# Adding Security to Removable Mass Storage

# 為移除式高容量儲存裝置加入保密防護

***作者: Cypress Semiconductor 公司***

***消費性產品與運算部門應用工程師 Mark Schultz***

## *Executive Summary*

As portable media proliferates into more and more consumer products, data security is becoming increasingly important. New products need to be secure in order to protect confidential information from theft.

Biometric security offers an economical solution that doesn't add significant user burdens such as extra passwords or additional log-in steps. Biometric security methods include fingerprint sensing, retina and iris scanning, signature analysis and hand geometry. Consider the case of fingerprint sensing. With a simple swipe of a finger, a user can authenticate himself to gain access to data on a portable storage device.

This article will provide a simple, step by step design sequence to add fingerprint security to a USB mass storage device.

## *介紹*

隨著可攜式媒體在消費性產品中的應用激增，資料儲存的安全性也就變得更加重要。新產品必須具備保密防護功能，防止機密資訊遭到竊取。

生物辨識（biometric）保密功能即為一項經濟實惠的解決方案，它不會為使用者在操作和使用上帶來困擾，例如不需要特別的密碼或額外的登錄步驟。生物辨識保密功能包括指紋感測、視網膜與虹膜掃瞄、簽名筆跡分析、以及掌紋辨識等。以指紋感測為例，使用者只需簡單的手指印模就可以完成使用者認證，取得可攜式儲存裝置中的資料。

本文將針對 USB 高容量儲存（mass storage）裝置上的指紋保密功能，簡單說明設計程序的各個步驟。

### *身份辨識與保密關鍵*

身份辨識的方法眾多，從密碼的使用、辨識裝置（dongle）到生物辨識都有。今天大家會發現做甚麼事情都需要密碼，而為了記住密碼，往往又將密碼記在某個地方，以保密的角度而言，這種作法無疑是違背了保密的原意。保密辨識裝置的製造成本偏高，而且容易產生辨識誤差的情況。然而，生物辨識應用則不用密碼，僅需要較便宜的簡單硬體，且指紋這種特徵是永遠不會遺失的。

有許多方法可以防止未經認證使用者對資料之存取以保護資料的安全，這些方法包括加密（encryption）、磁碟管理（drive manipulation）或其他方式。加密可分為軟體與硬體兩種方式。硬體加密會增加成本，也會讓產品的尺寸變大；而軟體加密則會在使用容量大的磁碟時速度變得較慢。磁碟管理的作法是鎖定磁碟中的硬體來防止未經認證之使用者對資料進行存取。現在新式的硬碟具備的 ATA Security 即為其中一種鎖定的機制，這種設計中有一組 32 位元的密碼傳送到磁碟電路中，讓磁碟進入「安全」模式。當系統開機後，磁碟就會處於鎖定狀態，一直到輸入正確密碼後，鎖定狀態才會被解除。由於只有磁碟內的微處理器知道密碼，因此該磁碟機如果裝在未受保護的系統則無法被讀取。

### *感測器類型*

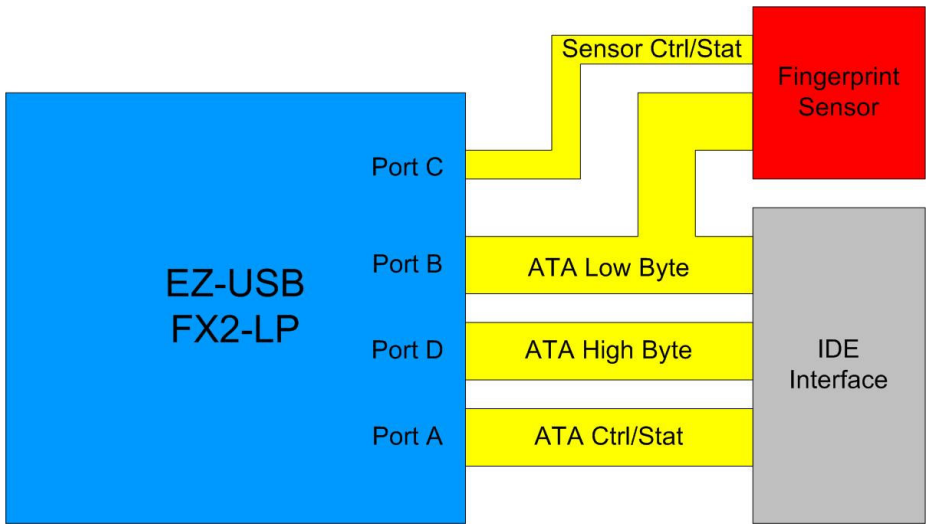
感測器的類型會因不同的資料和 USB 傳輸方式不同而有所差異。有些感測器解決方案需要在個人電腦上進行影像處理，而有些解決方案則運用協同處理器（co-processor）來處理影像資料。不同的感測器也會採用不同的 USB 介面將資料回傳至電腦中；這些介面包括印表機群組、大量儲存裝置群組、以及人機介面裝置群組。這三個介面各有優缺點，但它們共通的好處是僅需 Windows 本身的驅動程式即可，不必另外安裝。

