多重伺服器之三因子身分鑑別協定

許建隆[1,2] 陳志清[1] 黃美涓[2] 劉卜誠[3]

[1]長庚大學資訊管理學系
長庚大學健康老化中心
[2]長庚醫院
[3]長庚大學企業管理研究所資管組

摘要

身分鑑別在任何系統的作業流程內都是一個相當重要的關鍵，執行流程內的任何步驟都一定要經過身分的鑑別確認是否為合法的使用者，是一個相當重要的門檻，尤其在現今網際網路的發展使資訊傳遞非常迅速，應用個人電腦及通訊網路為基礎的伺服器系統，不受時空的限制，是最具經濟效益的方法之一。傳統身分鑑別協定是應用個人識別名稱及通行碼鑑別合法使用者的身分，但通行碼太複雜會讓使用者難以記憶，太簡單則可能遭受字典攻擊，且易受到重送攻擊。對於傳統身分鑑別協定所面臨的資訊安全問題，有許多相關學者進行相關研究，應用三因子（智慧卡、生物特徵、通行碼）的身分鑑別協定是其中之一，但大部分的三因子身分鑑別協定並未真正在伺服器驗證使用者的生物特徵。 本文提出一個新架構具三因子與金鑰協議的身分鑑別協定，可以達成減輕阻絕服務攻擊、防止伺服器假冒的問題、有生物特徵擷取容錯性並建立金鑰協議。此外在現階段使用者有多台伺服器協議，對於使用者如何管理多台伺服器的通行碼，本文提出一個具三因子的多重伺服器身分鑑別的協定，用於使用者在多台伺服器身分鑑別，使用者可以選擇一台以上的伺服器具有相同通行碼，但針對每台的伺服器驗證到的是不同的通行碼及生物特徵，可以幫助使用者管理多台伺服器的通行碼。

關鍵詞：生物特徵、智慧卡、身分鑑別、多重伺服、通行碼

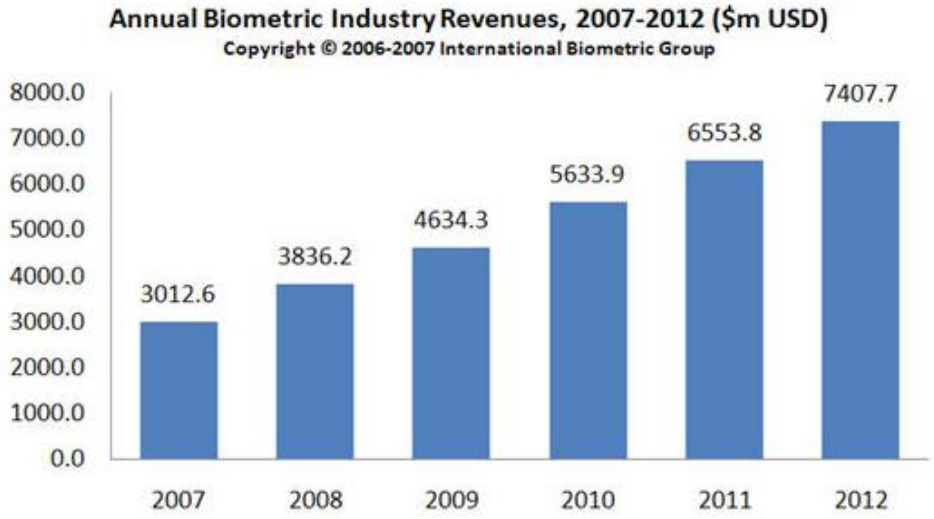
壹、前言

資訊科技發達的現今，在大街小巷常常可以看到人們手中拿著手機、PDA ，背著筆記型電腦，此一光景在繁忙的都市中更為常見。資訊科技改變社會的結構，使資訊傳遞訊息越來越快速，訊息可以在短時間內傳遞到世界，而要防止訊息被不相關的人士收到或是擷取，就需要保密的技術，可以得知資訊的安全是越來越重要。

身分鑑別是資訊安全領域中應用最廣的一門科技，在商業上、國防中，要使用任何資訊系統幾乎都需經過使用者的身分鑑別，而現今使用最廣的為傳統的通行碼認證技術，其亂數選取的通行碼不易被記憶，使用者自定的通行碼又可能受到字典攻擊法攻擊。故而有許多學者提出相關改良，其中生物特徵識別技術作為身分鑑別已經有實際應用的

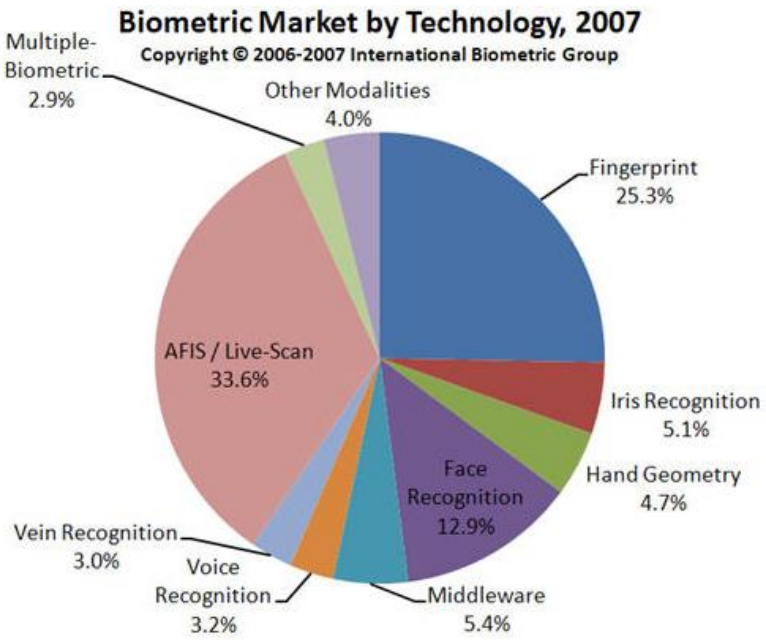
成熟商品存在。擁有使用者個人之特質的生物特徵資訊具有獨特性及不變性：獨特性能夠成為辨識使用者身分的依據，不變性則能夠提供不可否認性，且不會被遺忘、不需記憶、隨者使用者而移動，具有潛力能夠取代或是輔助傳統的通行碼，藉以提供更高的安全性，非常適合作為身分鑑別的依據。

美國麻省理工學院（Massachusetts Institute of Technology, MIT）將「生物鑑定科學」（Biometrics），視為最具有發展潛力的十大科技之一，在未來生物特徵的應用越來越廣泛（圖一）。



圖一：生物辨識技術收入統計圖[12]

生物特徵則分為兩類：生理上的特徵和行為上的特徵。生理上的特徵有虹膜、聲紋、指紋、掌紋、臉型、掌型、靜脈、體型及DNA等，行為上的特徵則有手寫簽名和語音模式 （圖二） 。



圖二：生物辨識技術使用統計圖[12]

美國911事件發生後，為防止恐怖攻擊，2002年「美國強化邊境安全及簽證改革法」，要求入境美國不需簽證的國家必須把該國國民護照改為具有生物特徵功能，可被生物特徵擷取裝置所讀取的護照，否則需求改為簽證才可入境，並且美國還施加影響力於國際民航組織（ICAO），研擬包含生物特徵資訊的新護照要求，目前香港、英國、德國、奧地利、我國等都即將啟用「電子生物護照」（圖三），國際民航組織所規畫的「電子生物護照」，包含無線射頻識別系統（RFID）、生物辨識系統（Biometrics）、公鑰架構（PKI）三大功能。

圖三：電子生物護照[14]

可以預期的生物特徵護照將在未來取代所有一般護照，生物特徵可說是目前最安全的護照，生物特徵更是被形容為隨時攜帶的身分證，在未來人口管理、民生交易、門禁防盜等等都會利用到生物特徵，所以生物特徵的安全應用方案是未來的一種趨勢。

同時，除了國境管理層面的運用之外，許多國家也計畫甚至已經將生物特徵辨識技術與傳統的辨識國民身分的方式結合，也就是將生物特徵資訊納入國民身分證明文件之中，將生物特徵資訊應用於國民身分的辨識。

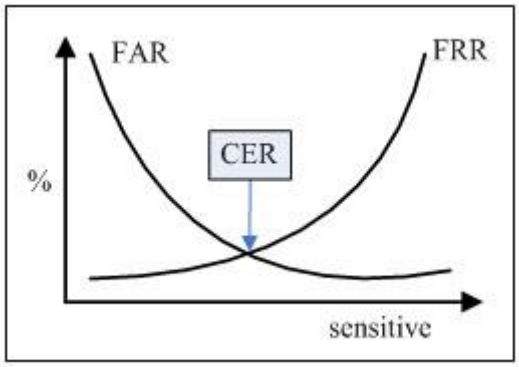
生物特徵應用在身分鑑別上目前有許多相關學者在探討，生物特徵的獨特性及不變性可以加強以往通行碼忘記、通行碼的安全性不足等眾多會影響系統安全的弱點，改進認證的安全性，且針對單一特徵易被取得及外洩的問題，已經有商品發展到多特徵認證，以提高單一特徵外洩的安全性，目前來說多特徵認證有指紋加簽名、靜脈加指紋等等的相關研究或應用，可說包含生物特徵的驗證已經有取代傳統的通行碼為基礎的身分鑑定。

本文將介紹生物特徵辨識技術於多重伺服器環境底下的身分鑑別協定，內容安排如下：第二節中簡介生物特徵及其相關應用科技；第三節中說明多重伺服器之三因子身分鑑別協定演算法之設計；第四節將評估演算法的效率與安全性之分析；第五節展示實作成果截圖；最後第六節則針對討論的內容作結論。

貳、生物特徵

生物特徵技術[16]可分為生理上的特徵和行為上的特徵，但其量測相關估計值有FTE（Failure to enroll）、FAR （False Acceptance Rate）、FRR （False Rejected Rate）、CER

（Crossover Error Rate）等四類，用以導入聖物特徵技術時使用者接受度、安全性之考量，圖四說明CER的環境參考值及各估計值的相關性。



圖四：CER示意圖[14]

2.1 指紋

基本上每個人的指紋及手指頭的紋路都不同，要找到相同的指紋機率約為十億分之一，從嬰幼兒到死亡指紋的紋路及結構幾乎不會改變，而指紋辨識技術[14]是將個人指紋先行採樣，並擷取其中重要的特徵作為特徵值，再比對特徵值以鑑別身分，而指紋特徵值只有250位元組到1K 位元組，指紋辨識技術的穩定性高及設備價格低廉，使指紋辨識系統成為目前最受歡迎的設備。

