I461952

(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 I461952 B

(45)公告日： 中華民國 103 (2014) 年 11 月 21 日

(21)申請案號：101150253 (22)申請日： 中華民國 101 (2012) 年 12 月 26 日

(51)Int. Cl.： *G06F21/10 (2013.01)* *G06F21/56 (2013.01)*

(71)申請人：國立臺灣科技大學 (中華民國) NATIONAL TAIWAN UNIVERSITY OF SCIENCE AND TECHNOLOGY (TW)

臺北市大安區基隆路 4 段 43 號

(72)發明人：李漢銘 LEE, HAHN MING (TW) ；吳東杰 WU, DONG JIE (TW) ；毛敬豪 MAO, CHING HAO (TW) ；魏得恩 WEI, TE EN (TW)

(74)代理人：詹銘文；葉璟宗

(56)參考文獻：

TW 200917020A CN 101977188A

US 7788724B2

審查人員：潘世光

申請專利範圍項數：10 項 圖式數：4 共 23 頁

(54)名稱

惡意程式偵測方法與系統

METHOD AND SYSTEM FOR DETECTING MALWARE APPLICATIONS

(57)摘要

一種惡意程式偵測方法。自數個正常及惡意訓練應用程式安裝檔的資訊設定檔及反編譯程式碼取出靜態行為特徵。利用群聚演算法產生至少一惡意應用程式群組，另產生出至少一正常應用程式群組。根據各惡意與正常應用程式群組中訓練應用程式安裝檔的靜態行為特徵，產生分別代表各惡意與正常應用程式群組的應用程式偵測模型。自待測應用程式安裝檔的待測資訊設定檔及反編譯程式碼取出待測靜態行為特徵，再利用分類演算法、待測靜態行為特徵、及各惡意與正常應用程式偵測模型判定待測應用程式安裝檔屬於其中一個惡意應用程式群組時，產生警告訊息。

A method for detecting malware applications is provided. The present method includes respectively obtaining a manifest file and de-compiled code from a plurality of training benign and malware application package files (APKs), and extracting at least one static feature from each manifest file and de-compiled code. The method also includes generating at least one malware application group based on the training malware APKs by using a clustering algorithm, generating at least one benign application group based on the training benign APKs by referring to classification rule designed by the application market, and generating application detecting models that respectively represent each malware application group and benign application group in accordance with the static feature of the training malware APKs in each malware application group and the static feature of the training benign APKs in each benign application group. The method also includes, when receiving a target APK, obtaining a target manifest file and de-compiled code, then accordingly extracting at least one target static feature. The method further includes using a classification algorithm, at least one target static feature and application models that respectively represent each malware application group and benign application group to determining whether the target APK is belonging to any malware application group or benign application group. Once the target APK is classified

as malware application group, the method further includes generating a warning message if the determination result is positive.

