200905516

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※申請案號：97135420

※申請日期：97.9.16　　※IPC 分類：G06F 21/24 (2006.01)

一、發明名稱：（中文/英文）

檔案資料外洩保護方法與系統

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

以柔資訊股份有限公司

代表人：（中文/英文）閆文瑩

住居所或營業所地址：（中文/英文）

台中市西屯區中港路三段 123 號 18 樓之 1

國　籍：（中文/英文）中華民國

三、發明人：（共 4 人）

姓　名：（中文/英文）

1. 羅文聰
2. 許瑞愷
3. 黃天賜
4. 盧惠傑

國　籍：（中文/英文）

中華民國(四人皆同)

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☐ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☐ 有主張專利法第二十七條第一項國際優先權：

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本發明係提供一種軟體檔案之技術領域，尤指提供一種檔案資料外洩保護方法與系統，特別是用於視窗系統所產生的檔案資料的保護。

【先前技術】

為防止檔案資料外洩，一般而言是利用檔案權限控管程序，搭配加解密演算法來達成資料保護的目的，然而檔案加密程式，通常是在檔案產生後，再決定是否將該檔案加解密，這種檔案資料外洩保護措施會有一致命的漏洞，即是短暫時間內存在一個未加密的檔案版本，造成有意或無意間資料外洩的機會。

為了完整保護檔案資料，加解密保護措施，在檔案新增、編輯及讀取的過程中，全方位的加解密是必要的，但目前尚未有相關保護機制。

習知保護機制有：

1．移轉特定格式，例如ＰＤＦ：藉由ＰＤＦ檔案特性，將欲保護的文件轉成ＰＤＦ保密文件。惟，其是檔案移轉後的保護，需要改變使用者習慣使用特定格式的檔案閱讀器，亦無法達到保護原始檔案資料內容之目的。

2．外掛程式：在應用軟體開發外掛程式保護檔案內容，但如此作法，因為應用軟體實在太多，版本更新又很快，所以都要寫外掛有寫不完的問題，成本也不划算。

3．暫存檔案：在檔案產生後，產生一相同內容之暫存檔案，而將原本檔案加密並鎖定禁止其他應用程式存取

該檔案。應用軟體對於該檔案的存取都先暫時寫入該暫存檔案，存取完畢後，再將檔案內容回存到原檔案內容。此作法的問題是為短暫時間內存在一個未加密的暫存檔案版本，造成有意或無意間的資料外洩的機會。

參閱第六圖所示，為其現今新版的微軟作業系統基本架構圖，該個人電腦（５）內之微軟作業系統內核模式層（６）內一定會有一輸出入管理員 (IO Manager)（１）及一過濾器管理員(Filter Manager)（２），其在使用者模式層（７）之應用程式的輸出入作業（４）一定會先經過輸出入管理員 (IO Manager)（１）及過濾器管理員(Filter Manager)（２），才到達檔案系統（３），而檔案系統（３）資料亦是經由輸出入管理員 (IO Manager)（１）及過濾器管理員(Filter Manager)（２），才到達應用程式的輸出入作業（４）。

是以，針對上述習知技術所存在之問題點，如何一種更具理想實用性之創新保護技術，實消費者所殷切企盼，亦係相關業者須努力研發突破之目標及方向。

有鑑於此，發明人本於多年從事相關產品之開發與設計經驗，針對上述之目標，詳加設計與審慎評估後，終得一確具實用性之新技術成為本發明。

【發明內容】

欲解決之技術問題點：習知保護機制的問題點有下列三種。

１．移轉特定格式，例如ＰＤＦ：藉由ＰＤＦ檔案特性，將欲保護的文件轉成ＰＤＦ保密文件。惟，其是檔案

移轉後的保護，需要改變使用者習慣使用特定格式的檔案閱讀器，亦無法達到保護原始檔案資料內容之目的。

2．外掛程式：在應用軟體開發外掛程式保護檔案內容，但如此作法，因為應用軟體實在太多，版本更新又很快，所以都要寫外掛有寫不完的問題，成本也不划算。

3．暫存檔案：在檔案產生後，產生一相同內容之暫存檔案，而將原本檔案加密並鎖定禁止其他應用程式存取該檔案。應用軟體對於該檔案的存取都先暫時寫入該暫存檔案，存取完畢後，再將檔案內容回存到原檔案內容。此作法的問題是為短暫時間內存在一個未加密的暫存檔案版本，造成有意或無意間的資料外洩的機會。

解決問題之技術特點：提供一種檔案資料外洩保護方法與系統，係基於微軟作業系統之檔案系統過濾器驅動程式 (File System Filter Driver) 主架構，加入一個人化安全控管代理程式及一隱形加解密驅動模組，該隱形加解密驅動模組放置在系統輸出入管理員 (IO Manager) 與檔案系統動程式 (File System Driver) 之間，作業系統上任何檔案的新增、編輯及讀取動作及資料流，都被隱形加解密驅動模組攔截。當新檔案產生或暫存時，隱形加解密驅動模組根據權限及安全控管模組及應用程式辨識模組，決定檔案是否予以加密，對於需要加密的檔案內容，隱形加解密驅動模組將透過加解密模組將攔截到的資料流加密後儲存於儲存器中，當應用程式欲讀取檔案內容時，隱形加解密驅動模組依據應用程式辨識模組及權限及安全控管模組決定是否將該檔案內容解密，沒有經過隱形加解密驅動模組及加解密

模組的檔案，不管經由任何方式傳送到何處，使用者將無法辨識檔案內容資料，達到完善防止資料外洩之保護。

對照先前技術之功效：

1．先前技術有暫存檔的漏洞，即其檔案是在完成後再保護，所以造成有意無意的資料外洩情形；而本發明之白名單內檔案之寫入動作均會自動加密，所以沒有空窗期。

2．應用程式的外掛，其版本相容/格式相容開發難度高；而本發明之檔案格式與應用程式不受限。

3．先前技術轉檔特定格式需要改變使用者操作習慣；而本發明係在系統核心攔截，所以使用者介面完全沒有改變，不用改變使用者使用習慣。

有關本發明所採用之技術、手段及其功效，茲舉一較佳實施例並配合圖式詳細說明於后，相信本發明上述之目的、構造及特徵，當可由之得一深入而具體的瞭解。

【實施方式】

本發明開發出一種利用隱形加解密技術以達成檔案資料外洩保護措施。其用於電腦之微軟視窗系統中，尤指檔案系統過濾器驅動程式 (File System Filter Driver) 架構下，當檔案在新增、編輯及讀取的過程中，自動加解密以防護檔案資料不外洩。以下依序說明本發明技術。