就硬體而言，其介面從 SPI 到並列式匯流排（Parallel bus）等許多種類，而介面的種類和速度則與影像處理的方法有關。內建協同處理器的感測器僅需每秒數百 Kb (kilobits per second)的速度，若是運用 PC 來處理影像的感測器則需高達每秒 6.5Mb（Megabit per second）的傳輸速率。這裡提到的感測器可支援 SPI 或是並列式匯流排等不同的介面。

## *系統需求*

移除式儲存裝置一般會包含 2.5 吋或更小的硬碟、磁碟機外殼、電源供應器、以及一組 USB 對 ATA 的轉接器。這種組合的解決方案可以作高度模組化的設計，因此要外加一個指紋感測器並非難事。這部分會在下文作介紹。這項設計所用的 USB 對 ATA 轉接器就是 Cypress EZ-USB FX2-LP。在下一節中將詳細介紹 Authentec AEES2510 外接裝置，這是一組滑動式的指紋感測器，可外接於既有的 USB 高容量儲存裝置上。AES2510 並不具備協同處理器，因此它與 USB 控制器之間的介面需支援每秒 6.5MB 資料傳輸速率，讓手指在按壓感測器時所產生的資料能用同樣速率傳送。由於 FX2-LP 支援與 UDMA-100 相同的傳送速率，因此感測資料傳輸不是問題。此外，由於影像處理是由 PC 完成，因此很多時候 USB 控制器需要在 ATA 與指紋感測器介面之間來回地作快速的切換。這項功能可藉由修改 FX2-LP 的介面就能夠輕易達成。下圖為 USB 對 ATA 轉接器與附加的指紋感測器之區塊圖。

**圖 1: USB 對 ATA 轉接器與附加的指紋感測器之區塊圖**




## *裝置實作*

針對這個設計，感測器介面上會加上一組運用 Cypress EZ-USB FX2-LP 的標準 USB 對 ATA 轉接器參考設計。而 FX2-LP 包含一個 USB 2.0 序列式介面引擎（Serial Interface Engine，SIE）、一個增強型 8051 微處理器、以及一組通用型介面（General Purpose Interface，GPIF）。其中 GPIF 是一個狀態控制器（state-machine）架構的介面，其資料傳輸速率可高達每秒 96 MB。GPIF 可支援 ATA、NAND、Utopia、EPP、以及 Compact Flash 等各種介面。由於 GPIF 是一個以 RAM 為

基礎的狀態控制器，因此多重控制波形之組合都能進行裡外複製作業，讓 GPIF 可透過韌體的控制成為可重組式（reconfigurable）的介面。由於 GPIF 直接與 FX2-LP 的 USB FIFOs 相連接，因此不需要透過韌體在感測器資料流上作任何資料處理作業。

在這個設計中，GPIF 波形會包含 PIO 讀取與寫入及 ATA 介面所用的 UDMA 讀取與寫入。本設計中也會加入讀取與寫入指紋感測器所用的波形。控制硬碟的韌體則來自於 CY4611 高容量儲存參考設計。至於指紋感測器所用的韌體則是參照感測器製造商所提供的程式碼。

