



(19) 中華民國智慧財產局

(12) 發明說明書公告本

(11) 證書號數：TW I507009 B

(45) 公告日：中華民國 104 (2015) 年 11 月 01 日

(21) 申請案號：101106438

(22) 申請日：中華民國 101 (2012) 年 02 月 24 日

(51) Int. Cl. : *H04M3/42 (2006.01)* *G06Q90/00 (2006.01)*

(71) 申請人：張維平 (中華民國) CHANG, WEI PING (TW)

桃園市桃園區文中路 47 巷 41 號 8 樓

(72) 發明人：張維平 CHANG, WEI PING (TW)；郭建明 GUO, GEN MING (TW)；李心瑜 LI, SIN YU (TW)；梁惠茹 LIANG, HUE RU (TW)；林愛華 LIN, AI HUA (TW)

(74) 代理人：蘇顯讀

(56) 參考文獻：

TW	M331255	TW	200704133A
TW	200726192A	TW	201203996A
TW	20019359A		

審查人員：范美華

申請專利範圍項數：4 項 圖式數：16 共 27 頁

(54) 名稱

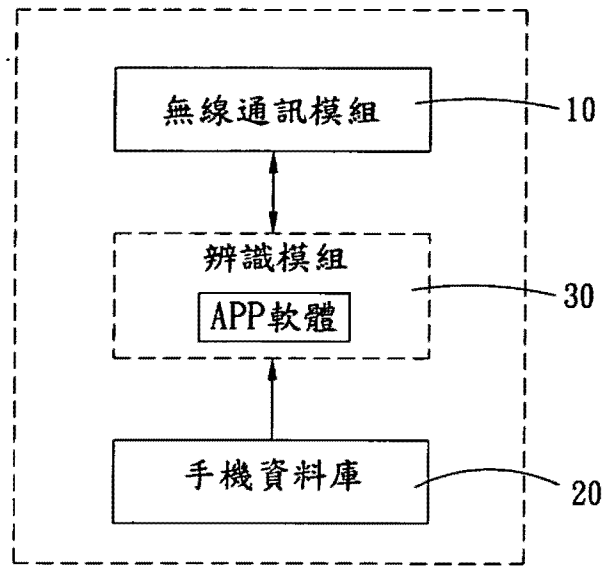
智慧型手機之防詐騙系統及其方法

SYSTEM AND METHOD OF SMARTPHONE FOR PREVENTING FRAUD

(57) 摘要

一種智慧型手機之防詐騙系統及其方法，係包括：一無線通訊模組、一手機資料庫及一辨識模組；其中無線通訊模組係用於接收來電訊息，而手機資料庫中係儲存有多筆詐騙者之來電號碼及聲紋等資料；令來電時，辨識模組亦可擷取來電訊息，並與該手機資料庫中之資料進行辨識比對，當來電內容中辨識出不安全之訊息時，辨識模組係會發出警示或自動斷線等處置。

The invention is related about a kind of system and method of smartphone for preventing fraud. It includes a wireless communication module, a mobile phone database and an identifying module, and the wireless communication module is used for receiving phone call message. It stores a lot of data like phone numbers and voiceprint called by the scammers in the mobile phone database. When the scammers call phone, the identifying module can capture the message of the phone call and take it to compare the data in the mobile phone database. When the identifying module identify a not safe message by the content of the phone call, the identifying module can alert or automatically disconnected.



(10) . . . 無線通訊  
模組

(20) . . . 手機資料  
庫

(30) . . . 辨識模組

第一圖



申請日: 101.2.24

IPC分類: H04M 3/42 (2006.01)

G06Q 90/00 (2006.01)

**【發明摘要】****公告本****【中文發明名稱】** 智慧型手機之防詐騙系統及其方法**【英文發明名稱】** SYSTEM AND METHOD OF SMARTPHONE FOR PREVENTING FRAUD**【中文】**

一種智慧型手機之防詐騙系統及其方法，係包括：一無線通訊模組、一手機資料庫及一辨識模組；其中無線通訊模組係用於接收來電訊息，而手機資料庫中係儲存有多筆詐騙者之來電號碼及聲紋等資料；令來電時，辨識模組亦可擷取來電訊息，並與該手機資料庫中之資料進行辨識比對，當來電內容中辨識出不安全之訊息時，辨識模組係會發出警示或自動斷線等處置。

**【英文】**

The invention is related about a kind of system and method of smartphone for preventing fraud. It includes a wireless communication module, a mobile phone database and an identifying module, and the wireless communication module is used for receiving phone call message. It stores a lot of data like phone numbers and voiceprint called by the scammers in the mobile phone database. When the scammers call phone, the identifying module can capture the message of the phone call and take it to compare the data in the mobile phone database. When the identifying module identify a not safe message by the content of the phone call, the identifying module can alert or automatically disconnected.

【指定代表圖】 第（一）圖。

【代表圖之符號簡單說明】

- (10) 無線通訊模組
- (20) 手機資料庫
- (30) 辨識模組

【特徵化學式】

無

## 【發明說明書】

【中文發明名稱】 智慧型手機之防詐騙系統及其方法

【英文發明名稱】 SYSTEM AND METHOD OF SMARTPHONE FOR PREVENTING  
FRAUD

### 【技術領域】

本發明係與防止詐騙有關，特別是指一種內建於智慧型手機中，藉以偵測來電訊息防止自身受騙的系統及其方法。

### 【先前技術】

近年來，拜網際網路科技快速發展所賜，使得人們可透過網路的搜尋及服務，而可輕易地取得各項欲查詢的資訊與服務；然而，卻有許多的不法份子亦利用網路的便利性，在未經核可的情況下，非法地駭入私人或公司的網路資料庫中，不當地截取各項資料，如個人的資料或各項機密資訊等，而所截取到的不法資料，卻經常在有心人的操作下，成為詐騙犯罪的工具；是以，雖然網路科技的確帶給人們快速取得資訊的服務優勢，但同時也提供了不法份子搜集被害人個人資料行詐騙取財的另一管道。

據上，目前的電話詐騙集團就是以非法管道取得的個人資料，來對被害人施以詐騙犯罪，惟詐騙的行為，從早期以家用電話通知被害人中獎或退稅等詐騙方式，到目前以手機傳送簡訊，再以各種名目要求被害人轉帳匯款不定的金額至特定的帳號中，可知電話詐騙集團的犯案不僅日益猖獗，且詐騙手法亦不斷地推陳出新，再加上手機的普及，電話詐騙集團以手機做為詐騙犯罪昀