參閱第一圖所示，係為本發明之其一實施例系統圖，其中個人電腦（１００）之內，區分有使用者模式層（７０）及內核模式層（８０）該微軟視窗作業系統中，其內核模式層（８０）內有輸出入管理員(IO Manager)（１１）

及過濾器管理員(Filter Manager)（１２），其係作為內部的控管及使用者模式層（７０）之應用程式的輸出入作業（１０）與檔案系統（４０）間之橋樑，本發明主要在使用者模式層（７０）下建立一安全控管代理程式（５０），並於內核模式層（８０）之過濾器管理員(Filter Manager)（１２）與檔案系統（４０）間建立隱形加解密驅動模組（２０），如此，應用程式的輸出入作業（１０）及檔案系統（４０）之資料流，則都會被隱形加解密驅動模組（２０）攔截，如果是白名單內應用程式存取的檔案就在讀取時解密並依權限開給使用者，而在開新檔或儲存或暫存時加密並加入識別證到檔案內容中。

一種檔案資料外洩保護方法，係包含有：

步驟一：於使用在檔案系統過濾器驅動程式 (File System Filter Driver) 架構之微軟視窗系統內，載入安裝一安全控管代理程式於該使用者模式層及一隱形加解密驅動模組安裝於該內核模式層之該過濾器管理員(Filter Manager)及該檔案系統間，該安全控管代理程式可與該隱形加解密驅動模組直接溝通；

步驟二：該隱形加解密驅動模組內設有數白名單或數權限；

步驟三：所有經過隱形加解密驅動模組之檔案均會比對白名單及權限，儲存前如為白名單則會加密加入識別證，而開啟檔案時如為白名單則會解密並依權限開啟給使用者。

上述該隱形加解密驅動模組內設之數白名單或數權限為經由安全控管代理程式經網路（６１）至安全控管伺服器（６０）下載或更新之數權限或數白名單。

參閱第一圖所示，一種檔案資料外洩保護系統，係包含有：

使用在檔案系統過濾器驅動程式 (File System Filter Driver)架構之微軟視窗系統之一安全控管代理程式（５０）及一隱形加解密驅動模組（２０），其中該安全控管代理程式（５０）設於作業系統使用者模式層（７０）內，而該隱形加解密驅動模組（２０）設於該內核模式層（８０）之該過濾器管理員(Filter Manager)（１２）及該檔案系統（４０）間，該安全控管代理程式（５０）可與該隱形加解密驅動模組（２０）直接溝通；

該應用程式的輸出入作業（１０）及檔案系統（４０）之所有檔案的新增、編輯及讀取動作及資料流，都被隱形加解密驅動模組（２０）攔截，白名單內檔案的隱形加解密、權限控管或識別證工作均在內核模式層（８０）內執行，使用者不會發覺，並以一權限及安全控管模組（２１）判定是否需進行安全控管，當新檔案產生時，該隱形加解密驅動模組（２０）根據權限及安全控管模組（２１），決定檔案是否予以加密，加密則利用一加解密模組（２２）加密，加密後的檔案嵌入有識別碼，其後檔案無論在何處，只要沒有隱形加解密驅動模組（２０）及權限，則無法正確開啟或編輯。

上述該隱形加解密驅動模組（２０）包含有一權限及

安全控管模組（２１）、一加解密模組（２２）、一輸出入控制模組（２３）、一識別碼管理模組（２４）及一應用程式辨識模組（２５）。

上述該加解密模組（２２）使用之演算法可為對稱式加解密演算法。

上述該識別證包含有儲存產生檔案環境、權限或安全控管的資訊，該識別證作為檔案未來讀取編輯時的控管依據。

參閱第一、二圖所示，其電腦新加入本發明時，會安裝一安全控管代理程式（５０）及一隱形加解密驅動模組（２０），該安全控管代理程式（５０）設於使用者模式層（７０），該隱形加解密驅動模組（２０）放置在該內核模式層（８０）之輸出入管理員(IO Manager)（１１）與檔案系統（４０）之間；

其權限/白名單初始化之動作上，開始（１１０）時安全控管代理程式由安全控管伺服器取得權限及白名單（１１１），其後安全控管代理程式將權限資料傳送到權限及安全控管模組（１１２），且安全控管代理程式將白名單資料傳送到應用程式辨識模組（１１３）。

參閱第三圖所示，該新增檔案程序動作為，開始（１２０），應用程式送出新增檔案之作業請求（１２１），輸出入管理員攔截該新增檔案請求，並將該請求送給過濾器管理員（１２２），過濾器管理員將該新增檔案請求送給隱形加解密驅動模組（１２３），輸出入控制模組接手新增檔案作業（１２４），詢問權限及安全控管模組是否

有權限新增檔案（１２５），否，新增檔案失敗（１２６），是，詢問應用程式辨識模組該應用程式是否在白名單內（１２７），否，新增檔案失敗（１２６），是，輸出入控制模組新增檔案到檔案系統（１２８），新增檔案完成（１２９）。

參閱第四圖所示，該讀取文件程序動作為，開始（１３０），應用程式送出「讀取檔案」之作業請求（１３１），輸出入管理員攔截該讀取檔案請求，並將該請求送給過濾器管理員（１３２），過濾器管理員將該讀取檔案請求送給隱形加解密驅動模組（１３３），輸出入控制模組接手讀取檔案作業（１３４），輸出入控制模組從檔案系統讀取檔案內容（１３５），詢問應用程式辨識模組該應用程式是否在白名單內（１３６），否，則輸出入控制模組回傳檔案內容給過濾器管理員（１３６１），再將檔案內容回傳給輸出入管理員（１３６２），再輸出入管理員將檔案內容回傳給應用程式（１３６３）。是，則詢問識別碼管理模組檔案內容是否有識別證（１３７），是，則加解密模組將檔案內容解密（１３７１），其後輸出入控制模組回傳檔案內容給過濾器管理員（１３６１），再將檔案內容回傳給輸出入管理員（１３６２），再輸出入管理員將檔案內容回傳給應用程式（１３６３）。否，則識別碼管理模組嵌入識別證到檔案內容（１３８），加解密模組將檔案內容加密（１３９），輸出入控制模組將檔案內容回存到檔案系統（１３９１）。

