線上與離線兩用之嵌入式防竄改監視系統

On-line and off-line monitoring system that prevent distorting

蔡哲民
崑山科技大學資訊管理系 助理教授
tjm@mail.ksut.edu.tw

曾嘉薪、賴峻廷
崑山科技大學資訊管理系

摘要

本論文介紹一套具數位簽章與加密驗證機制的嵌入式防竄改監視系統，該系統使用 Open Source 的 SPB-Linux、OpenSSL 以及其他自由軟體為基礎，配合 bash shell script 開發而成，並使用廉價的 USB Web-cam 取得監視影像。在數位簽章與加密驗證防竄改機制中，透過每次系統亂數隨機產生之 private key 對監視影像進行簽章，並利用系統中具有唯一性且不易被 end-user 取得之硬體序號，搭配 private key 對系統記錄檔進行加密，以確保監視影像合乎資訊安全中之完整性與不可否認性。系統開機時產生的 public key 將會被置放在可移除之 USB Flash memory 中，以便移至安全的地方收藏，減少被變造的機會。

在監視影像儲存方面，本系統提供線上及離線兩種模式。於通訊正常情形下，可利用網路傳輸方式將監視影像儲存於遠端設備中，在無網路通訊或網路被破壞的環境下，則可將監視影像儲存於 USB Flash memory 中。透過使用 Motion 套件，當系統偵測到環境影像產生變化時才進行影像拍攝，可有效節省影像儲存的成本，延長離線拍攝的時間。

關鍵詞：數位簽章、嵌入式監視系統

一、前言

隨著現代人對生活安全日趨重視，市面上的監視系統亦不斷推陳出新，傳統監視系統大多藉由攝影機取得監視影像，並以錄影帶作為儲存媒體便於監視影像存檔備查，但此做法的缺點在於錄影帶本身保存不易，且隨著留存備查時間的增長，使用者必須預先準備大量的影帶作為錄影替換之用，無形中增加許多設備及金錢上的花費。

目前已經有人提出了一些嵌入式的網路監視系統[1][2]，透過數位化的方式改善了傳統監視系統的缺點，將監視影像以 JPEG 壓縮後透過網路傳輸並儲存於遠端的 server 上，但這些系統仍有許多缺失；雖然藉由資訊化與數位化的方式節省了許多人力與物力的花費，但這些影像資料在安全性上卻面臨了更大的挑戰，如何避免影像資料在網路傳送的過程中遭到惡意竄改，或是日後發生重大事故，需要監視影像作為佐證時，如何證明該資料即為原始影像，而非事後變造產生；再者這些系統皆屬線上作業，當網路通訊發生異常時亦缺乏一套穩固可靠的備援機制。

因此，一套數位化的監視系統必須面對網路通訊正常與否、人為的硬體設施破壞、監視影像是否遭到竄改，及監視影像來源正當性等問題。

有鑑於此，我們製作了一套線上與離線兩用的防竄改監視系統，透過系統隨機產生的 private key 對監視影像做數位簽章，並搭配系統中不易得知的唯一硬體序號，對系統記錄檔進行加密，確保監視影像之完整性與不可否認性；除此之外，本系統於網路通訊正常情形下，監視影像會透過網路傳送的方式，存放於遠端的儲存媒體上，當遇到網路通訊異常時，我們採用儲存容量大且廉價化之 USB Flash memory 做為備援的儲存媒體。目前市面上的 USB Flash memory 已經足以存放 50 分鐘以上的即時影像，且根據摩爾定律[5]的推論，未來這類小型固態儲存媒體的容量將以指數的方式持續成長。因此非常適合當成本系統之離線備援儲存媒體用。

本系統亦利用 Motion Detection[6]的機制，當偵測環境影像產生變化時才進行影像拍攝擷取的動作，如此可於網路通訊時降低網路流量，並節省影像儲存成本。

既有的嵌入式監視系統[1][2]使用 ARM[4]的硬體設備搭配 uClinux[9]系統，雖然使用此架構可縮小硬體系統的體積，降低電力消耗，但在整體執行效能上比較難以加入快速的影像簽章及檔案加密運算，而且也不容易使用大量現成之 Open Source 套件來加速開發時間。除此之外，在 USB 裝置的擴充性上仍嫌不足；因此，為了改善執行效能，增加實際使用的彈性，本系統採用 SPB-Linux[8]為基礎並將系統建置於 USB Flash memory 中，並於 VIA EPIA-SP[10]的 x86 硬體平台上執行，提升作業硬體環境的相容性與系統修改的便利性。