工具，更使得民眾防不勝防。

然而，爲了防止民眾不斷地被詐騙，一美國專利第7,447,302號係揭露一種藉由驗證電話號碼以防止被詐騙的系統，然而，此種系統必需搭配網際網路取得驗證電話號碼之PIN Code，方能確認來電號碼爲合法而非詐騙電話，惟在實施時，需一邊接收來電一邊上網取得所需驗證的PIN Code，因而造成來電接聽及/或驗證的不便，而致防止詐騙的效果不彰。

有鑑於此，於手機上增設一種無需驗證，且可快速偵測或辨識詐騙電話的系統及其方法，以改善習用技術效果不佳等問題。

#### 【發明內容】

本發明係在解決目前電話詐騙集團行手機詐騙時，民眾無法防範而易受到詐騙，終致損失財物及身心受創等問題。

因此，本發明係提供一種智慧型手機之防詐騙系統及其方法，係包括：

一無線通訊模組，係用於接收一來電訊息；

一手機資料庫，其內儲存有多筆詐騙者之來電號碼、聲紋及詐騙類別之關鍵語等資料；及

一辨識模組，係電性連接於該無線通訊模組及該手機資料庫之間，令來電時，該辨識模組亦可接收來電訊息，並與該手機資料庫中之資料行辨識比對。

上述來電訊息係包括來電號碼及談話內容等。

上述辨識模組係利用該無線通訊模組以無線上網的方式至特定網站下載APP軟體並內建於其中，而該APP軟體係可擷取來電訊息，再與該手機資料庫中之資料行辨識比對。而該APP軟體與該

手機資料庫中之資料行辨識比對時，該APP軟體係可偵測ATM提款機的位置並發出警告。

上述智慧型手機之防詐騙系統更包括一雲端伺服器，而該雲端伺服器中包含一雲端資料庫，該雲端資料庫中內存有一詐騙類別關鍵字庫資料、一詐騙的來電號碼資料、一ATM位址資料、一詐騙者之聲紋資料、一地理資訊資料及一最新的詐騙新聞、案例及新方法暨統計報表資料；令該無線通訊模組可透過網路連接下載該雲端資料庫中的資料，藉以更新該手機資料庫中各項的資料。而該雲端伺服器更包括一聲紋比對模組、一關鍵字比對模組、一詐騙統計分析模組、一提款機位置比對模組、一案件暨新聞更新宣導模組、一資料推播更新模組及一發話地理資訊模組。

再者，本發明亦提供一種智慧型手機之防詐騙方法，其至少包括下列步驟：

- a、接獲來電；
- b、擷取來電訊息；
- c、辨識來電號碼；
- d、辨識詐騙類別之關鍵語；
- e、辨識來電者的聲紋；以及
- f、辨識來電的發話處。

上述步驟c、d、e及f中，若遇有不安全的訊息時，該步驟c、d、e及f之後各包括一步驟，該步驟係為通報司法機關查詢及通報。

上述步驟c之前，更包括一步驟，而該步驟為：連接一雲端伺服器。而該雲端伺服器連接之步驟中係下載該雲端伺服器中最新的詐騙新聞、案例及新方法暨統計報表等資料。

本發明的具體特點及功效在於：

一、由於本發明詐騙比對資料中係包含有詐騙者或詐騙集團的電話號碼，令來電未接聽前，即可得知來電者係為詐騙者或詐騙集團；使受話者能立即判斷而拒接，因而能完全阻絕與詐騙者或詐騙集團接觸而有受騙的機率發生。

二、詐騙比對資料中更包含有詐騙者的聲紋及詐騙類別的關鍵語等資料，令來電時，可藉由談話內容的辨識即可得知是否為詐騙者或詐騙集團，進而警示受話者來電者可能是來自詐騙者或詐騙集團，使受話者有心理準備的情況下，而能做出適當的防備，因而可有效地避免民眾受到詐騙。

三、詐騙比對資料係可藉由無線上網的方式，隨時自雲端伺服器中下載更新最新的詐騙比對資料，令詐騙的辨識比對可更為精準，藉以降低民眾被詐騙的機率。

四、隨時可提供最新的詐騙新聞、詐騙方式及詐騙的統計分析運算等資訊，令民眾防詐騙的能力與能詐騙集團日益精進的詐騙手段同步成長，而使詐騙集團的詐騙伎倆無所遁形。

#### 【圖式簡單說明】

第一圖：係本發明之系統第一較佳實施例之示意圖。

第二圖：係本發明之系統第一較佳實施例中手機資料庫之示意圖。

第三圖：係本發明之系統之第一較佳實施例之辨識方塊圖。

第四圖：係本發明中有關 來電號碼辨識預警系統之示意圖。



第五圖：係本發明中有關 提款機偵測與斷話系統之示意圖

。

第六圖：係本發明之系統之第二較佳實施例之示意圖。

第七圖：係本發明中提供新的詐騙方式與新聞等訊息之示意圖。

第八圖：係本發明中有關詐騙個案分析報告之示意圖。

第九圖：係本發明中有關詐編統計分析報告之示意圖。

第十圖：係本發明中有關電信公司暨拍賣網站詐欺統計報告之示意圖。

第十一圖：係本發明中有關詐欺電話號碼分類排名分析報告之示意圖。

第十二圖：係本發明中有關通報檢舉之示意圖。

第十三圖：係本發明中有關向服務機關詐騙檢詢之示意圖。

第十四圖：係本發明之方法之第一較佳實施例之步驟流程圖之一。

第十五圖：係本發明之方法之第一較佳實施例之步驟流程圖之二。

第十六圖：係本發明之方法之第二較佳實施例之步驟流程圖

。

### 【實施方式】

一無線通訊模組(10)，係用來接收一來電訊息；而該來電訊

息中係包括來電號碼及談話內容，其中該談話內容係包括來電號碼、聲紋及詐騙類別之關鍵語等訊息。

一手機資料庫(20)，其內儲存有多筆詐騙者之來電號碼、聲紋及詐騙類別之關鍵語等資料(如第二圖所示)。

一辨識模組(30)，其係利用該無線通訊模組(10)以無線上網(如WiFi)等方式至特定網站(如Android Market)下載一APP軟體並內建於其中，以令該辨識模組(30)可循該APP軟體的指令而具有辨識比對的功能，且該辨識模組(30)係電性連接於該無線通訊模組(10)及該手機資料庫(20)之間；以令來電時，該辨識模組(30)依可利用該APP軟體擷取來電訊息，再與該手機資料庫(20)中之資料行辨識比對；再者，該APP軟體中係建制有一關鍵字辨識與警告、一來電號碼辨識預警、一來電聲紋辨識比對、一提款機偵測與斷話、一提供詐騙方式與新聞、一詐騙統計分析報告及一線上警告或自動離線等辨識比對功能(如第六圖所示)。

