互動及可程式化的功能、任務分派與執行的元件等。

本研究所使用的嵌入式系統為Raspberry Pi，OS 為Linux-based，屬於ARM 架構的處理器。

嵌入式系統是一種完全嵌入控制器內部專為特定應用設計的作業系統。嵌入式系統是在電子裝置中所嵌入之計算系統，而所謂計算系統則是指除了桌上型電腦之外的任何計算機系統[13]。

與個人電腦的通用系統不同，嵌入式系統通常執行帶有特定需求與預先定義的任務。由於嵌入式系統只需執行任務，因此開發設計人員能夠對其進行優化，縮小尺寸與降低成本。且嵌入式系統的核心是由一個或數個預先編譯好，僅針對特定功能而執行幾

項任務的微處理器或微控制器所組成。而個人電腦則功能較為廣泛，以實現一般使用者的各類需求，生活中常見的許多小型控制裝置都利用嵌入式系統進行控制。

嵌入式系統包含軟體與硬體兩大部份。硬體部分包含：微處理器、記憶體、I/O以及控制相關硬體元件的驅動程式。軟體部分包括：作業系統與執行特定功能的應用程式，目前市面上已經開發出多種嵌入式作業系統(Embedded Operating System)來搭配嵌入式系統，目前較為熱門的嵌入式作業系統包括：Windows CE、Embedded Linux、FreeRTOS、uClinux 等等。

2.GPIO原理：

提到嵌入式系統的應用，必定與GPIO有關[14]，GPIO為General Purpose I/O 的縮寫，中文為「通用型之輸入輸出」，其功能相當於8051單晶片的P0-P3埠。

Raspberry Pi可藉由暫存器的設定來選擇功能，例如讓接腳進行通用輸入（GPI）可以透過某個暫存器的讀取來確定接腳電位的高低，或進行通用輸出（GPO）可以透過某個暫存器的寫入來讓該接腳輸出高電位及低電位，通用輸入與輸出（GPIO）也有另外的暫存器可以控制其他特殊功能，因此可以透過軟體設置來滿足各種系統配置與設計需求，但是必須要定義每一個用到的接腳功能，以實現各種通訊介面、時脈產生器或是作為晶片的選擇接腳。

3.Raspberry Pi 樹莓派：

本研究所使用的嵌入式系統為Raspberry Pi（樹莓派）[15]，是一款基於Linux 系統，大小約一張信用卡的單板機電腦，修改自Debian 系統，系統針對Raspberry Pi 硬體進行最佳化，稱為Raspbian，也是官方所推薦的作業系統。另外也提供基於ARMCPU架構的Debian 和Arch Linux 的發行版供大眾下載，以Python作為主要的程式語言，嚴格說起來Linux僅是一個內核，一個完整的操作系統尚需要包含驅動程式、服務與應用程式等各種元件。不同版本的作業系統都會在特定應用程式進行優化，並且有不同支持的用戶群。樹莓派是由英國的樹莓派基金會所開發，目的是希望以低價硬體與自由軟體刺激學校的基本電腦科學教育。

本研究的Raspberry Pi 嵌入式開發板使用Broadcom BCM2836處理器，採用ARM Cortex-A7核心，運作時脈高達900MHz，一共有40 個接腳可以使用，可以設定各控制接腳。

Raspberry Pi擁有體積小，低成本等特性，並提供通用型之輸入輸出(General Purpose I/O)接腳，開發者能夠依需求來撰寫程式控制，並整合其他設備來開發各種應用[12]。

(二)語音辨識

語音辨識（Speech Recognition）起源於西元1950年，一開始是在Bell實驗室研發可成功辨識10個英文的數位實驗系統，從此之後語音的相關研究逐漸吸引大家的目光，最早期語音訊息參數大多是利用頻域(Frequency Domain)特徵參數[4]，而後動態規劃、快

速傅立葉轉換(Fast Fourier Transform, FFT)、倒頻譜分析(Cepstral Analysis)和(Linear Predictive Coding, LPC)技術等重要技術的突破。西元1980年，非特定語者語音技術的系統成功被開發並提出HMM(Hidden Markov Model)理論。到了西元1990年因電腦技術的快速發展，語音辨識開始實用化。

語音辨識的主要目的是讓電腦聽懂人類說話的聲音，進而與電腦溝通，命令電腦執行相對應的任務。辨識機制為：聲音原本為類比訊號，透過轉換機制轉換成數位訊號輸入電腦及儲存後，語音辨識程式便將所接收的語音樣本與事先儲存的語音樣本資料庫進行比對工作。電腦經由比對找出相似度最高的聲音樣本序號，進而理解使用者的指示與命令，進而命令電腦做事。蘋果（Apple）公司的Siri軟體即是結合語音辨識、人工智慧及搜尋技術等機制，能自動搜尋相關資訊，並將最適切的答案提供給使用者。例如當使用者欲查詢氣象，Siri便能自動回報氣象資訊，而非僅提供氣象網站的超連結供使用者自行查詢。

一套語音辨識程式的開發，至少涉及兩方面的知識，包括：

- 電腦如何接收外界的聲音訊號並轉換成機器可以處理的數位訊號
- 聲音比對原理

而在本研究中，為了能夠有效運用網路上的現有資源，而不必再費時開發新的語音辨識系統，因此希望運用智慧型手機所提供的語音辨識功能來開發APP，實現協助防制詐騙電話與預警的目的。