本論文將針對「系統架構與運作」、「防竄改與出處機制」與「線上及離線兩用功能」與三點來加強說明整個監視系統的製作方法，最後再針對本系統的成果作一個討論。

二、系統架構與運作

本系統是採用 Open Source 的 SPB-Linux 系統為基礎，並以 bash shell script 作為程式開發工具，利用 Web-cam 取得監視影像，透過 Open Source 的 Motion 套件轉換成 JPEG 格式後，以 OpenSSL[7] 執行影像的簽章，系統架構圖如圖 1 所示，硬體結構照片如圖 2 所示。系統硬體採用 VIA EPIA-SP 的主機板，CPU 為 VIA Eden 800MHz，256MB DDR，40MB ramdisk。

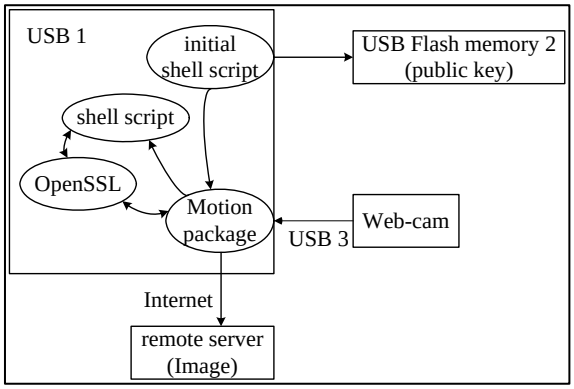

圖 1 系統架構圖

為了避免監視影像拍攝後遭人惡意竄改，系統開機時將會執行一支 shell script，檢查除了存放檔案系統之 USB Flash memory 外，是否另有其他 USB Flash memory 存在；若另有 USB Flash memory，則系統於產生金鑰後便將 public key 存於該 Flash memory 上，並於儲存完畢後發出提示音，告知使用者將存有 public key 之 Flash memory 拔除，置於較為安全的環境中妥善保存，避免遭人任意取得破壞，以作為日後監視影像驗證之用。而 private key 則儲存於 ramdisk 中，利用該揮發性記憶體之特性，當系統遭受破壞或電源消失重新啟動後，private key 便隨之消失，使得入侵者不易盜取系統中的 private key，開機流程如圖 3 所示。

系統完成開機程序後，利用 Motion 套件進行環境監視，當環境影像發生變化時便藉由 Web-cam 拍攝影像，透過 Motion 套件將影像轉為 JPEG 格式，呼叫 OpenSSL 程式對該監視影像做數位簽章；影像簽章完成後，利用 shell script 測試網路通訊狀態，進行資料檔案的儲存，影像監視與簽章流程如圖 4 所示。

為了使監視影像更具有法律效益，且證明該影像來源確實為本系統於特定時間拍攝所得，而非使用者私自產生一組 public 與 private key 自行簽章變造產生。本系統於對影像簽章時，同時利用 ramdisk 中的 private key 與硬體序號對系統開機時間、簽章時間與相關系統記錄進行加密儲存，以作為日後驗證檔案來源的依據。

