一個以手寫方式產生數位簽章的方法
A Method of Generating Digital Signature via Handwriting

謝濱燦
德明財經科技大學
資訊科技系
助理教授
bintsan@takming.edu.tw

林文松
德明財經科技大學
資訊管理系
研究生
vecent5231@gmail.com

摘　要

網際網路普及，使著網路上的服務更加多元化，犯罪型態也因此發生了極大的改變，在網路上的資料、資產，時而發生被他人竊取或是被冒用身份等事件。因此，網路上應用密碼學，針對電子文件加密，有些密碼演算法在加密時需要以個人的私鑰當成演算參數才得以取得數位簽章。因此使用者就必需隨身攜帶私鑰備用，這也會讓此加密機制產生風險及不便性。本研究提出應用類神經網路，對手寫簽名真偽予以判斷。為真者，再予產生數位簽章。可以改善使用硬體存放私鑰的不便、私鑰被竊取及密碼被破解的風險，並以個人手寫簽名的獨特性強化資訊安全的強度。

關鍵詞：手寫簽名、類神經網路、數位簽章、資訊安全。

一、緒論

本研究之目的在提升現行公開金鑰基礎建設(PKI)中的私鑰使用認證及其安全性。以手寫簽章來產生私密金鑰並且可用以進行數位簽章，以固定之公開金鑰進行驗證。或是以手寫簽名來產生私密金鑰以便對密文進行解密。

類神經網路是一個仿生物神經系統的架構，生物神經系統包含神經細胞核（Soma）、神經軸（Axon）、神經樹（Dendrites）、神經節（Synapses）等四部分，有著大容量處理單元以及平行處理的能力，同一時間運算速度及記憶容量是數位電腦無法比擬的。類神經網路具有平行處理、容錯特性、聯想記憶等特性，個人手簽名經由類神經網路的訓練後，可以記憶在網路之中進而達到判斷簽章真偽的特性。公開金鑰基礎建設(PKI)將私鑰儲存於智慧卡，使用時依使用者輸入的 PIN(Personal Identification Number) 個人身份確認碼來認證使用者，然而 PIN 容易被猜中，並不是十分的安全。

本研究利用類神經網路學習人類的手寫簽名特徵，判斷簽章之真偽。並利用類神經網路將簽章轉換為私密金鑰。並利用私密金鑰來進行文件的簽署，最後能讓固定的個人公開金鑰完成簽章驗證。

本研究之貢獻為：使用手寫簽名來產生數位簽章，除了保有原本數位簽章機制的安全性，還可強化私鑰使用時以 PIN 進行認證脆弱性。一、以手寫簽名對使用者進行認證較傳統以 PIN 碼對使用者進行認證具有較高的認證安全性。二、傳統私密金鑰儲存於智慧卡中，透過硬體的封裝保護之。然而隨科技進步難保日後能突破硬體保護而在未經認證情況下將私鑰自智慧卡中取出。本研究可無需將私密金鑰儲存於硬體中，無需擔心私鑰被取出的問題。

二、文獻探討與相關技術

(一) 手寫簽名

手寫簽名為一種生物特徵，藉著手寫簽名的獨特性，已被廣泛的使用在許多身分識別的應用上。

近年來採用類神經網路為基礎的辨識工具逐漸受到重視，有許多研究利用手寫簽名來辨識個人身份，例如：2004 年，林銀議等人提出以分流式抑制類神經網路(Shunting Inhibitory Neural Networks，SIANN)、一般化前饋式類神經網路(Generalized Feedforward Neural Networks，GFNN)等二種演算法，加上倒傳遞演算法(Back-propagation Network)來進行手寫數字辨識之研究，再將得到的結果與多層感知器產出結果進行比較，驗證其提出的演算法具有高辨識率及實用性[2]。 2008 年，李偉誌、葉經緯、王進賢，應用體感裝置相同原理的加速度感測器，來擷取出 8 種手寫簽名的特徵值。這使得使用者要手寫簽名的時間及地點受到了限制，投入運作後的硬體設備的功能及產出結果是否一致令人懷疑[3]。2010 年，何姿燕提出以下筆、提筆等參數來分析使用者的身份，認為手寫簽名辨識系統可以取代人工辨識，避免人為因素影響準確度[1]。2012 年，Kumara 認為手寫簽名是很久以前就用來作為文件及個人身分驗證的方法，常用於銀行支票、信用卡交易等用途[11]。2013 年，Kovari, Charaf 提出以基準線、圈圈等特徵為基