參閱第五圖所示，該檔案儲存程序為，開始（１４０

），應用程式送出「檔案儲存」之作業請求（１４１），輸出入管理員攔截該檔案儲存請求，並將該請求送給過濾器管理員（１４２），過濾器管理員將該檔案儲存請求送給隱形加解密驅動模組（１４３），輸出入控制模組接手檔案儲存作業（１４４），詢問權限及安全控管模組該應用程式是否有權限（１４５），否，輸出入控制模組回傳儲存失敗訊息給過濾器管理員（１４５１），過濾器管理員將回傳儲存失敗訊息給輸出入管理員（１４５２），輸出入管理員回傳儲存失敗訊息給應用程式（１４５３）。是，則詢問應用程式辨識模組該應用程式是否在白名單內（１４６），是，則識別碼管理模組嵌入識別證到檔案內容（１４７），加解密模組將檔案內容加密（１４８），輸出入控制模組將檔案內容回存到檔案系統（１４９），輸出入控制模組回傳儲存成功訊息給過濾器管理員（１４９１），過濾器管理員將回傳儲存成功訊息給輸出入管理員（１４９２），輸出入管理員回傳儲存成功訊息給應用程式（１４９３）。否，則輸出入控制模組將檔案內容回存到檔案系統（１４９），輸出入控制模組回傳儲存成功訊息給過濾器管理員（１４９１），過濾器管理員將回傳儲存成功訊息給輸出入管理員（１４９２），輸出入管理員回傳儲存成功訊息給應用程式（１４９３）。

藉由上述，本發明達到了完整保護檔案資料及隱形加解密保護，而且其係在於檔案之新增、編輯及讀取的新增、暫存或儲存過程均自動加解密，使得想要竊取該原始檔案或未加密的檔案變成不可能，進而使得本發明的防護得

以滴水不漏。

前文係針對本發明之較佳實施例為本發明之技術特徵進行具體之說明；惟，熟悉此項技術之人士當可在不脫離本發明之精神與原則下對本發明進行變更與修改，而該等變更與修改，皆應涵蓋於如下申請專利範圍所界定之範疇中。

【圖式簡單說明】

第一圖：係本發明其一實施例之系統圖。

第二圖：係本發明權限/白名單初始化流程圖。

第三圖：係本發明新增檔案程序流程圖。

第四圖：係本發明讀取文件程序流程圖。

第五圖：係本發明檔案儲存程序流程圖。

第六圖：係習知微軟作業系統基本架構圖。

【主要元件符號說明】

・習用部份・

（１）輸出入管理員 (IO Manager)

（２）過濾器管理員(Filter Manager)

（３）檔案系統　　（４）應用程式的輸出入作業

（５）個人電腦　　（６）內核模式層

（７）使用者模式層

・本發明部份・

（１０）應用程式的輸出入作業

（１１）輸出入管理員 (IO Manager)

（１２）過濾器管理員(Filter Manager)