請參閱第三圖所示，本實施例於接獲來電時，該辨識模組(30)利用該APP軟體擷取來電訊息，並利用該來電號碼辨識預警功能先比對來電號碼是否與該手機資料庫(20)中內存詐騙者的電話號碼相同，若相符，該辨識模組(30)即會利用該APP軟體上的該來電號碼辨識預警功能發出辨識預警(如第四圖所示)，告知民眾此來電號碼為列管號碼，是否要拒接此一來電；若不相符時，係讓智慧型手機保持通話狀態讓民眾可接聽來電；然而，當談話內容中出現詐騙類別之關鍵語時，該辨識模組(30)中該APP軟體中的該關鍵字辨識與警告功能係會顯示出辨識警告並自動斷話，若談話內容中無出現詐騙類別之關鍵語時，該智慧型手機則無任何警示訊息出現，且讓智慧型手機保持於通話正常的狀態下，而

不干擾來電的接聽；更甚者，該詐騙類別之關鍵語更包含銀行帳號、密碼或金額等，當該辨識模組(30)之該關鍵字辨識與警告功能於來電訊息中偵測到前述的關鍵語時，該APP軟體中之該提款機偵測與斷話功能，若偵測判斷該來電訊息的位置在ATM提款機附近(如第五圖所示)，則會發出警告，告知此來電可能具有高度風險性並警告民眾不要匯款，或自動斷話不讓民眾繼續受騙；接下，該辨識模組(30)中之該來電聲紋辨識比對功能係會再辨識來電者的聲紋及來電的發話處；其中若該聲紋與該手機資料庫(20)中聲紋資料比對相符，該APP軟體則發出警告並且自動斷話，但當不相符時，則繼續接聽來電；再者，當偵測來電發話處不在本地端，該APP軟體係會發出警示更甚者自動斷話，防止民眾受騙；例如，該辨識模組(30)中的該APP軟體在擷取來電訊息，並行偵測及辨識後國碼或區域碼非本地的國碼或區域碼時，係會發出警示是否拒接、或自動斷話(如第四圖所示)；惟當辨識來電的發話處在本地端，則不會干擾而維持正常的通話；再者，該APP軟體係可隨時提供並顯示新的詐騙方式與新聞、一詐騙統計分析報告等資訊給使智慧型手機使用者。

如第六圖所示，係本發明一種智慧型手機之防詐騙系統之第二較佳實施例，本實施例係包括該無線通訊模組(10)、該手機資料庫(20)、該辨識模組(30)及一雲端伺服器(40)，其中該無線通訊模組(10)、該手機資料庫(20)及該辨識模組(30)之作用及功效係與該第一較佳實施例相同而不再贅述；而且在本實施例中，係可利用該無線通訊模組(10)以無線上網(如WiFi)的方式與該雲端伺服器(40)連接，而該雲端伺服器(40)中包含有一雲端資料庫(41)，而該雲端資料庫(41)中內存有一詐騙類別關鍵字庫資料、

一詐騙者來電號碼資料、一ATM位址資料、一詐騙者之聲紋資料、一地理資訊系統資料及一最新的詐騙新聞、案例及新方法暨統計報表資料等等；而該雲端資料庫(41)中的資料係可透過網路連接隨時做資料之更新，意即民眾使用智慧型手機即可隨時至該雲端資料庫(41)中下載最新詐騙資料，使民眾不會因資料過久未更新，而被新的詐騙者詐騙。

是以，在本實施例中，係可藉由該無線通訊模組(10)直接與該雲端伺服器(40)之該雲端資料庫(41)連接，並由該無線通訊模組(10)下載該雲端伺服器(40)中之該雲端資料庫(41)內的資料至該智慧型手機中，再由該辨識模組(30)中的該APP軟體擷取資料後進行辨識比對，而辨識比對的方式係與第一較佳實施例相同外，該雲端伺服器(40)中之該雲端資料庫(41)係可提供最新的詐騙方式與新聞(如第七圖所示)、及詐騙統計分析報告(如第八圖至第十一圖所示，係提供個案分析報告、統計分析報告、電信公司暨拍賣網站詐欺統計報告及詐欺電話號碼分類排名分析報告)等資料，供民眾可藉由該APP軟體顯示該等資訊，讓民眾瞭解詐騙集團不斷推陳出新的詐騙手段，並可培養及提高民眾防止受騙的意識，藉以降低民眾受騙的機率；再者，當本實施例於辨識時，若於談話內容中發現聲紋或來電號碼屬於不安全之訊息時，係會將此一訊息收納於一待分析之可疑案件資料庫(圖中未示)中，待日後再進一步透過網路連結交付相關單位進行分析鑑定，且同時該等不安全之訊息係會透過該APP軟體顯示，藉以告知民眾此訊息屬可疑的來電，應小心防範以免受騙。

