



(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 I494751 B

(45)公告日：中華民國 104 (2015) 年 08 月 01 日

(21)申請案號：099125055 (22)申請日：中華民國 99 (2010) 年 07 月 29 日
(51)Int. Cl. : G06F11/07 (2006.01) G06F21/00 (2013.01)
(30)優先權：2009/07/29 美國 61/229,497
(71)申請人：瑞凡辛實驗室股份有限公司 (RS) REVERSINGLABS CORPORATION (RS)
美國
(72)發明人：皮瑞欣 托米斯拉夫 PERICIN, TOMISLAV (RS)
(74)代理人：陳翠華
(56)參考文獻：
TW 446872 TW 451125
US 5892904 US 5953534
US 5983366 US 7058928B2
WO 1998/033106A1
審查人員：林巧宜
申請專利範圍項數：21 項 圖式數：4 共 38 頁

(54)名稱

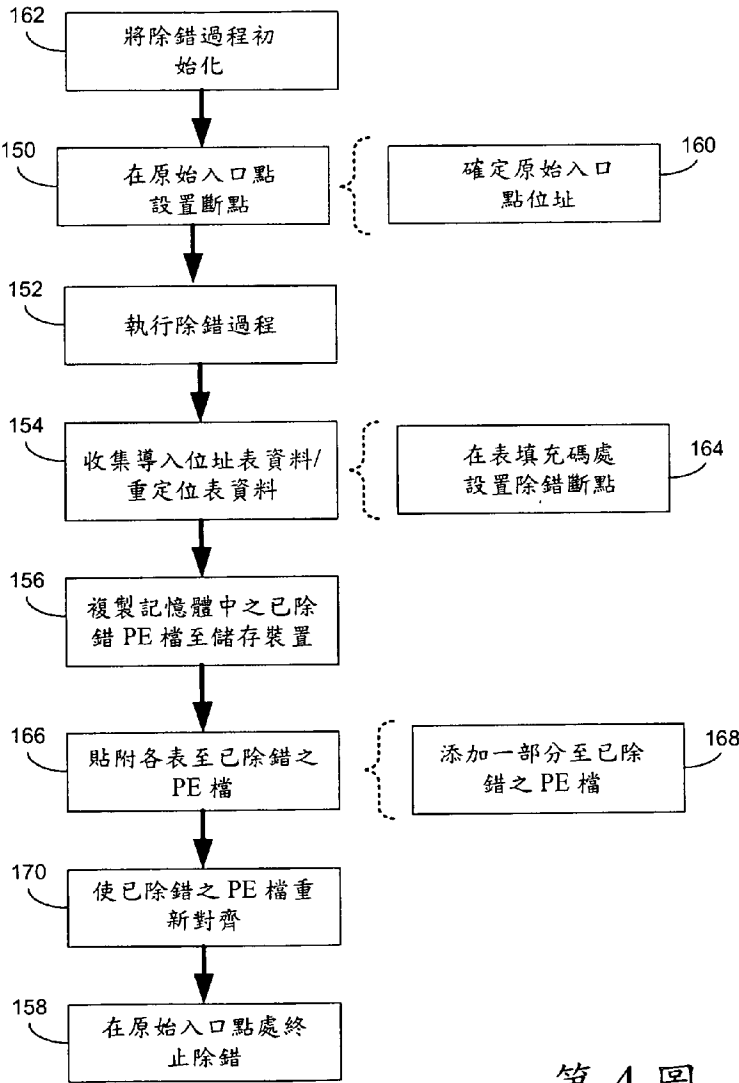
自動化解碼攜帶式可執行檔之系統、方法及其電腦程式產品

AUTOMATED UNPACKING OF PORTABLE EXECUTABLE FILES

(57)摘要

自動化解碼攜帶式可執行檔包含：在已編碼之攜帶式可執行檔之原始入口點位址設置除錯斷點；對已編碼之攜帶式可執行檔執行除錯過程，以在記憶體中獲得已除錯之攜帶式可執行檔；在對已編碼之攜帶式可執行檔執行除錯過程期間，收集導入位址表資料與重定位表資料至少其中之一；複製記憶體中之已除錯之攜帶式可執行檔至儲存媒體；以及終止除錯過程。

Automated unpacking of a portable executable file includes setting a debugging breakpoint at an original entry point address of a packed portable executable file. A debugging process is executed for the packed portable executable file to obtain a debugged portable executable file in memory. One or more of import address table data and relocation table data are collected during execution of the debugging process for the packed portable executable file. The debugged portable executable file in memory is copied to a storage medium, and the debugging process is terminated.



第 4 圖

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：099125055

※ 申請日：99 年 7 月 29 日

※IPC 分類：

G06F 11/67 (2006.01)

G06F 21/00 (2013.01)

一、發明名稱：(中文/英文)

自動化解碼攜帶式可執行檔之系統、方法及其電腦程式產品/
AUTOMATED UNPACKING OF PORTABLE EXECUTABLE FILES

二、中文發明摘要：

自動化解碼攜帶式可執行檔包含：在已編碼之攜帶式可執行檔之原始入口點位址設置除錯斷點；對已編碼之攜帶式可執行檔執行除錯過程，以在記憶體中獲得已除錯之攜帶式可執行檔；在對已編碼之攜帶式可執行檔執行除錯過程期間，收集導入位址表資料與重定位表資料至少其中之一；複製記憶體中之已除錯之攜帶式可執行檔至儲存媒體；以及終止除錯過程。

三、英文發明摘要：

Automated unpacking of a portable executable file includes setting a debugging breakpoint at an original entry point address of a packed portable executable file. A debugging process is executed for the packed portable executable file to obtain a debugged portable executable file in memory. One or more of import address table data and relocation table data are collected during execution of the debugging process for the packed portable executable file. The debugged portable executable file in memory is copied to a storage medium, and the debugging process is terminated.

四、指定代表圖：

(一)本案指定代表圖為：第(4)圖。

(二)本代表圖之元件符號簡單說明：

無

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】

本申請案概言之係關於反向工程化軟體 (reverse engineering software)，更具體而言，係關於解碼軟體及對軟體檔之有效性分析。

【先前技術】

Microsoft 公司在「Microsoft 攜帶式可執行檔及通用目標檔格式規範 (Microsoft Portable Executable and Common Object File Format Specification)」中所定義之攜帶式可執行檔格式 (PE 檔格式) 係為一種用於可執行碼、目標碼及 DLL (動態鏈接庫 (dynamic link libraries)) 之檔案格式。PE 檔係用於 Microsoft Windows 作業系統之 32 位元版本及 64 位元版本。PE 檔格式係為一種非常通用之格式，可用於諸多作業系統環境中並支援各種處理器解決方案。

軟體開發者可利用各種方案來保護軟體，包括 PE 檔。舉例而言，可利用軟體編碼器 (packer) 來壓縮二進制資料，此可減小與傳送二進制資料相關聯之頻寬使用量以及儲存量。類似地，可利用編碼器來保護收錄於軟體內之智慧財產並防止代碼盜竊。編碼可涉及各種可使可執行碼之內容模糊難辨之壓縮及/或加密方案。運行經壓縮之可執行檔可將原始可執行碼解碼 (例如，其可包括解壓縮及/或解密) 並接著傳送控制訊息至原始可執行碼。因此，直到實際執行軟體時方知可執行碼之性質。舉例而言，若可執行碼係為惡意軟體 (malware) 或其他非所欲之軟體，則此可造成問題，乃因得知此種軟體之性質時為時已晚。

【發明內容】

根據一實施方式，一種由電腦執行之方法包含：由一計算裝置在一已編碼之攜帶式可執行檔（packed portable executable file）之一原始入口點位址（original entry point address）設置一除錯斷點（debugging point）。該方法亦包含由該計算裝置對該已編碼之攜帶式可執行檔執行一除錯過程，以在記憶體中獲得一已除錯之攜帶式可執行檔。在對該已編碼之攜帶式可執行檔執行該除錯過程期間，由該計算裝置收集一導入位址表資料（import address table data）與一重定位表資料（relocation table data）至少其中之一。由該計算裝置複製記憶體中之該已除錯之攜帶式可執行檔至一儲存媒體。該方法亦包含由該計算裝置終止該除錯過程。

可包含以下特徵其中之一或多者。該已編碼之攜帶式可執行檔之該原始入口點位址可由該計算裝置至少部分地根據該已編碼之攜帶式可執行檔之映像基底（ImageBase）欄位資料以及該已編碼之攜帶式可執行檔之進入點位址（AddressOfEntryPoint）資料、以及可能之其他數值計算而確定，該等可能之其他數值計算可至少部分地基於軟體編碼器（software packer）佈局本身。該除錯過程可由該計算裝置初始化，包括至少部分地根據該已編碼之攜帶式可執行檔創建一除錯過程。

收集該導入位址表資料與該重定位表資料至少其中之一之步驟可包括：設置與一函式庫讀取（LoadLibrary）呼叫、一模組處理獲取（GetModuleHandle）呼叫及一程序位址獲取（GetProcAddress）呼叫相關聯之一或多個除錯斷點、以及用於重定位記憶體中之該