語音訊號充滿了變數及太多特性，因此需要特定的方式，取出語音的特徵資料，再建立比對資料庫，才能達成語音辨識的目的。

1. 語音辨識之機制：

電腦透過將語音資料數位化後處理與儲存，對電腦而言，即使相同的人於相同環境下使用相同的麥克風連續講兩次相同的句子，電腦接收到的語音資料也不可能完全相同。因此語音辨識的機制在於將語音進行歸類，異中求同。

一般作法是在事前蒐集相當數量的語音樣本，從中抽取適當的語音特徵（Feature Extraction），經過系統的訓練程序（Training Procedure），建立參考聲學模型（Acoustic Model）所需的參數；在語音辨識階段，使用者輸入語音樣本，系統抽取語音特徵之後，與語音辨識資料庫中的參考聲學模型進行比對，找出機率最高的樣本，即為辨識結果。

2. 現行語音辨識之相關應用：

根據 TMA Associates 市調公司的調查報告中，將語音辨識產品分為四大類[10]：

（1） 電腦產品：利用電腦連接麥克風，辨識結果呈現在電腦螢幕上，由於電腦使用者較為固定且長時間使用，適用語者相關或語者調適技術；應用包括語音輸入法、PC 語音控制、語音資料存取、遊戲軟體、語言訓練等。

（2） 電話產品：將通話語音透過有線/無線傳輸給辨識系統，辨識結果以聲音回饋給使用者，由於通話對象非特定，宜採用語者無關技術；應用包括電話語音撥號或辨識/驗證身分服務、互動語音回應系統(IVR)、通訊助理、互動語音回應系統、電話語音辨識等。

（3） 消費性電子產品：應用包括可攜式電子記事簿、家電控制、語音撥號行動電話、聲控玩具、語言學習等。

（4） 汽車及工業：應用包括汽車導覽系統、音響控制、工業品管、包裝處理、汽車通訊等。

(三) 關鍵詞擷取技術

關鍵詞擷取技術能夠針對訊息內容進行分類剖析，從中辨識有意義的關鍵字或詞彙，如能結合語音辨識服務，用於通話內容的分析，藉以偵測常見之詐欺電話關鍵詞，達到詐欺電話預警之目的，目前關鍵詞擷取技術主要可分為三種方法[11]，包括詞庫比對法、文法剖析法及統計分析法，相關介紹如下：

1. 詞庫比對法：

詞庫比對法透過預先設定的詞庫，來對訊息或文章進行比對，擷取內文中與詞庫相同的文字，其優點為處理快速與設計容易，缺點是需要手動建立詞庫，而詐欺手法日新月異，如出現新的詐騙術語，且在未更新詐欺關鍵詞資料庫的情況下，便無法偵測出關鍵詞彙，且當詞彙資料庫愈來愈大時，將影響關鍵詞比對之速度。

2. 文法剖析法：

文法剖析法係利用自然語言的文法剖析程式，透過詞庫比對方式，將訊息中的名詞片語進行剖析，並利用相關方法與準則，過濾不適合之訊息文字。其剖析結果即為我們所要的詞彙，但仍需透過預先建立的詞典或語料庫[9]，因此亦無法避免詞庫比對法之缺點。

3. 統計分析法：

統計分析法係以詞彙出現之頻率或詞彙之間的相關程度來進行關鍵詞之擷取，其透過大量樣本資料之統計分析，擷取出符合特定條件(如出現次數)之詞彙。由於是透過統計之方式，因此不用事先建立詞彙庫，但如果某些詐欺關鍵詞的出現次數不高，便可能無法成功將其比對出來。

在電信詐欺犯罪中，犯罪者通常會使用特字詞彙，如拍賣網站詐欺案例中常出現的「解除分期付款」、假冒檢警詐欺案例中的「至超商接收法院傳票」、「金融帳戶已被列管」等，僅管每通詐騙電話的完整內容不盡相同，但犯罪者仍須向被害者傳達某些特定關鍵詞才能達到其特定目的，因此本研究嘗試以詞庫比對法來進行詐欺電話內容中的關鍵詞偵測比對。

(四) 電信詐欺犯罪手法分析

犯罪手法是指犯罪者如何成功實現其犯案行為，主要探討犯罪者如何犯罪；而電信詐欺犯罪利用被害人的貪念、恐懼、無知、資訊不對稱、對政府機關的信任等，結合當前社會時事發展出各種詐騙手法，並透過網路通訊科技及跨境組織來躲避司法機關查緝，以遂行其詐欺之行為；電信詐欺犯罪手法可由詐欺管道、詐欺內容及交付手法等三個面

向來探討，詐欺管道係指詐騙集團傳送詐騙訊息給被害人所使用的工具；詐欺內容係指詐騙集團所使用的詐騙訊息內容；交付手法係指詐騙集團取得被害人財物的方式，分述如下：

1. 詐欺管道：

電信詐欺犯罪管道可分為電話詐欺、手機簡訊詐欺及網路詐欺等三類，電話詐欺盛行於1997年至2000年間，並於2005年達到高峰，於2006 年開始下降；網路詐欺發跡於1999年，並逐年呈現倍數成長[8]；手機簡訊詐欺開始於2001年，並於2005年出現高峰期，於2006年逐漸下降。傳統以「與人直接接觸」為管道的詐騙手法已不符時宜，現今詐騙集團主要是藉由電信、通訊等工具傳送訊息給民眾，詐欺管道也由「接獲騙徒電話」演進至「接獲電話語音」。僅管詐騙集團會隨著時間更新詐欺管道，惟仍以電信工具作為主要詐欺管道；2014年起由於智慧型手機的普及，網路無遠弗屆及低成本的特性使得詐騙集團開始利用免費的通訊軟體傳送附有惡意連結的短訊息，亦使手機簡訊詐欺漸趨式微，一旦被害人點選連結後即遭植入惡意程式或被歹徒拿來向電信業者進行小額付費交易，因此詐欺案件於2014年再度呈現上升之趨勢。