指紋識別技術主要分為四個功能：讀取指紋圖形、提取特徵值、保存特徵值及比對特徵值，以下將分別說明此四功能。

（1）讀取指紋圖形

經由指紋讀取裝置讀取指紋的圖形，取得圖形後進行初步 處理，使圖像更清晰。

（2）提取特徵值

從指紋圖形上找到指紋紋路的分叉、終止或打圈處的坐標位置，這些點同時具有七種以上的唯一性特徵被稱為節點（minutiae），節點類型通常有：脊斷點、分岔點、交叉點、孤立點、環點、島形區域、孔等（圖五），指紋上平均具有70個節點，大約會產生490個特徵數據。

（3）保存特徵值

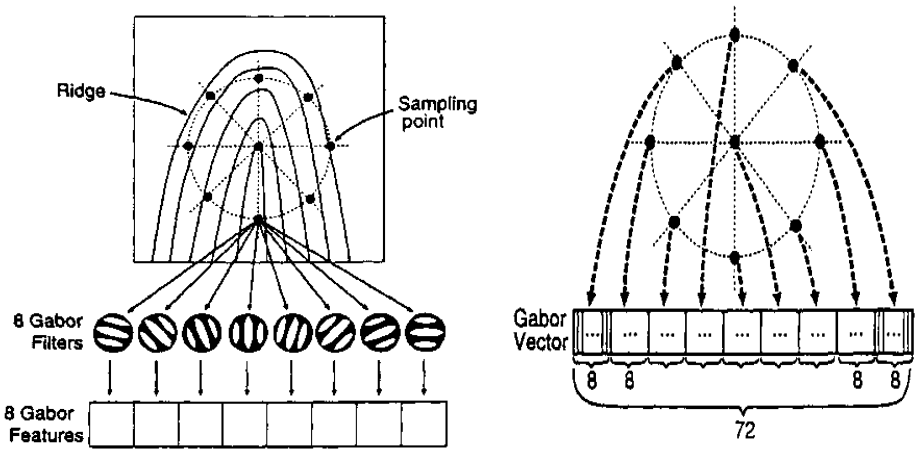
將取得之特徵值妥善存放於安全的存取裝置之中，以利比對。

（4）比對特徵值

Gabor 特徵比對法基於Yamada [5]的方法上，先找出二指紋的核心點作為圓心，以相同半徑的圓周上等分找出八個取樣點（圖六（a）），將此八個取樣點跟Gabor設計的八個影像濾波器運算後得到八個特徵值，將此八個特徵值及各取樣點上的七十二個特徵值，組合成指紋的特徵（圖六（b）），二指紋特徵進行比對，比對的差異小於一個門檻值t，則二指紋為同一人的指紋。

細微特徵種類	紋線形狀
點(dot)	
端點(ending)	
分叉點(bifurcation)	
島(island)	
刺(spur)	
交叉(crossover)	
橋(bridge)	
短脊脈(short ridge)	

圖五：節點的類型[14]



（a） （b）

圖六：(a）被抽取出的Gabor特徵值（b） Gabor向量的抽取法[5]

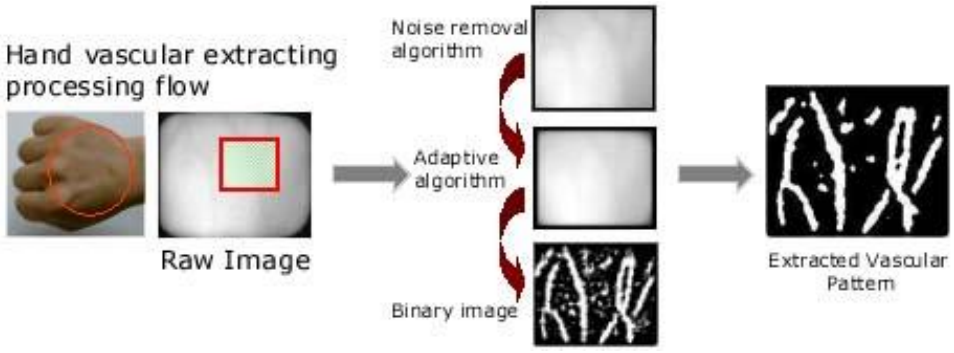
2.2 靜脈（Palm Vein）

靜脈識別系統[12]分為掌靜脈跟指靜脈跟手掌靜脈三種系統（圖七），其原理是應用靜脈內紅血球中的血紅蛋白可以充分吸收紅外光，突出靜脈圖像，而弱化手指肌肉和骨骼及手指的其他部分，從而得到人體的靜脈血管圖。

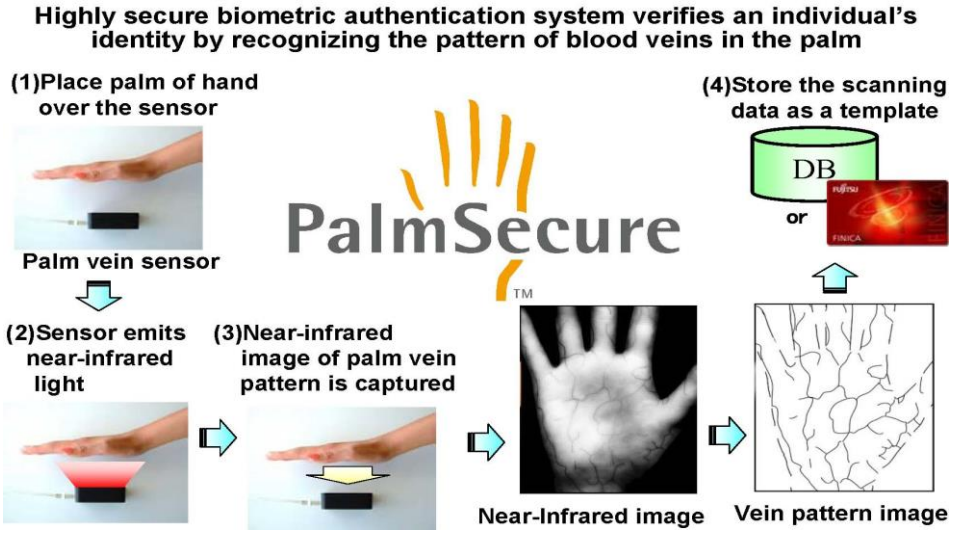
靜脈識別系統就是首先通過靜脈識別儀取得個人靜脈分佈圖，從靜脈分佈圖依據專用比對算法提取特徵值，通過紅外線影像裝置獲取靜脈的圖形，運用濾波、圖像二值化、細化手段對擷取靜脈的特徵，全過程採用非接觸式（圖八、圖九、圖十），僅需0.04秒即

能辨識使用者，FAR0.00008%及FRR0.1%，誤判率極低，可適用於99.98%可用性，比指紋辨識系統有3%成人無法使用，擁有更高的可靠性。

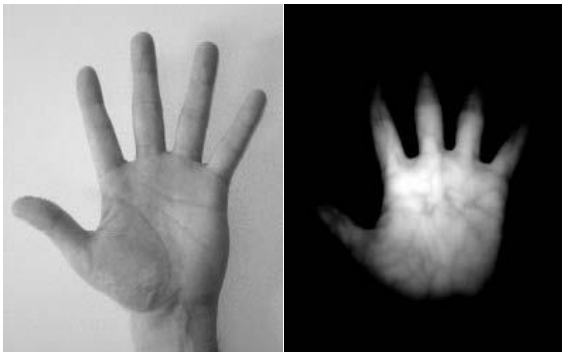
圖七：靜脈類型比較[12]



圖八：手掌靜脈特徵擷取示意圖[12]



圖九：掌靜脈系統架構圖[12]



圖十： （a） 可見的射線圖像圖 （b） 紅外線圖像圖

2.3 掌形（Hand geometry）

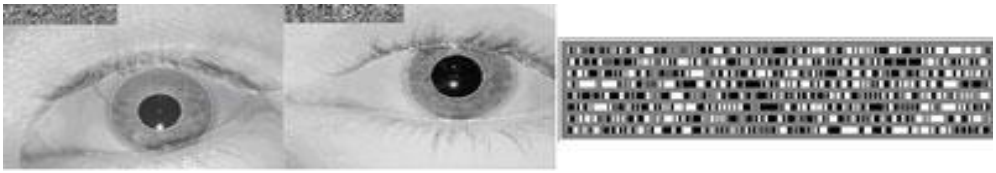
掌形辨識技術是利用每個人的手掌形狀彼此不同，來進行辨識，利用影像裝置，擷取手掌的形狀及特徵，來鑑別身分，有些掌型辨識系統只紀錄中指及食指的形狀及特徵，因此特徵檔案很小幾乎低於100 個位元組。

2.4 虹膜 （Iris）

虹膜[16]位於眼球角膜與水晶體之間，每個虹膜都是獨一無二的構造，虹膜基於像冠、水晶體、細絲、斑點、結構、凹點、射線、皺紋和條紋等特徵，虹膜辨識是利用每個人的虹膜特徵都是獨一無二的特性、不會發生變化，且不像指紋容易因為受傷或污染而無法辨識，因此漸漸被用來做身分辨識（圖十一）。

虹膜辨識系統採用非接觸式，利用影像裝置當虹膜開始聚焦開始採集虹膜影像，再將虹膜影像轉換成一個512個字節的虹膜特徵值。

虹膜辨識算法用3、4個字節的數據來代表每平方毫米的虹膜訊息，虹膜特徵值約有266個特徵點，而一般的生物辨識技術只有13到60個特徵點，因此虹膜識別技術有較高的辨識準確度，但虹膜辨識系統需要有較好的光源才能取得較好的虹膜影像。



圖十一：虹膜圖案[14]

2.5 人臉 （Face）

人臉辨識技術是目前各辨識技術中不需要特殊裝置，只要有一個高解析度的影像攝影裝置即可使用。人臉辨識技術注重於影像處理為基礎的演算法作為辨識準確度的依

據。人辨識系統的演算法主要分為，由統計測量方法取得由臉部特徵向量集合為臉部型態的相關特徵和關係；另一種方法是以樣版為基礎，當結構預知，可變形樣版對找出臉部特徵型態是一種有效技術。