S310~S390・・・本發明之一實施例所述之惡意程式偵測方法之各步驟

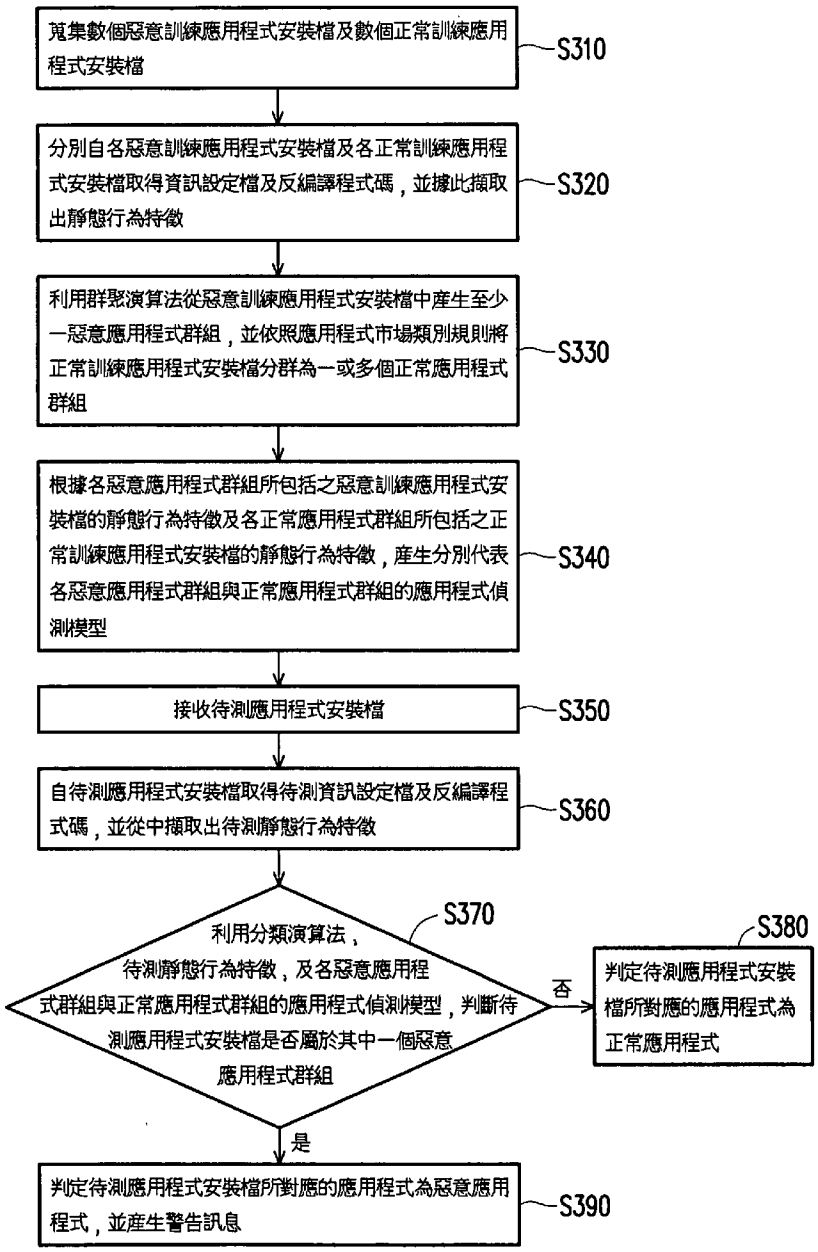

圖3

公告本

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：(011502S3

※ 申請日：101.12.26　　※IPC 分類：G06F 21/10 (2013.01)
21/56 (2013.01)

一、發明名稱：

惡意程式偵測方法與系統 / METHOD AND SYSTEM FOR DETECTING MALWARE APPLICATIONS

二、中文發明摘要：

一種惡意程式偵測方法。自數個正常及惡意訓練應用程式安裝檔的資訊設定檔及反編譯程式碼取出靜態行為特徵。利用群聚演算法產生至少一惡意應用程式群組，另產生出至少一正常應用程式群組。根據各惡意與正常應用程式群組中訓練應用程式安裝檔的靜態行為特徵，產生分別代表各惡意與正常應用程式群組的應用程式偵測模型。自待測應用程式安裝檔的待測資訊設定檔及反編譯程式碼取出待測靜態行為特徵，再利用分類演算法、待測靜態行為特徵、及各惡意與正常應用程式偵測模型判定待測應用程式安裝檔屬於其中一個惡意應用程式群組時，產生警告訊息。

三、英文發明摘要：

A method for detecting malware applications is provided. The present method includes respectively obtaining a manifest file and de-compiled code from a plurality of training benign and malware application package files (APKs), and extracting at least one static feature from each manifest file and de-compiled code. The method also includes generating at least one malware application group based on the training malware APKs by using a clustering algorithm, generating at least one benign application group based on the training benign APKs by referring to classification rule designed by the application market, and generating application detecting models that respectively represent each malware application group and benign application group in accordance with the static feature of the training malware APKs in each malware application group and the static feature of the training benign APKs in each benign application group. The method also includes, when receiving a target APK, obtaining a target manifest file and de-compiled code, then accordingly extracting at least one target static feature. The method further includes using a classification algorithm, at least one target static feature and application models that respectively represent each malware application group and benign application group to

determining whether the target APK is belonging to any malware application group or benign application group. Once the target APK is classified as malware application group, the method further includes generating a warning message if the determination result is positive.

四、指定代表圖：

（一）本案之指定代表圖：圖 3

（二）本代表圖之元件符號簡單說明：

S310～S390：本發明之一實施例所述之惡意程式偵測方法之各步驟

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

六、發明說明：

【發明所屬之技術領域】

本發明是有關於一種應用程式的檢測方法，且特別是有關於一種檢測安裝於行動電子裝置之惡意應用程式的方法與系統。

【先前技術】

隨著智慧型手機與平板電腦的興起，現代人的生活也與這類行動電子裝置日愈緊密結合。而智慧型手機與平板電腦的普及化更帶動了應用程式（Application）產業的蓬勃發展。

以基於安卓（Android）平台開發的應用程式為例，由於近年來 Android 應用程式逆向工程技術的成熟，許多有心人士會將 Android 惡意應用程式重新包裝後散播於應用程式市場，基此讓一般使用者容易在無意間下載了包括惡意程式碼或病毒的應用程式，造成私人資訊被任意竊取等風險。然而，若使用傳統偵測惡意應用程式的方法，多半會因為必須依賴已知的病毒碼或程式行為而無法偵測新型變種病毒，且由於上述被重新包裝後的惡意應用程式與原先正常的應用程式十分相似，差別僅在於部分被注入的惡意元件，而這些被注入之惡意元件多半在背景運作以躲避偵測，因此也不易有效偵測。基此，實有必要研發一套能有效針對惡意應用程式進行偵測及示警的機制。

【發明內容】

有鑑於此，本發明提供一種惡意程式偵測方法與系統，能快速且有效地識別可安裝於行動電子裝置的應用程式是否為惡意應用程式。

本發明提出一種惡意程式偵測方法，此方法包括蒐集多個惡意訓練應用程式安裝檔及多個正常訓練應用程式安裝檔。分別自各惡意訓練應用程式安裝檔及各正常訓練應用程式安裝檔取得資訊設定檔（Manifest file）及反編譯程式碼，並從各資訊設定檔及反編譯程式碼中擷取出靜態行為特徵。利用群聚演算法從惡意訓練應用程式安裝檔中產生至少一惡意應用程式群組。此外，依照應用程式市場類別規則，將正常訓練應用程式安裝檔分群為至少一正常應用程式群組。根據各惡意應用程式群組所包括之惡意訓練應用程式安裝檔的靜態行為特徵及各正常應用程式群組所包括之正常訓練應用程式安裝檔的靜態行為特徵，產生分別代表各惡意應用程式群組與正常應用程式群組的應用程式偵測模型。當接收到一待測應用程式安裝檔時，自待測應用程式安裝檔取得待測資訊設定檔及反編譯程式碼，並從待測資訊設定檔及反編譯程式碼中擷取出待測靜態行為特徵，再利用分類演算法、上述待測靜態行為特徵及各惡意應用程式群組與正常應用程式群組的應用程式偵測模型，判斷待測應用程式安裝檔是否屬於其中一個惡意應用程式群組。若是，則產生警告訊息。