再請參閱第六圖所示，該雲端伺服器(40)更包括一聲紋比對模組、一關鍵字比對模組、一詐騙統計分析模組、一提款機位置

比對模組、一案件暨新聞更新宣導模組、一資料推播更新模組及一發話地理資訊模組等；而當接獲來電且利用該無線通訊模組(10)與該雲端伺服器(40)無線上網連接時，該APP軟體係可選擇由該雲端伺服器(40)進行詐騙資料比對、或由該APP軟體內建的功能進行比對，惟由該APP軟體以內建的功能進行比對的方式已於上述內容中揭示而不再贅述；而當由該雲端伺服器(40)進行比對時，可藉由前述模組將來電訊息與該雲端資料庫(41)中的資料進行辨識比對，再由該無線通訊模組(10)回傳至該辨識模組(30)中，經該APP軟體擷取該辨識比對結果，再由該APP軟體中之該線上警告或自動離線功能提出警告或離線等運作；而該雲端資料庫(41)中係包含有一詐騙者的來電號碼資料、一詐騙者的聲紋資料、一詐騙類別之關鍵語資料、一ATM地址資料、一發話地理位置資料、一最新的詐騙新聞案例資料、一新方法暨統計報表資料及一電信業者及/或協力廠商自建資料庫，其中該電信業者及/或協力廠商自建資料庫中亦包含自建之詐騙者的來電號碼資料、詐騙者的聲紋資料、詐騙類別之關鍵語資料、ATM地址資料、發話地理位置資料、最新的詐騙新聞案例資料、新方法暨統計報表資料等等；故藉由該無線通訊模組(10)可下載該雲端資料庫(41)中的資料外，該無線通訊模組(10)亦可下載該雲端資料庫(41)中電信業者及/或協力廠商自建資料庫內的資料至該智慧型手機中。

請參閱第十二圖及第十三圖所示，當該APP軟體對來電訊息發出或顯示警示、或拒接、或自動斷話後，該APP軟體係可向司法機關通報檢舉外，對可疑的來電亦可透過該APP軟體向相關的服務機關查詢。

請參閱第十四圖所示，係本發明一較佳實施例之方法之步驟

流程圖，如圖所示，本發明一種智慧型手機之防詐騙方法之第一較佳實施例，其至少包括下列步驟：

- a、接獲來電；
- b、擷取來電訊息；
- c、辨識來電號碼；
- d、辨識詐騙類別之關鍵語；
- e、辨識來電者的聲紋；以及
- f、辨識來電的發話處。

其中在該步驟b及該步驟c中，該辨識模組(30)係於通話前或後，擷取來電訊息，並先比對來電號碼是否與該手機資料庫(20)中內存詐騙集團的電話號碼相同，若相符，該辨識模組(30)即會發出辨識預警，告知民眾應拒接電話，若不相符時，係讓智慧型手機保持通話狀態讓民眾可接聽來電。

而在該步驟d中，若談話內容中出現詐騙類別之關鍵語時，該辨識模組(30)係會發出辨識警告並自動斷話，若談話內容中無出現詐騙類別之關鍵語時，該智慧型手機則無任何警示訊息出現，且讓智慧型手機保持於通話正常的狀態下，而不干擾來電的接聽；再者，該詐騙類別之關鍵語更包含銀行帳號、密碼或金額等，當該辨識模組(30)於來電的訊息中辨識到前述的關鍵語時，則會被判定民眾在ATM提款機附近，則會發出警示，告知此來電是詐騙電話不要匯款，或自動斷話不讓民眾匯款受騙。

又在該步驟e及該步驟f中，該辨識模組(30)係會再辨識來電者的聲紋及來電的發話處；其中若該聲紋與該手機資料庫(20)中聲紋資料比對相符，則發出警告並且自動斷話，但當不相符時，則可繼續通話；再者，當偵測來電發話處不在本地端，該辨識模

組(30)係會發出警示更甚著自動斷話，防止民眾受騙；例如國碼或區域碼非本地的國碼或區域碼時，該辨識模組(30)則在偵測及辨識下發出警示或自動斷話；惟當辨識來電的發話處在本地端，則不會干擾而維持正常的通話。

又如第十五圖所示，於該步驟c、d、e及f中，若遇有不安全的訊息時，該步驟c、d、e及f之後各包括一步驟c-1、一步驟d-1、一步驟e-1及一步驟f-1，且該步驟c-1、該步驟d-1、該步驟e-1及該步驟f-1係為向司法機關通報檢舉外，亦對可疑的來電向相關的服務機關查詢。

請參閱第十六圖所示，係本發明一種智慧型手機之防詐騙方法之第二較佳實施例，其至少包括下列步驟：

- g、接獲來電；
- h、擷取來電訊息；
- i、連接該雲端伺服器(40)
- j、辨識來電號碼；
- k、辨識詐騙類別之關鍵語；
- l、辨識來電者的聲紋；以及
- m、辨識來電的發話處。

在本實施例，該步驟j、k、l及m中所述的方法係與第一較佳實施例的步驟方法同，惟其差異之處在於：該步驟j、k、l及m辨識比對的資料係為該雲端伺服器(40)之雲端資料庫(41)中預存詐騙者的來電號碼、聲紋及詐騙類別之關鍵語等資料，惟辨識方法均相同，且當遇有不安全的訊息時，亦相同會發出警示或使智慧型手機自動斷線，故不贅述；再者，於該步驟i與該雲端伺服器(40)連接時，係可藉由該無線通訊模組(10)將該雲端伺服器(40)

中最新的詐騙新聞、案件及新方法暨統計報表等資料，下載傳送回手機中供民眾讀取，藉以讓民眾瞭解詐騙集團不斷推陳出新的詐騙手段，進而培養及提高民眾防止受騙的意識，期降低民眾受騙的機率。

惟，以上所述者，僅為本發明之較佳實施例而已，並非用以侷限本發明之技術特徵，舉凡利用本發明相關之技術手段、創設原理之再發明，仍屬本發明的發明範疇，因此本發明圖式及說明書所述之陳並非用以限定本發明之範圍，任何熟習此技藝者，在不脫離本發明之精神與範圍下所作之均等變化與修飾，皆應涵蓋於本發明之申請專利範圍，方為合理。

#### 【符號說明】

- ( 1 0 ) 無線通訊模組
- ( 2 0 ) 手機資料庫
- ( 3 0 ) 辨識模組
- ( 4 0 ) 雲端伺服器
- ( 4 1 ) 雲端資料庫



## 【發明申請專利範圍】

1. 一種智慧型手機之防詐騙系統，其包括：
  - 一無線通訊模組，係用於接收一來電訊息；
  - 一手機資料庫，其內儲存有多筆詐騙者之來電號碼、聲紋及詐騙類別之關鍵語資料；及
  - 一辨識模組，係電性連接於該無線通訊模組及該手機資料庫之間，令來電時，該辨識模組亦可接收來電訊息，並與該手機資料庫中之資料行辨識比對；

該辨識模組係利用該無線通訊模組以無線上網的方式至特定網站下載APP軟體並內建於其中，而該APP軟體係供擷取來電訊息，再與該手機資料庫中之資料進行辨識比對，該APP軟體係可偵測ATM提款機的位置並發出警告；