由本文以上所述可以大約了解各辨識系統的操作原理，且可以由圖三中看出，因為指紋辨識系統的構造便宜及攜帶方便，是目前來說最廣泛應用的生物辨識系統。但指紋辨識系統其在靜脈辨識系統中可看到有3%的人員無法使用且指紋容易在任何地方遺留是其一大缺點，在安全性上可說有很大不足之處。

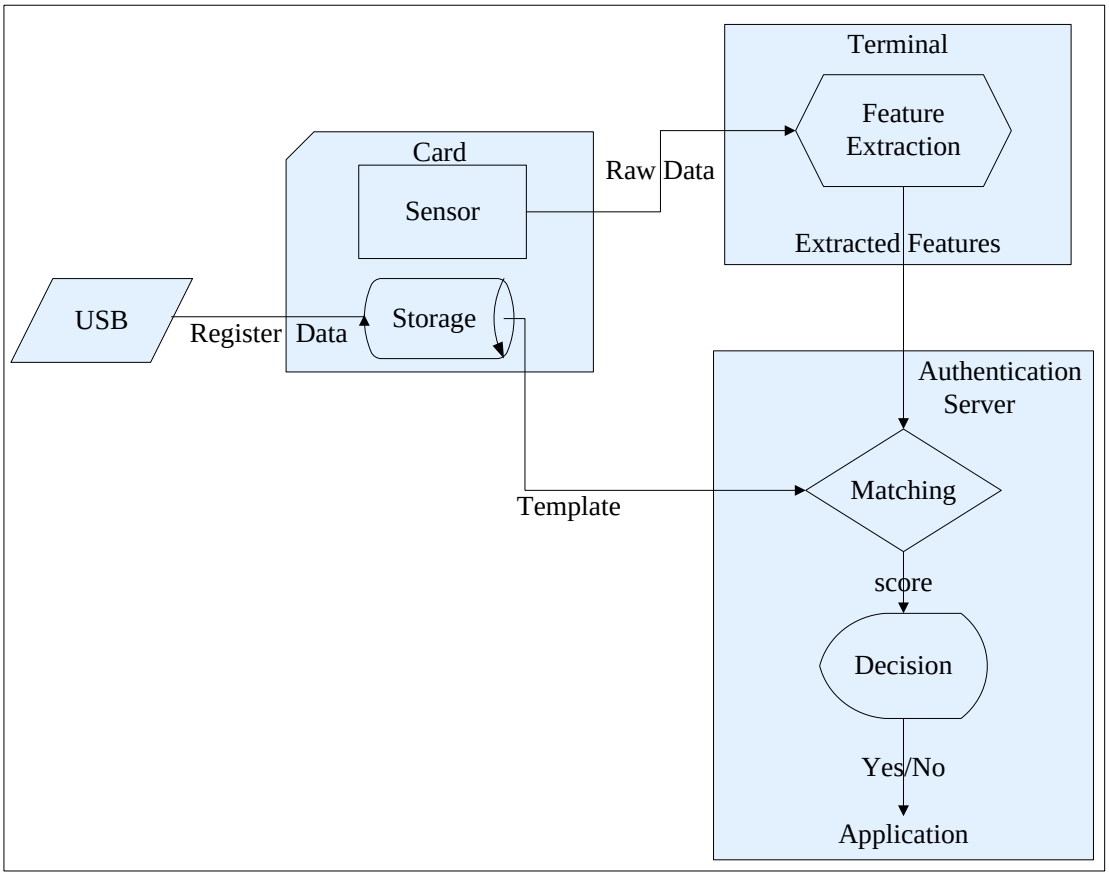
在圖三中可以看出人臉辨識系統也佔有很大區塊，目前在美國海關中所利用的辨識系統即為人臉辨識系統，其優點在於設備取得容易且不需接觸使用者。主要安全性基於其所應用的圖像演算法，但如果使用者透過整容或是臉部受傷會影響系統安全性。在本文中所述的辨識系統中唯有靜脈辨識系統是偵測人體內部的靜脈分佈，其最不容易被取得，變化性最小，是本文較推崇的生物特徵辨識系統。

參、多重伺服器之三因子身分鑑別協定

本文主要在利用生物辨識技術應用於身分鑑別，使其具安全性及效益。且對目前使用者同時會有在多台伺服器註冊，使用多種服務而提出多重伺服身分鑑別協定，以利使用者管理帳戶。在本節中註冊及登入階段會新增一個裝置用於儲存使用者的註冊資料，防止因為智慧卡記憶體儲存方面的限制，造成限定其註冊伺服器的數量，在本文中儲存裝置主要是利用隨身碟（USB）、行動硬碟（Mobile Hard Discs）等，可以隨身攜帶的行動裝置。本架構亦基於三因子身分鑑別協定，但其中智慧卡及儲存裝置成為一個因子，在身分鑑別時其中一因子錯誤就無法通過身分驗證，並保障使用者不會因為其中一個因子的的機密外洩，影響到系統的安全性。

3.1 系統架構

此節主要在述說多重伺服器遠端驗證的系統架構及所用到的符號，如圖十二所示，使用者經過生物特徵感應器採集生物特徵值跟智慧卡上的資料作運算傳送的伺服器，並且將隨身碟（USB）所存放的註冊資訊傳送到智慧卡，透過智慧卡運算後傳送到伺服器作比對，以判別是否為正確的使用者。



圖十二：多重伺服器之三因子身分鑑別協定架構示意圖

3.2 初始化階段

初始化階段為伺服器首次啟用時會產生 p_j, q_j, x_j 等變數，當伺服器重啟後，此三變數必須由伺服器之前存放的資料中重新取得，否則會造成使用者必須重新註冊才可使用系統。

智慧卡初次啟用時必須進行智慧卡初始化產生智慧卡參數 存放於智慧卡中，此變數為註冊時用以演算各伺服器的通行碼及為防止存放在隨身裝置內的註冊資訊被攻擊者破解造成系統安全性的不穩定，故當智慧卡 v_{ij} 遺失則必須重新註冊，否則使用者無法登入。以下敘述初始化階段的步驟：

※ 伺服器端：

（1）伺服器隨機選擇二個大質數（ p_j, q_j ）

$$p_j \equiv q_j \equiv 3 (\mathrm{mod}\, 4)$$

$$n_j = p_j \times q_j$$

（2）伺服器隨機選擇一個字串

（ p_j, q_j, x_j ）作為加密跟保存的祕密。

※ 智慧卡端：

（1）智慧卡會隨機選擇一個字串 σ_i 存放到智慧卡中。

表一：多重伺服器遠端驗證符號表

符號	解釋
j	j 個伺服器
i	i 個使用者
S_j	伺服器 S_j
U_i	使用者 U_i
$h(.)$	單向雜湊函數（One-way hash function）
$\oplus$	互斥或運算元
p_j	隨機選擇的大質數，為 S_j 私密金鑰
q_j	隨機選擇的大質數，為 S_j 金鑰
n_j	$n_j = p_j \times q_j$ ，為 S_j 公開金鑰
x_j	隨機選擇的亂數字串，為 S_j 的對稱式金鑰
T_{ij}	時間參數
σ_i	U_i 產生的隨機選擇的亂數字串
r_{ij}	U_i 產生的隨機選擇的亂數字串
r_{ij}'	U_i 產生的隨機選擇的亂數字串
v_{ij}	U_i 產生的隨機選擇的亂數字串
uid_i	U_i 的識別碼
sid_j	S_j 的識別碼
B_i	生物特徵特徵值
PW_i	U_i 的通行碼
sk_{ij}	U_i 跟 S 的交談金鑰
[]usb	表示將資料存入隨身碟（USB）
$[]_{smart\ ccard}$	表示將資料存入智慧卡

3.3 註冊階段

在本階段中為能夠讓使用者可以在多台伺服器使用相同通行碼，會利用通行碼、智慧卡參數、伺服器識別碼及使用者識別碼在智慧卡中進行運算產生新的通行碼，利用此通行碼作為註冊時之通行碼，則伺服器無法得知使用者真正通行碼，且每台伺服器註冊資訊都不相同，存入註冊資訊到隨身碟，在智慧卡上只有智慧卡參數，而生物特徵的運算參數，並不存放，如此真正的生物特徵資訊，並無實際存放在任何裝置中，本階段步驟如下所示：

（1）隨機選擇一個亂數字串 ，設定通行碼 ，擷取指紋特徵

$$BB_{ij} = r_{ij} \oplus B_i$$
$$W_{ij} = h(h(PW_i \| \sigma_i) \| h(uid_i \oplus sid_j) \oplus \sigma_i)$$

（2）傳送 uid_i, W_{ij}, BB_{ij} 到伺服器。

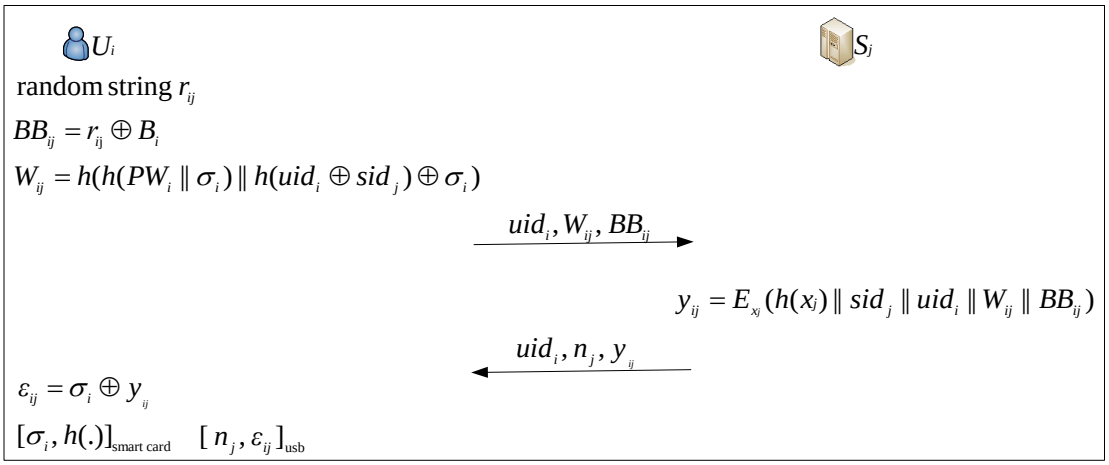
（3）利用伺服器的秘密 x_j 加密

$$y_{ij} = E_{xj}(h(xj) \| sid_j \| uid_i \| W_{ij} \| BB_{ij})$$

（4）伺服器傳送 到智慧卡。

$$\varepsilon_{ij} = \sigma_i \oplus y_{ij}$$

（5）將伺服器傳送的資訊存入隨身碟（USB）中 。



圖十三：多重伺服器之三因子身分鑑別協定註冊示意圖

3.4 登入階段

本階段中如同註冊時將通行碼經過運算，並產生新的亂數字串用於與特徵值作運算，將驗證資訊傳遞到伺服器，在伺服器驗證時透過時間參數防止遭受重放攻擊發生，並解密註冊資訊將註冊時特徵運算值與新的特徵運算值運算產生比對用特徵值用於鑑別身分，身分鑑別通過則傳送變更之註冊資訊到智慧卡，變更註冊資訊，如此每次驗證時註冊資訊都不一樣，能達到一次性通行碼的效果。圖十四為本階段示意圖。