從另一觀點來看，本發明提出一種惡意程式偵測系

統，包括特徵擷取單元、群聚單元以及判別單元。其中，特徵擷取單元用以接收多個惡意訓練應用程式安裝檔及多個正常訓練應用程式安裝檔，並分別自各惡意訓練應用程式安裝檔及各正常訓練應用程式安裝檔取得資訊設定檔及反編譯程式碼，且從各資訊設定檔及反編譯程式碼擷取出靜態行為特徵。群聚單元耦接特徵擷取單元，以利用群聚演算法從惡意訓練應用程式安裝檔中產生至少一惡意應用程式群組；此外，依照應用程式市場類別規則，將正常訓練應用程式安裝檔分群為至少一正常應用程式群組。根據各惡意應用程式群組所包括之惡意訓練應用程式安裝檔的靜態行為特徵及各正常應用程式群組所包括之正常訓練應用程式安裝檔的靜態行為特徵，產生分別代表各惡意應用程式群組與正常應用程式群組的應用程式偵測模型。判別單元耦接特徵擷取單元與群聚單元，以在接收待測應用程式安裝檔時，控制特徵擷取單元自待測應用程式安裝檔取得待測資訊設定檔及反編譯程式碼，並從待測資訊設定檔及反編譯程式碼擷取出待測靜態行為特徵。判別單元利用分類演算法、待測靜態行為特徵及各惡意應用程式群組與正常應用程式群組的應用程式偵測模型，判斷待測應用程式安裝檔是否屬於其中一個惡意應用程式群組，並且在判定待測應用程式安裝檔屬於其中一個惡意應用程式群組時，產生警告訊息。

基於上述，本發明是利用應用程式之資訊設定檔及反編譯程式碼所包括的各種靜態行為特徵來建立惡意與正常

應用程式群組，據此針對待測的應用程式，亦可透過解析其安裝檔中的資訊設定檔及反編譯程式碼，以利用其靜態行為特徵來識別是否為惡意應用程式。據此，在不需要應用程式原始碼的前提下，能產生快速且準確的偵測結果。

為讓本發明之上述特徵和優點能更明顯易懂，下文特舉實施例，並配合所附圖式作詳細說明如下。

【實施方式】

圖 1 是依照本發明之一實施例所繪示之惡意程式偵測系統的方塊圖。請參閱圖 1，惡意程式偵測系統 100 包括特徵擷取單元 110、群聚單元 120，以及判別單元 130。群聚單元 120 則包括權重決定單元 121、群數評估單元 123，以及模型產生單元 125。其中，特徵擷取單元 110 耦接至群聚單元 120，而判別單元 130 分別耦接至特徵擷取單元 110 與群聚單元 120。

惡意程式偵測系統 100 主要是透過靜態分析來辨別應用程式是否為含有病毒、惡意程式碼的應用程式。特別是，惡意程式偵測系統 100 能有效偵測適於安裝在行動電子裝置之應用程式的安全性，以達到行動電子裝置之安全防護功效。其中，行動電子裝置可為智慧型手機、個人數位助理、或平板電腦等，而應用程式例如是基於安卓（Android）平台的應用程式，但本發明並不以此為限。

在本實施例中，惡意程式偵測系統 100 的運作流程主要包含兩個階段。請參閱圖 2，在步驟 S210 所示之訓練階

段中，透過特徵擷取單元 110 與群聚單元 120 的運作，惡意程式偵測系統 100 會根據蒐集而來的數個正常訓練應用程式安裝檔及數個惡意訓練應用程式安裝檔建立至少一正常及惡意應用程式偵測模型，據以讓判別單元 130 在步驟 S220 所示之檢測階段時，利用上述應用程式偵測模型分析待測的應用程式是否為惡意應用程式。

值得一提的是，本實施例之特徵擷取單元 110 係從各訓練應用程式安裝檔的資訊設定檔（Manifest file）及反編譯程式碼中擷取訓練應用程式的靜態行為特徵。而群聚單元 120 將根據上述靜態行為特徵產生用於分析應用程式是否正常的應用程式偵測模型。也就是說，本實施例之惡意程式偵測系統 100 主要係利用訓練應用程式安裝檔之資訊設定檔及反編譯程式碼所提供的資訊，以產生用於檢測階段的惡意與正常應用程式偵測模型。

在另一實施例中，惡意程式偵測系統 100 還包括網路單元（未繪示）。據此，使用者可在終端裝置（例如，智慧型手機）透過網路連接惡意程式偵測系統 100，以對特定應用程式進行檢測。

上述各個單元可由硬體、軟體，或硬體及軟體的組合來實作。舉例而言，硬體可以是中央處理單元（Central Processing Unit，CPU）、其他可程式化之一般用途或特殊用途的微處理器（Microprocessor）、數位訊號處理器（Digital Signal Processor，DSP）、可程式化控制器、特殊應用積體電路（Application Specific Integrated Circuit，