該辨識模組中的該APP軟體在擷取來電訊息，並執行偵測及辨識該來電訊息之發話處的國碼或區域碼非本地的國碼或區域碼時，則會發出警示是否拒接或自動斷話；

  - 一雲端伺服器，包含一雲端資料庫、一聲紋比對模組、一關鍵字比對模組、一詐騙統計分析模組、一提款機位置比對模組、一案件暨新聞更新宣導模組、一資料推播更新模組及一發話地理資訊模組；

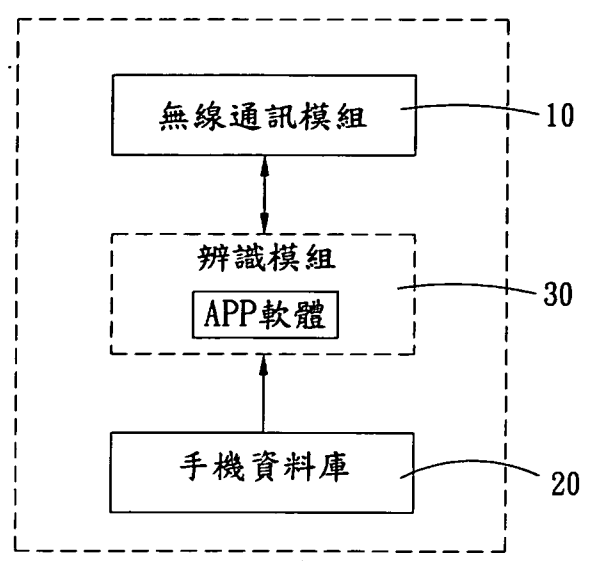
該雲端資料庫中內存有一詐騙類別關鍵字庫資料、一詐騙的來電號碼資料、一ATM位址資料、一詐騙者之聲紋資料、一地理資訊資料及一最新的詐騙新聞、案例及新方法暨統計報

表資料；

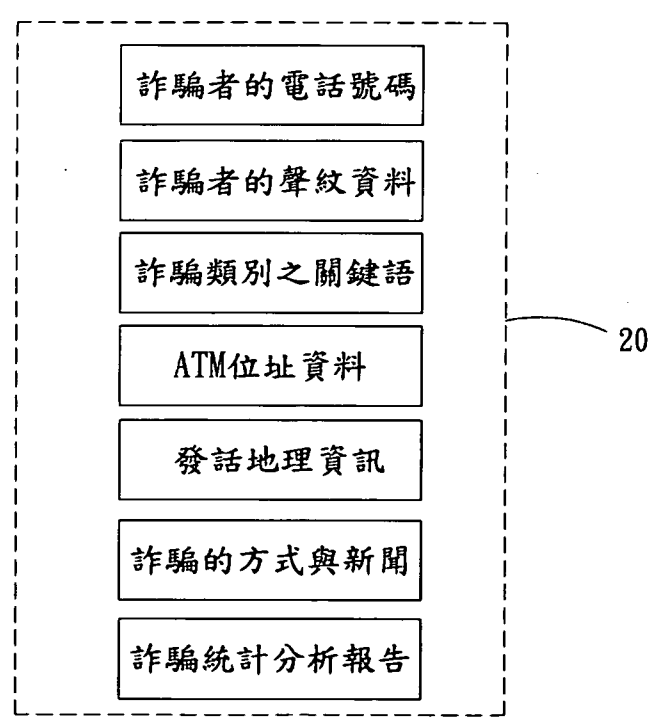
透過執行該APP軟體，令該無線通訊模組可透過網路連接下載該雲端資料庫中的資料，藉以更新該手機資料庫中各項的資料。

2. 如申請專利範圍第1項所述之智慧型手機之防詐騙系統，其中該來電訊息係包括來電號碼及談話內容。
3. 一種智慧型手機之防詐騙方法，係於該智慧型手機執行一APP軟體，連接至一雲端伺服器，並於該雲端伺服器下載最新的詐騙新聞、案例及新方法暨統計報表資料，其至少包括下列步驟：
  - a、接獲來電；
  - b、擷取來電訊息；
  - c、辨識來電號碼；
  - d、辨識詐騙類別之關鍵語；
  - e、辨識來電者的聲紋；以及
  - f、辨識來電的發話處之ATM提款機位置及國碼或區域碼。
4. 如申請專利範圍第3項所述之智慧型手機之防詐騙方法，其中於該步驟c、d、e及f中，若遇有不安全的訊息時，該步驟c、d、e及f之後各包括一步驟，該步驟係為通報司法機關查詢及通報。