檔之該軟體編碼器之一部分。可由該計算裝置向複製至儲存媒體之該已除錯之攜帶式可執行檔中貼附以下至少其中之一：一導入位址表，其至少部分地基於該等所收集之導入位址表資料；以及一重定位表，其至少部分地基於該等所收集之重定位表資料。向複製至儲存媒體之該已除錯之攜帶式可執行檔中貼附之步驟可包括：添加一新部分至複製至儲存媒體之該已除錯之攜帶式可執行檔。該方法亦可包含：由該計算裝置使複製至儲存媒體之該已除錯之攜帶式可執行檔重新對齊（realigning）。

根據另一實施方式，一種電腦程式產品包含一儲存有複數個指令之電腦可讀取記錄媒體。該等指令在由一處理器執行時，使該處理器執行包含以下之操作：在一已編碼之攜帶式可執行檔之一原始入口點位址設置一除錯斷點。亦包含用於如下之指令：對該已編碼之攜帶式可執行檔執行一除錯過程，以在記憶體中獲得一已除錯之攜帶式可執行檔。在對該已編碼之攜帶式可執行檔執行該除錯過程期間，收集一導入位址表資料與一重定位表資料至少其中之一。亦包含用於如下之指令：複製記憶體中之該已除錯之攜帶式可執行檔至一儲存媒體。更包含用於如下之指令：終止該除錯過程。

可包含以下特徵其中之一或多者。可包含用於以下之指令：至少部分地根據該已編碼之攜帶式可執行檔之映像基底（ImageBase）欄位資料以及該已編碼之攜帶式可執行檔之進入點位址（AddressOfEntryPoint）資料、以及可能之其他數值計算而確定該已編碼之攜帶式可執行檔之該原始入口點位址，該等可能之

其他數值計算可至少部分地基於軟體編碼器本身。可包含用於以下之指令：初始化該除錯過程，包括至少部分地根據該已編碼之攜帶式可執行檔創建一除錯過程。

收集該導入位址表資料與該重定位表資料至少其中之一之步驟可包括：設置與一函式庫讀取（LoadLibrary）呼叫、一模組處理獲取（GetModuleHandle）呼叫及一程序位址獲取（GetProcAddress）呼叫相關聯之一或多個除錯斷點、以及用於重定位記憶體中之該檔之該軟體編碼器之一部分。可包含用於向該已除錯之攜帶式可執行檔中貼附以下至少其中之一之指令：一導入位址表，其至少部分地基於該等所收集之導入位址表資料；以及一重定位表，其至少部分地基於該等所收集之重定位表資料。向該已除錯之攜帶式可執行檔中貼附可包括：添加一新部分至該已除錯之攜帶式可執行檔。

可更包含用於使該已除錯之攜帶式可執行檔重新對齊（realigning）之指令。

根據再一實施方式，一種系統包含一處理器以及耦接該處理器之一記憶體。一第一軟體模組可由該處理器及該記憶體執行。該第一軟體模組用以在一已編碼之攜帶式可執行檔之一原始入口點位址設置一除錯斷點。一第二軟體模組可由該處理器及該記憶體執行。該第二軟體模組用以對該已編碼之攜帶式可執行檔執行一除錯過程，以在記憶體中獲得一已除錯之攜帶式可執行檔。一第三軟體模組可由該處理器及該記憶體執行。該第三軟體模組用以在對該已編碼之攜帶式可執行檔執行該除錯過程期間，收集一導

入位址表資料與一重定位表資料至少其中之一。一第四軟體模組可由該處理器及該記憶體執行。該第四軟體模組用以複製記憶體中之該已除錯之攜帶式可執行檔至一儲存媒體。一第五軟體模組可由該處理器及該記憶體執行。該第五軟體模組用以終止該除錯過程。

可包含以下特徵其中之一或多者。一第六軟體模組可由該處理器及該記憶體執行。該第六軟體模組用以至少部分地根據該已編碼之攜帶式可執行檔之映像基底 (ImageBase) 欄位資料以及該已編碼之攜帶式可執行檔之進入點位址 (AddressOfEntryPoint) 資料、以及可能之其他數值計算而確定該已編碼之攜帶式可執行檔之該原始入口點位址，該等可能之其他數值計算至少部分地基於軟體編碼器佈局本身。一第七軟體模組可由該處理器及該記憶體執行。該第七軟體模組用以初始化該除錯過程，包括至少部分地根據該已編碼之攜帶式可執行檔創建一除錯過程。

用以收集該導入位址表資料與該重定位表資料至少其中之一之該第三軟體模組可用以：設置與一函式庫讀取 (LoadLibrary) 呼叫、一模組處理獲取 (GetModuleHandle) 呼叫及一程序位址獲取 (GetProcAddress) 呼叫相關聯之一或多個除錯斷點、以及用於重定位記憶體中之該檔的該軟體編碼器之一部分。一第八軟體模組可由該處理器及該記憶體執行。該第八軟體模組可用以由該計算裝置向該已除錯之攜帶式可執行檔中貼附以下至少其中之一：一導入位址表，其至少部分地基於該等所收集之導入位址表資料；以及一重定位表，其至少部分地基於該等所收集之重定位表資

料。用以向該已除錯之攜帶式可執行檔中貼附之該第八軟體模組可用以：添加一新部分至該已除錯之攜帶式可執行檔。

一第九軟體模組可由該處理器及該記憶體執行。該第九軟體模組可用以使該已除錯之攜帶式可執行檔重新對齊。

在附圖及下文說明中闡述一或多種實施方式之細節。根據本說明、附圖及申請專利範圍，其他特徵及優點將變得顯而易見。

【實施方式】

熟習此項技術者應理解，本發明可實施為一種系統、方法或電腦程式產品。因此，本發明可為一完全硬體實施例、一完全軟體實施例（包括韌體、駐存軟體、微碼等）、或一將軟體與硬體態樣相結合之實施例之形式，所有此等實施例皆可被統稱為「電路」、「模組」或「系統」。此外，本發明可為電腦程式產品之形式，該電腦程式產品實施於一或多個收錄有電腦可用程式碼之電腦可讀取（即電腦可使用的）媒體中。

可利用一或多個電腦可讀取記錄媒體之任意組合。該電腦可讀取記錄媒體包括一電腦可讀取儲存媒體，電腦可讀取儲存媒體可例如（但不限於）為電性、磁性、光學、電磁、紅外或半導體系統、裝置、器件、或其任意適當組合。實例性電腦可讀取儲存媒體可包括但不限於：攜帶式電腦磁碟、硬碟、固態碟驅動機、隨機存取記憶體（random access memory；RAM）、唯讀記憶體（read-only memory；ROM）、可抹除可程式化唯讀記憶體（erasable programmable read-only memory；EPROM，或快閃記憶體）、光纖、攜帶式光碟唯讀記憶體（compact disc read-only memory；

CD-ROM)、光學儲存裝置、磁性儲存裝置、或其任意適當組合。在本文之上下文中，電腦可讀取儲存媒體可為可包含或儲存有一程式之任何媒體，該程式供一指令執行系統、裝置或器件使用或與該指令執行系統、裝置或器件結合使用。

用於執行本發明操作之電腦程式碼可使用諸如 Java、Smalltalk、C++或類似之物件導向程式設計語言 (object oriented programming language) 進行編寫。然而，用於執行本發明操作之電腦程式碼亦可使用諸如「C」程式設計語言或類似程式設計語言等習知程式設計語言進行編寫。程式碼可完全在一單個計算裝置上執行 (例如作為一獨立軟體包)，及/或可至少部分地在多個可彼此遠離之計算裝置上執行。在後一種情形中，遠程計算裝置可透過一局部區域網路 (local area network; LAN) 或一廣域網路 (wide area network; WAN) 相互連接，或者可連接至一或多個遠程計算裝置 (例如，利用網際網路服務提供商透過網際網路進行連接)。

以下，將參照根據本發明實施例之方法、裝置 (系統) 及電腦程式產品之流程圖及/或方塊圖來說明本發明。應理解，可由電腦程式指令執行該等流程圖及/或方塊圖之每一方塊、以及該等流程圖及/或方塊圖中各方塊之組合。該等電腦程式指令可提供給一通用電腦、專用電腦、或其他可程式化資料處理裝置之處理器以形成一機器，俾使該等指令在透過電腦或其他可程式化資料處理裝置之該處理器執行時形成用於執行流程圖及/或方塊圖之一或多個方塊中所規定之功能/動作。

該等電腦程式指令亦可儲存於一電腦可讀取記憶體中，該電腦

可讀取記憶體可令一電腦或其他可程式化資料處理裝置以一特定方式運作，俾使儲存於該電腦可讀取記憶體中之指令形成一包含指令構件之製品，該等指令構件執行在流程圖及/或方塊圖之一或多個方塊中所規定之功能/動作。

電腦程式指令亦可加載至一電腦或其他可程式化資料處理裝置中，以在該電腦或其他可程式化裝置上執行一序列操作步驟來形成一由電腦執行之過程，俾使該等指令在該電腦或其他可程式化裝置上執行時提供用於執行在流程圖及/或方塊圖之一或多個方塊中所規定之功能/動作之步驟。