ASIC）、或任何具備運算及處理能力的裝置或上述裝置的組合。軟體則包括作業系統、應用程式或驅動程式。

以下將以另一實施例來說明惡意程式偵測系統100之各單元的詳細運作方式。圖3是依照本發明之一實施例所繪示之惡意程式偵測方法的流程圖。請同時參閱圖1與圖3。

在步驟S310中，惡意程式偵測系統100蒐集多個訓練應用程式安裝檔。上述訓練應用程式安裝檔包括數種惡意應用程式的安裝檔（簡稱為惡意訓練應用程式安裝檔）及數種正常應用程式的安裝檔（簡稱為正常訓練應用程式安裝檔）。

接著如步驟S320所示，特徵擷取單元110接收蒐集到的惡意訓練應用程式安裝檔與正常訓練應用程式安裝檔，並解除各惡意及正常訓練應用程式安裝檔的封裝，以分別自各惡意訓練應用程式安裝檔及各正常訓練應用程式安裝檔取得資訊設定檔及反編譯程式碼，並從各資訊設定檔及反編譯程式碼中擷取出各惡意訓練應用程式安裝檔及各正常訓練應用程式安裝檔所對應之應用程式的靜態行為特徵。其中，靜態行為特徵至少包括使用權限（Permission）、元件（Component）及所屬元件類型、意圖（Intent）、應用程式介面呼叫（API call）其中之一及其組合者。而所屬元件類型例如是活動（Activity）、服務（Service）、接收器（Receiver）、提供器（Provider）等。

在步驟S330中，群聚單元120利用群聚演算法從所

有惡意訓練應用程式安裝檔中產生至少一惡意應用程式群組，並依照應用程式市場類別規則將所有正常訓練應用程式安裝檔分群為至少一正常應用程式群組。並且在步驟S340中，群聚單元120根據各惡意應用程式群組所包括之惡意訓練應用程式安裝檔的靜態行為特徵及各正常應用程式群組所包括之正常訓練應用程式安裝檔的靜態行為特徵，產生分別代表各惡意應用程式群組與各正常應用程式群組的應用程式偵測模型。詳言之，群聚單元120係將特徵擷取單元110所萃取出的所有靜態行為特徵以向量形式表示，並套用群聚演算法產生數群具有相似之靜態行為特徵的惡意應用程式群組；此外，群聚單元120依照應用程式市場類別規則來產生數群具有相似之靜態行為特徵的正常應用程式群組。而各惡意及正常應用程式群組均對應特定的應用程式偵測模型（分別簡稱為惡意應用程式偵測模型及正常應用程式偵測模型）。值得一提的是，群聚單元120可根據蒐集之訓練應用程式安裝檔的特性不同而選用適當的群聚演算法。

以下特別以圖4來說明群聚單元120的詳細運作流程。請參閱圖4。

首先如步驟S410所示，權重決定單元121評估各靜態行為特徵於惡意訓練應用程式安裝檔的權重。舉例來說，針對每一惡意訓練應用程式安裝檔，權重決定單元121將統計每一靜態行為特徵在每一惡意訓練應用程式安裝檔中的出現次數。而針對各靜態行為特徵，權重決定單元121

統計具備此靜態行為特徵的惡意訓練應用程式數量。並且，權重決定單元 121 利用詞頻-逆向文件頻率（Term Frequency-Inverse Document Frequency，TF-IDF）公式計算各靜態行為特徵於各惡意訓練應用程式安裝檔的權重。進一步來說，權重的高低可反映各靜態行為特徵的重要性。

接著在步驟 S420 中，群數評估單元 123 將各惡意訓練應用程式安裝檔之靜態行為特徵表示為向量形式並產生聚類群數。詳言之，群數評估單元 123 利用奇異值分解（Singular Value Decomposition，SVD）公式計算特徵值（eigenvalue），並取得前 N 個涵蓋一特定百分比的頻譜能量（spectral energy）以代表聚類群數。其中，群數評估單元 123 是由大到小計算得到特徵值及其涵蓋頻譜能量，並優先取得前 N 個頻譜能量來使用。須注意的是，N 為正整數但本發明並不將 N 限定為一個固定常數，N 的大小是取決於特定百分比的數值。舉例來說，特定百分比例如為 95%，但本發明並不以此為限。

並且如步驟 S430 所示，模型產生單元 125 將各惡意訓練應用程式安裝檔之靜態行為特徵的權重及向量形式套用至群聚演算法，藉以產生至少一惡意應用程式群組。其中，屬於同一惡意應用程式群組的所有訓練應用程式安裝檔具有相似之靜態行為特徵。而針對正常應用程式群組的訓練應用程式安裝檔，模型產生單元 125 則依照市場應用程式類別規則，將正常訓練應用程式安裝檔分群為至少一正常應用程式群組。

圖 3 之步驟 S310 至步驟 S340 即為惡意程式偵測系統 100 的訓練階段。日後當惡意程式偵測系統 100 進入檢測階段，亦即，使用者欲對一待測應用程式安裝檔的安全性進行檢測之際，使用者可透過網路將待測應用程式安裝檔上傳至惡意程式偵測系統 100。而惡意程式偵測系統 100 將利用訓練階段所產生的正常及惡意應用程式偵測模型來檢測待測應用程式安裝檔的安全性。