（1）使用者輸入 PW_i* 及擷取新指紋特徵值 B_i* 傳送到智慧卡，

選取新的亂數字串 r_{ij}', v_{ij}

$$BB_{ij}* = r_{ij} \oplus B_i*$$

$$W_{ij}' = h(h(PW_i* \| \sigma_i) \| h(uid_i \oplus sid_j) \oplus \sigma_i)$$

$$y_{ij} = \sigma_i \oplus \varepsilon_{ij}$$

$$\alpha_{ij} = (BB_{ij}* \oplus W_{ij}' \oplus T_{ij})$$

$$k_{ij} = (sid_j \| uid_i \| y_{ij} \| v_{ij} \| \alpha_{ij})^2 \bmod n_j$$

（2）傳送 $(uid_i \| k_{ij})$ 到伺服器。

（3）伺服器用Rabin's解密 k_{ij} ，伺服器可以得到 $(sid_j \| uid_i \| y_{ij} \| v_{ij} \| \alpha_{ij})$

伺服器用 x_j 當作金鑰解密 y_{ij} 得 $(h(x_j) \| sid_j \| uid_i \| W_{ij} \| BB_{ij})$

檢查 $h(x_j), sid_j, uid_i$

$$u_{ij} = \alpha_{ij} \oplus BB_{ij} \oplus W_{ij} \oplus T_{ij}$$

$BB_{ij}' = u_{ij} \oplus BB_{ij}$

$\alpha_{ij}' = (BB_{ij}' \oplus W_{ij} \oplus T_{ij})$

檢查是否 $\alpha \cong \alpha'$

$y_{ij}' = E_{x_j}(h(x_j) \| sid_j \| uid_i \| W_{ij} \| BB_{ij}')$

$\beta_{ij} = (h(v_{ij}) \oplus T_{ij})$

$C_{ij} = E_{v_{ij}}(\beta_{ij} \| y_i' \| u_{ij})$

（4）傳送C_{ij} 到智慧卡。

（5）智慧卡利用u_{ij}解密C_{ij} 得到$(\beta_{ij} \| y_i' \| u_{ij})$

$\beta_{ij}' = (h(v_{ij}) \oplus T_{ij})$

檢查是否$\beta_{ij} \cong \beta_{ij}'$

$sk_{ij} = h(u_{ij} \oplus v_{ij})$

$\varepsilon_{ij}' = \sigma_i \oplus y_{ij}'$

變更註冊資訊將ε_{ij}'替代ε_{ij}。

肆、安全性分析與效能評估

4.1 安全性分析

（1）生物特徵資訊隱藏：

在多伺服器的架構下，本文所提之方法在註冊時的生物特徵資訊都是必須經過亂數字串 才會傳送出去。另外在本文內多伺服器的架構，亂數字串r是不存在任何地方，故可以完全穩藏生物特徵資訊，防止個人資訊外洩。

（2）抵擋重複攻擊（replay attack）：

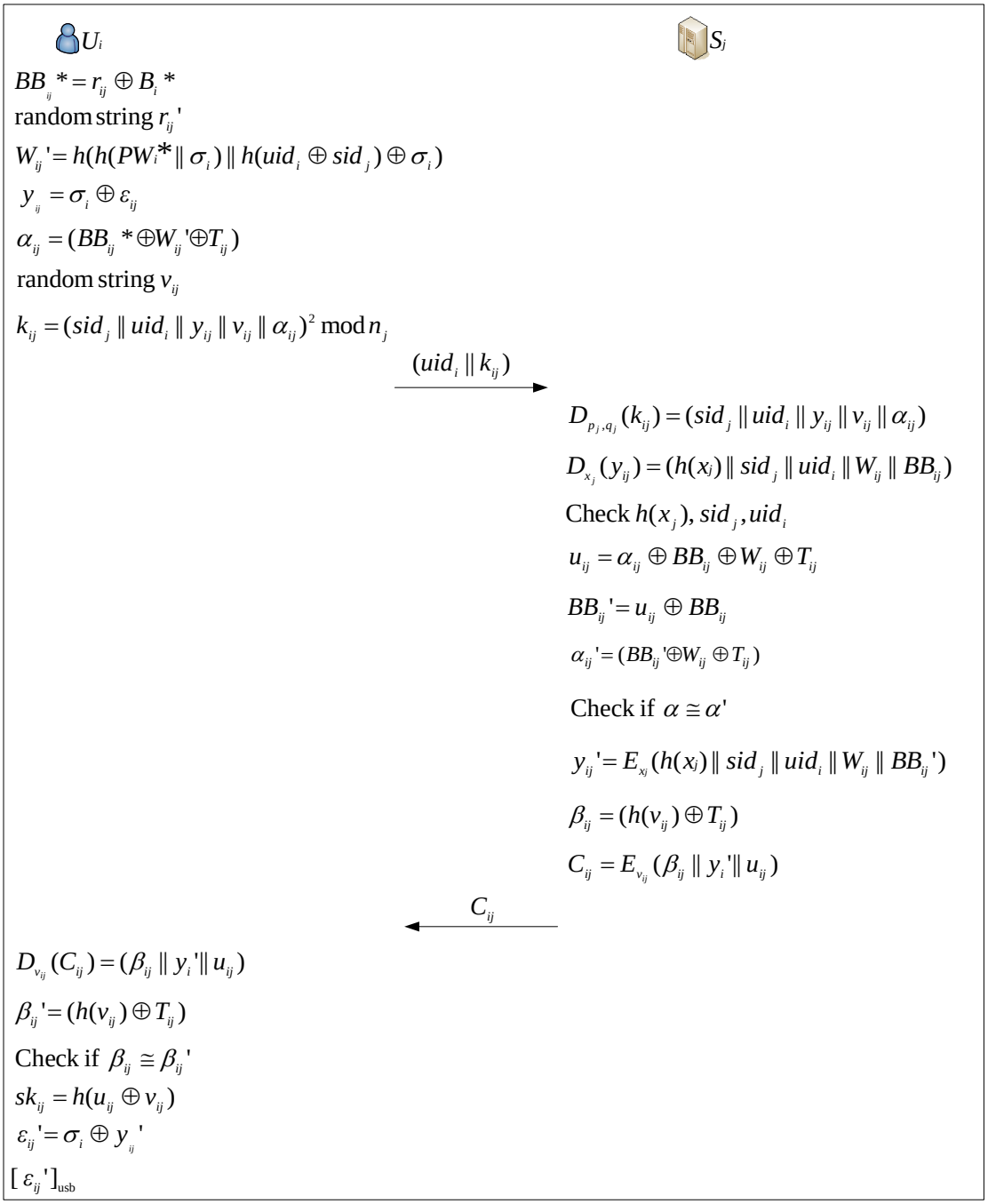
當智慧卡傳送資訊$(uid \| k)$到伺服器時，攻擊者不知道伺服器的私密金鑰無法破解訊息假冒使用者，當伺服器傳送資訊C到智慧卡上時，攻擊者不知道u，無法破解訊息假冒伺服器，由此可知本文可以抵擋重複攻擊（replay attack）。

（3）透過伺服器驗證（Server authentication）：

在本文中所有的身分驗證都是要在伺服器下做驗證，註冊資訊y的對稱金鑰x只有伺服器才有，所以本文身分驗證必須經過伺服器把關才可以驗證。

（4）抵擋離線字典攻擊（offline-dictionary attack）：

在本文中傳遞訊息都是經過加密，攻擊者本身不知道伺服器私密金鑰則無法解密k，當伺服器傳送資訊 到智慧卡上時，攻擊者不知道u則無法解密C，且這些訊息會在每次登入時做改變，所以攻擊者取得訊息作離線字典攻擊，所破解的訊息並無法在下次登入時使用，且在多伺服架構下，攻擊者盜取使用者存放在隨身碟內的註冊資訊y，用離線攻擊方式破解y，但也無法取得真正使用者生物特徵資訊B及真正的通行碼PW，因為亂數字串r，系統架構下不會存放，且正式登入通行碼W_{ij}，只有在登入時經過智慧卡內的σ_i作運算才會產生，所以本文可以抵擋離線字典攻擊（offline-dictionary attack）。



圖十四：多重伺服器之三因子身分鑑別協定登入示意圖

在本文中還可以達成以下的安全性上的考量：

（1）減輕阻絕服務攻擊（DoS）：

利用時間戳記 T，可以防止攻擊者攔截使用者訊息，利用相同訊息封包，攻擊伺服器，在使用者登入時第一次就檢查登入訊息是否正確，減輕伺服器的工作量，

較能減輕因阻絕服務攻擊（DoS）對伺服器的影響。

（2）防止擷取生物特徵錯誤合法使用者無法登入：

本文中在登入階段，使用者傳送的加密訊息k內就有使用者登入資訊，在驗證完成再去變更註冊資訊，可以更適合目前因為生物特徵的擷取裝置，擷取生物特徵的錯誤率而影響正確使用者的登入。

（3）防止智慧卡遺失遭冒用問題及隨身碟資料被取得：

本文中多伺服器的架構下，智慧卡遺失，並不會影響使用者安全性，在多伺服器的架構內，只存放σ_i，註冊資訊在隨身碟內ε_{ij}，如智慧卡遺失註冊資訊並不在智慧卡中，就算攻擊者假冒使用者的註冊資訊y_{ij}，因為無法取得x_j，也無法冒用使用者身分，隨身碟內ε_{ij}如被攻擊者取得但攻擊者沒有σ_i則無法取得註冊資訊y_{ij}破解x_j。在攻擊者無法取得正確的生物特徵資訊 及真正的通行碼 ，防止攻擊者冒用使用者身分。