參見第 1 圖，其顯示可分別駐存於一計算裝置 16 上並可由計算裝置 16 執行之有效性檢查過程 10、修復過程 12 及自動化解碼過程 14。儘管圖中顯示有效性檢查過程 10、修復過程 12 及自動化解碼過程 14 中每一者皆駐存於計算裝置 12 上，然此僅供用於例示目的，乃因有效性檢查過程 10、修復過程 12 及自動化解碼過程 14 其中之一或多者亦可分別駐存於一單獨之計算裝置上。

計算裝置 16 之實例可包括但不限於：一個人電腦、一伺服器電腦、一系列伺服器電腦、一迷你電腦及一主機電腦（mainframe computer）。計算裝置 16 可運行一作業系統，例如 Microsoft® Windows® XP 或 Red Hat® Linux。亦可同等地使用各種其他/替代計算裝置及作業系統。舉例而言，計算裝置 16 可為一分佈式計算網路之一部分，其中完全地或部分地在透過一資料網路（例如 LAN、WAN、網際網路等）與計算裝置 16 相耦合之另一計算裝置上執行有效性檢查過程 10、修復過程 12 及自動化解碼過程 14 其

中之一或多者。

如下文所將更詳細論述，有效性檢查過程 100 可剖析一攜帶式可執行檔之一二進制影像，以產生一已剖析欄位（parsed field）。有效性檢查過程 10 亦可確定該已剖析欄位之一屬性。有效性檢查過程 10 可至少部分地根據一攜帶式可執行檔格式規範（portable executable file format specification），將該已剖析欄位之屬性與一有效對應欄位之一有效特性相比較。有效性檢查過程 10 亦可判斷該已剖析欄位之該屬性是否與該有效對應欄位之該有效特性相符。

此外，亦如下文所將更詳細論述，修復過程 12 可辨識一攜帶式可執行檔之一無效欄位。修復過程 12 亦可確定修復該攜帶式可執行檔之該無效欄位之一可能性。修復過程 12 可產生一修復模型（repair model），以用於修復該攜帶式可執行檔之該無效欄位。修復過程 12 可至少部分地根據該修復模型，修復該攜帶式可執行檔之該無效欄位。

同樣地，亦如下文所將更詳細論述，自動化解碼過程 14 可在一已編碼之攜帶式可執行檔（packed portable executable file）之一原始入口點位址（original entry point address）設置一除錯斷點（debugging point）。自動化解碼過程 14 亦可對該已編碼之攜帶式可執行檔執行一除錯過程，以在記憶體中獲得一已除錯之攜帶式可執行檔。自動化解碼過程 14 亦可在對該已編碼之攜帶式可執行檔執行該除錯過程期間，收集一導入位址表資料（import address table data）與重定位表資料（relocation table data）其中之一或多

者。自動化解碼過程 14 可複製記憶體中之該已除錯之攜帶式可執行檔至一儲存媒體，並可終止該除錯過程。

有效性檢查過程 10、修復過程 12 及自動化解碼過程 14 之指令集及次常式 (subroutine) 可包括一或多個軟體模組並可儲存於耦合至計算裝置 16 之儲存裝置 18 中，此等指令及次常式可由包含於計算裝置 16 中之一或多個處理器 (圖未示出) 及一或多個記憶體模組 (圖未示出) 執行。儲存裝置 18 可包括但不限於：一硬碟機；一固態驅動機；一磁帶驅動機；一光學驅動機；一 RAID 陣列；一隨機存取記憶體 (RAM)；以及一唯讀記憶體 (ROM)。

歸因於 PE (攜帶式可執行) 檔包含可執行碼之事實，可能期望在執行二進制對象 (例如，PE 檔之二進制影像) 之前執行檔檢查。有效性檢查過程 10 可在一 PE 二進制影像執行之前分析該 PE 二進制影像，以判斷該 PE 檔是否係為一有效二進制影像。一有效二進制影像可係指一可由一給定作業系統使用之檔，其或者為包含可執行碼之影像或者為其他類型之多媒體資訊。

亦參見第 2 圖，如上文所述，有效性檢查過程 10 可剖析 50 一攜帶式可執行檔 (例如 PE 二進制影像 20，其駐存於儲存裝置 18 上，如第 1 圖所示) 之一二進制影像，以產生 52 一已剖析欄位。有效性檢查過程 10 亦可確定 54 該已剖析欄位之一屬性。進一步，有效性檢查過程 10 可至少部分地根據一攜帶式可執行檔格式規範，將該已剖析欄位之屬性與一有效對應欄位之一有效特性相比較 56。有效性檢查過程 10 亦可判斷 58 該已剖析欄位之該屬性是否與該有效對應欄位之該有效特性相符。

有效性檢查過程 10 可剖析 50 該 PE 二進制影像 20，以產生 52 一已剖析欄位。有效性檢查過程 10 可剖析 50 該 PE 二進制影像 20，以產生 52 複數個符合 PE 檔格式 100 之欄位。舉例而言，有效性檢查過程 10 可一般將 PE 二進制影像剖析 50 成一攜帶式可執行格式簽名 (portable executable format signature)、一映像基底 (ImageBase) 欄位、一影像大小 (SizeOfImage) 欄位、一檔對齊 (FileAlignment) 欄位、一部分對齊 (SectionAlignment) 欄位、一入口點 (EntryPoint) 位址、一導入表 (import table)、一導入位址表 (import address table)、一導出表 (export table)、一重定位表 (relocation table)、一資源表 (resource table)、一執行緒本地儲存表 (thread local storage table)、一加載配置表 (load configuration table)、一邊界導入表 (bound import table)、一 COM 表、以及一攜帶式可執行部分表 (portable executable section table)。

儘管上文已指出數個欄位，然而此等欄位僅用於例示目的，乃因有效性檢查過程 10 可將 PE 二進制影像 20 剖析 50 成根據設計準則及使用者需求而加以選擇之各種其他/替代欄位。另外，剖析 50 該 PE 二進制影像 20 以產生 52 一或多個已剖析欄位可包括但不限於：以物理方式隔離每一欄位（例如，複製每一欄位於一單獨檔、資料庫欄位等中）、分別讀取每一欄位、使一偏移量與每一欄位之起點（及/或終點）相關聯等等。如此一來，藉由剖析 50 該 PE 二進制影像 20 以產生 52 一或多個已剖析欄位，便可分別檢查每一欄位。

如上文所述，有效性檢查過程 10 亦可確定 54 已剖析欄位之一屬性。有效性檢查過程 10 所確定 54 之屬性可包括一欄位辨識符、一欄位長度、及一欄位內容其中之一或多者。舉例而言，有效性檢查過程 10 可確定 54 該 PE 二進制影像 20 包括一值為 0x00400000 之 ImageBase 欄位、一值為 0x1000 之 SectionAlignment 欄位及一值為 0x200 之 FileAlignment 欄位。

有效性檢查過程 10 可至少部分地根據一攜帶式可執行檔格式規範，將該已剖析欄位之該一或多個所確定 54 屬性與一有效對應欄位之一有效特性相比較 56。一有效對應欄位可包括由 Microsoft 公司發佈之「Microsoft 攜帶式可執行檔及通用目標檔格式規範 (Microsoft Portable Executable and Common Object File Format Specification; PECOFF)」所要求或容許之欄位，且該欄位對應於一已剖析欄位。舉例而言，已剖析 ImageBase 欄位之一有效對應欄位可係為被 PECOFF 容許作為一可選 Windows 專用欄位之 ImageBase 欄位。一有效對應欄位之一有效特性可包括 PECOFF 可容許之特性。舉例而言，PECOFF 可規定一所接受 PE 二進制影像之可接受之欄位辨識符、欄位長度及欄位內容。舉例而言，PECOFF 可定義一缺設 ImageBase 值 0x00400000，並可要求該值為 64K 之倍數。同樣地，PECOFF 可規定 SectionAlignment 欄位具有大於或等於 FileAlignment 之值。進一步，PECOFF 可規定 FileAlignment 具有介於 512 與 64K 之間的為 2 的冪數之值。相應地，上述可為所辨識欄位之有效特性之實例。

有效性檢查過程 10 可至少部分地根據已剖析欄位之屬性與一有

效對應欄位之一有效特性之間的比較 56，判斷 58 該已剖析欄位之該屬性是否與該有效對應欄位之該有效特性相符。繼續說明上述實例，對於 PE 二進制影像 20 之 FileAlignment 欄位，所確定 54 屬性為 512。亦如上所述，PECOFF 可規定 FileAlignment 欄位具有介於 512 與 64K 之間的為 2 的冪數之值。相應地，有效性檢查過程 10 可確定 58 已剖析 FileAlignment 欄位（例如，其值為 512）之屬性與一有效 FileAlignment 欄位之一有效特性相符。