2. 詐欺內容：

詐騙集團所使用的詐騙訊息內容，往往結合時事並推陳出新，根據刑事警察局165防制詐騙諮詢專線統計，典型的詐欺手法包括假冒公務機關、ATM解除分期付款、猜猜我是誰、網路拍賣詐欺、騙取個人資料、假推銷、假投資、假借銀行貸款、假綁架（恐嚇）、假借催討欠款、假中獎通知等。2014年以後以假冒公務機關、ATM解除分期付款及小額付款詐欺為最大宗。其中「ATM解除分期付款」犯罪手法以網路購物消費者為目標，常見於被害人於網路購物交易後，接獲自稱○○購物網站的客服來電，誆稱被害人因網路購物交易時的付款方式設定錯誤而將重覆分期付款，並告知消費者已通報銀行客服人員處理，隨即由假冒的銀行客服來電，要求被害人前往ATM自動櫃員機解除分期付款設定，依其指示操作將金錢轉帳至詐騙集團人頭帳戶；「小額付費詐欺」則是詐騙集團透過電子郵件或智慧型手機的通訊軟體或SMS文字簡訊服務，傳送包含「這是上次聚會的照片」、「這是那晚你沒來的照片、「宅急便快遞通知」、「電費網上支付」等附加短網址連結的訊息，誘騙被害人點選連結後即遭植入木馬程式，使被害人手機內的個人資料與通訊錄資料外洩，並被詐騙集團拿來向電信業者進行小額付費交易，直到被害人收到下期的電信帳單消費金額時才驚覺被詐騙。

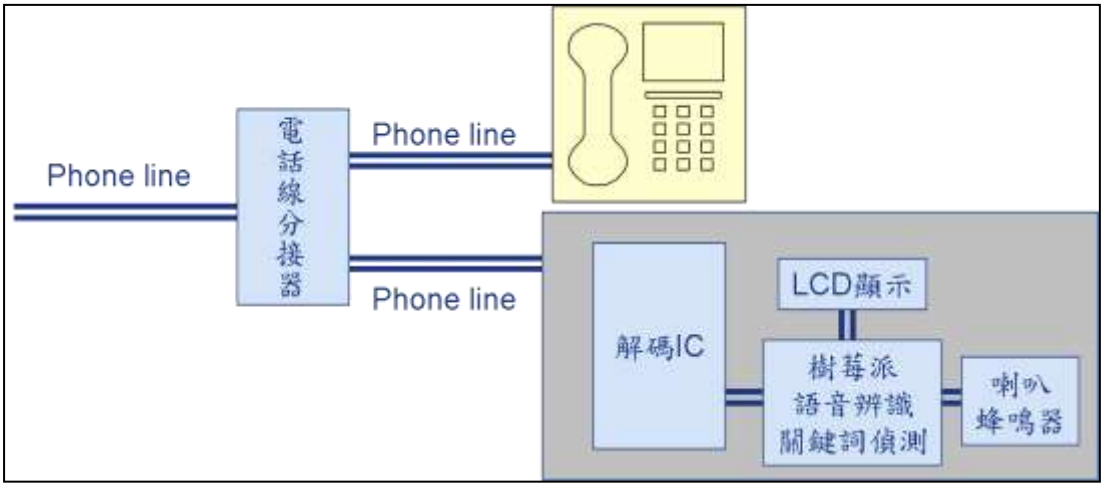
3. 交付手法：

詐騙集團主要透過ATM轉帳、信用卡刷卡、當面交付現金、電話語音轉帳、網路銀行轉帳、臨櫃匯款等方式使被害人交付財物，2005年至2006 年間61以臨櫃匯款、ATM 轉帳、語音轉帳、當面交付為主，2006年至2008年網路轉帳件數則逐漸增加[3]。

三、家用電話詐欺預警系統

(一)系統簡介

在前述文獻探討裡所介紹的現有詐欺預警機制中，都是為智慧型手機所量身打造的功能與服務，如Whoscall、APP防駭通等詐騙防制與預警APP，智慧型手機之反詐騙預警機制已經發展相當成熟，包括來電號碼黑名單過濾、簡訊詐騙關鍵詞比對等。反觀傳統家用電話尚無相關防制機制，儘管傳統家用電話已逐漸式微，但大多數家庭仍有配置家用電話，且有相當大比例之使用者為年齡層偏高之民眾，其接觸反詐騙資訊的管道也相對較少，因此為詐騙被害者之高危險群，若僅憑政府宣導反詐騙資訊之政策仍顯不



足，僅管預防勝於治療，但發展應用於傳統家用電話之預警機制仍有其必要性，因此本研究提出了以嵌入式系統基礎，結合語音處理與通話內容關鍵詞比對，來發展家用電話詐欺預警機制之系統，系統構想如圖二所示。