礎的 Off-line 手寫簽名辨識系統，經實驗證明對拉丁系文字有很好的辨識準確率，然而在中文字辨識準確率則明顯不足[12]。

依手寫簽名系統運作方式，可分為 On-line 、Off-line 二個類別。On-Line 系統是由使用者在手寫板等電腦輸入裝置直接簽名。傳統使用者手寫簽名方式則是屬於 Off-line，需要透過掃瞄或是照相等方式，取得數位影像後匯入辨識系統。雖然 Off-line 在簽名影像取得過程，所需要的影像輸入工具取得較為容易，工具成本也相對便宜。使用個人手寫簽名目的，是要避免個人簽名遭到他人冒用，但是，如果是使用影像匯入方式，卻無法確認手寫簽名是不是一個複製品。有可能是第三者取得他人手寫簽名後，加以影印，再利用影像輸入工具匯入辨識系統，可輕易的通過系統的個人手寫簽名驗證；這是使用影像輸入手寫簽名的其中一個缺點。

(二) 類神經網路

類神經網路，是人工智慧的一種，類神經網路理論起源於 1957 年，當時的科學家，仿造人類大腦的組織及運作方式，提出「感知機」（Perceptron）的神經元模型，這是最簡單且是最早的類神經模型。它是一種計算系統，包含軟體及硬體，使用大量而簡單的相連人工神經元來模擬生物的神經反應。感知機通常拿來做分類器（Classifier） 之用途。但是在 1980 年前，由於專家系統(Expert System)仍是當時最流行的人工智慧基礎，加上類神經網路的理論還不成熟，因此類神經網路沒有受到較多的重視[10]。

直到 1982 年之後，由於霍普菲爾神經網路（Hopfield Neural Network， HNN）被提出，而恰巧專家系統開始遇到了瓶頸，類神經網路理論才逐漸受到重視。之後有學者提出倒傳遞類神經網路(BPN)及雙向聯想類神經網路(BAM)等理論，直到今日為止，類神經網路仍不斷有新的架構及理論被提出，也因為電腦硬體技術大幅進步，使得類神經網路的功能更為強大，運用層面也更為廣泛。

類神經網路分為監督式及非監督式，依特性而言，分為倒傳遞類神經網路(Back-propagation Neural Network)、雙向記憶網路(Bidirectional Associative Memory，BAM)。倒傳遞網路類神經網路可以辨別正確性，但其學習慢，不易收斂，如果有新的 PATTERN 加入，還需要重新學習訓練。雙向聯想網路(BAM)，則有訓練快，回想記憶的特性。

BPN 訓練過程，學習率不當，均方根誤差(Mean-square Error，MSE)會有震蕩而不易收斂現象、容易掉入區域最小值，即使網路達到收斂，但可能是假性收斂，進而影響網路正確性。學習率及輸入的 Node 數量都會影響到 BPN 網路的訓練速度。

BPN 學習訓練的樣本數，也會影響到網路的正確性，同時也會使網路的學習時間更加長。學習樣本數量太少，會因其表性過低，無法得到正確的結果。訓練過程中學習率會影響到學習的快慢。學習率如果設定的太小則會使學習達到收斂的時間拉到很長，學習率設定的太大，雖然可以很快收斂，卻很可能是局部最小值，得到的權重是無法發揮 BPN 網路原有的特性。