判斷 58 已剖析欄位之屬性是否與有效對應欄位之有效特性相符可包括判斷 60 已剖析欄位之屬性是否可有效地用於一預定作業系統。同樣，繼續說明上述實例，有效性檢查過程 10 可能已確定 PE 二進制影像 20 之一 ImageBase 欄位值為 0x00400000。該所確定值可係為 Windows NT、Windows 2000、Windows XP、Windows 95、Windows 98 及 Windows Me 作業系統之缺設值。然而，根據 PECOFF，Windows CE 之 ImageBase 欄位缺設值係為 0x00010000。因此，有效性檢查過程 10 可確定 60 該 PE 二進制影像 20 之已剖析 ImageBase 欄位不能有效地用於 Windows CE。

有效性檢查過程 10 可判斷 58 已剖析欄位是否與有效對應欄位之有效特性不符。繼續說明上述實例，PECOFF 規定 SectionAlignment 欄位具有大於或等於 FileAlignment 之值。進一步，有效性檢查過程 10 可能已確定 54 該 PE 二進制影像 20 之一 SectionAlignment 欄位屬性為 256 且一 FileAlignment 欄位屬性為 512。因此，由於對於 PE 二進制影像 20，所確定 54 之 SectionAlignment 欄位屬性（即 256）不大於或等於所確定 54 之

FileAlignment 欄位屬性 (即 512)，故有效性檢查過程 10 可確定 58 已剖析 SectionAlignment 欄位不與一有效對應欄位之一有效特性相符 (即所確定 54 之 SectionAlignment 欄位屬性不大於或等於所確定 54 之 FileAlignment 欄位屬性)。因此，有效性檢查過程 10 可提供一指示符 (例如，可在一圖形使用者介面中提供一指示符 (圖未示出))。

若已剖析欄位不與有效對應欄位之有效特性相符，則有效性檢查過程 10 可確定 62 對與該有效對應欄位之該有效特性不符之該已剖析欄位進行修改而產生一有效欄位之一可能性。有效性檢查過程 10 可至少部分地根據不與一有效對應欄位之有效特性相符的欄位中錯誤之數目及性質，來確定 62 對該已剖析欄位進行修改而產生一有效欄位之一可能性。舉例而言，繼續說明上述實例，由於值小於 FileAlignment 欄位之值，PE 二進制影像 20 之已剖析 SectionAlignment 欄位不與一有效 SectionAlignment 欄位之一有效特性相符。有效性檢查過程 10 可確定 62 能夠對 PE 二進制影像 20 之該 SectionAlignment 欄位進行修改而產生一有效特性之可能性很大，乃因 PE 二進制影像 20 之已剖析 SectionAlignment 欄位包含單個非常明確之錯誤 (即，其值小於 FileAlignment 欄位)。舉例而言，可將 SectionAlignment 欄位修改成包含大於或等於 FileAlignment 欄位之值。儘管可能需要進行某種遞歸測試來修改 PE 二進制影像 20 之 SectionAlignment 欄位以獲得一有效欄位，然而非常有可能可達成此種修改。

可至少部分地根據一或多種經驗法則來確定 62 對一欄位進行修

改而產生一有效欄位之可能性。該一或多種經驗法則可至少部分地基於在各種欄位中可發生之各種可能之錯誤類型以及為修正該等錯誤而可採取之可能修改方式。因此，對於一給定欄位中之一錯誤類型，當可存在的一般能達成一有效欄位之可能修改方式相對很少時，有效性檢查過程 10 可確定 62 對該欄位進行修改以產生一有效欄位之可能性相對高。相反，對於具有許多可能修改方式之一錯誤類型，由於其中之許多可能修改方式可能無法達成一有效欄位，故有效性檢查過程 10 可確定 62 對該欄位進行修改而產生一有效欄位之可能性相對低。類似地，若在已剖析欄位與一有效對應欄位之間所偵測之錯誤數目相對大，則有效性檢查過程 10 亦確定 62 對該欄位進行修改以產生一有效欄位之可能性相對低。

有效性檢查過程 10 亦可判斷 64 該攜帶式可執行檔之二進制影像是否包含一動態鏈接庫、一核心驅動程式 (kernel driver) 或一可執行對象。有效性檢查過程 10 可藉由根據可能之有效特性及可能之有效欄位對已剖析欄位進行評價，而基於例如所包含欄位、所包含欄位之內容等其中之一或多者而確定 64 PE 二進制影像 20 之性質。可類似地確定 PE 二進制影像 20 之各種其他/替代特性。舉例而言，有效性檢查過程 10 可確定以下其中之一或多者：可在其中執行該 PE 檔之一環境，該 PE 檔是否係為一控制台 (console) 或其他具有一圖形使用者介面之應用程式，該 PE 檔是否包含附屬檔以及該等附屬檔是否存在於目標系統上，該 PE 檔是否包含附屬功能以及附屬功能是否存在於可在目標系統上得到之庫中，等等。

如上文所簡要說明，有效性檢查過程 10 可提供一輸出以指示各種已剖析欄位、欄位屬性、欄位之有效性、PE 檔之性質等。在一實施例中，有效性檢查過程 10 可提供一圖形使用者介面，可透過該圖形使用者介面而渲染該等不同之輸出。另外/另一選擇為，有效性檢查過程 10 可提供一輸出至一資料庫、檔等，進而一使用者可透過一恰當之程式（例如一資料庫應用程式）而使用該輸出。熟習此項技術者將得知各種其他適宜之輸出。

PE 二進制影像可能會因各種機制而受損。舉例而言，當 PE 檔自一個媒體傳送至另一媒體時，該等 PE 檔可能會受損。類似地，軟體編碼器（例如 UPX、PECompact、ASPack 等）可能會引入錯誤。軟體編碼器所引入之錯誤可能會使某些檔僅對於某些能支援 PE 檔格式之作業系統版本有效。相應地，可執行修復過程 12 來修復受損之 PE 檔。

亦參照第 3 圖，修復過程 12 可辨識 100 一攜帶式可執行檔（例如，第 1 圖所示之 PE 二進制檔 20）之一無效欄位。此外，修復過程 12 可確定 102 對攜帶式可執行檔之無效欄位進行修復之一可能性。修復過程 12 可產生 104 一修復模型，該修復模型用於修復攜帶式可執行檔之無效欄位。修復過程 12 可至少部分地根據修復過程 12 所產生 104 之修復模型而修復 106 攜帶式可執行檔之無效欄位。

修復過程 12 可利用各種機制來辨識 100 PE 二進制影像 20 之一無效欄位。舉例而言，修復過程 12 可自有效性檢查過程 10（已詳述於上文中）接收 108 一指示符，該指示符指示 PE 二進制影像

20 及/或 PE 二進制影像 20 之子集部分（即，PE 二進制影像 20 之各個欄位之有效性）之有效性。修復過程 12 可直接自有效性檢查過程 10 接收 108 指示符。另外/另一選擇為，在其中有效性檢查過程 10 可產生一有效性報告（例如，以一檔案、資料庫表項或類似之形式）之一實施例中，修復過程 12 可藉由存取 110 該有效性報告並解譯其內容而辨識 100 一無效欄位（及/或複數個無效欄位）。

在其他實施例中，修復過程 12 可藉由對 PE 二進制影像 20 執行一或多次有效性檢查而辨識 100 PE 二進制影像 20 之一無效欄位。舉例而言，修復過程 12 可按類似於上文參照有效性檢查過程 10 所述之方式，對 PE 二進制影像 20 執行一或多次有效性檢查。舉例而言，修復過程 12 可大體將 PE 二進制影像 20 剖析成複數個欄位，並可將該等欄位之屬性與有效對應欄位之有效特性相比較。如上文所述，有效對應欄位之有效特性可由 PECOFF 規定。相應地，可至少部分地根據該等各個欄位及屬性是否符合 PECOFF 而確定欄位之有效性（及/或 PE 二進制影像 20 整體之有效性）。因此，修復過程 12 可將一無效欄位辨識 100 為所具有之一屬性不符合 PECOFF 所規定之一有效對應欄位之一有效特性之欄位。

當辨識 100 一無效欄位時，修復過程 12 可檢查 PE 二進制影像 20 之所有欄位，及/或可特別關注 PE 二進制影像 20 之最緊要欄位。可能特別重要之欄位（例如，其可對 PE 二進制影像 20 具有最大影響）之實例可包括但不限於：PE 格式簽名、PE 專用欄位（例如 ImageBase、SizeOfImage、FileAlignment、SectionAlignment 及 EntryPoint 位址）以及 PE 專用表（例如導入表、導入位址表、導

出表、一重定位表、一資源表、執行緒本地儲存表、加載配置表、邊界導入表、COM 表以及 PE 部分表 (PE section table))。

如上文所述，修復過程 12 可確定 102 對 PE 二進制影像 20 之該無效欄位（或多個無效欄位）進行修復之一可能性。修復過程 12 可至少部分地根據對該無效欄位中與一有效對應欄位之一有效特性不符之屬性之數目及特性之確定 114 而確定 102 對 PE 二進制影像 20 之無效欄位進行修復之一可能性，所述確定 114 係至少部分地根據一攜帶式可執行檔格式規範（例如 PECOFF）而進行。舉例而言，需說明者，不同之錯誤可具有較其他錯誤為高之可修復可能性。類似地，具有相對很少之錯誤之一 PE 檔可具有較具有相對大量錯誤之一 PE 檔為高之可修復可能性。