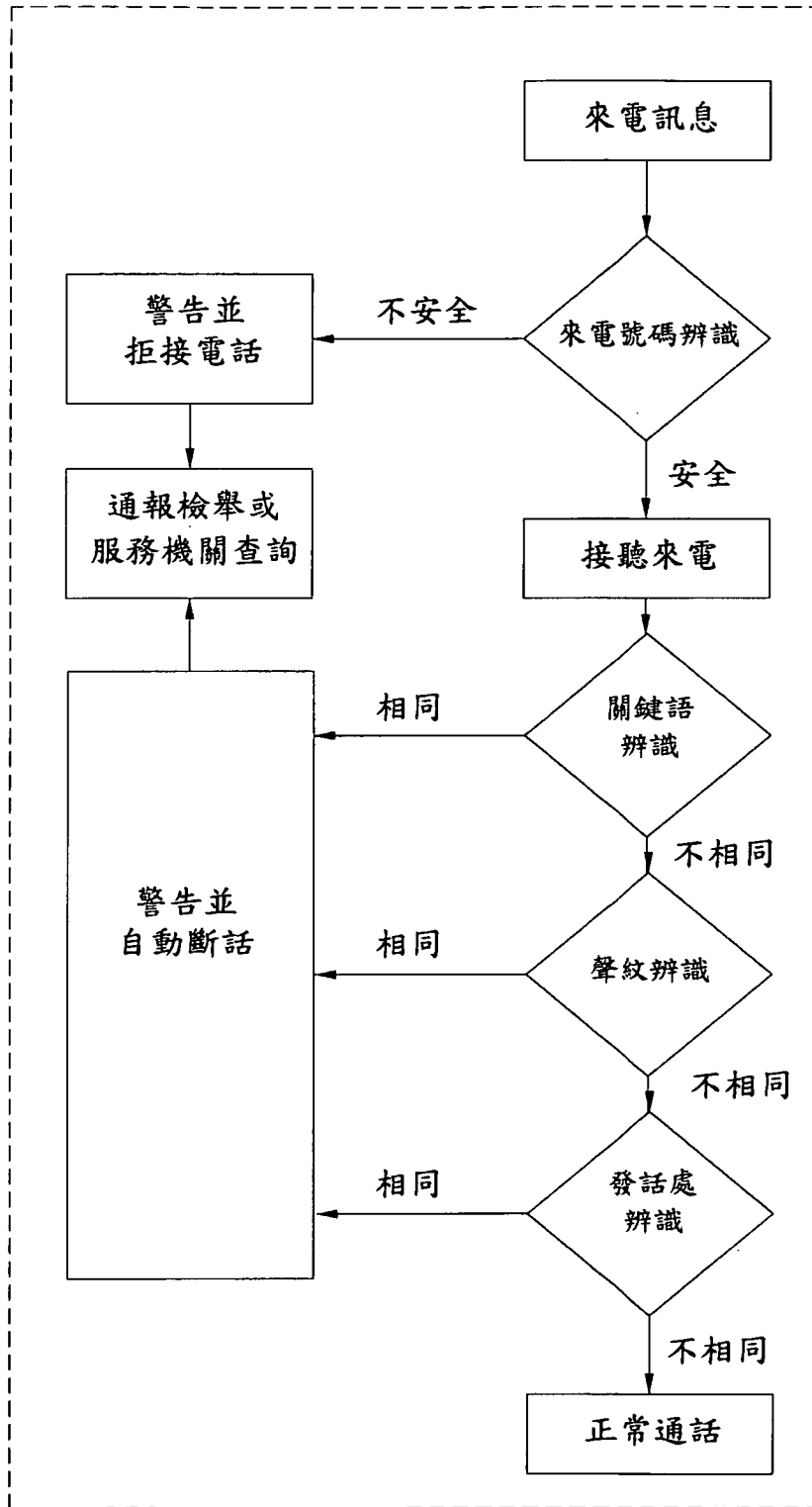
# 【發明圖式】



第一圖



第二圖



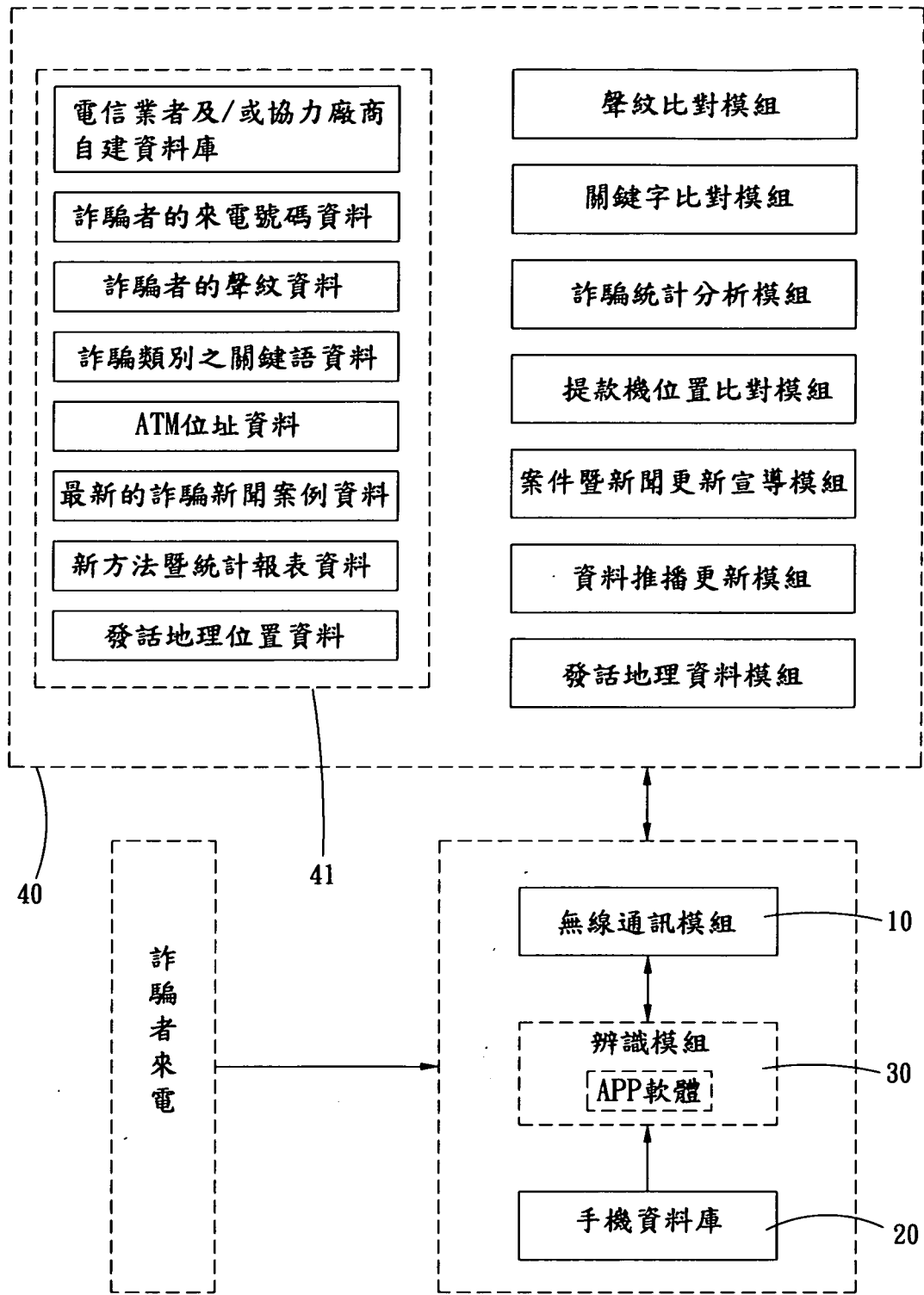
第三圖



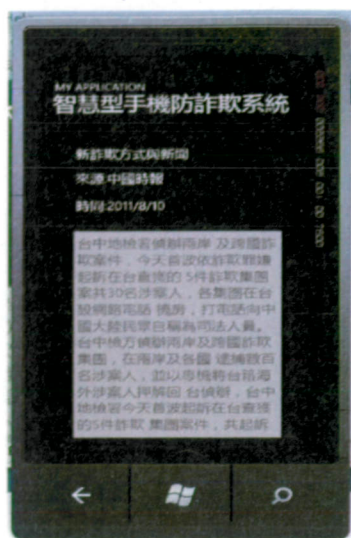
第四圖



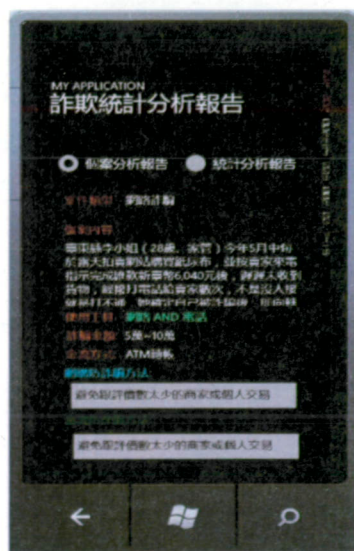
第五圖



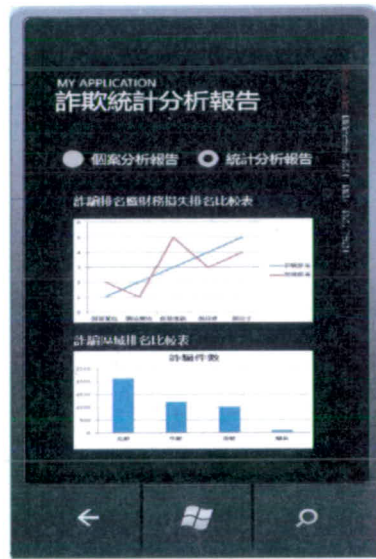
第六圖



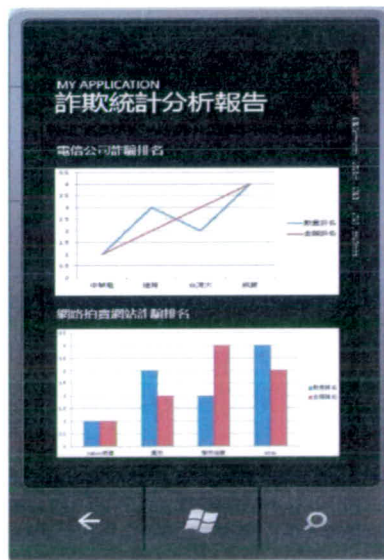
第七圖



第八圖

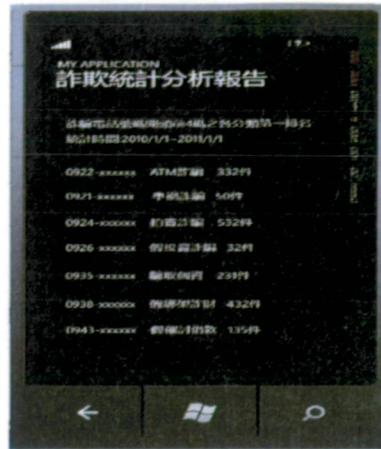


第九圖



第十圖





第十一圖

MY APPLICATION  
165全民防詐騙檢舉