AES2510 可選擇 SPI 或並列式匯流排的介面。由於我們現有的硬體已經採用並列式介面，因此我們選擇支援並列式介面的 AES2510。I/O 的需求包括一組 8 位元的資料匯流排，加上六個控制—RD、WR、CS、A0、INT，以及 PWR_CTRL。如果我們小心設定晶片指定的感測器與 ATA 匯流排的輸入時，就可以共用 ATA 匯流排中較低的位元組作為資料傳輸之用途。另外，我們還可以利用 FX2-LP 的 Port C 作為控制與狀態方面的用途。

感測器與應用軟體之間的通訊是透過 SCSI Pass Thru 介面達成，這是一個 Windows 高容量儲存驅動程式（Windows Mass Storage Driver）的延伸軟體。藉由 SCSI Pass Thru，感測器就可以使用一般高容量儲存裝置所用的 USB 介面，因此裝置不需要額外的驅動程式。

當感測器接收到 Pass Thru 的指令時，感測器程式庫（sensor library）中的韌體就會進行指令作業。韌體首先會覆寫 GPIF 波形記憶體，用感測器波形取代 ATA 波形。接著韌體就會依照 Pass Thru 的指令動作，執行對感測器的讀取與寫入作業。當 Pass Thru 指令週期完成時，ATA 波形則又會被複製回 GPIF 記憶體中。

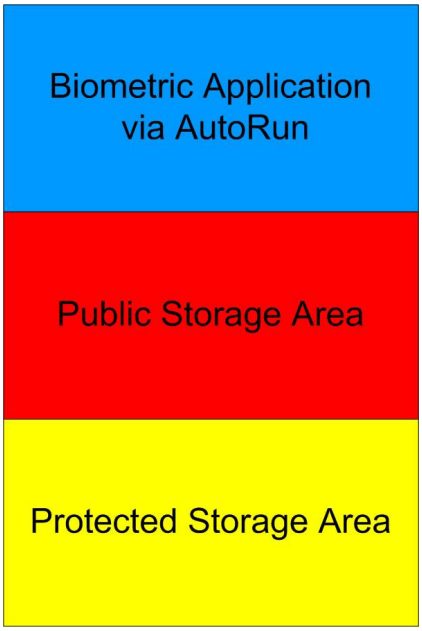
### *使用者介面*

典型具備保密功能的磁碟會包含三個分割區，其中一個有生物辨識應用軟體。這個分割區通常會模擬成 CD-ROM，其原因有二：

- 在 Windows 環境中，CD-ROM 比磁碟機有更好的自動執行（AutoRun）反應
- CD-ROM 具備防寫入保護，因此生物辨識應用軟體不會被意外刪除

另外兩個分割區中的一個是用作非保密性的儲存區。使用者可以任意存取裡面的資料。最後一個分割區中的資料則會受到保護。若一開始沒有透過指紋確認其擁有權，就無法存取其中的資料。

**圖 2：磁碟分割區結構圖**




當磁碟機啟動時，生物辨識應用程式就會從模擬成 CD-ROM 的分割區中自動執行。該應用程式接著會處理經由 Pass Thru 介面傳入的指紋影像資料，進行使用者登錄與確認的動作。其中確認的動作是根據使用者按壓指紋印與原指紋影像紀錄的比對。一旦使用者身份經確認後，保密的磁區就會被「解鎖」，使用者就可以取得其中的資料。若該磁碟的 USB 連線中斷或電源中斷時，該使用者就無法繼續從這個保護磁區中存取資料。

## *總結*

本文描述了 USB 高容量儲存裝置上附加的生物辨識保密防護設計。Cypress EZ-USB FX2-LP 的彈性化特質與可設定式的介面連接埠，讓這個設計的建置作業更加容易。也由於 FX2-LP 的高度彈性，因此要新增生物辨識功能也變得極其簡單。再加上一些專利設計的韌體，就能夠實現完整的磁碟機資料安全保護。

而另外加入生物辨識功能的元件成本不到七美元。至於針對其他儲存媒體，例如專為 NAND-Flash 而設的解決方案，目前正在開發中。

欲知 Cypress EZ-USB FX2-LP 的相關資訊，請瀏覽 www.cypress.com 網站；而有關 AES2510 指紋感測器的相關資訊，請瀏覽 www.authentec.com 網站。

Cypress Semiconductor
198 Champion Court
San Jose, CA 95134-1709
Phone: 408-943-2600
Fax: 408-943-4730
http://www.cypress.com