（２０）隱形加解密驅動模組

（２１）權限及安全控管模組

（２２）加解密模組　　（２３）輸出入控制模組

（２４）識別碼管理模組（２５）應用程式辨識模組

（４０）檔案系統　　（５０）安全控管代理程式

（６０）安全控管伺服器（６１）網路

（７０）使用者模式層　（８０）內核模式層

（１００）個人電腦

（１１０）開始

（１１１）安全控管代理程式由安全控管伺服器取得權限及白名單

（１１２）安全控管代理程式將權限資料傳送到權限及安全控管模組

（１１３）安全控管代理程式將白名單資料傳送到應用程式辨識模組

（１２０）開始

（１２１）應用程式送出新增檔案之作業請求

（１２２）輸出入管理員攔截該新增檔案請求，並將該請求送給過濾器管理員

（１２３）過濾器管理員將該新增檔案請求送給隱形加解密驅動模組

（１２４）輸出入控制模組接手新增檔案作業

（１２５）詢問權限及安全控管模組是否有權限新增檔案

（１２６）新增檔案失敗

（１２７）詢問應用程式辨識模組該應用程式是否在白名單內

（１２８）輸出入控制模組新增檔案到檔案系統

（１２９）新增檔案完成

（１３０）開始

（１３１）應用程式送出「讀取檔案」之作業請求

（１３２）輸出入管理員攔截該讀取檔案請求，並將該請求送給過濾器管理員

（１３３）過濾器管理員將該讀取檔案請求送給隱形加解密驅動模組

（１３４）輸出入控制模組接手讀取檔案作業

（１３５）輸出入控制模組從檔案系統讀取檔案內容

（１３６）詢問應用程式辨識模組該應用程式是否在白名單內

（１３６１）輸出入控制模組回傳檔案內容給過濾器管理員

（１３６２）將檔案內容回傳給輸出入管理員

（１３６３）輸出入管理員將檔案內容回傳給應用程式

（１３７）詢問識別碼管理模組檔案內容是否有識別證

（１３７１）加解密模組將檔案內容解密

（１３８）識別碼管理模組嵌入識別證到檔案內容

（１３９）加解密模組將檔案內容加密

（１３９１）輸出入控制模組將檔案內容回存到檔案系統

（１４０）開始

（１４１）應用程式送出「檔案儲存」之作業請求

（１４２）輸出入管理員攔截該檔案儲存請求，並將該請求送給過濾器管理員

（１４３）過濾器管理員將該檔案儲存請求送給隱形加解密驅動模組

（１４４）輸出入控制模組接手檔案儲存作業

（１４５）詢問權限及安全控管模組該應用程式是否有權限

（１４５１）輸出入控制模組回傳儲存失敗訊息給過濾器管理員

（１４５２）過濾器管理員將回傳儲存失敗訊息給輸出入管理員

（１４５３）輸出入管理員回傳儲存失敗訊息給應用程式

（１４６）詢問應用程式辨識模組該應用程式是否在白名單內

（１４７）識別碼管理模組嵌入識別證到檔案內容

（１４８）加解密模組將檔案內容加密

（１４９）輸出入控制模組將檔案內容回存到檔案系統

（１４９１）輸出入控制模組回傳儲存成功訊息給過濾器管理員

（１４９２）過濾器管理員將回傳儲存成功訊息給輸出入管理員

（１４９３）輸出入管理員回傳儲存成功訊息給應用程式

五、中文發明摘要：

一種檔案資料外洩保護方法與系統，係基於微軟作業系統之檔案系統過濾器驅動程式架構，加入一安全控管代理程式於使用者模式層及一隱形加解密驅動模組於內核模式層，作業系統上任何檔案的動作，都被隱形加解密驅動模組攔截並依內部各模組，決定檔案是否予以加密，對於需要加密的檔案內容，將加密後儲存於檔案系統中，當應用程式欲讀取檔案內容時，依應用程式辨識模組及權限及安全控管模組決定是否將該檔案內容解密。經過加密後的檔案，不管經由何種方式傳送到何處，沒有經過隱形加解密驅動模組解密，應用程式將無法辨識檔案內容資料，達完善防止資料外洩之保護。

六、英文發明摘要：

十、申請專利範圍：

1．一種檔案資料外洩保護方法，係包含有：

步驟一：於具有檔案系統過濾器驅動程式(File System Filter Driver) 架構之微軟作業系統內，載入安裝一安全控管代理程式於使用者模式層及一隱形加解密驅動模組安裝於內核模式層之過濾器管理員(Filter Manager)及檔案系統間，該安全控管代理程式可與該隱形加解密驅動模組直接溝通；

步驟二：該隱形加解密驅動模組內設有數白名單或數權限；

步驟三：所有經過隱形加解密驅動模組之檔案均會比對白名單及權限，開新檔或儲存或暫存時，如為白名單則會加密加入識別證，新檔或外界進入的檔案，要儲存或暫存時亦會比對白名單及權限，儲存或暫存前如為白名單則會加密加入識別證，而開啟檔案時如為白名單則會解密並依權限開啟給使用者。

2．如申請專利範圍第1項所述之檔案資料外洩保護方法，其中該隱形加解密驅動模組內設之數白名單或數權限為內鍵之數白名單或數權限。

3．如申請專利範圍第1項所述之檔案資料外洩保護方法，其中該隱形加解密驅動模組內設之數白名單或數權限為經由安全控管代理程式經網路至安全控管伺服器下載或更新之數權限或數白名單。

4．一種檔案資料外洩保護系統，係包含有：

使用在檔案系統過濾器驅動程式(File System Filter Driver)架構之微軟視窗系統之一安全控管代理程式及一隱形加解密驅動模組，其中該安全控管代理程式設於使用者模式層，而該隱形加解密驅動模組設於內核模式層之過濾器管理員(Filter Manager)及檔案系統間，該安全控管代理程式可與該隱形加解密驅動模組直接溝通；

該使用者模式層之應用程式的輸出入作業及內核模式層之所有檔案的新增、編輯及讀取動作及資料流，都被隱形加解密驅動模組攔截，白名單內檔案的隱形加解密、權限控管或識別證工作均在內核模式層執行，使用者不會發覺，並以權限及安全控管模組判定是否需進行安全控管，當新檔案產生或暫存或儲存時，隱形加解密驅動模組根據權限及安全控管模組，決定檔案是否予以加密，加密則利用加解密模組，加密後的檔案嵌入有識別證，其後檔案無論在何處，只要沒有隱形加解密驅動模組及權限，則無法正確開啟或編輯。