（4）產生通訊金鑰：

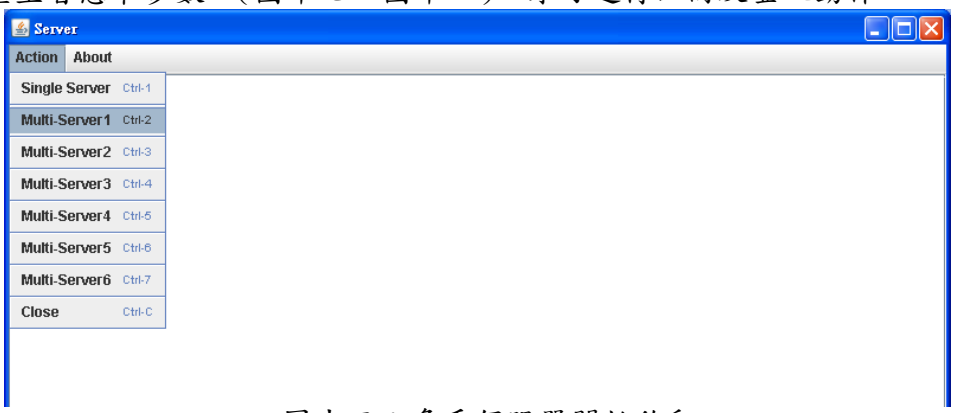
在本文中只要登入身分是正確的那在本文中登入便更註冊資訊都會產生sk作為使用者跟伺服器的通訊金鑰。

伍、系統實作與討論

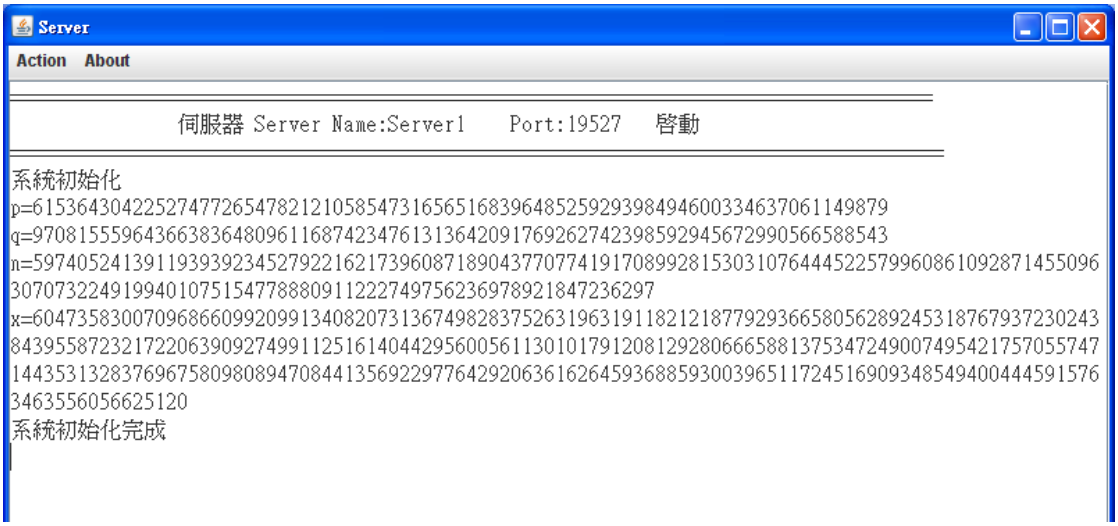
本系統的利用Java語言JDK1.6版本及eclipse 3.3編輯器進行編輯，而執行時以Vaio SZ-46筆記型電腦記憶體為2G的裝置，在作業系統WinXP SP3.0的環境下，進行測試。

5.1 系統初始化

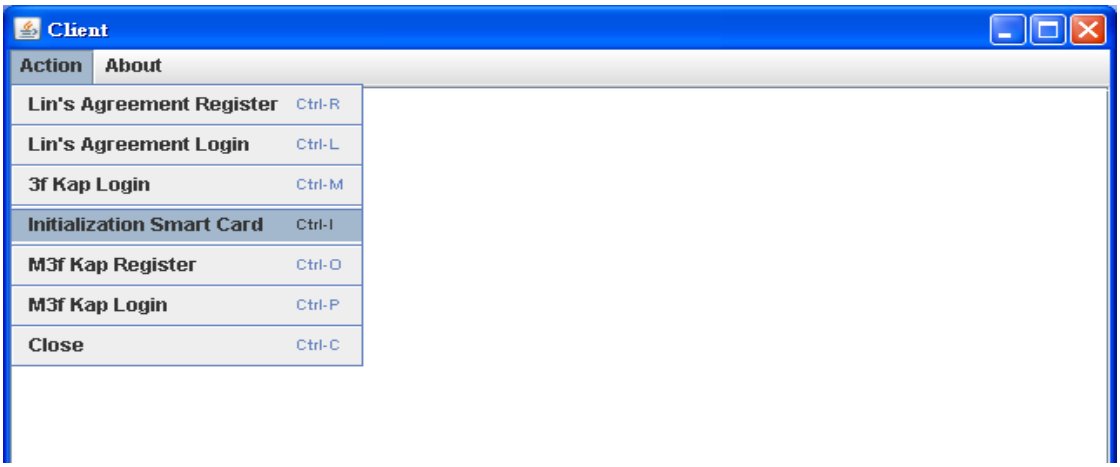
在多重伺服器啟動時，需要選擇要啟動的伺服器，伺服器可以選擇Server1~6其中一台(圖十五)，要開啟不同伺服器則要另外開啟伺服器端程式，伺服器啟動後會產生 ,, 等伺服器參數（圖十六），不同於單伺服器架構，在多重伺服器架構下，智慧卡首次使用必須初始化產生智慧卡參數 （圖十七，圖十八），才可進行註冊及登入動作。