詳言之，請回到圖 3 之步驟 S350，判別單元 130 接收目前要進行檢測的待測應用程式安裝檔，並在步驟 S360 中，判別單元 130 控制特徵擷取單元 110 自待測應用程式安裝檔取得待測資訊設定檔及反編譯程式碼，並從待測資訊設定檔及反編譯程式碼擷取出待測靜態行為特徵。待測靜態行為特徵至少包括使用權限（Permission）、元件（Component）及所屬元件類型、意圖（Intent）、應用程式介面呼叫（API call）其中之一及其組合者。而所屬元件類型例如是活動（Activity）、服務（Service）、接收器（Receiver）、提供器（Provider）等。

接著在步驟 S370 中，判別單元 130 利用分類演算法、特徵擷取單元 110 萃取出的待測靜態行為特徵，以及群聚單元 120 產生的各種惡意應用程式偵測模型與正常應用程式偵測模型，來判斷待測應用程式安裝檔是否屬於其中一個惡意應用程式群組。

若待測應用程式安裝檔並不屬於任何惡意應用程式群組，則如步驟 S380 所示，判別單元 130 判定待測應用

程式安裝檔所對應的應用程式為正常應用程式。

然而，倘若待測應用程式安裝檔屬於某一惡意應用程式群組，則在步驟 S390 中，判別單元 130 判定待測應用程式安裝檔所對應的應用程式為惡意應用程式，並產生警告訊息。

如圖 3 所示，由於惡意程式偵測系統 100 是基於取自應用程式安裝檔的資訊設定檔及反編譯程式碼來建立用於檢測的惡意與正常應用程式偵測模型。因此當需對某一待測應用程式進行檢測時，惡意程式偵測系統 100 僅需要此待測應用程式的安裝檔而不需要其完整原始碼，便可從待測應用程式安裝檔的資訊設定檔及反編譯程式碼中取得進行分析所需要的資訊。

綜上所述，本發明所述之惡意程式偵測方法與系統係利用應用程式安裝檔之資訊設定檔及反編譯程式碼所提供的使用權限、元件及所屬元件類型、意圖、應用程式介面呼叫等靜態行為特徵來產生用於檢測的模型，據此在檢測應用程式的安全性時，不需要應用程式的原始碼，而僅需編譯好的安裝檔即可完成分析。此外，基於靜態分析的檢測流程不僅不會佔據過多的系統資源，同時亦能提供更有效率且具準確性的分析結果。

雖然本發明已以實施例揭露如上，然其並非用以限定本發明，任何所屬技術領域中具有通常知識者，在不脫離本發明之精神和範圍內，當可作些許之更動與潤飾，故本發明之保護範圍當視後附之申請專利範圍所界定者為準。

【圖式簡單說明】

圖 1 是依照本發明之一實施例所繪示之惡意程式偵測系統的方塊圖。

圖 2 是依照本發明之一實施例所繪示之惡意程式偵測系統的運作流程圖。

圖 3 是依照本發明之一實施例所繪示之惡意程式偵測方法的流程圖。

圖 4 是依照本發明之一實施例所繪示之群聚單元的運作流程圖。

【主要元件符號說明】

100：惡意程式偵測系統

110：特徵擷取單元

120：群聚單元

121：權重決定單元

123：群數評估單元

125：模型產生單元

130：判別單元

S210～S220：本發明之一實施例所述之惡意程式偵測系統的運作步驟

S310～S390：本發明之一實施例所述之惡意程式偵測方法之各步驟

S410～S430：本發明之一實施例所述之群聚單元的運作步驟

七、申請專利範圍：

1. 一種惡意程式偵測方法，該方法包括：

蒐集多個惡意訓練應用程式安裝檔及多個正常訓練應用程式安裝檔；

分別自各該些惡意訓練應用程式安裝檔及各該些正常訓練應用程式安裝檔取得一資訊設定檔（manifest file）及反編譯程式碼，並從各該資訊設定檔及反編譯程式碼中擷取出一靜態行為特徵；

利用一群聚演算法從該些惡意訓練應用程式安裝檔中產生至少一惡意應用程式群組，依照一應用程式市場類別規則，將該些正常訓練應用程式安裝檔分群為至少一正常應用程式群組，並根據各該至少一惡意應用程式群組所包括之惡意訓練應用程式安裝檔的該靜態行為特徵及各該至少一正常應用程式群組所包括之正常訓練應用程式安裝檔的該靜態行為特徵，產生分別代表各該至少一惡意應用程式群組的一應用程式偵測模型以及分別代表各該至少一正常應用程式群組的一應用程式偵測模型；

接收一待測應用程式安裝檔；

自該待測應用程式安裝檔取得一待測資訊設定檔及反編譯程式碼，並從該待測資訊設定檔及反編譯程式碼擷取出一待測靜態行為特徵；

利用一分類演算法、該待測靜態行為特徵、各該至少一惡意應用程式群組的該應用程式偵測模型、及各該至少一正常應用程式群組的該應用程式偵測模型，判斷該待測

應用程式安裝檔是否屬於該至少一惡意應用程式群組的其中之一；以及

若是，則產生一警告訊息。

2. 如申請專利範圍第 1 項所述之惡意程式偵測方法，其中該靜態行為特徵至少包括一使用權限（permission）、一元件（component）及所屬元件類型、一意圖（intent）、一應用程式介面呼叫（API call）其中之一及其組合者。