修復過程 12 可確定 102 修復一無效欄位之可能性，包括將所辨識 100 之無效欄位（包括不符合 PECOFF 之無效欄位之屬性）與一可能錯誤之庫相比較，並確定能修復錯誤之可能性。該可能錯誤之庫（例如駐存於儲存裝置 18 上之函式庫 22）可包括先前已遇到的各種錯誤之經驗資料以及是否可修復錯誤而獲得一可執行檔。

如上文所述，修復過程 12 可產生 104 一修復模型，該修復模型用於修復所辨識 100 之無效欄位。修復過程 12 所產生 104 之修復模型可包含一或多種用於修復該一或多個所辨識 100 之無效欄位之演算法。類似於對修復無效欄位之可能性之確定 102，修復過程 12 可至少部分地根據一或多個經驗法則（例如，可包含於函式庫 22 中）而產生 104 修復模型。舉例而言，修復過程 12 可產生 104

一用於修復具異常值之無效 SizeOfImage 欄位之修復模型，其中法則可包含重新計算一正確之 SizeOfImage 值。類似地，修復過程 12 可產生 104 一用於修復不包含一可執行屬性之無效入口點部分之修復模型，其中法則可包含修正該等部分之屬性。在又一實例中，修復過程 12 可產生 104 一用於修復無法進行物理定位之無效資源表資料之修復模型，其中法則可包含暫時移除 PE 報頭 (header) 中之無效資源表值。另外，函式庫 22 可包含經驗法則，該等經驗法則係基於不同作業系統版本以及該等不同作業系統版本處理該 PE 檔格式之方式之間的比較而得出。

修復過程 12 可至少部分地根據修復過程 12 所產生 104 之修復模型而修復 106 攜帶式可執行檔之無效欄位。某些錯誤 (即無效欄位) 可藉由修改駐存於儲存裝置 18 上之 PE 二進制影像 20 而「在碟上 (on disk)」修復。相應地，修復過程 12 可藉由靜態地修復 116 無效欄位而修復 106 該無效欄位。靜態地修復 116 該無效欄位可包括在儲存裝置 18 上修改 118 攜帶式可執行檔之影像 (例如 PE 二進制影像 20)。修復過程 12 可將已修改之 PE 影像儲存 120 於儲存裝置 18 上。

舉例而言，繼續說明上述其中 PE 欄位 SizeOfImage 因具有一異常值而被辨識 100 為無效欄位之實例，修復過程 12 可靜態地修復 PE 二進制影像 20 之 SizeOfImage 欄位。舉例而言，修復過程可重新計算一正確之 SizeOfImage 值。修復過程 12 可將 PE 二進制影像 20 修改成包含正確之 SizeOfImage 值。修復過程 12 可將已修改之 PE 二進制影像 20 儲存於儲存裝置 18 上。

除可「在碟上」修復之錯誤外，其他錯誤可在記憶體中修復。關於何種錯誤可「在碟上」修復以及何種錯誤可在記憶體中修復之判斷可至少部分地基於經驗法則（例如，可駐存於函式庫 22 中）。對於可在記憶體中修復之錯誤，修復過程 12 可動態地修復 122 無效欄位。為動態地修復 122 一無效欄位，修復過程 12 可執行 124 攜帶式可執行檔（例如，PE 二進制影像 20）。修復過程 12 可更修改 126 在執行期間駐存於記憶體（例如，RAM）中之攜帶式可執行檔，其中在執行期間駐存於記憶體中之攜帶式可執行檔係基於該攜帶式可執行檔（例如，基於 PE 二進制影像 20）。

此外，修復過程可藉由禁用 128 無效欄位而修復 106 該無效欄位。舉例而言，修復過程可藉由在執行攜帶式可執行檔之前，自儲存於儲存裝置 18 上之攜帶式可執行檔之一影像（例如，PE 二進制影像 20）移除 130 一無效欄位而暫時禁用 128 該無效欄位。

在某些實施例中，修復過程 12 可藉由禁用 128 一無效欄位並動態地修復 122 該無效欄位而修復 106 該無效欄位。舉例而言，參見上述其中無法對資源表資料進行物理定位之實例，修復過程 12 可暫時地移除 130 PE 報頭中之無效資源表值。然後，修復過程 12 可執行 124 PE 二進制影像 20（例如，修復過程 12 可執行 PE 二進制影像 20 之一解碼器）直至該攜帶式可執行檔之原始入口點。該原始入口點可包含在該攜帶式可執行檔受到保護（例如，編碼）之前該攜帶式可執行檔之第一程式指令。一旦 PE 二進制影像 20 之執行到達該原始入口點，便可將過程記憶體轉儲（dumped）132 至儲存裝置 18。換言之，可將與駐存於 RAM 上之 PE 二進制影像

20 之執行相關聯之過程記憶體保存至儲存裝置 18。在 PE 二進制影像 20 之解碼期間自記憶體擷取之資源表資料可被恢復至一原始狀態，且可儲存一新 PE 檔，該新 PE 檔至少部分地基於所轉儲之過程記憶體。相應地，可獲得一有效 PE 檔（即，一符合 PECOFF 之 PE 檔）。

在一實施例中，一 PE 二進制影像 24 可包含一已編碼之攜帶式可執行檔。一已編碼之攜帶式可執行檔可包含攜帶式可執行檔（符合 PECOFF，如上文所述），該攜帶式可執行檔可包含一或多種軟體保護方式，例如壓縮、加密、壓縮與加密之組合等等。一般而言，自動化解碼過程 14 可對該已編碼之攜帶式可執行檔執行一除錯過程，並可利用各種斷點及回叫（callback）來收集導入位址表填充資料、以及各種其他可用於根據已編碼（例如，受保護）之 PE 二進制影像 24 來構建一未受保護之有效攜帶式可執行檔之資料。

亦參見第 4 圖，大體而言，自動化解碼過程 14 可於一已編碼之攜帶式可執行檔（例如，第 1 圖所示之已編碼 PE 二進制影像 24）之一原始入口點位址設置 150 一除錯斷點。自動化解碼過程 14 亦可對該已編碼之攜帶式可執行檔執行 152 一除錯過程，以在記憶體中（例如，在 RAM 中）獲得一已除錯之攜帶式可執行檔。自動化解碼過程 14 可在對該已編碼之攜帶式可執行檔執行 152 該除錯過程期間，收集 154 一導入位址表資料與一重定位表資料（relocation table data）至少其中之一。自動化解碼過程 14 可複製 156 記憶體中所儲存之該已除錯之攜帶式可執行檔至一儲存媒

體（例如儲存裝置 18）。自動化解碼過程 14 可在該攜帶式可執行檔之原始入口點處終止 158 該除錯過程。

如上文所述，自動化解碼過程 14 可在已編碼 PE 二進制影像 24 之一原始入口點位址設置 150 一除錯斷點。已編碼 PE 二進制影像 24 之原始入口點位址可係為在該檔受到保護之前可執行碼之第一指令。藉由在已編碼 PE 二進制影像 24 之原始入口點位址設置 150 一除錯斷點，便可在將控制傳送至收錄於已編碼 PE 二進制影像 24 內之可執行檔之前暫止已編碼 PE 二進制影像 24 之執行。本文所述之「已編碼 PE 二進制影像之執行」及「執行已編碼 PE 二進制影像」可係指由已編碼 PE 二進制影像所收錄之檔之執行以及執行由已編碼 PE 二進制影像所收錄之 PE 檔。自動化解碼過程 14 可確定 160 已編碼攜帶式可執行檔之 ImageBase 欄位資料以及已編碼攜帶式可執行檔之 AddressOfEntryPoint 資料。ImageBase 欄位資料以及 AddressOfEntryPoint 資料可自己編碼 PE 二進制影像 24 加載。已編碼 PE 二進制影像 24 之原始入口點位址可係為 ImageBase 資料與 AddressOfEntryPoint 資料之和。確定原始入口點可另外包含其他數值計算，該等數值計算可至少部分地基於軟體編碼器佈局本身。自動化解碼過程 14 可自己編碼 PE 二進制影像 24 載入各種其他資料，例如但不限於：ImageBase 資料、SizeOfImage 資料及 PE 部分資料。

自動化解碼過程 14 可初始化 162 該除錯過程。初始化 162 該除錯過程之步驟可包括至少部分地根據已編碼之 PE 二進制影像 24 創建一除錯過程。換言之，初始化 162 該除錯過程之步驟可建立

一可在其中執行已編碼 PE 二進制影像 24 之除錯環境。在該初始化除錯過程中，自動化解碼過程 14 可在原始入口點上設置 150 一除錯斷點。在執行收錄於已編碼 PE 二進制影像 24 內之可執行檔之第一指令之前，一旦已除錯之過程結束加載，便將調用原始入口點上設置之除錯斷點。