BPN 除了學習很慢、局部最小化(Local Minimum)的困擾外，BPN 網路架構和相關參數(如學習速率、慣量、隱藏層數目、隱藏層神經元個數等)的設定，均需隨著環境及學習樣本的不同而改變，這些也需要長時間的嘗試錯誤(Try and Error)才能得到一個良好的輸出結果[11]。

類神經網路，是一種網路模型，可利用類神經網路來模擬人工智慧以作出決定，經過長久的演進，類神經網被利用來解決問題，甚至拿來預測未來的事物。許多學者提出以類神經網路來進行文字辨識，並且針對類神經網路的缺點提出改善的方法。

2012 年，莊尚仁使用機率性類神經網路(Probabilistic Neural Network，PNN)以及倒傳遞類神經網路來辨識簽名以及預測標準普爾 500 指數，在取得二十人的簽名範本後，經過一連串的前置步驟把範本正規化，莊尚仁認為正規化後網路的平滑參數會影響到辨識度。莊尚仁以倒傳遞與迴響狀態網路來預測標準普爾 500 指數，倒傳遞比迴響狀態網路結果更接近實際結果[4]。

羅德章、陳震武、鄭宇祈等人，以測站資料及颱風資料，驗證預測颱風走向及降雨量，只有颱風走向預測接近實際結果[5]。

陳松安、陳詠隆，以太陽及月球引力二個參數當作輸入， 使用倒傳遞類神經網路預報潮位，訓練疊代14次後得到收斂，在過程中網路模型中如果加入時間參數條件，可以得到較佳結果[6]。

李中彥、蘇偉庭，提出類神經網路來預測，驗證結果所有台灣上市公司的傳統產業有相當好的預測準確度[7]。

(三) 數位簽章

數位簽章由私鑰所產生。私鑰就像是一張在網路環境中使用的個人身份證明，利用公開金鑰密碼技術來達到身份識別的能力，藉以保護網路上所傳遞資料的正確性、保密性等。

沈淵源、李永霖，認為彩券銷售系統的資料正確性及安全性是很重要的，因此提出利用RSA非對稱加密演算法及密碼學技術將銷售系統資料加密，以確保彩券客戶、彩券經銷商、銀行等三方的權益[8]。

薛夙珍認為以特定金鑰對電子書內容及數位版權加以保護，可以防止電子書被非法複製[9]。目前的網路環境已十分成熟，有很多的應用及服務都使用網路平台，藉以達到高效率、方便的目的。也因為方便，資料安全性及正確性也

變得更顯其重要。在網路上有成千上萬的使用者及應用程式，也包括部份惡意的使用者及應用程式，目的在非法竊取或修改他人的資料。它可以代表一個使用者、機器、組織機構甚至是應用程式的身份。數位簽章通常是由一個具公信力憑證管理機構應用數位簽章技術所簽發，包含一個公開在網路上的公開金鑰及私有金鑰，藉以產生獨一無二的數位簽章。所謂的個人數位憑證的需求，它是由憑證管理機構應用數位簽章技術所簽發的一組資料，內容包含個體(Entity)的公開金鑰、憑證擁有者、簽發單位以及其他一些訊息。由於數位憑證是由一個具公信力的憑證管理機構所核發的資料，第三者除非取得憑證管理機構的私有金鑰，否則無法假造出由該憑證管理中心簽發的憑證。

(四) 資訊安全

在網路上傳輸資料有其風險，現今大部份人的日常生活也都跟網路脫不了關係。舉凡金融服務、線上購物、個人資料等都是經由網路，或是個人為了資料存取便利性，直接就把個人資料存放於雲端。如果對資料沒有任何防護，就如同將自家門戶大開，心懷不軌的人，可以毫無障礙，任意竊取而不留痕跡。

本研究仍使用 On-line 方式，取得手寫簽名此一生物特徵，再利用類神經網路的記憶回想特性來達到真偽手寫簽名辨識的目的。進一步，系統再演算出數位簽章，可避免在他人電腦輸入個人密碼時，造成可能的資安疑慮。