3. 如申請專利範圍第 1 項所述之惡意程式偵測方法，其中利用該群聚演算法從該些惡意訓練應用程式安裝檔中產生該至少一惡意應用程式群組，依照該應用程式市場類別規則，將該些正常訓練應用程式安裝檔分群為該至少一正常應用程式群組，並根據各該至少一惡意應用程式群組所包括之惡意訓練應用程式安裝檔的該靜態行為特徵及各該至少一正常應用程式群組所包括之正常訓練應用程式安裝檔的該靜態行為特徵，產生分別代表各該至少一惡意應用程式群組的該應用程式偵測模型以及分別代表各該至少一正常應用程式群組的該應用程式偵測模型的步驟包括：

評估各該靜態行為特徵於該些惡意訓練應用程式安裝檔的一權重；

將各該些惡意訓練應用程式安裝檔之該靜態行為特徵表示為一向量形式並產生一聚類群數；以及

將各該些惡意訓練應用程式安裝檔之該靜態行為特

徵的該權重及該向量形式套用至該群聚演算法，藉以產生該至少一惡意應用程式群組，其中屬於同一惡意應用程式群組的所有惡意訓練應用程式安裝檔具有相似之靜態行為特徵。

4. 如申請專利範圍第 3 項所述之惡意程式偵測方法，其中評估各該靜態行為特徵於該些惡意訓練應用程式安裝檔的該權重的步驟包括：

針對各該些惡意訓練應用程式安裝檔，統計各該靜態行為特徵在該些惡意訓練應用程式安裝檔中的一出現次數；

針對各該靜態行為特徵，統計具備該靜態行為特徵的一惡意訓練應用程式數量；以及

利用一詞頻-逆向文件頻率（Term Frequency-Inverse Document Frequency，TF-IDF）公式計算各該靜態行為特徵於各該些惡意訓練應用程式安裝檔的該權重。

5. 如申請專利範圍第 3 項所述之惡意程式偵測方法，其中將各該靜態行為特徵表示為該向量形式的步驟包括：

利用一奇異值分解（Singular Value Decomposition，SVD）公式計算特徵值（eigenvalue）；以及

取得前 N 個涵蓋一特定百分比的頻譜能量（spectral energy）以代表該聚類群數，其中 N 為正整數。

6. 一種惡意程式偵測系統，包括：

一特徵擷取單元，接收多個惡意訓練應用程式安裝檔

及多個正常訓練應用程式安裝檔，並分別自各該些惡意訓練應用程式安裝檔及各該些正常訓練應用程式安裝檔取得一資訊設定檔及反編譯程式碼，且從各該資訊設定檔及反編譯程式碼中擷取出一靜態行為特徵；

一群聚單元，耦接該特徵擷取單元，以利用一群聚演算法從該些惡意訓練應用程式安裝檔中產生至少一惡意應用程式群組。依照一應用程式市場類別規則，將該些正常訓練應用程式安裝檔分群為至少一正常應用程式群組，並根據各該至少一惡意應用程式群組所包括之惡意訓練應用程式安裝檔的該靜態行為特徵及各該至少一正常應用程式群組所包括之正常訓練應用程式安裝檔的該靜態行為特徵，產生分別代表各該至少一惡意應用程式群組的一應用程式偵測模型以及分別代表各該至少一正常應用程式群組的一應用程式偵測模型；以及

一判別單元，耦接該特徵擷取單元與該群聚單元，以在接收一待測應用程式安裝檔時，控制該特徵擷取單元自該待測應用程式安裝檔取得一待測資訊設定檔及反編譯程式碼，並從該待測資訊設定檔及反編譯程式碼擷取一待測靜態行為特徵，

該判別單元利用一分類演算法、該待測靜態行為特徵、各該至少一惡意應用程式群組的該應用程式偵測模型、及各該至少一正常應用程式群組的該應用程式偵測模型，判斷該待測應用程式安裝檔是否屬於該至少一惡意應用程式群組的其中之一，並且在判定該待測應用程式安裝

檔屬於該至少一惡意應用程式群組的其中之一時，產生一警告訊息。

7. 如申請專利範圍第 6 項所述之惡意程式偵測系統，其中該靜態行為特徵至少包括一使用權限（permission）、一元件（component）及所屬元件類型、一意圖（intent）、一應用程式介面呼叫（API call）其中之一及其組合者。

8. 如申請專利範圍第 6 項所述之惡意程式偵測系統，其中該群聚單元包括：

一權重決定單元，以評估各該靜態行為特徵於該些惡意訓練應用程式安裝檔的一權重；

一群數評估單元，耦接該權重決定單元，以將各該些惡意訓練應用程式安裝檔之該靜態行為特徵表示為一向量形式並產生一聚類群數；以及

一模型產生單元，耦接該群數評估單元，以將各該些惡意訓練應用程式安裝檔之該靜態行為特徵的該權重及該向量形式套用至該群聚演算法，藉以產生該至少一惡意應用程式群組，其中屬於同一惡意應用程式群組的所有惡意訓練應用程式安裝檔具有相似之靜態行為特徵。