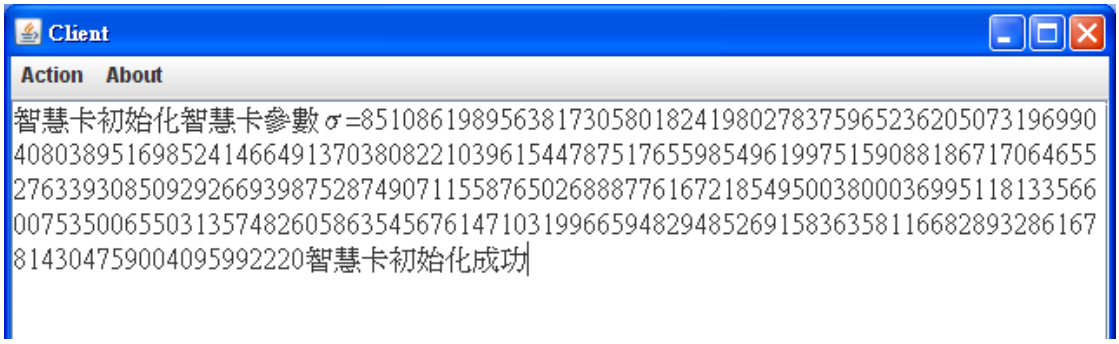
圖十五：多重伺服器開始啟動



圖十六：多重伺服器完成啟動



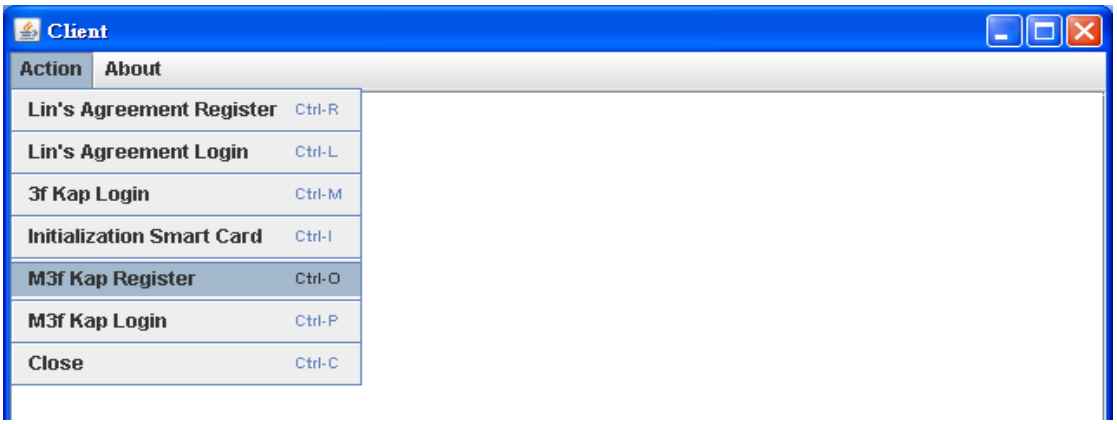
圖十七：初始化智慧卡



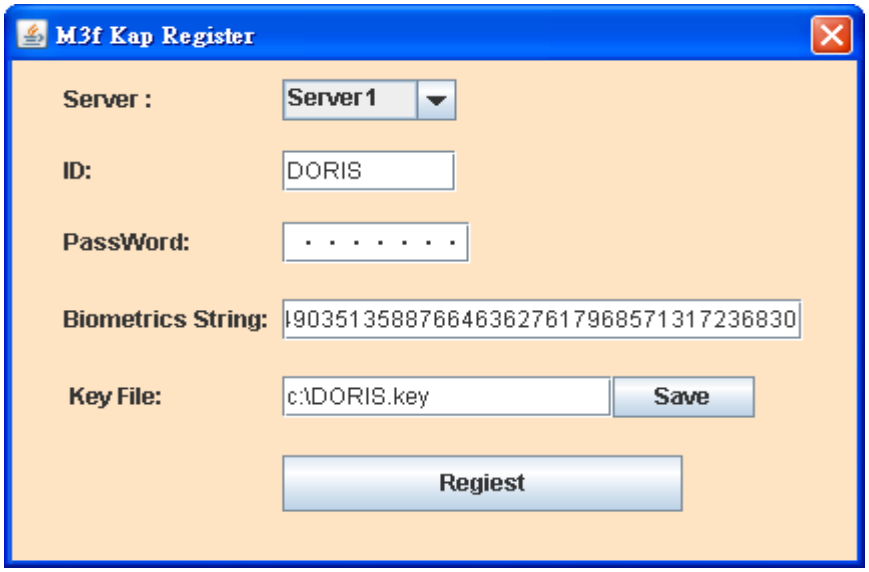
圖十八：智慧卡初始化完成

5.2 註冊階段

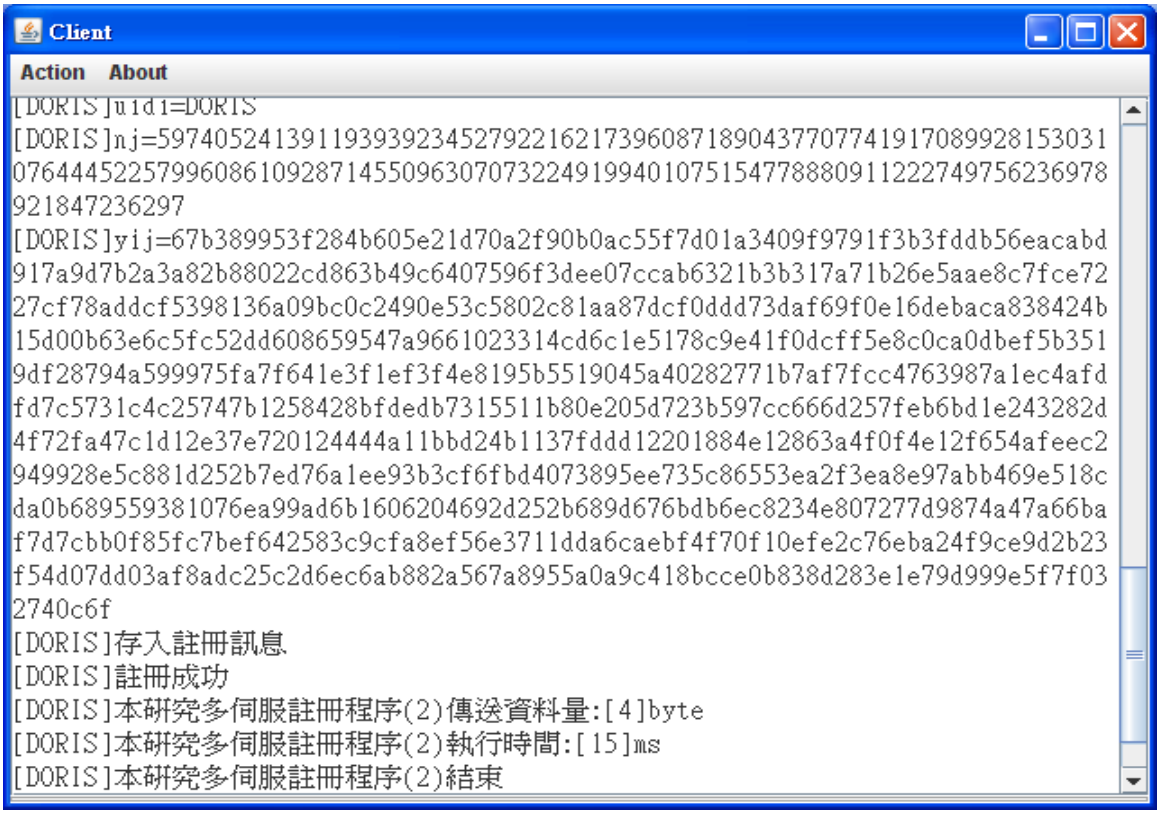
要啟動多重伺服器註冊程序必須選擇多伺服註冊（M3f Kap Register，圖十九），進入註冊畫面（圖二十），在本階段不同於單伺服註冊在於使用者必須多輸入註冊資訊（Key File）要存放在那個位置，此階段執行的演算法可以在執行畫面（圖二十一，圖二十二）及紀錄檔（圖二十三，圖二十四）中取得。