5．如申請專利範圍第4項所述之檔案資料外洩保護系統，其中該加解密模組使用之演算法可為對稱式加解密演算法。

6．如申請專利範圍第4項所述之檔案資料外洩保護系統，其中該識別證包含有儲存產生檔案環境、權限或安全控管的資訊，該識別證作為檔案未來讀取編輯時的控管依據。

7．如申請專利範圍第4項所述之檔案資料外洩保護系統，其中該隱形加解密驅動模組包含有一權限及安全控

管模組、一加解密模組、一輸出入控制模組、一識別碼管理模組及一應用程式辨識模組。

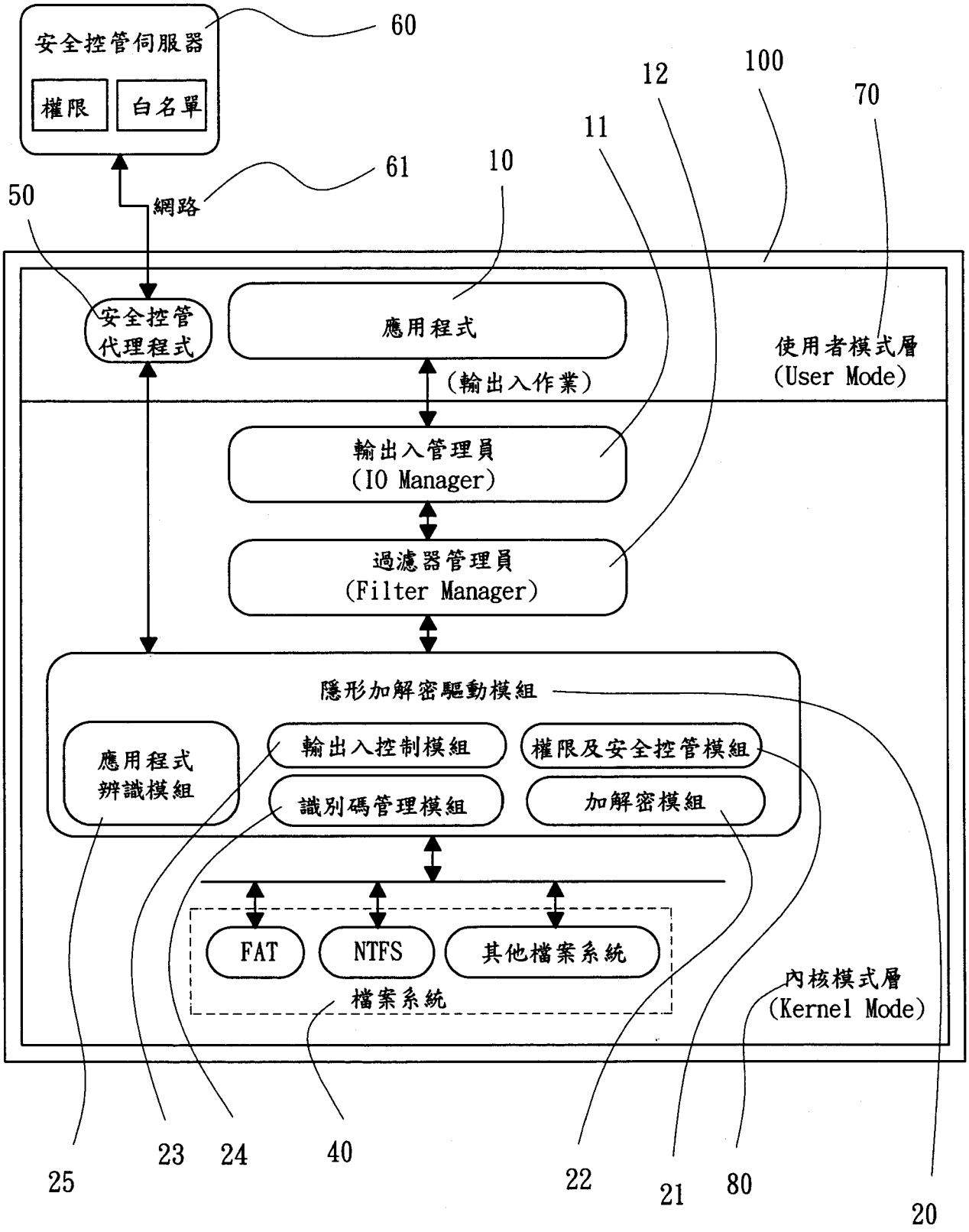
十一、圖式：

如次頁

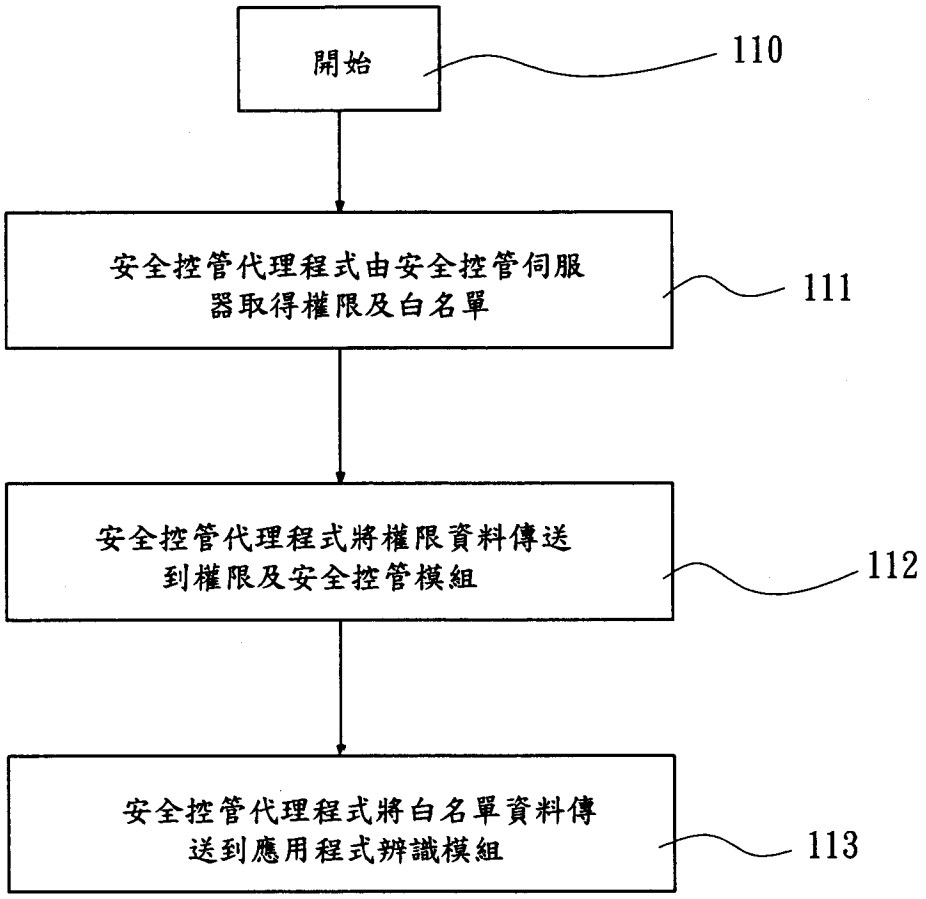