9. 如申請專利範圍第 8 項所述之惡意程式偵測系統，其中該權重決定單元針對各該些惡意訓練應用程式安裝檔，統計各該靜態行為特徵在該些惡意訓練應用程式安裝檔中的一出現次數，並針對各該靜態行為特徵，統計具備該靜態行為特徵的一惡意訓練應用程式數量，以及利用

一詞頻-逆向文件頻率公式計算各該靜態行為特徵於各該些惡意訓練應用程式安裝檔的該權重。

10. 如申請專利範圍第 8 項所述之惡意程式偵測系統，其中該群數評估單元利用一奇異值分解公式計算特徵值，並取得前 N 個涵蓋一特定百分比的頻譜能量以代表該聚類群數，其中 N 為正整數。

八、圖式：

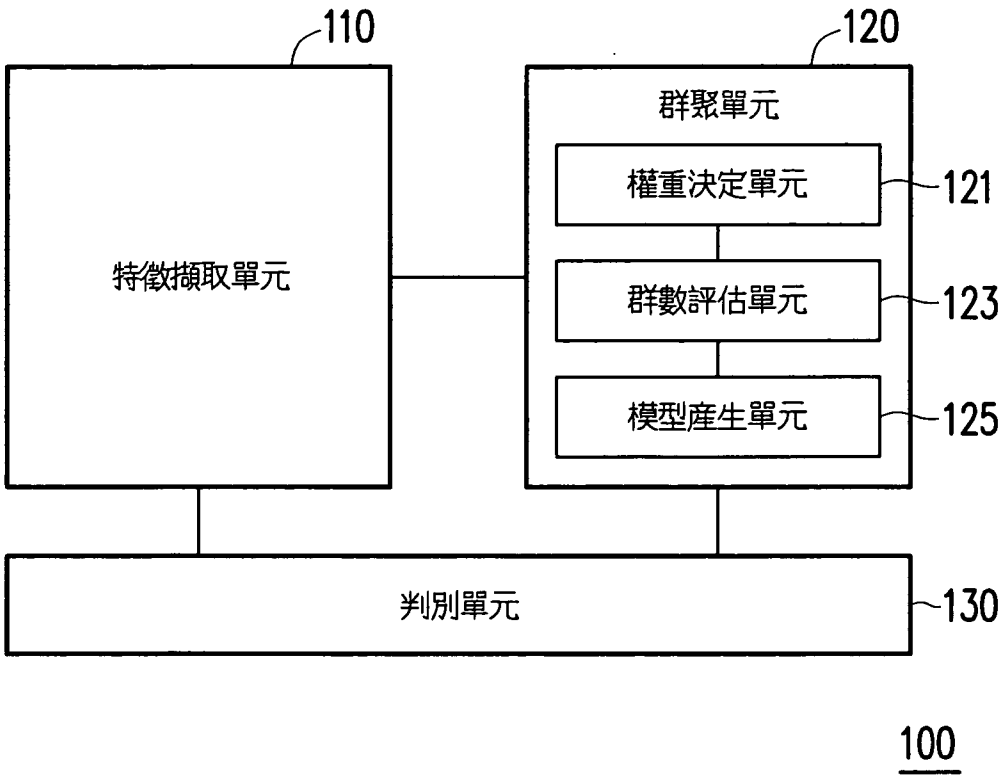
110
120
群聚單元
權重決定單元
121
特徵擷取單元
群數評估單元
123
模型產生單元
125
判別單元
130
100