我要檢舉  
 通報檢舉     服務機關查詢

詐騙縣市:

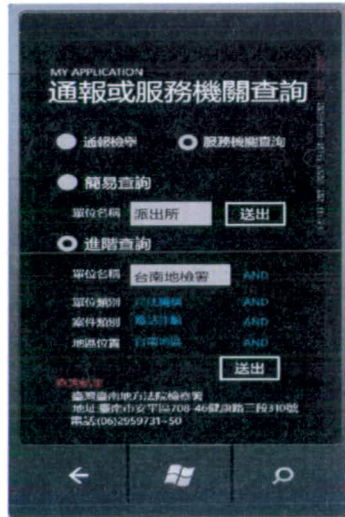
詐騙時間:

詐騙方式:  網路     文件  
 電話     會面

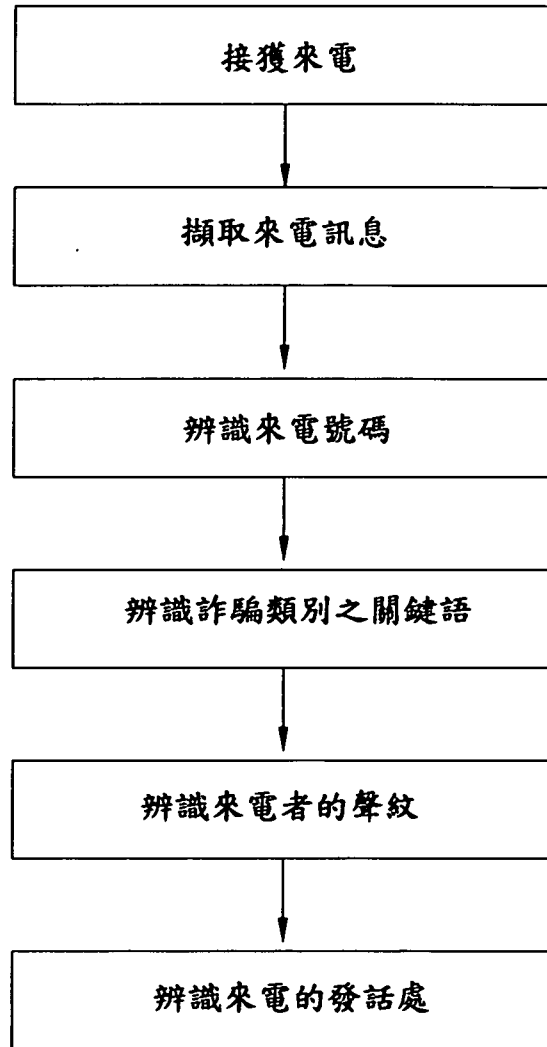
詐騙方式:

<input checked="" type="checkbox"/> 退費或退稅	<input type="checkbox"/> 中獎通知
<input type="checkbox"/> 金光票	<input type="checkbox"/> 假求職
<input type="checkbox"/> 假交友	<input type="checkbox"/> 假廣告
<input type="checkbox"/> 假車禍	<input type="checkbox"/> 假慈善機構