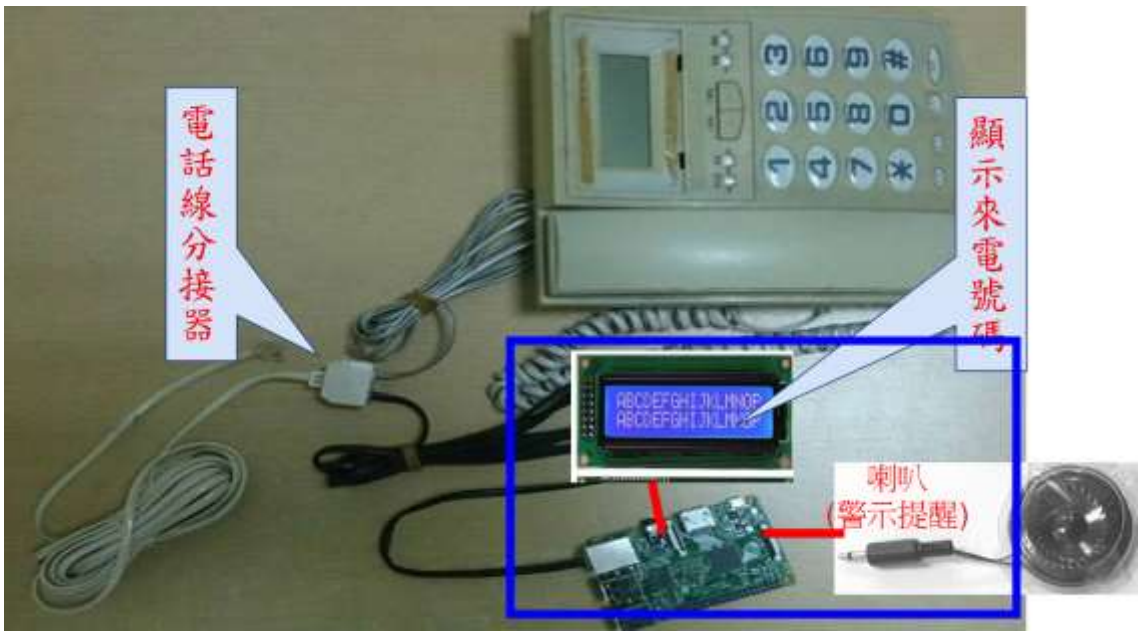
圖二：系統構想

(二)系統設計與運作流程

1.系統設計

（1） 訊號解析

本研究將電話線路透過並聯的方式，將家用電話與嵌入式系統連接起來(如圖三)，中間透過電容器過濾電話線原本提供的直流電壓，後端再接上變壓器，以更完整達到過濾直流電壓的目的，提供後端元件一個保護效果，並保留住電話的類比變動頻率，如圖一。



圖三：系統實體圖

欲應用Raspberry Pi進行訊號運算之前，需要將欲處理的訊號轉換為數位訊號，方可由電話線輸入端經由GPI通用輸入來接收訊息，進行處理的工作。我們使用電話解碼IC，將來自電話線之訊號解碼為脈波訊號輸入raspberry pi進行處理，因此解析電話訊號中的電話號碼為我們第一步的目標。

電話撥號聲為雙音複頻訊號(Dual Tone Multifrequency Dialing , DTMF)。撥號端透過傳送此訊號對電信公司提出通話要求，電信公司則依據所接收之訊號，找出對方位置後將兩通話端連接，完成連線。此研究之目的，是為識別來電號碼所做的前端準備作業，因此須將所接收之DTMF訊號，轉換為數位訊號，以利後端的訊號處理。HT9170 DTMF Receiver 電話解碼晶片 ，便提供此訊號解碼之功能。

（2） 來電號碼警示

依據165反詐騙諮詢專線的詐騙排行統計，時下流行之詐騙主題多為「假冒公務機關詐財」、「拍賣網站詐騙」與「假中獎詐騙」等，故本研究的來電警示對象將以上述詐騙主題為主。

本研究透過if判斷式來判斷是否進行警示。判斷先後順序如下：

A. 判斷來電是否為國際電話或網路電話：目前國際來話話務的顯示機制，於市話端顯示「00x」、行動電話端顯示「+」，提供民眾判斷來電顯示號碼是否異常。詐騙集團往往透過境外或竄改電話號碼或使用網路電話進行詐騙以躲避偵查，因此本研究擬將第一階段之警示條件設為：當傳統家用電話接到來電號碼顯示為「00x」開頭之國際話務與「026」、「027」等開頭之網路電話，以及來電號碼中出現「852」、「861」等香港、大陸地區國碼之來電號碼，以判斷該通來電是否為國際電話或網路電話。

B. 若確認為國際電話或網路電話號碼，則與白名單內之號碼做比對，白名單內之號碼為使用者自行登錄之國外親友或有在使用網路電話之親友之號碼，其餘國際電話或

網路電話則視為詐騙集團所撥打之電話，此時系統便會進行過濾與警示，即使多數民眾對於這類顯號格式缺乏認識，若能在接收警示訊息後提高警覺，較能進行即時的處理與查證。

C. 若非國際電話則有可能是詐騙集團利用人頭電話或在大陸沿海地區，透過臺灣在離島的基地台溢波撥打詐騙電話，因此詐騙電話仍有機會為非國際電話，此時進入預警機制，如果通話內容又提及「法院檢察官法官」、「警察局偵辦案件」、「涉及刑案」、「帳戶凍結等」，當事人便可判斷該通來電極有可能為詐騙電話。