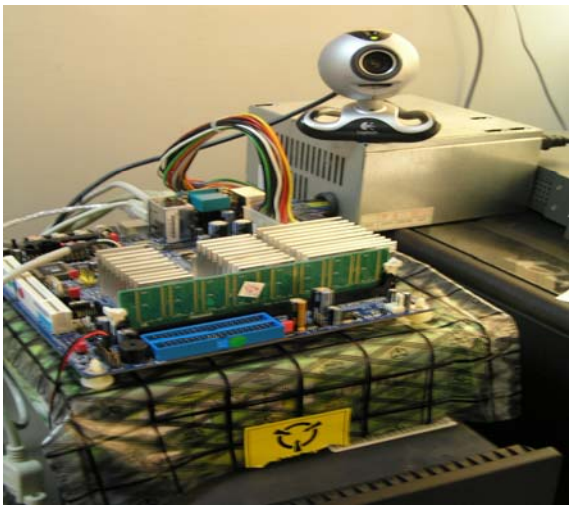

圖 2 硬體結構照片

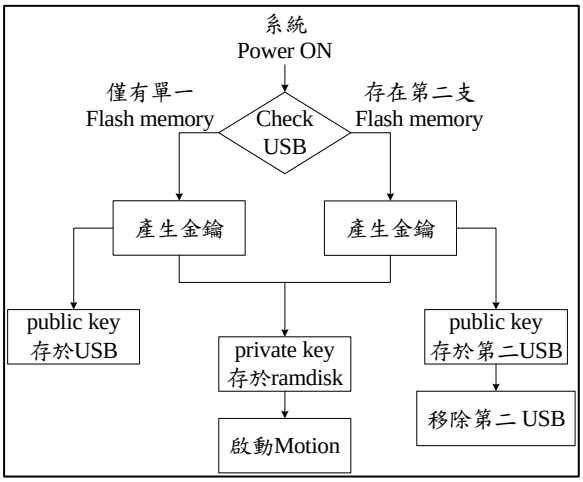

圖 3 系統開機啟動流程圖

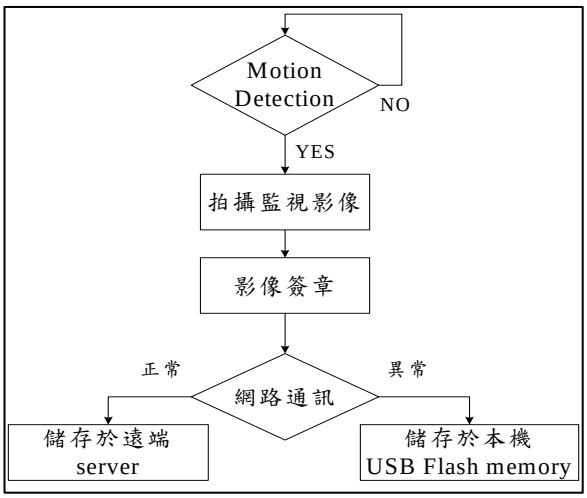

圖 4 監視影像取得與簽章

三、防竄改與出處驗證機制

在監視影像數位化後，為了讓影像檔案在遭人惡意變造後能便於察覺，且可驗證該監視影像出處避免偽造；當發生意外狀況時，證明監視影像來源的正當性，使影像檔案更具法律效用，作為佐證，本系統建立了一套防止竄改與影像出處驗證的機制。

本系統的防竄改機制是藉由使用 public key 的數位簽章演算法對每一張拍攝的影像作數位簽章完成。至於本系統之影像出處驗證機制，是透過使用 public key 加密法加上對稱式加密法來加密系統記錄檔完成，示意圖如圖 5 所示。當 Web-cam 取得之監視影像時，系統使用 ramdisk 中的 private key 對監視影像做數位簽章；在影像出處驗證機制部份，我們採用具唯一性且不易取得之硬體序號先對系統記錄檔進行 AES 加密，再使用 private key 對 AES 加密後之檔案以 RSA 演算法重新加密一次，如圖 6 所示。

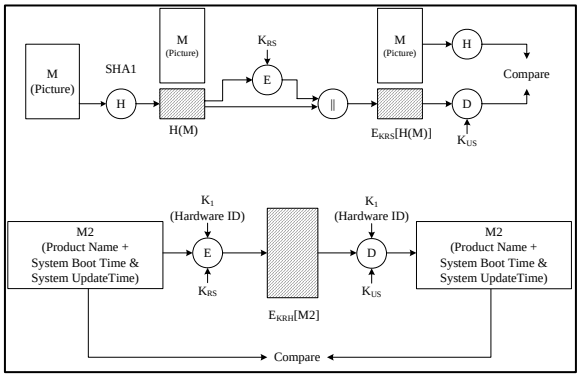

圖 5 防竄改與影像驗證機制示意圖

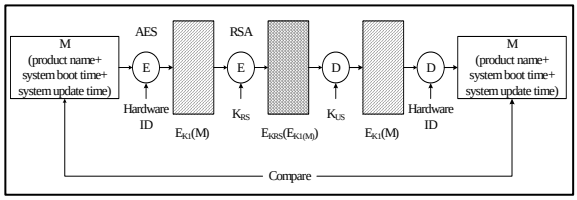

圖 6 影像出處驗證機制加密示意圖

在本機制中，由於系統每次開機所產生之 private key 儲存於 ramdisk 中，當系統斷電、關機或重新開機後，該 private key 便隨之消失，使得這個 private key 不易被入侵者取得；除此之外，我們於系統開發完成後便將所有不必要之帳號移除，並將帳號設定為無法登入，避免因為系統中帳號密碼遭盜用或破解，造成入侵者成功進入系統中，竊取 private key 偽造簽章影像。因此日後只要藉由預先儲存之 public key 進行數位簽章驗證，便可檢驗影像檔案是否遭到竄改。