自動化解碼過程 14 可執行 152 該已初始化之除錯過程。換言之，可在所建立之除錯環境內執行已編碼之 PE 二進制影像 24。自動化解碼過程 14 可收集 154 一導入位址表資料與一重定位表資料至少其中之一。收集 154 一導入位址表資料與一重定位表資料至少其中之一之步驟可包括運行該除錯過程，直至其到達導入位址表填充碼。部分地，自動化解碼過程 14 可藉由設置 164 與一函式庫讀取 (LoadLibrary) 呼叫、一模組處理獲取 (GetModuleHandle) 呼叫及一程序位址獲取 (GetProcAddress) 呼叫相關聯之一或多個除錯斷點而收集 154 一導入位址表資料與一重定位表資料至少其中之一。其他斷點亦可與用於對記憶體中之檔進行重定位之軟體編碼器之一部分相關聯。在某些實施例中，與一函式庫讀取 (LoadLibrary) 呼叫、一模組處理獲取 (GetModuleHandle) 呼叫及一程序位址獲取 (GetProcAddress) 呼叫相關聯之斷點可在除錯過程之初始化 162 期間設置。

在除錯過程內執行之已編碼 PE 二進制影像 24 可利用一 LoadLibrary API 呼叫或一 GetModuleHandle API 呼叫，以加載一附屬動態鏈接庫。設置 164 與一 LoadLibrary 呼叫或一 GetModuleHandle 呼叫相關聯之一或多個斷點可使得當正在執行

之已編碼 PE 二進制影像 24 加載一動態鏈接庫時回叫自動化解碼過程 14。因應與一 LoadLibrary 呼叫或一 GetModuleHandle 呼叫相關聯之斷點回叫，自動化解碼過程 14 可收集 154 藉由執行已編碼 PE 二進制影像 24 而載入之動態鏈接庫之名稱。

類似地，在除錯過程中執行之已編碼 PE 二進制影像 24 可利用一 GetProcAddress API 呼叫以找到所需 API（應用程式設計介面）之位置。設置 164 與一 GetModuleHandle API 呼叫相關聯之一或多個斷點可使得當正在執行之已編碼 PE 二進制影像 24 加載所需 API 之位址時回叫自動化解碼過程 14。因應與一 GetModuleHandle API 呼叫相關聯之斷點回叫，自動化解碼過程 14 可收集 154 藉由執行已編碼 PE 二進制影像 24 而得到定位之 API 位址。正在執行之已編碼 PE 二進制影像 24 可在二位置處呼叫 GetProcAddress API，例如，用於字符串 API 定位及序數 API 定位。自動化解碼過程 14 可設置 164 與每一 GetProcAddress API 呼叫相關聯之一斷點。自動化解碼過程 14 可添加藉由 GetProcAddress API 呼叫所定位之 API 之位置至最新收集之動態鏈接庫。

自動化解碼過程 14 可自記憶體（例如 RAM）複製 156 一已除錯之 PE 檔至一電腦可讀取記錄媒體（例如儲存裝置 18）。一旦在除錯環境內執行之已編碼 PE 二進制影像 24 到達其中所收錄之可執行檔之原始入口點，該檔之解碼便可實質上完成。換言之，該檔可被解壓縮及/或解密等（端視與已編碼 PE 二進制影像 24 相關聯之保護之性質而定）。因此，此時，一已解碼之 PE 檔可駐存於與計算裝置 16 相關聯之記憶體中（例如，如第 1 圖所示位於記憶

體 26 中之 PE)。自動化解碼過程 14 可複製記憶體 26 中之已解碼 PE 例如至一駐存於儲存媒體 18 上之檔。因此，自動化解碼過程 14 可至少部分地根據已編碼 PE 二進制影像 24 而創建已儲存之 PE 28，該已儲存之 PE 28 可係為一已解碼攜帶式可執行檔之至少一部分。

自動化解碼過程 14 可貼附 166 一導入位址表與一重定位表至少其中之一至已除錯之攜帶式可執行檔（例如，已儲存之 PE 28），該導入位址表係至少部分地基於所收集 154 之導入位址表資料，該重定位表則至少部分地基於所收集 154 之重定位表資料。舉例而言，自動化解碼過程 14 可至少部分地根據自動化解碼過程 14 在除錯過程之執行 152（例如，其可包括在一除錯環境內執行已編碼 PE 二進制影像 24）期間所收集 154 之導入位址表資料及重定位表資料而構造一導入位址表與一重定位表至少其中之一。

貼附 166 一至少部分地基於所收集 154 之導入位址表資料之導入位址表與一至少部分地基於所收集 154 之重定位表資料之重定位表至少其中之一至已除錯之攜帶式可執行檔（例如，已儲存之 PE 28）可包含添加 168 一新部分至已除錯之攜帶式可執行檔。舉例而言，已儲存之 PE 28 可不包含一用於一導入位址表之部分及/或一用於一重定位表之部分。相應地，自動化解碼過程 14 可在已儲存之 PE 28 內騰出用於一導入位址表及/或用於一重定位表之空間（例如，藉由在已儲存之 PE 28 內添加 168 一用於一導入位址表及/或一重定位表之適當部分）。接著，自動化解碼過程 14 可貼附 166 該導入位址表及/或該重定位表至已儲存 PE 28 之恰當位置。

一旦已貼附 166 該導入位址表及/或該重定位表至已儲存之 PE 28，自動化解碼過程 14 便可使已除錯之 PE 檔（例如，已儲存之 PE 28）重新對齊 170。一般而言，使已除錯之 PE 檔重新對齊 170 可包含壓縮該檔並驗證該檔係為一有效影像，例如，此可包含驗證該檔之各別 PE 部分之物理尺寸是否正確且盡可能小。另外，自動化解碼過程 14 可讀取、寫入及執行已除錯 PE 檔（例如，已儲存之 PE 28）之所有部分屬性。因此，自動化解碼過程 14 可創建一有效 PE 檔，該有效 PE 檔可實質類似於編碼之前（即，在修改經軟體保護及/或壓縮之檔之前）之已編碼 PE 二進制影像 24。

在解碼過程完成後，自動化解碼過程 14 可在原始入口點終止 158 對已編碼 PE 二進制影像 25 之除錯。

儘管上文係論述各種分立之過程，然而如此分開論述係為了易於說明。該等分立之過程（及/或其部分）可包含一較大應用程式之可交互作用之各模組。另外，該等過程之各特徵及步驟可與本文所述其他過程之特徵及步驟結合使用。因此，本發明不應被視為僅限於上文所述之分立過程。

上文已闡述了本發明之多種實施方式。然而，應理解，可對其作出各種修飾。因此，其他實施方式亦處於下文申請專利範圍之範疇內。

【圖式簡單說明】

第 1 圖示意性地繪示一計算裝置，該計算裝置可執行一有效性檢查過程、一修復過程及一自動化解碼過程其中之一或多者；

第 2 圖係為由第 1 圖之有效性檢查過程執行之一過程之流程圖；

第 3 圖係為由第 1 圖之修復過程執行之一過程之流程圖；以及
第 4 圖係為由第 1 圖之自動化解碼過程執行之一過程之流程圖。

【主要元件符號說明】

10：有效性檢查過程

12：修復過程

14：自動化解碼過程

16：計算裝置

18：儲存裝置

20：PE 二進制影像

22：函式庫

24：PE 二進制影像

26：記憶體

28：已儲存之 PE

七、申請專利範圍：

1. 一種由電腦執行之方法，包含：

由一計算裝置在一已編碼之攜帶式可執行檔（packed portable executable file）之一原始入口點位址（original entry point address）設置一除錯斷點（debugging point）；

由該計算裝置對該已編碼之攜帶式可執行檔執行一除錯過程，以在記憶體中獲得一已除錯之攜帶式可執行檔；

在對該已編碼之攜帶式可執行檔執行該除錯過程期間，由該計算裝置收集一導入位址表資料（import address table data）與一重定位表資料（relocation table data）至少其中之一；

由該計算裝置複製記憶體中之該已除錯之攜帶式可執行檔至一儲存媒體；以及

由該計算裝置終止該除錯過程。

2. 如請求項 1 所述之由電腦執行之方法，更包含：由該計算裝置至少部分地根據該已編碼之攜帶式可執行檔之映像基底（ImageBase）欄位資料以及該已編碼之攜帶式可執行檔之進入點位址（AddressOfEntryPoint）資料，確定該已編碼之攜帶式可執行檔之該原始入口點位址。

3. 如請求項 1 所述之由電腦執行之方法，更包含：由該計算裝置初始化該除錯過程，包括至少部分地根據該已編碼之攜帶式可執行檔創建一除錯過程。

4. 如請求項 1 所述之由電腦執行之方法，其中收集該導入位址表資料與該重定位表資料至少其中之一之步驟包括：設置與

一函式庫讀取 (LoadLibrary) 呼叫、一模組處理獲取 (GetModuleHandle) 呼叫及一程序位址獲取 (GetProcAddress) 呼叫相關聯之一或多個除錯斷點。