D. 根據165專線統計，高風險網路賣場與詐騙電話名單如圖四所示。

165專線統計 高風險賣場與詐騙電話名單

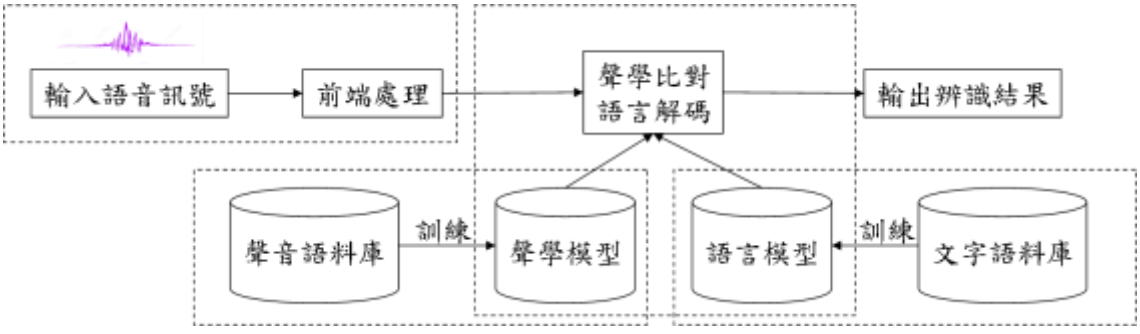
高風險賣場(網站)		詐騙電話排名
露天拍賣	1	+886229399210
HITO本舖	2	+02770565
Facebook	3	+886436810
衣芙日系	4	+0332181017
奇集集	5	+8673687610
奇摩拍賣	6	+8621541235
奇摩超級商城	7	+89326272
VACANZA	8	+8643681030
森田藥妝	9	+09713611
潮物部落格	10	+0423289100

圖四：高風險網路賣場與詐騙電話名單

（3） 通話內容語音處理

電話通話內容屬於連續語音，處理難度高於一般常見的聲控及語音指令，對於連續語音之關鍵詞偵測，本研究歸納出以下兩種處理方式[2]：

A. 第一種是先利用語音辨識文字技術，在特定語音模型下先進行語音辨識，將語音轉換成文字，再將轉換得到的文字以關鍵詞偵測的方式進行搜尋。語音辨識文字技術(如圖五)，事前須蒐集相當數量的語音樣本，從中抽取適當的語音特徵，經過系統的訓練程序，建立參考聲學模型所需的參數；在語音辨識階段，使用者輸入語音樣本，系統抽取語音特徵之後，與語音辨識資料庫中的參考聲學模型進行比對，找出機率最高的樣本，即為辨識結果。



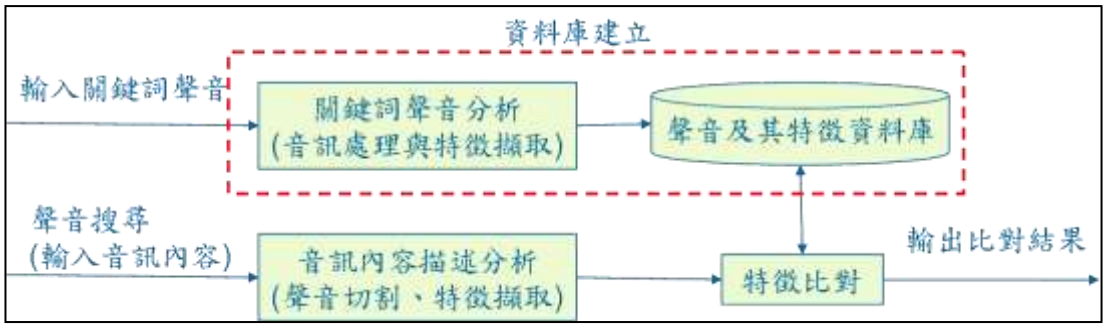
圖五：語音辨識機制

B. 第二種是以音訊關鍵詞為基礎進行檢索。在語音檢索中，不須考慮語音模型，而是直接以關鍵詞語音的特徵參數，在另一語音文件中進行比對，找出特徵參數最接近的語音內容。首先定義使用者感興趣的關鍵詞，之後系統便能從一段連續語音中檢測這類關鍵詞。例如將「分期付款」作為與詐騙電話有關的關鍵詞。

語音檢索技術的架構主要可分為兩部分，包括音訊資料庫的建立與關鍵詞的搜尋，分別介紹如下(如圖六)：

a. 資料庫建立：首先輸入關鍵詞的音訊資料，並進行特徵分析等步驟以得到該音訊的特徵向量並且將其歸檔到資料庫

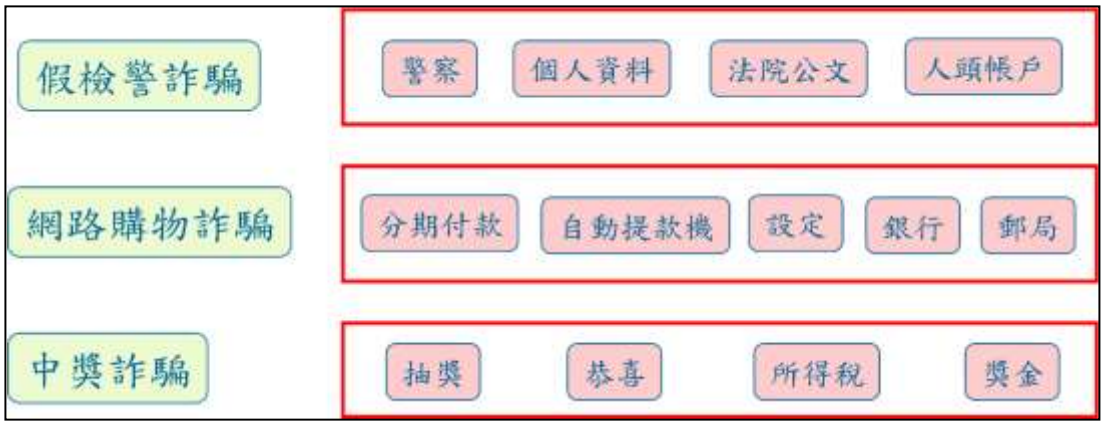
b. 關鍵詞搜尋：輸入聲音資料或內容，接著進行聲音特徵分析，把得到的特徵向量與資料庫進行比對，找出相似度最高的比對結果