三、轉換機制塑模

本研究係以類神經網路來達成手寫簽名真偽判定以及基於類神經網路來產生個人化的私鑰密碼。

由於網路及相關技術日趨成熟，各項與民生相關的服務相繼提供網路上的服務，不論是電子郵件、網路購物、金融業網路銀行、網路 ATM.. 等等，都已是日常生活中不可或缺的一部份。

在網路銀行服務的實務上，銀行並無法如同臨櫃受理時，可以明白服務對象的外貌及身份證件等等的特徵。因此需要有一個健全、具有獨特性的資訊安全機制，來確保銀行客戶的資料及財產安全。

以企業架構方法來建構一個安全可以辨識個人特徵的手寫簽名來產生數位簽章，將個人的生物特徵經由類神經網路，轉化成為網路上的數位身份證明。

以 ArchiMate 繪製相關架構視圖，包括動機架構(Motivation Architecture)、應用架構(Application Architecture)等塑模類別[13][14]。

3.1 動機架構(Motivation Architecture)

首先找出網路上資訊安全相關有服務提供者、Hacker、使用者等利害關係人視圖(Stakeholder View)如圖 1 所示。

各利害關係人關注:

(1) 服務提供者關注: 保障使用者資料安全、強化私鑰使用時以 PIN 進行認證之脆弱性。服務提供者所關心的是提供服務的對象的身份是否被偽造冒用。這可是會涉及使用者的個人資料及財產安全。

(2) Hacker 關注: 密碼破解、竊取受害人個人資料。

Hacker 所關注的是要如何破解被害人的密碼、破解網路加密機制，取得被害人的個人資料，進而冒用被害人身份，竊取被害人的財物或者是個人資料。

(3) 使用者關注: 資訊安全、無需攜帶金鑰方便使用。

使用者平時一般不會隨身攜帶委很多的證件底、金融卡等等，如果可以經由轉換機制將個人的身份特徵轉化成數位的身份證明，既可以保障使用者的資訊安全，也可以解決使用者隨身太多卡片及證件的問題。

利害關係人、關注、以及目標如圖 2 所示。

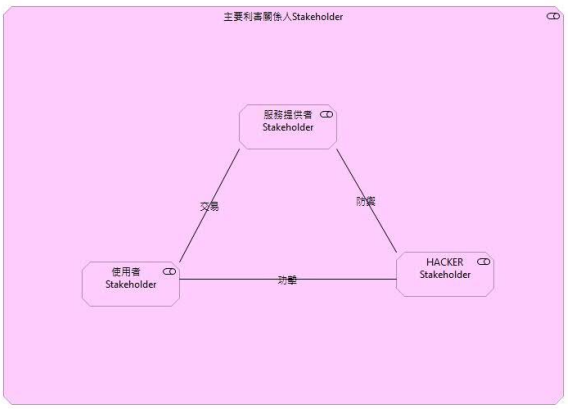

圖 1 利害關係人關注視圖

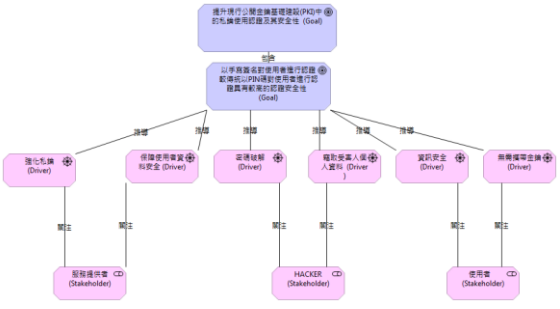

圖 2. 利害關係人關注及目標視圖

3.2 應用架構(Application Architecture)

(1) 應用系統(Application System)