上述之防竄改機制能夠讓系統的擁有者檢驗監視器所拍攝的影像是否被入侵者竄改過，但無法證明系統的擁有者是否自行竄改監視器所拍攝的影像。因為系統擁有者只要自行產生一組金鑰，對偽造或竄改過之影像進行簽章，辯稱其監視影像為系統拍攝所得，就無法用 public key 數位簽章的方式加以驗證。

為了解決影像出處驗證的問題，我們引進了硬體序號（必須是使用者無法輕易取得的硬體序號）當對稱式加密法的 key，加密一個記錄系統開機與運作時間等的系統檔案，再用 private key 做進一步的加密以增加破解的困難度。這樣惟有系統原始產生之 public key 搭配硬體序號才可將記錄檔解密還原，藉此檢驗金鑰來源是否為拍攝影像之監視系統產生，以達成影像出處驗證之功能。且因為該檔案記錄了系統的開機與運作時間等資料，可以提供該監視影像更多的可信的佐證資訊。

四、線上及離線兩用功能

目前的網路監視系統皆採線上作業，將拍攝得之監視影像透過網路傳送至遠端 server 上儲存，但若網路通訊發生異常時，則欠缺一套備援機制，將造成監視影像遺失。

本系統為了改善此一缺點，建立了一套較為妥善的備援機制；當網路運作正常時，我們利用 Linux 的網路檔案系統（Samba 或 NFS）機制將遠端伺服器的儲存空間 mount 上本系統，作為影像檔案的主要儲存媒體。

當 Motion 套件偵測到環境變化，便透過 Web-cam 進行影像拍攝並轉換成 JPEG 格式檔案暫存於本機 ramdisk 中，藉由 Motion 的控制檔於影像檔案儲存後，直接呼叫一支 shell script 程式先對該監視影像進行簽章，並於簽章完成後檢查網路檔案系統的狀態。當網路檔案系統正常時，系統便將 Web-cam 拍攝所得之監視影像及簽章後的檔案透過網路傳送至遠端 server 存放，防止監視影像因儲存於本機上而直接遭人盜取或破壞；若網路檔案系統異常時，該 shell script 就做即時的調整，將影像及簽章後的檔案儲存於本機的 USB Flash memory 中，待網路檔案系統恢復正常後，亦將原先存於本機之檔案備存於遠端 server 上。且由於本系統在影像儲存部份是與 Motion 套件的影像寫入機制整合，並採用檔案複製暫存的方式製作，故於通訊異常時不會造成影像遺失的現象，使監視系統能順應環境變化，達到線上與離線兩用的功能，增加系統應用之彈性。

目前每張 640×480 的 JPEG 監視影像大約是 24300Bytes，系統本機採用現今普及的 1GB USB Flash memory，扣除安裝 SPB-Linux 及存放相關程式所花費空間，約可存放 3 萬張監視影像，若以

10 frame/sec 計算，可持續拍攝 50 分鐘；本系統採用 Motion Detection 的機制，當環境影像出現變化時才進行影像拍攝，除了可以減少網路傳輸流量外，並可有效節省儲存媒體空間，當環境變動頻率較低時，在有限的儲存媒體下，可獲得較長的拍攝時間。

五、比較與討論

相較於現有的監視系統，本系統提供了一套防竄改的機制，透過影像的數位簽章，可快速檢驗監視影像是否遭到不法竄改；當事故發生，需要以監視影像作為法律上的佐證時，藉由本系統的影像出處驗證機制，可驗證監視影像的來源，確保資料檔案的完整性與不可否認性，並且可以獲得拍攝時間之確切紀錄。在影像的儲存方面，除了利用網路傳輸將檔案存於遠端儲存設備，避免檔案在本機上有直接遭受竊取及破壞的危機外，本系統亦建立了一套可靠的備援機制，於網路通訊異常時快速切換檔案儲存路徑，將監視影像改以存放於本機的 USB Flash memory 中，使監視影像不至於因網路傳輸異常而有所遺失或損毀，具備線上與離線兩用之功能。在影像拍攝方面，應用 Motion 套件提供之 Motion Detection 功能，當偵測環境影像變動時才進行影像的拍攝，除了可以降低網路傳輸流量外，在儲存媒體有限的情形下，可儲存更長時間之監視影像檔案，節省購買儲存媒體的花費。