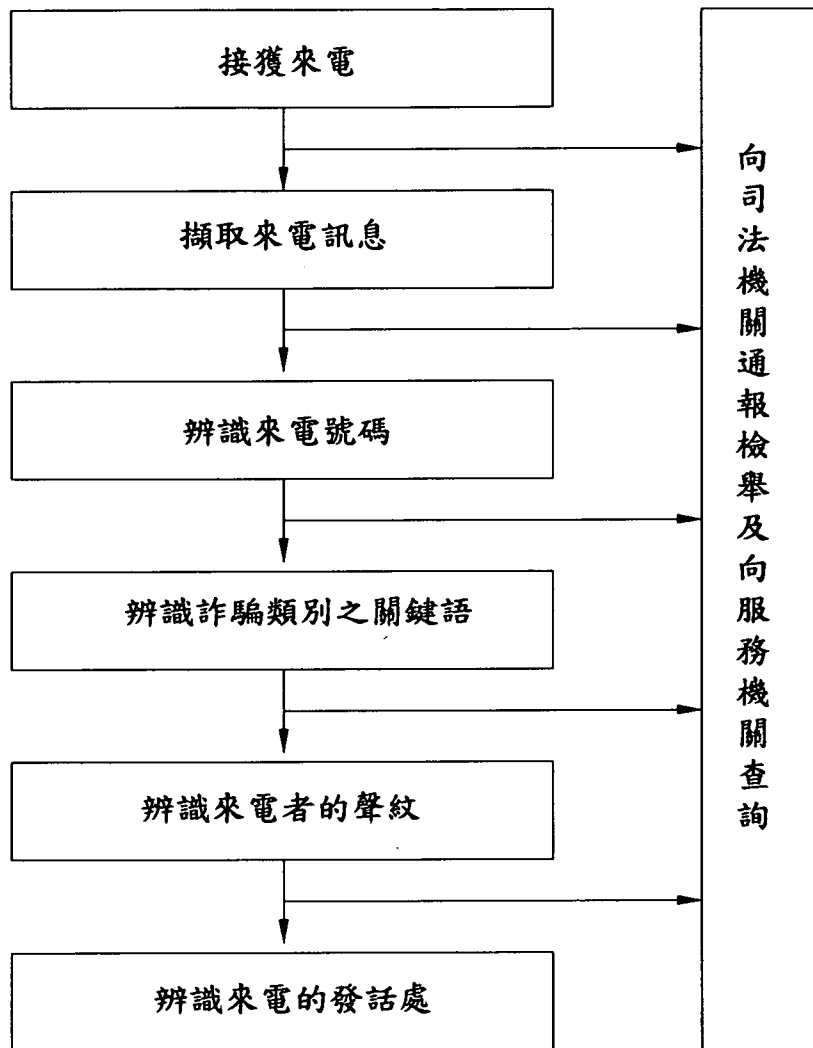
第十二圖



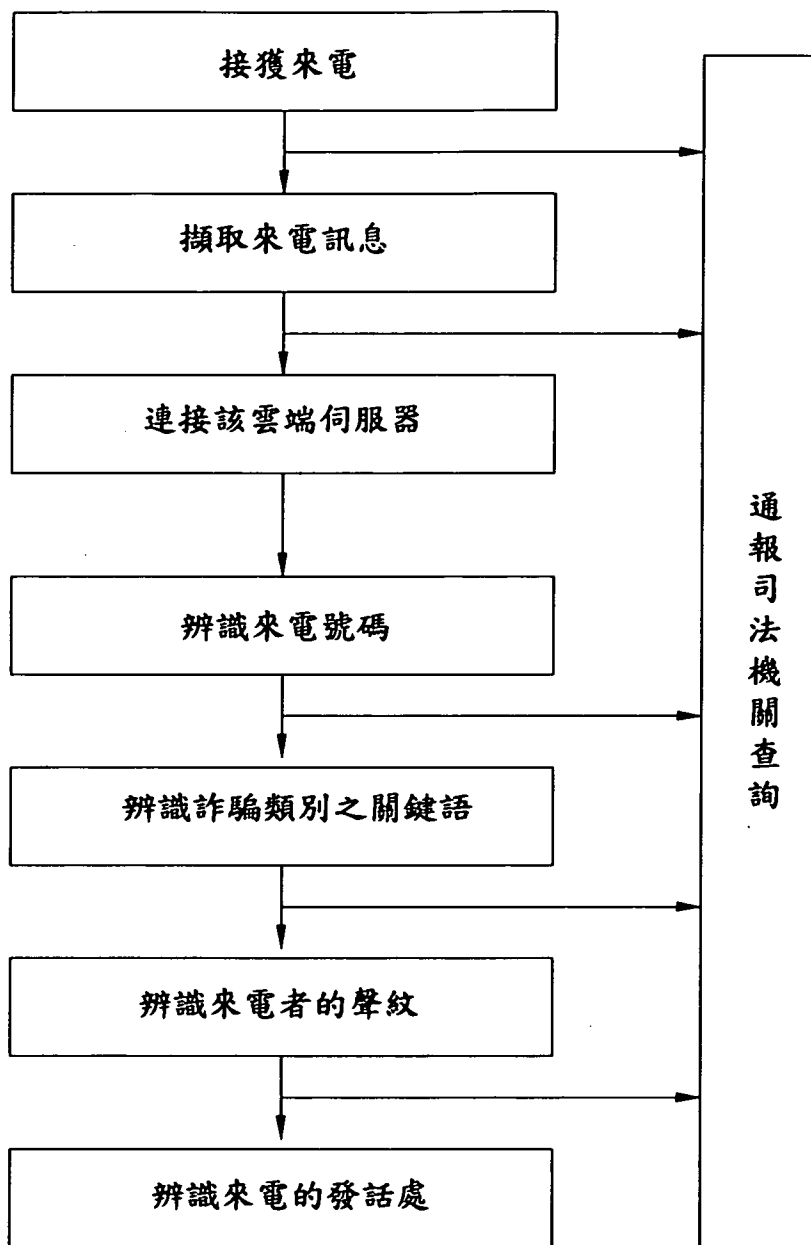
第十三圖



第十四圖



第十五圖



第十六圖