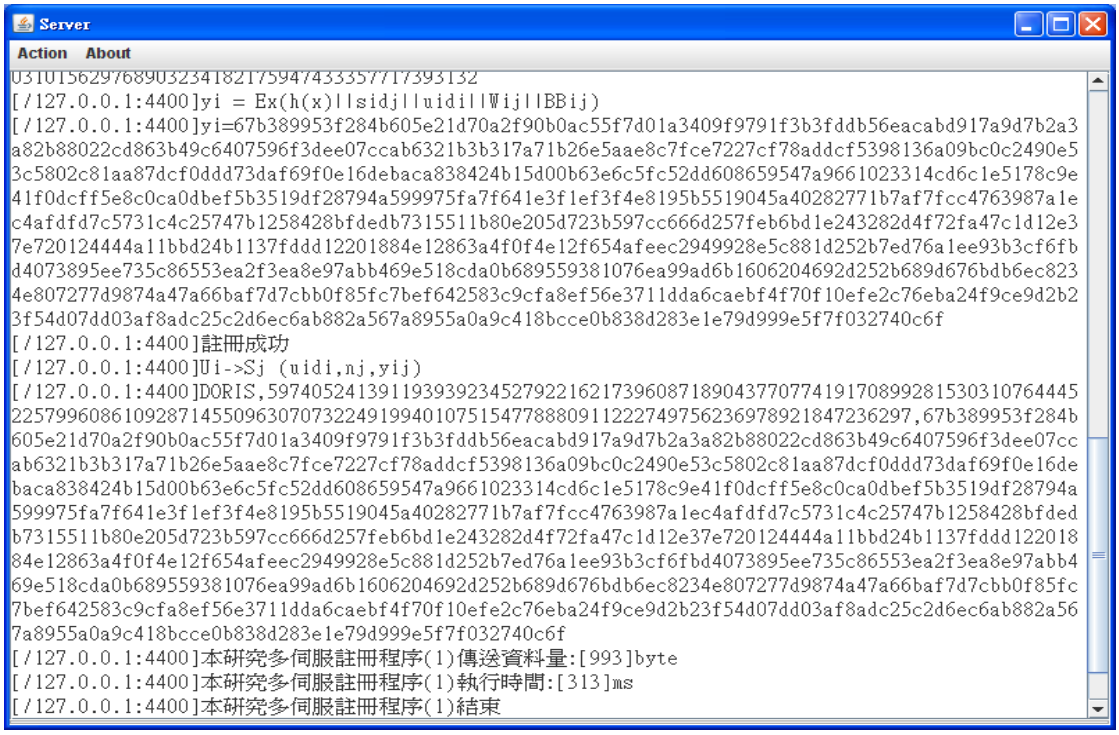
圖十九：多重伺服器註冊客戶端畫面



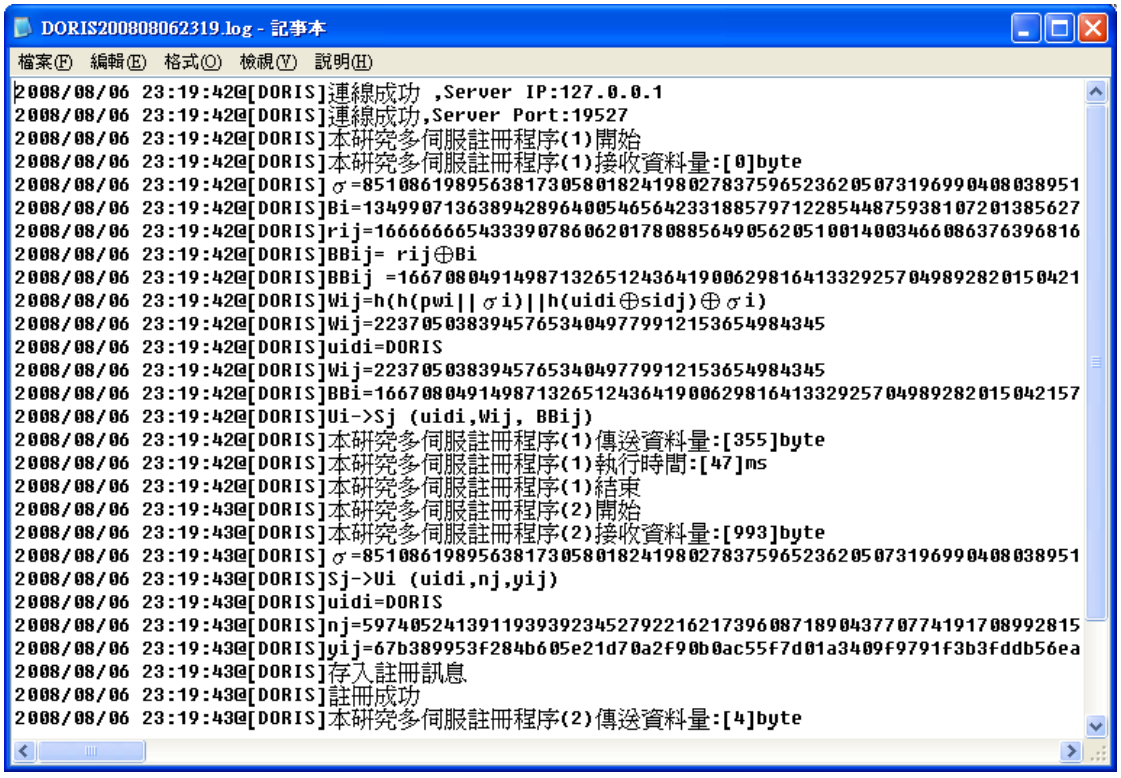
圖二十：多重伺服器註冊畫面



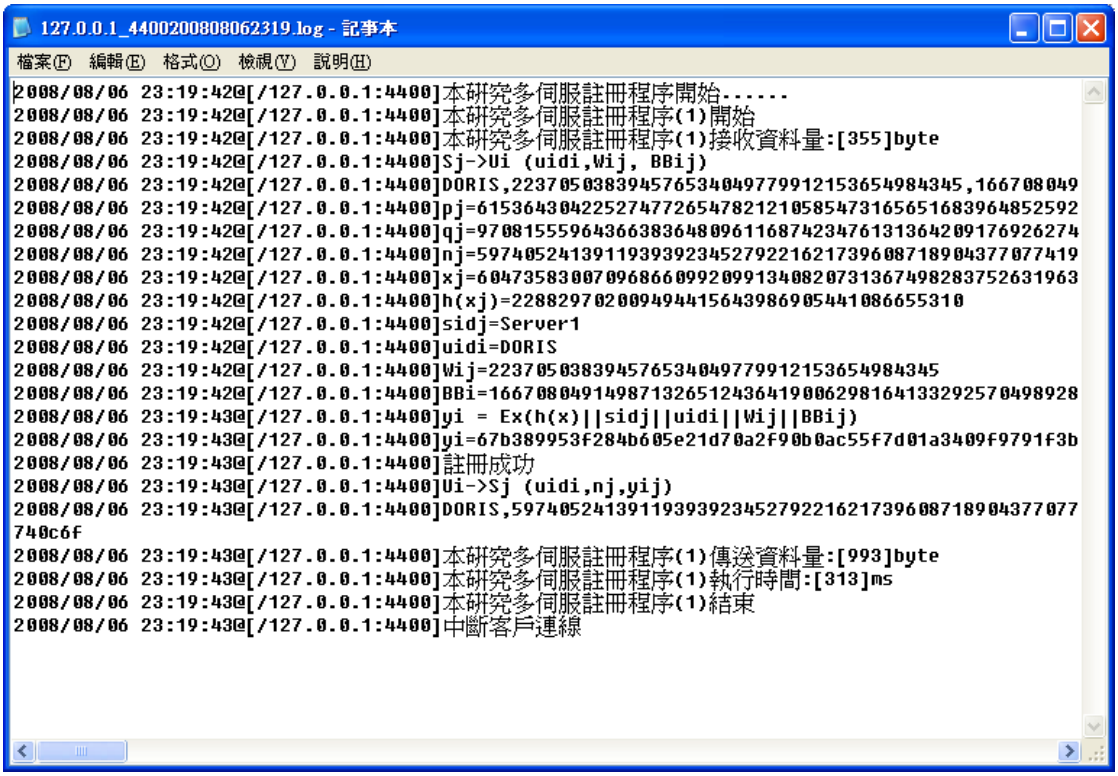
圖二十一：多重伺服器註冊客戶端畫面



圖二十二：多重伺服器註冊伺服器端畫面



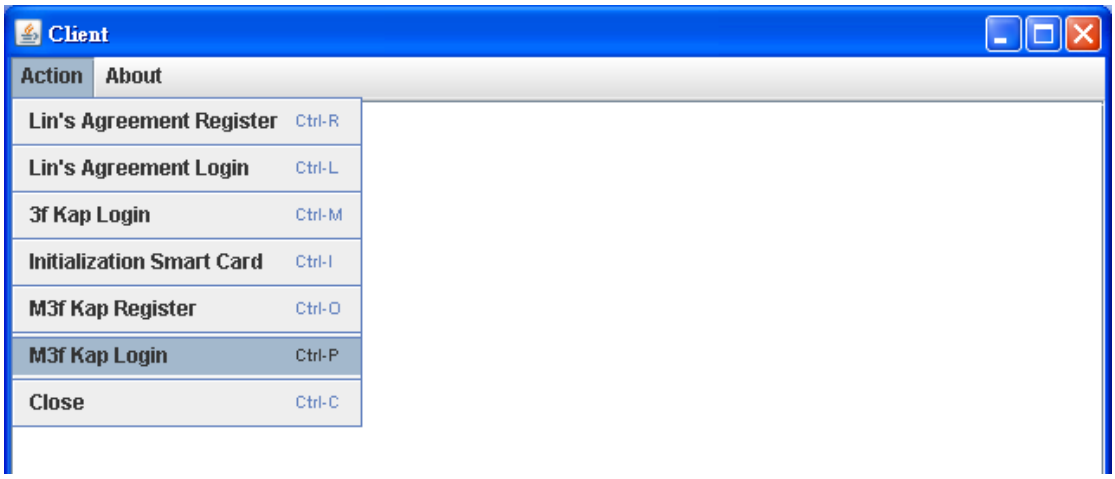
圖二十三：多重伺服器註冊客戶端記錄檔



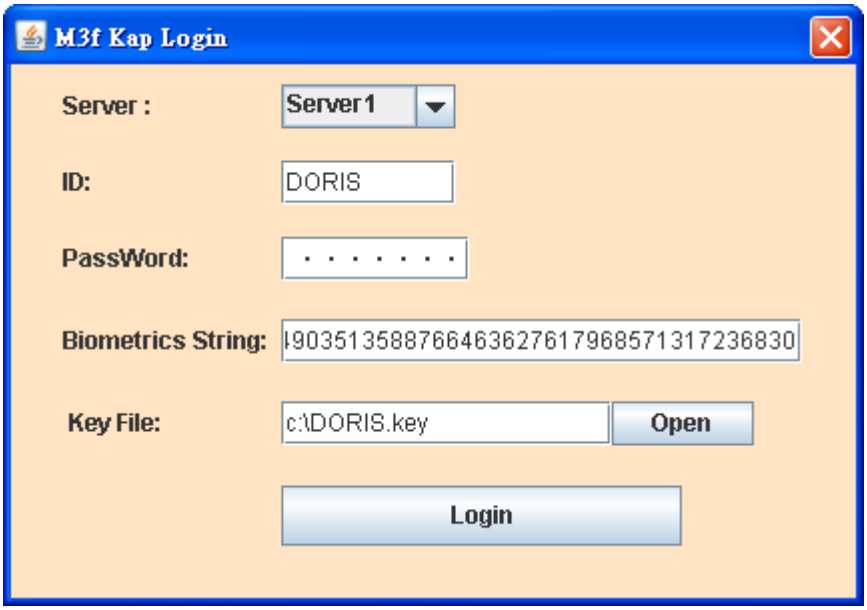
圖二十四：多重伺服器註冊伺服器端記錄檔

5.3 登入階段

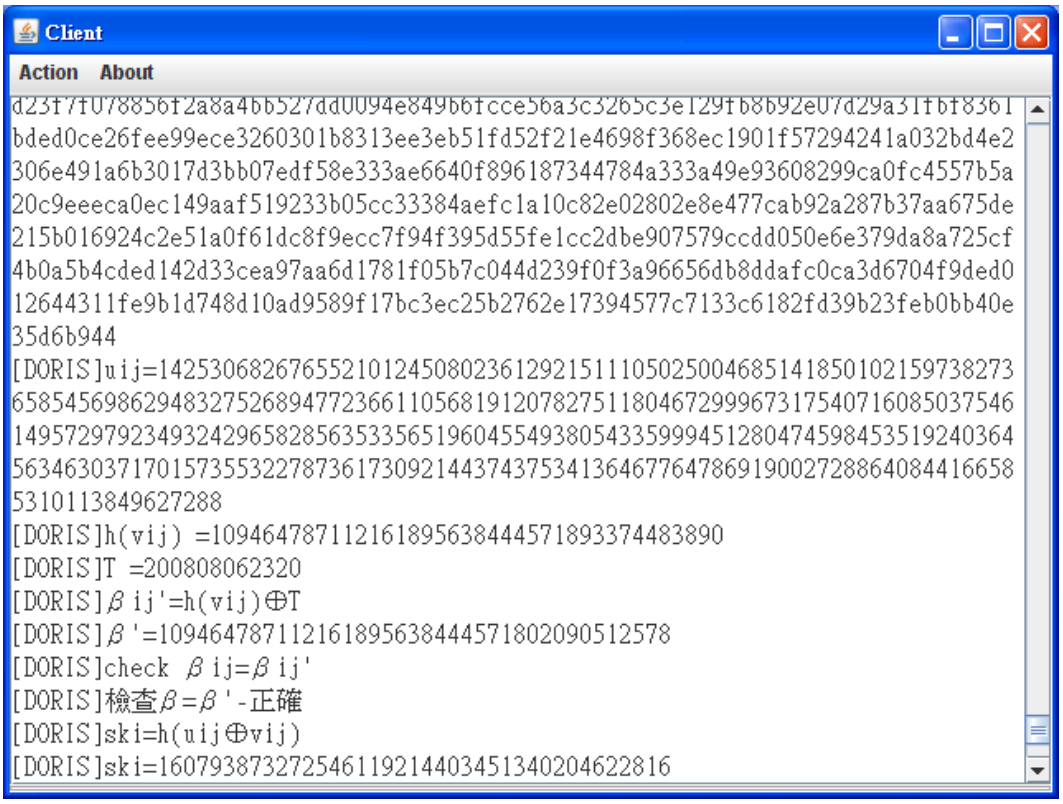
多重伺服的登入啟動首先要選擇（M3f Kap Login，圖二十五），進入登入畫面（圖二十六），輸入資訊後選擇登入（Login），其執行動作會在執行畫面（圖二十七，圖二十八）及紀錄檔（圖二十九，圖三十）中顯示。