有別於現存的嵌入式監視系統，以 uClinux 系統為基礎，於 ARM 的硬體平台上執行，本系統軟體採用 Open Source 的 SPB-Linux 為基礎，並以 bash shell script 為程式開發工具，於 VIA EPIA-SP 嵌入式的硬體平台上執行；相較於本系統，雖然使用 ARM 的硬體平台可縮小系統硬體體積且更加省電，但在整體系統開發建置過程中需要花費更長的時間，日後進行系統修改維護時亦較為不易且費時；在硬體擴充性、硬體發展速度與未來系統發展趨勢上，x86 皆較 ARM 的硬體平台佔有較大的優勢；在電力消耗方面，目前 x86 系統的主流硬體廠商已經投入相當資源持續研發[3]，因此電力消耗問題在日後將可獲得改善，使本系統可以隨著 x86 硬體系統的進步邁向省電與小型化。

由於目前的嵌入式 Linux 系統大量運用了壓縮技術以節省儲存空間，但也因此延長了開機的時間。由於本系統為了離線儲存影像，使用了較大的 USB Flash memory，足以搭載不經壓縮的系統程式。因此我們為了加快系統開機啟動速度，將嵌入式 Linux 作業系統所在的 USB Flash memory 切割成兩個分割區，一個分割區僅存放作業系統及系統運作所需的程式，另一分割區則用來存放監視影像檔案，減少開機時檔案的搜尋讀取時間。經過這樣的處理，整個系統開機的時間可以由大約 300 秒鐘縮短到 140 秒鐘。

本論文在驗證實作影像出處驗證機制過程中，對系統記錄檔加密所使用之硬體序號初步是採用網路卡 MAC 位址進行測試。但由於網路卡 MAC 位址容易被取得，日後應與硬體生產廠商合作，實際使用具唯一性且不易取得之硬體序號做為加密金鑰，提高資料安全性。

本系統是以監視系統作為實作標的，事實上類似的機制也非常適合用於數位相機的防竄改與出處驗證。唯數位相機的應用與監視設備不同，出處驗證之需求大於防竄改之需求。在硬體架構上如果要做到防竄改機制，則數位相機必須多設置一個低容量之記憶卡，將會增加成本，並且大幅修改目前的硬體結構。退而求其次則可以把 public key 存放在放置數位影像的記憶卡中以節省成本。出處驗證功能較容易整合進入目前的數位相機中，只要在記憶卡上多記錄加密過的系統時間資訊即可。然而相機內的 DSP 晶片就必須多負擔加密與簽章的運算量。

本系統除可作為監視系統外，利用其離線運作之特性，改用更省電之系統，搭載高蓄電量電池或太陽能電源供應設備，提供長效電源系統，亦可應用於生態保育上，減少人為活動所造成的干擾，作為野外生態觀測之用。

六、結論

我們完成一套可供線上與離線兩用之嵌入式防竄改監視系統，該系統使用 Open Source 的 SPB-Linux 與其他免費軟體套件為基礎，於 x86 之硬體平台執行，以廉價的 Web-cam 配合 Open Source 的 Motion 套件取得監視影像，並利用 shell script 為開發工具製作完成。本系統除可用於一般日常生活安全監視外，亦可應用於危險環境監控或野外生態觀測之用。

七、參考文獻

[1] 林昌廣,「嵌入式網路監視系統」, 國立交通大學電機與控制工程學系, 碩士論文, July 2002.

[2] 黃文增、陳盛琳、陳首元、吳賀瓏,「嵌入式 DHCP 網路監視系統研究與實作」,台北科技大學學報第三十八之一期, pp.69-80.

[3] AMD Embedded CPU http://taiwan.cnet.com/news/ce/0,2000062982,20099536,00.htm

[4] 「ARM」 http://www.arm.com/markets/embedded_solutions/index.html

[5] 「Moore's Law」 http://www.intel.com/museum/archives/history_docs/mooreslaw.htm

[6] 「Motion」 http://www.lavrsen.dk/twiki/bin/view/Motion/WebHome

[7] 「OpenSSL」, http://www.openssl.org/

[8] 「SPB-Linux」, http://spblinux.sourceforge.net/

[9] 「uClinux」, http://www.uclinux.org/

[10] VIA EPIA-SP http://www.viaembedded.com/product/epia_sp_spec.jsp?motherboardId=261