圖六：語音檢索技術

（4） 關鍵詞處理模組

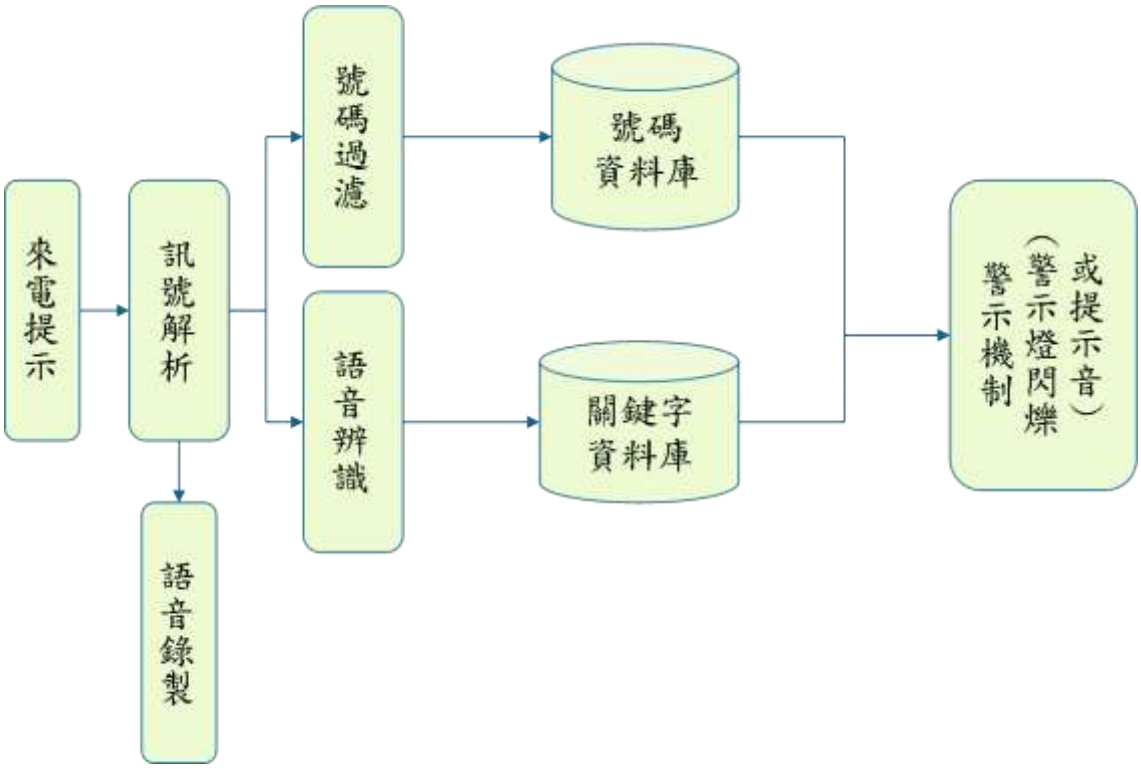
本研究透過實際的詐欺電話案例進行分析與實驗。詐欺電話關鍵詞的比對，須針對所收到的通話內容進行判別，經由本研究的整理與歸納，將所蒐集的詐欺案例針對其特性予以描述定義，並將不同事件所提供的結構化與非結構化資料加以紀錄分析。根據刑事局165專線所提供之資料顯示，歸納出下列三種常見的電話詐騙事件，分別為假檢警詐騙、網路購物詐騙與假中獎詐騙，此三種詐騙事件所傳遞的詐騙訊息關鍵詞皆不相同，並歸納各個詐騙案例情境中所應用到最常見之關鍵詞，如圖七所示，當通話過程中系統偵測到數個以上之關鍵詞，便會判定該通電話為詐騙，進行警示



圖七：常見詐騙案例情境關鍵詞

（5） 警示模組

若使用者依然選擇接聽疑似高風險詐騙來電，則系統便啟動錄音與語音處理功能，並透過嵌入式系統內的語音辨識模組與關鍵詞偵測模組進行處理與比對，並藉由所設定的關鍵詞權重及出現次數計算其權重值以判斷是否符合詐欺訊息的標準[7]，若達標準則由系統進行警示(LCD屏幕閃爍與喇叭警示)告知使用者目前通話可能為詐騙電話，而儲存下來的通話錄音可用來提供執法單位進行後續偵查與防制作為。整個系統之架構如圖八所示。



圖八：系統架構圖

(二)情境模擬

本研究以電話詐騙中的假檢警詐騙作為案例，當通話過程中系統偵測到數個以上之關鍵詞，便會判定該通電話為詐騙，進行警示。

本研究設計一則假冒警察機關之詐騙電話如下：這裡是○○○警察局，請問是○○○先生嗎？您因為個資外洩，歹徒冒用您的名字去銀行開戶作為人頭帳戶，現在已經有被害人出來指控，並要進行提告。請您現在立即前往超商，我們要傳真法院傳票給您。目前您的金融帳戶已被列管，請核對您的基本資料後，儘快將您帳戶內的錢轉帳至○○帳戶，由國家替您保管，等到證明您的清白便會將錢還給您。過程中請勿與任何人交談，尤其是銀行行員已與歹徒勾結，涉嫌盜賣個人資料，只要依照我們的指示進行操作即可。