5. 如請求項 1 所述之由電腦執行之方法，更包含由該計算裝置向該已除錯之攜帶式可執行檔中貼附以下至少其中之一：

一導入位址表，其至少部分地基於該等所收集之導入位址表資料；以及

一重定位表，其至少部分地基於該等所收集之重定位表資料。

6. 如請求項 5 所述之由電腦執行之方法，其中向該已除錯之攜帶式可執行檔中貼附之步驟包括：添加一新部分至該已除錯之攜帶式可執行檔。

7. 如請求項 1 所述之由電腦執行之方法，更包含：由該計算裝置使該已除錯之攜帶式可執行檔重新對齊 (realigning)。

8. 一種電腦程式產品，包含一儲存有複數個指令之電腦可讀取記錄媒體，該等指令在由一處理器執行時，使該處理器執行包含以下之操作：

在一已編碼之攜帶式可執行檔之一原始入口點位址設置一除錯斷點；

對該已編碼之攜帶式可執行檔執行一除錯過程，以在記憶體中獲得一已除錯之攜帶式可執行檔；

在對該已編碼之攜帶式可執行檔執行該除錯過程期間，收集一導入位址表資料與一重定位表資料至少其中之一；

複製記憶體中之該已除錯之攜帶式可執行檔至一儲存媒

體；以及

終止該除錯過程。

9. 如請求項 8 所述之電腦程式產品，更包含用於以下之指令：
至少部分地根據該已編碼之攜帶式可執行檔之映像基底
(ImageBase) 欄位資料以及該已編碼之攜帶式可執行檔之進
入點位址 (AddressOfEntryPoint) 資料，確定該已編碼之攜帶
式可執行檔之該原始入口點位址。
10. 如請求項 8 所述之電腦程式產品，更包含用於以下之指令：
初始化該除錯過程，包括至少部分地根據該已編碼之攜帶式
可執行檔創建一除錯過程。
11. 如請求項 8 所述之電腦程式產品，其中收集該導入位址表資
料與該重定位表資料至少其中之一之步驟包括：設置與一函
式庫讀取 (LoadLibrary) 呼叫、一模組處理獲取
(GetModuleHandle) 呼叫及一程序位址獲取
(GetProcAddress) 呼叫相關聯之一或多個除錯斷點。
12. 如請求項 8 所述之電腦程式產品，更包含用於向該已除錯之
攜帶式可執行檔中貼附以下至少其中之一指令：
一導入位址表，其至少部分地基於該等所收集之導入位
址表資料；以及
一重定位表，其至少部分地基於該等所收集之重定位表
資料。
13. 如請求項 12 所述之電腦程式產品，其中向該已除錯之攜帶式
可執行檔中貼附包括：添加一新部分至該已除錯之攜帶式可
執行檔。

14. 如請求項 8 所述之電腦程式產品，更包含用於使該已除錯之攜帶式可執行檔重新對齊（realigning）之指令。

15. 一種系統，包含：

一處理器；

一記憶體，耦接該處理器；

一第一軟體模組，可由該處理器及該記憶體執行，該第一軟體模組用以在一已編碼之攜帶式可執行檔之一原始入口點位址設置一除錯斷點；

一第二軟體模組，可由該處理器及該記憶體執行，該第二軟體模組用以對該已編碼之攜帶式可執行檔執行一除錯過程，以在記憶體中獲得一已除錯之攜帶式可執行檔；

一第三軟體模組，可由該處理器及該記憶體執行，該第三軟體模組用以在對該已編碼之攜帶式可執行檔執行該除錯過程期間，收集一導入位址表資料與一重定位表資料至少其中之一；

一第四軟體模組，可由該處理器及該記憶體執行，該第四軟體模組用以複製記憶體中之該已除錯之攜帶式可執行檔至一儲存媒體；以及

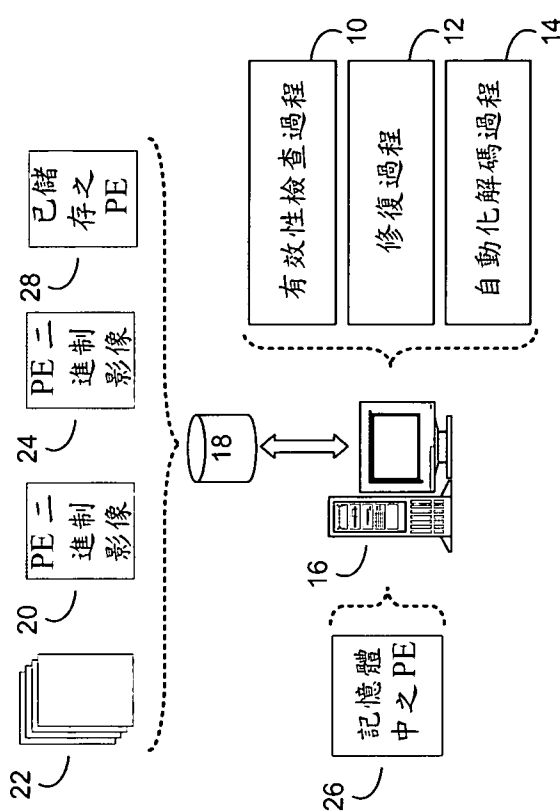
一第五軟體模組，可由該處理器及該記憶體執行，該第五軟體模組用以終止該除錯過程。

16. 如請求項 15 所述之系統，更包含可由該處理器及該記憶體執行之一第六軟體模組，該第六軟體模組用以至少部分地根據該已編碼之攜帶式可執行檔之映像基底（ImageBase）欄位資料以及該已編碼之攜帶式可執行檔之進入點位址

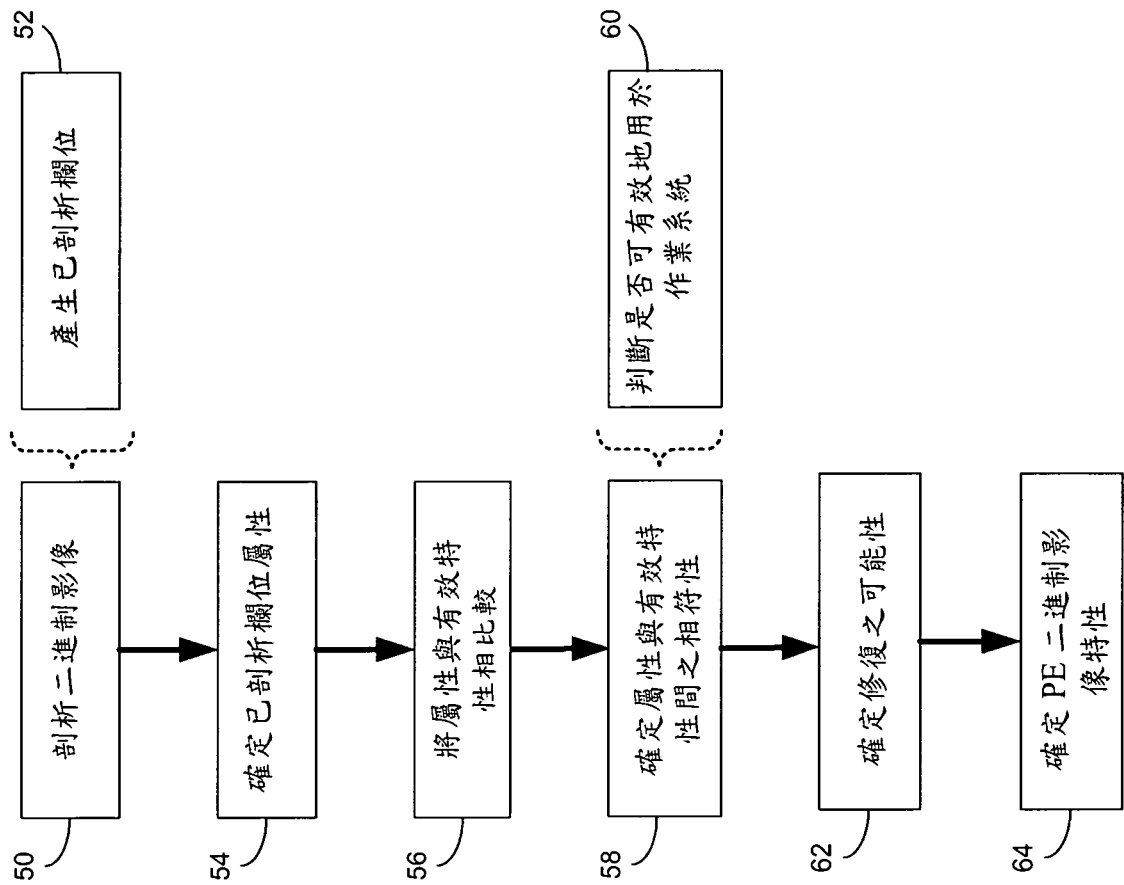
(AddressOfEntryPoint) 資料，確定該已編碼之攜帶式可執行檔之該原始入口點位址。