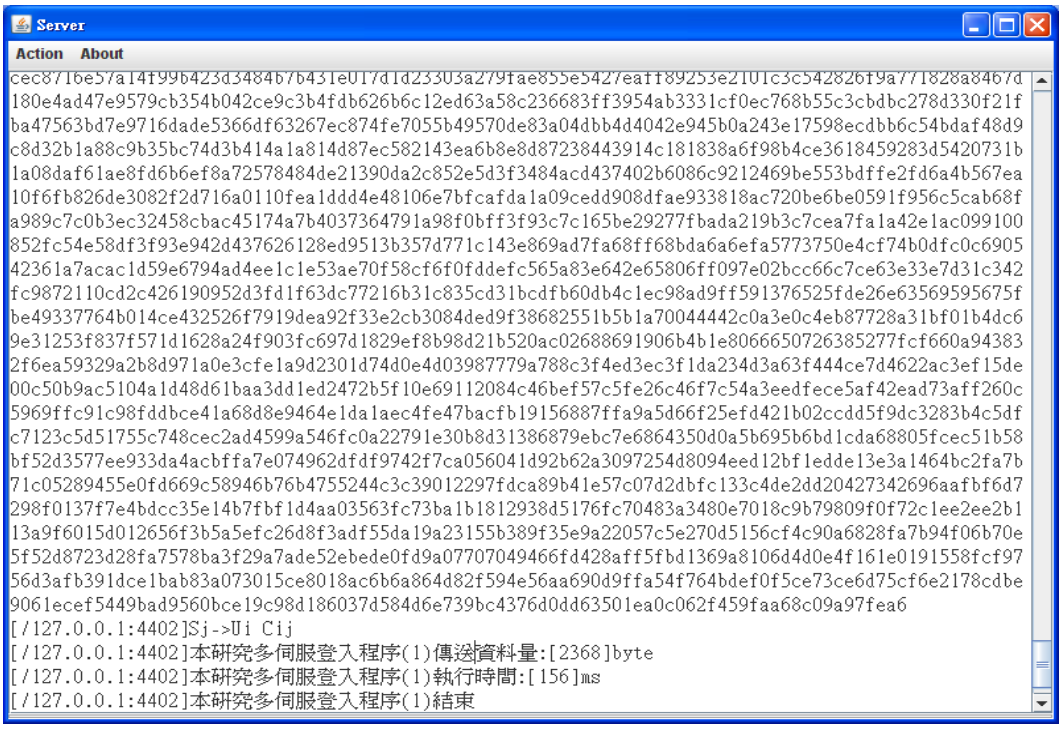
圖二十五：多重伺服器登入客戶端畫面



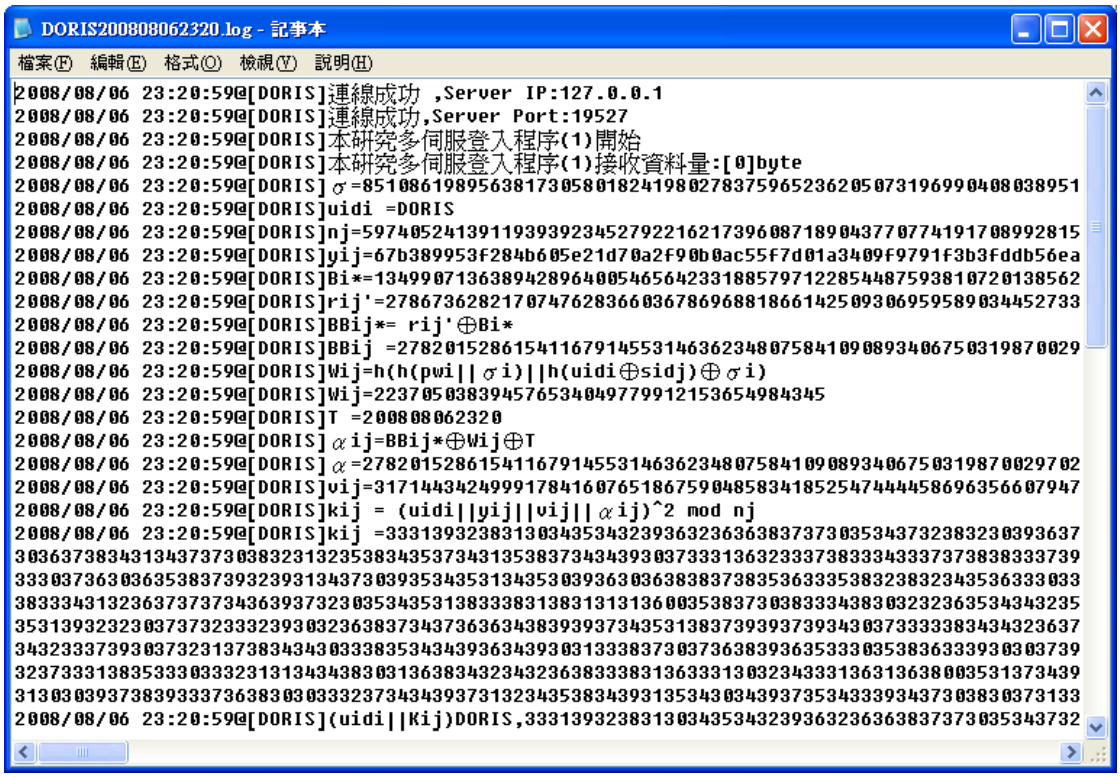
圖二十六：多重伺服器登入畫面



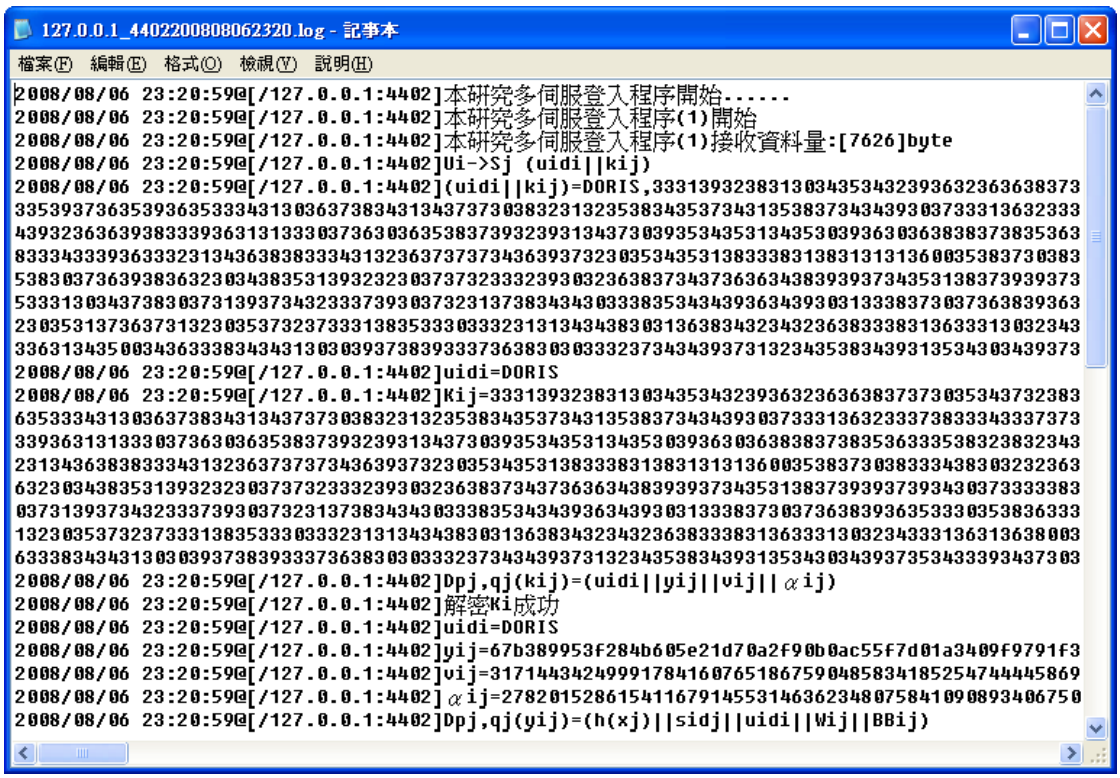
圖二十七：多重伺服器登入客戶端畫面



圖二十八：多重伺服器登入伺服器端畫面



圖二十九：多重伺服器登入客戶端記錄檔



圖三十：多重伺服器登入伺服器端記錄檔

陸、結論

在現行的環境下生物特徵取代或是輔助傳統身分驗證方式在未來可以想見是一種潮流，目前現行實際的應用並未真正發揮生物特徵身分驗證的效力，多重伺服身分驗證目前已經應用到很廣泛，也有許多學者這項課題進行探討。本研究架構提出的多重伺服驗證的架構下，可以更廣泛的應用，且更具保護個人生物特徵，在所有系統下都不存在完整的生物特徵資訊，並達成安全性改良及降低計算成本，符合目前智慧卡低功率的運算。

捌、誌謝

本論文為國科會編號NSC- 100-2628-H-182 -001 -MY3以及長庚醫院研究計畫編號CMRPG590043和CMRPG590053之計畫經費支持，使本研究得以順利進行，特此致上感謝之意。

參考文獻

[1] Rivest. R, Shamir. A and Adleman. L, “A method for obtaining Digital signatures and public-key cryptosystems.” Communications of the ACM, （21）, 120-126，1978.

[2] ElGamal. T,”A public-key cryptosystem and a signature scheme based on discrete logarithms .”IEEE Transaction on Information Theory, 31, 469-472,1985.

[3] Menezes. A and Vanstone. S “ Elliptic curve cryptosystems and their implementation.” Journal of Cryptology, 6, 209-224，2004.

[4] M.O. Rabin, “Digitalized signatures and public-key functions as intractable as factorizations,” Technical Report, MIT/LCS/TR212, MIT Lab, Computer Science, Cambridge, Mass. 1979.

[5] Yamada.H, Saito. T and Mori. S, “An improvement of correlation method — Locally Maximized correlation —” IECE Transactions of the Institute of Electronics and Communication Engineers of Japan, Vol. J64-D（10）, pp. 970-976（in Japanese）, 1981.

[6] A.R. Roddy and J.D. Stosz, “Fingerprint Feature Processing Techniques and Horoscopy,” Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC Press LLC, pp. 37, 1999.

[7] Masaki Watanabe, Toshio Endoh, Morito Shiohara, and Shigeru Sasaki“Palm vein authentication technology and its applications” Fujitsu Laboratories Ltd., 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki, , Japan,2005.

[8] H.S. Kim, J.K. Lee, and K.Y. Yoo, “ID-based password authentication scheme using

smart cards and fingerprints," ACM SIGOPS Operating Systems Review, Vol.37, No. 4, pp. 32-41, 2003

[9] C.H. Lin and Y.Y. Lai, "A flexible biometrics remote user authentication Scheme," Computer Standards & Interfaces, Vol. 27, Issue 1, pp. 19-23, 2004.

[10] J.K. Lee, S.R. Ryu, and K.Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," Electronics Letters, Vol. 38, No. 12, pp. 554-555, 2002.

[11] M.O. Rabin, "Digitalized signatures and public-key functions as intractable as factorizations," Technical Report,MIT/LCS/TR212, MIT Lab., Computer Science, Cambridge, Mass. 1979.

[12] T.Kurosawa," Biometrics for Ubiquitous Society Biometrics Society"， FUJITSU LIMITED， 2006.

[13] International Biometric Group, " Biometrics Market and Industry Report 2007-2012"，2007，http://www.biometricgroup.com/reports/public/market_report.html

[14] 張景銘、王進賢（民國 92 年）,「實驗室規模指紋辨識系統之設計與實現」,碩士論文，國立中正大學電機工程研究所。

[15] 台灣科技大學電子商務研究中心，「密碼學與資訊安全」，http://140.118.108.62/mic

[16] 許勇信（民國 95 年）,「淺談生物辨識技術及部署」,「財金資訊雙月刊 48 期」，http://www.fisc.com.tw/FISCWeb/

[17] 楊慶隆、蘇嘉興、陳澤世、張仕翰（民國 96 年）,「嵌入式指紋特徵比對技術於智慧卡的高安全性憑證存取系統之研製」,國立東華大學資訊工程學系,「開放原始碼」技術與應用研討會, P0043。

[18] William Stallings、賴榮樞譯（民國 96 年）,「密碼學與網路安全--原理與實務」，培生教育出版集團。

[19] 中時電子報（民國 96 年 1 月 15 日）