（1） 來電號碼解析與過濾

當事人接獲一通來電號碼顯示為002886912024626之來電，經系統判斷為國際電話，此時raspberry pi於螢幕上顯示電話號碼與警示訊息提醒使用者，同時透過音源輸出裝置發出「疑似詐騙電話」之警示音。

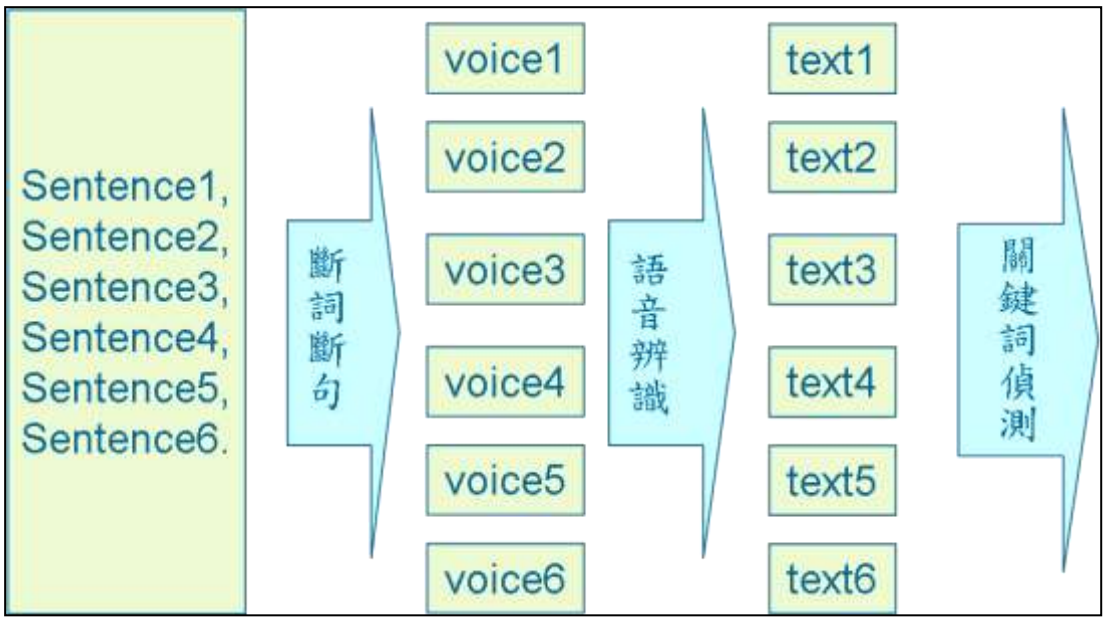
（2） 電話錄音

若當事人不理會系統之警訊選擇接聽電話，則系統會同時啟動錄音功能，雙向錄製雙方通話內容，以進行後續之偵防作為。

（3） 語音處理與關建詞比對

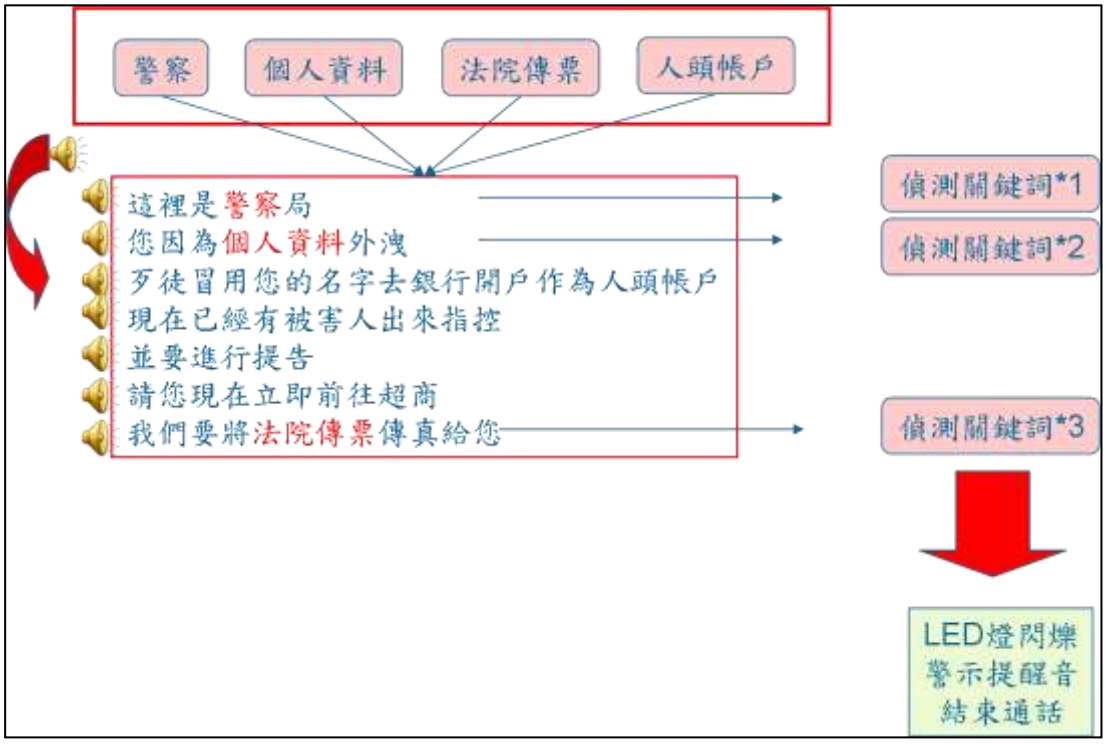
通話過程中，系統會先將所接收到的電話訊號轉換為電腦能夠處理的語音訊號，結合現有之語音辨識模組進行處理，將處理所得的文字辨識結果進行關建詞比對。