圖 1

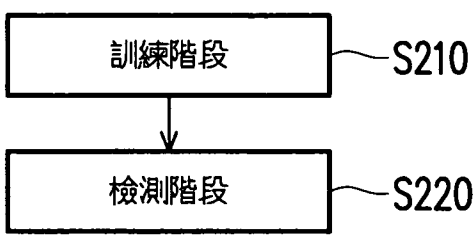
訓練階段
S210
檢測階段
S220

圖 2

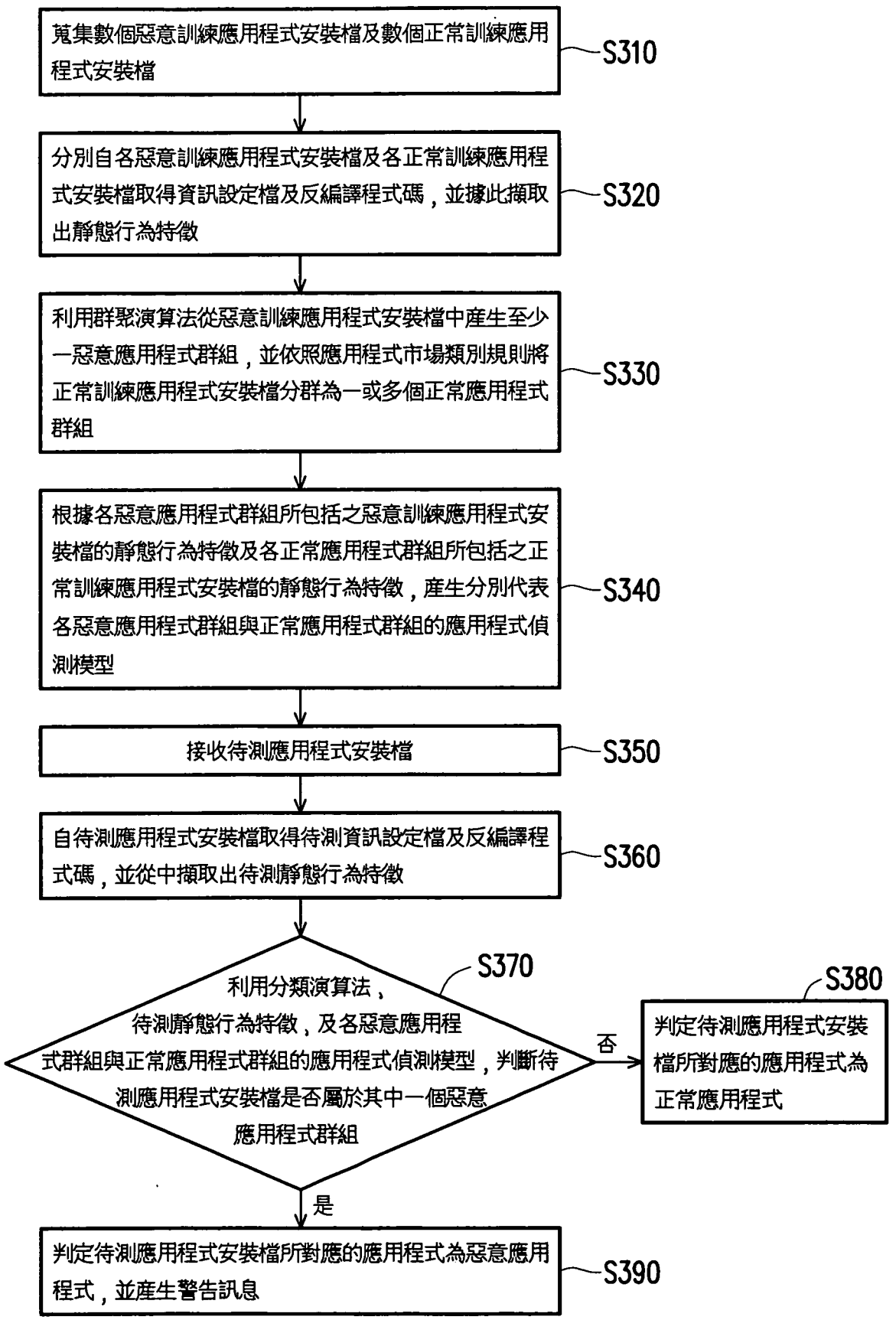
蒐集數個惡意訓練應用程式安裝檔及數個正常訓練應用程式安裝檔
S310
分別自各惡意訓練應用程式安裝檔及各正常訓練應用程式安裝檔取得資訊設定檔及反編譯程式碼，並據此擷取出靜態行為特徵
S320
利用群聚演算法從惡意訓練應用程式安裝檔中產生至少一惡意應用程式群組，並依照應用程式市場類別規則將正常訓練應用程式安裝檔分群為一或多個正常應用程式群組
S330
根據各惡意應用程式群組所包括之惡意訓練應用程式安裝檔的靜態行為特徵及各正常應用程式群組所包括之正常訓練應用程式安裝檔的靜態行為特徵，產生分別代表各惡意應用程式群組與正常應用程式群組的應用程式偵測模型
S340
接收待測應用程式安裝檔
S350
自待測應用程式安裝檔取得待測資訊設定檔及反編譯程式碼，並從中擷取出待測靜態行為特徵
S360
利用分類演算法，待測靜態行為特徵，及各惡意應用程式群組與正常應用程式群組的應用程式偵測模型，判斷待測應用程式安裝檔是否屬於其中一個惡意應用程式群組
S370
否
判定待測應用程式安裝檔所對應的應用程式為正常應用程式
S380
是
判定待測應用程式安裝檔所對應的應用程式為惡意應用程式，並產生警告訊息
S390

圖 3

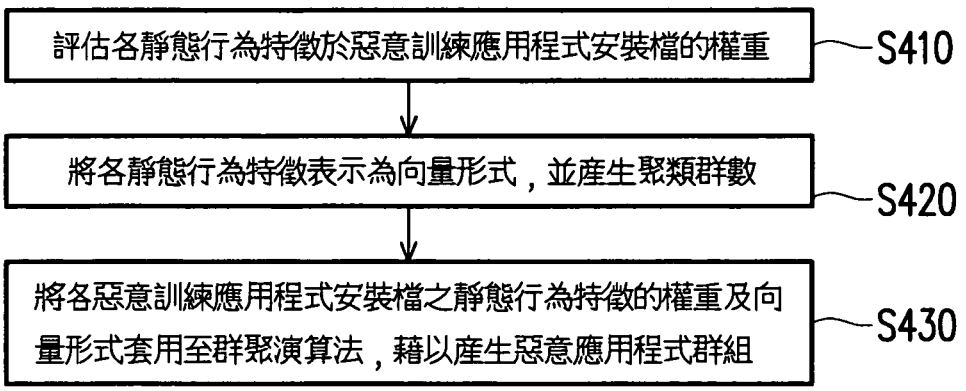
評估各靜態行為特徵於惡意訓練應用程式安裝檔的權重
S410
將各靜態行為特徵表示為向量形式，並產生聚類群數
S420
將各惡意訓練應用程式安裝檔之靜態行為特徵的權重及向量形式套用至群聚演算法，藉以產生惡意應用程式群組
S430

圖 4