管模組、一加解密模組、一輸出入控制模組、一識別碼管理模組及一應用程式辨識模組。

十一、圖式：

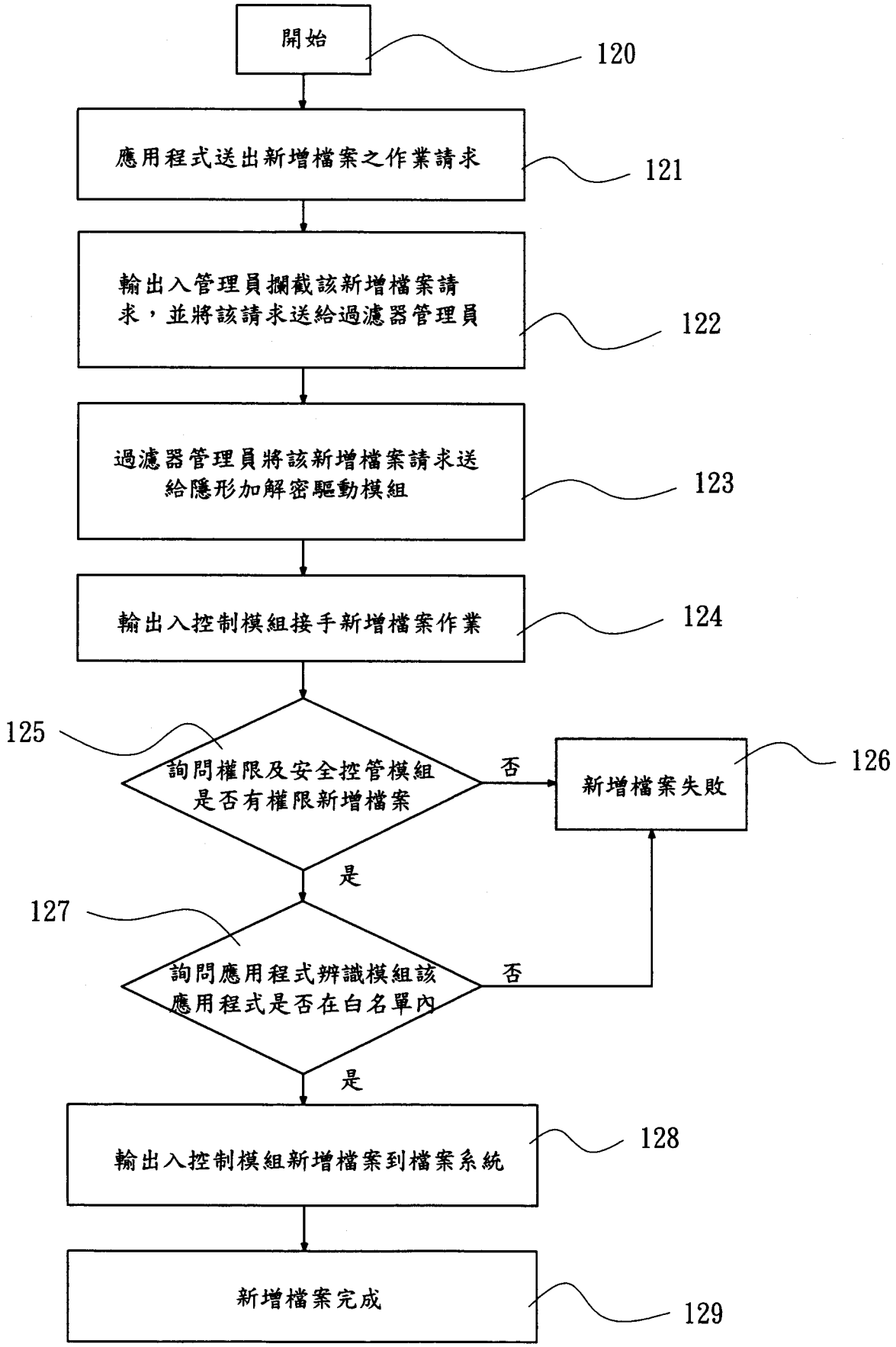
如次頁


安全控管伺服器
權限
白名單
60
61
網路
50
安全控管
代理程式
10
應用程式
(輸出入作業)
12
100
70
11
使用者模式層
(User Mode)
輸出入管理員
(IO Manager)
過濾器管理員
(Filter Manager)
隱形加解密驅動模組
應用程式
辨識模組
輸出入控制模組
權限及安全控管模組
識別碼管理模組
加解密模組
FAT
NTFS
其他檔案系統
檔案系統
內核模式層
(Kernel Mode)
25
23
24
40
22
21
80
20