17. 如請求項 15 所述之系統，更包含可由該處理器及該記憶體執行之一第七軟體模組，該第七軟體模組用以初始化該除錯過程，包括至少部分地根據該已編碼之攜帶式可執行檔創建一除錯過程。
18. 如請求項 15 所述之系統，其中用以收集該導入位址表資料與該重定位表資料至少其中之一之該第三軟體模組係用以：設置與一函式庫讀取 (LoadLibrary) 呼叫、一模組處理獲取 (GetModuleHandle) 呼叫及一程序位址獲取 (GetProcAddress) 呼叫相關聯之一或多個除錯斷點。
19. 如請求項 15 所述之系統，更包含可由該處理器及該記憶體執行之一第八軟體模組，該第八軟體模組用以由該計算裝置向該已除錯之攜帶式可執行檔中貼附以下至少其中之一：
 - 一導入位址表，其至少部分地基於該等所收集之導入位址表資料；以及
 - 一重定位表，其至少部分地基於該等所收集之重定位表資料。
20. 如請求項 19 所述之系統，其中用以向該已除錯之攜帶式可執行檔中貼附之該第八軟體模組係用以：添加一新部分至該已除錯之攜帶式可執行檔。
21. 如請求項 15 所述之系統，更包含可由該處理器及該記憶體執行之一第九軟體模組，該第九軟體模組用以使該已除錯之攜帶式可執行檔重新對齊 (realigning)。

八、圖式：

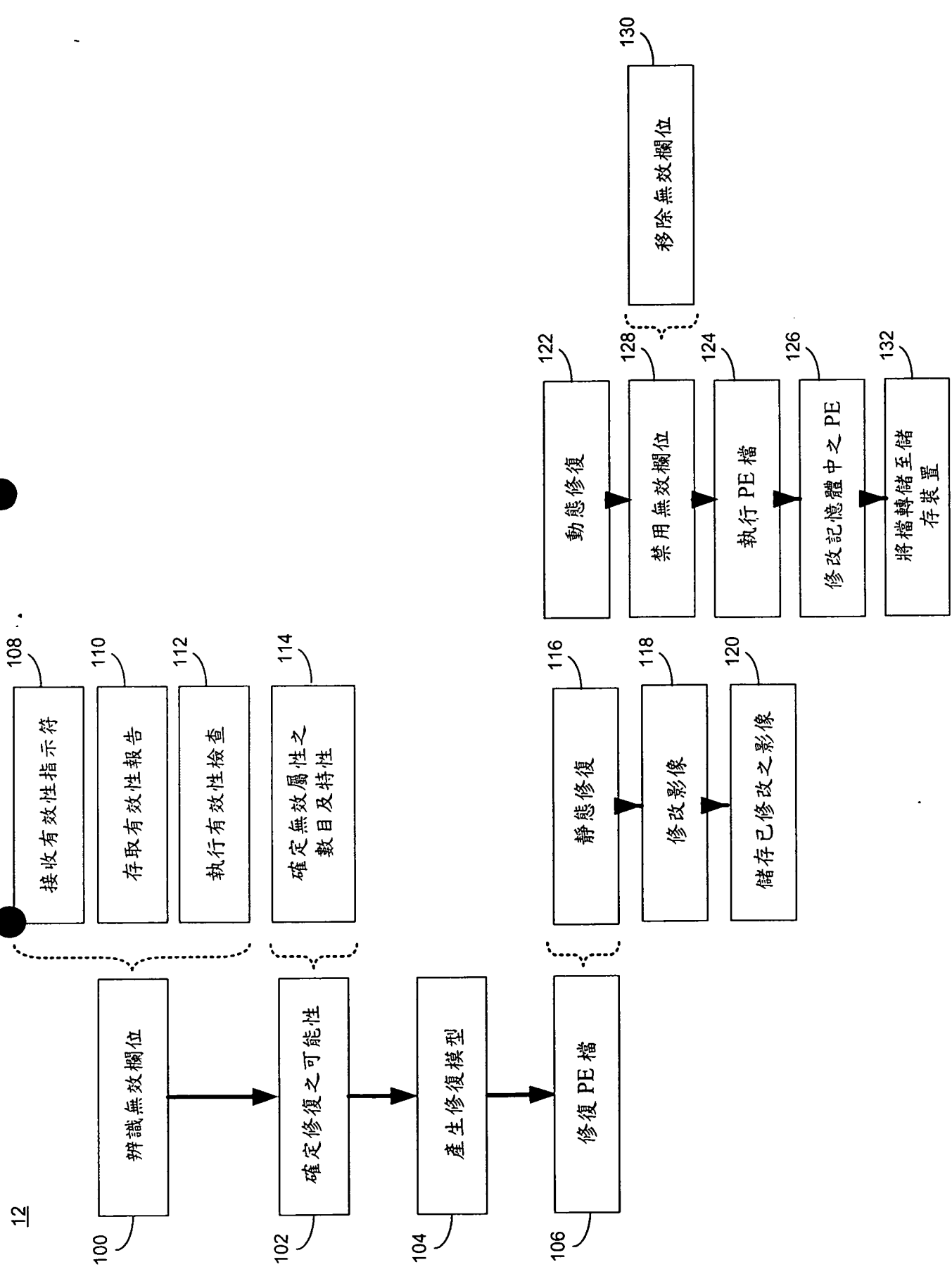


第 1 圖

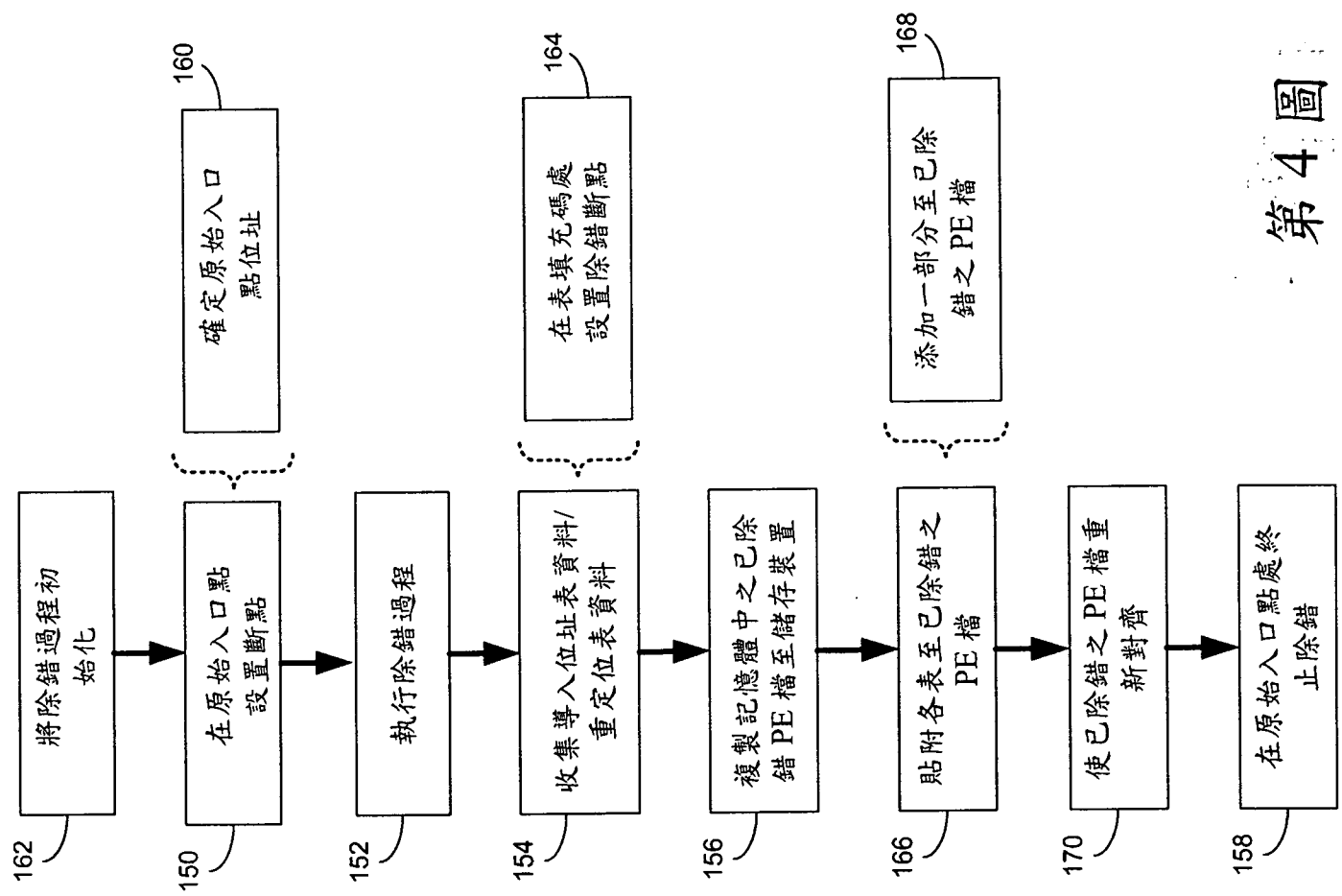


第 2 圖

12



第 3 圖



第4圖