在接收到電話線所傳送之類比訊號後，經由訊號解析模組並轉換為系統可以識別與處理的數位語音訊號後，系統首先將發話方傳送過來的每一句話，通常以發話方話語停頓處作為分割點，進行錄製與存成聲音檔，每個聲音檔再經由語音辨識模組轉化為文字格式並存成文字檔，設計關鍵詞偵測程式，利用詞庫比對法進行比對，概念如圖九所示。將預先設計的各類案例之關鍵詞資料庫內的詞彙逐一進行比對[1]，若比對結果符合特定條件即進行下一階段的警示功能。



圖九：通話內容語音辨識

以本案例為例，通話過程中因系統偵測到「個資外洩」、「人頭帳戶」、「法院傳票」等關鍵詞，系統經計算權重值後判斷該通話內容為詐騙電話之可能性極高，因此進行下一階段的警示動作，如圖27所示，在嵌入系系統中則跳出比對到關鍵詞後的警告視窗，如圖十所示。



圖十：詐騙關鍵詞偵測

（4） 詐騙警示

當系統判定為詐騙電話後，即再透過與raspberry pi連接之螢幕顯示文字訊息、led燈閃爍與喇叭發出警示提醒來告知使用者目前通話為詐騙電話，透過各階段的警示機制提高使用者之警覺性，進一步進行查證之動作，降低受騙上當之機會。

四、結論及後續研究

經由探討相關文獻後可以發現，詐欺案件往往利用人性貪婪、恐懼與無知的弱點，透過各種精心設計的詐騙劇本，即使僅是採用相同的劇本，在配合經專業訓練的詐騙人員在電話另一端以其逼真的聲音、語調與情境便可容易取得被害對象的信任，使其深信不疑後進而交付財物，直到冷靜下來後才驚覺為詐騙手法。

而本研究所研擬之防制方法期望透過偵測通話內容中之詐騙關鍵詞來提醒使用者提高警覺或強制直接結束通話，當電話另一端的詐騙集團無法繼續與被害對象互動時，詐欺訊息便無法傳遞，設計再精巧的詐騙劇本亦無法繼續實行下去，如再結合文字訊息關鍵詞檢查，偵測包含疑似詐騙或惡意網址的高風險訊息；另外可將詐騙電話之通話內容，以文字格式輸出，並進行編輯與儲存，提供165防制詐騙彙整為語音詐騙案例資料庫，再由各政府機關輔以平面文宣、影音媒體等管道宣導民眾防詐騙觀念，當民眾接到相似的詐騙電話內容即可明確辨識，如此各種防制管道雙管齊下，自然能夠有效防制各類電信詐騙案件。

本研究目前僅針對來電話號碼過濾與通話內容辨識進行探討，而詐騙集團手法日新月異，詐騙劇本推陳出新，若詐騙集團變更話術中所使用的關鍵字或是使用黑名單資料庫以外的號碼便無法繼續防治，因此，未來研究方向將探討嵌入式系統內的關鍵詞資料庫與黑名單資料庫更新機制，以增強防護能量，全面預防電信詐騙。

參考文獻

[1] 王傑立，以自然語言為基礎之雲端應用-以台北市公車查詢為例，世新大學管理學院資訊管理學系碩士論文，2014

[2] 王駿發，多媒體影音檢索系統，科學發展第 411 期，2007：頁 6~13。

[3] 林山田，刑法通論，臺北市：臺大法學院圖書部，2008。

[4] 林佳奇、吳弘庭、陳俊良，電話應用裝置-語音解碼-語音答錄，逢甲大學自動控制工程學系專題製作專題論文，2007

[5] 林耿徽，電信詐欺犯罪偵查管理之研究，中央警察大學刑事警察研究所碩士論文，2012。

[6] 柯博斌，嵌入式感測盒的實作議題-Raspberry Pi 系統模組案例，國立台灣科技大學自動化及控制研究所碩士論文 2014。

[7] 洪憲能，智慧型手機詐欺防制之研究，中央警察大學資訊管理研究所碩士論文，2015

[8] 陳永鎮，台灣地區新興詐欺犯罪趨勢與歷程之研究，中央警察大學犯罪防制研究所碩士論文，2005。

[9] 陳光華，資訊檢索查詢之自然語言處理，中國圖書館學會會報 57 期，1996 年。

[10] 傅首僖，以類比按鍵輔助語音操控導航系統，國立臺北科技大學創新設計研究所碩士論文，2013

[11] 曾元顯，關鍵字自動擷取技術與相關詞回饋，中國圖書館學會會報 59 期，1997：頁 53~60。

[12] Dudas, R., VandenBussche, C., Baras, A., Ali, S. Z., Olson, M.T., Inexpensive telecytology solutions that use the Raspberry Pi and the iPhone. Journal of the American Society of Cytopathology, Volume 3, Issue 1, 2014: pp. 49-55.

[13] Frank Vahid & Tony Givargis, Embedded System Design: A Unified Hardware/Software Introduction. Wiley, New York, 2001.

[14] Gourab Sen Gupta, Embedded Microcontroller Interfacing: Designing Integrated Projects. Lecture Notes in Electrical Engineering, Volume 65. Springer, Berlin, 2010.

[15] Nicki Peter Petrikowski, Getting to Know the Raspberry Pi. Rosen Classroom, New York, 2014 .