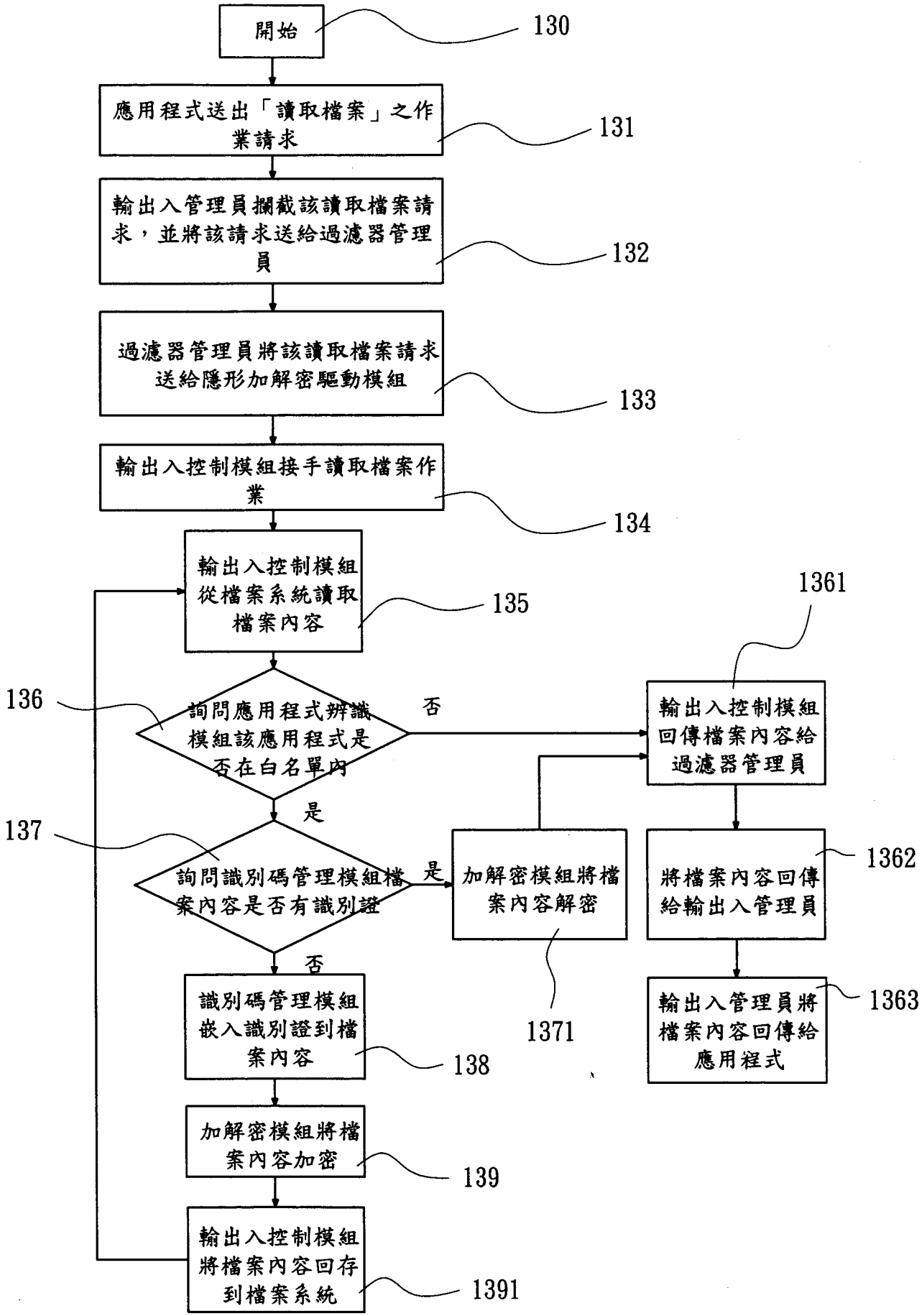
第一圖


開始
110
安全控管代理程式由安全控管伺服器取得權限及白名單
111
安全控管代理程式將權限資料傳送到權限及安全控管模組
112
安全控管代理程式將白名單資料傳送到應用程式辨識模組
113

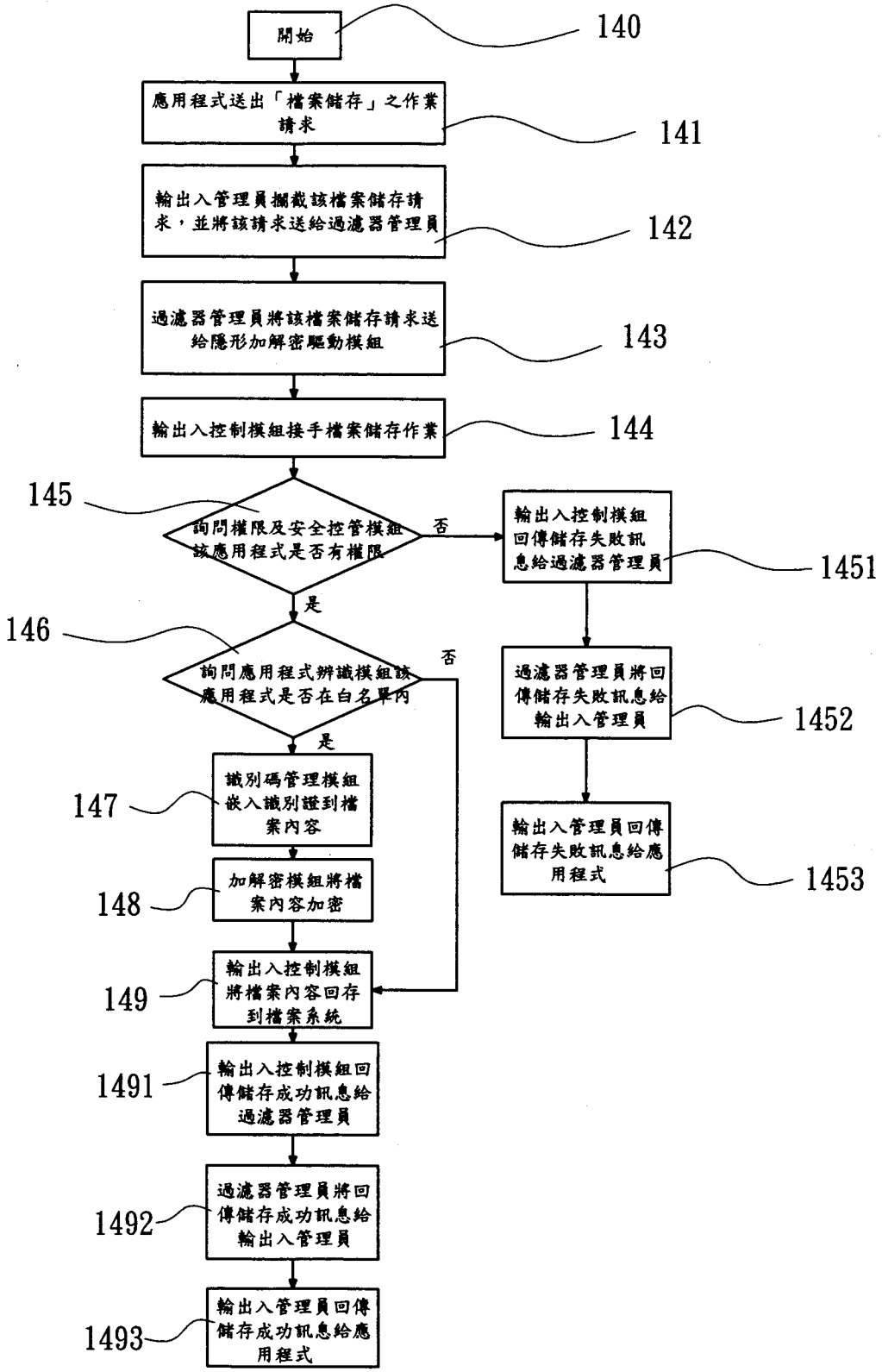
第二圖


開始
120
應用程式送出新增檔案之作業請求
121
輸出入管理員攔截該新增檔案請求，並將該請求送給過濾器管理員
122
過濾器管理員將該新增檔案請求送給隱形加解密驅動模組
123
輸出入控制模組接手新增檔案作業
124
125
詢問權限及安全控管模組是否有權限新增檔案
否
新增檔案失敗
126
是
127
詢問應用程式辨識模組該應用程式是否在白名單內
否
是
輸出入控制模組新增檔案到檔案系統
128
新增檔案完成
129

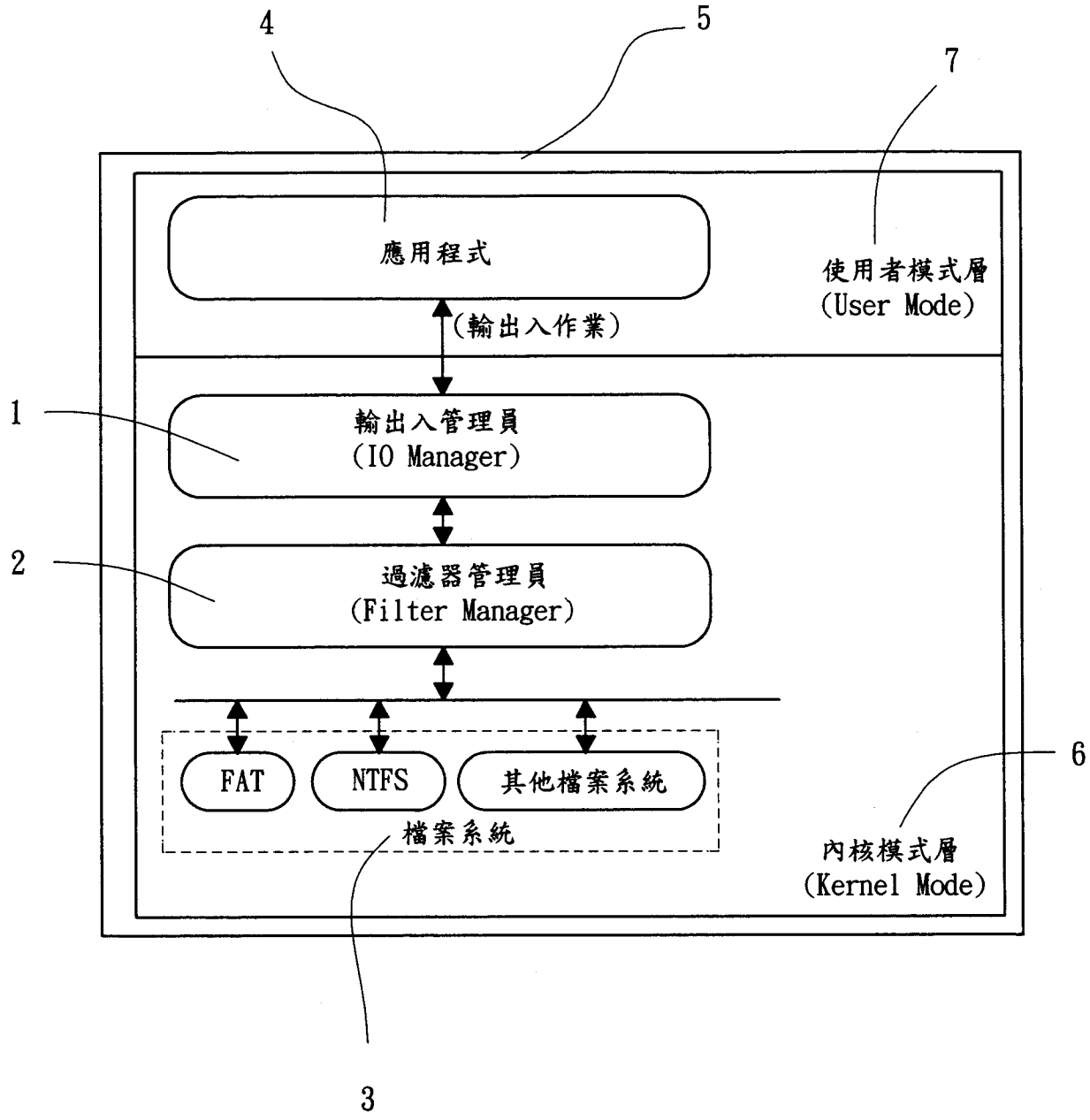
第三圖


開始
130
應用程式送出「讀取檔案」之作業請求
131
輸出入管理員攔截該讀取檔案請求，並將該請求送給過濾器管理員
132
過濾器管理員將該讀取檔案請求送給隱形加解密驅動模組
133
輸出入控制模組接手讀取檔案作業
134
輸出入控制模組從檔案系統讀取檔案內容
135
136
詢問應用程式辨識模組該應用程式是否在白名單內
否
是
1361
輸出入控制模組回傳檔案內容給過濾器管理員
137
詢問識別碼管理模組檔案內容是否有識別證
是
否
加解密模組將檔案內容解密
1371
將檔案內容回傳給輸出入管理員
1362
輸出入管理員將檔案內容回傳給應用程式
1363
識別碼管理模組嵌入識別證到檔案內容
138
加解密模組將檔案內容加密
139
輸出入控制模組將檔案內容回存到檔案系統
1391

第四圖


開始
140
應用程式送出「檔案儲存」之作業請求
141
輸出入管理員攔截該檔案儲存請求，並將該請求送給過濾器管理員
142
過濾器管理員將該檔案儲存請求送給隱形加解密驅動模組
143
輸出入控制模組接手檔案儲存作業
144
145
詢問權限及安全控管模組該應用程式是否有權限
否
輸出入控制模組回傳儲存失敗訊息給過濾器管理員
1451
是
146
詢問應用程式辨識模組該應用程式是否在白名單內
否
過濾器管理員將回傳儲存失敗訊息給輸出入管理員
1452
是
147
識別碼管理模組嵌入識別證到檔案內容
輸出入管理員回傳儲存失敗訊息給應用程式
1453
148
加解密模組將檔案內容加密
149
輸出入控制模組將檔案內容回存到檔案系統
1491
輸出入控制模組回傳儲存成功訊息給過濾器管理員
1492
過濾器管理員將回傳儲存成功訊息給輸出入管理員
1493
輸出入管理員回傳儲存成功訊息給應用程式

第五圖


4
5
7
應用程式
使用者模式層
(User Mode)
(輸出入作業)
1
輸出入管理員
(IO Manager)
2
過濾器管理員
(Filter Manager)
FAT
NTFS
其他檔案系統
檔案系統
6
內核模式層
(Kernel Mode)
3

第六圖

七、指定代表圖：

（一）本案指定代表圖為：第（一）圖。

（二）本代表圖之元件符號簡單說明：

（１００）個人電腦

（１０）應用程式的輸出入作業

（１１）輸出入管理員 (IO Manager)

（１２）過濾器管理員(Filter Manager)

（２０）隱形加解密驅動模組

（２１）權限及安全控管模組

（２２）加解密模組

（２３）輸出入控制模組

（２４）識別碼管理模組

（２５）應用程式辨識模組

（４０）檔案系統

（５０）安全控管代理程式

（６０）安全控管伺服器

（６１）網路

（７０）使用者模式層

（８０）內核模式層

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：