使用者端使用數位板、觸控面板等等輸入設備，書寫個人手寫簽名。本研究提出的系統因為屬於 On-Line 系統，因此可以即時取得簽名的

Pixel 陣列資料。系統所得到的 Pixel 陣列資料再交付使用者電腦內的數位簽章系統處理。數位簽章系統內的類神經網路會依手寫簽名 Pixel 陣列資料判斷真偽性。如果簽名為真，則由類神經網路輸出簽名者的私鑰，再利用私鑰、標的電子檔經由密碼演算法產生數位簽章。

使用者電腦端將電子檔及數位簽章一併經由網路或外接儲存媒體的方式傳送給服務提供主機。再以網路上可取得的公鑰，驗證接收到的電子檔的真偽。應用系統架構視圖(Application System Architecture) 視圖，如圖 3 所示。

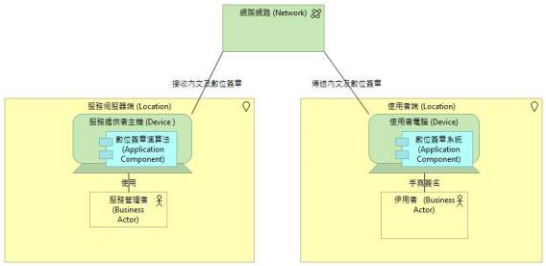

圖 3. 應用系統架構視圖

(2)應用系統功能(Application System Function)

- 手寫簽名應用系統功能(Application System Function)視圖，如圖 4 所示。使用者可以利用手寫板撰寫個人獨特性的手寫簽名，此時系統會立即由手寫板讀取到使用者的簽名 Pixel 陣列資料。

  本研究之手寫輸入系統可依需求將手寫簽名的 Pixel 陣列存檔以作為訓練及測試使用，而不是如其他系統是使用網路上的簽名資料庫，實用性更高。也可以在撰手寫簽名後立即將手寫簽名陣列資料傳送到類神經網路進行訓練或測試。

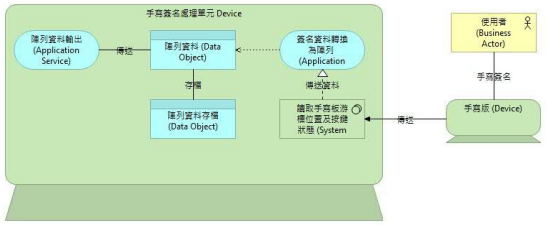

圖 4. 手寫簽名應用系統功能視圖

- 類神經網路應用系統功能(Application System Function)視圖，如圖 5 所示。

  本研究之數位簽章系統在接收到手寫簽名陣列資料後，由類神經網路主控台依照管理者指令，將簽名陣列資料分別傳遞到類神經網路進行網路訓練程序、網路回想程序。類神經網路經過網路訓練程序後而且成功收斂後，即具有判斷手寫簽名真偽的能力。

  之後，類神經網路主控台將手寫簽名陣列資料，傳遞給網路回想程序判斷手寫簽名真偽。判斷如果為真，則會由類神經網路輸出使用者的私鑰。將私鑰、要加密的電子檔或資訊交由密碼演算單元，即可產生對應的數位簽章。判斷如果為偽，則由數位簽章系統產生一個訊習，通知使用者判斷結果為偽。

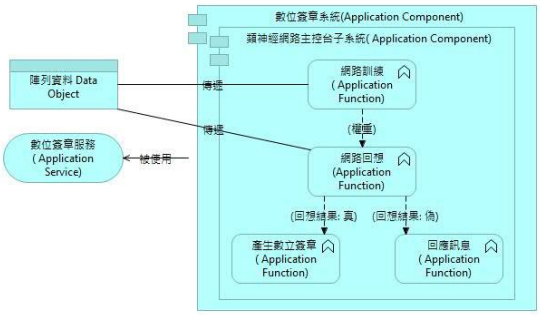

圖 5. 類神經網路系統應用系統功能視圖

四、研究心得

資訊安全是一門無止境的習題，如同正邪二方的戰爭，從古至今道高一尺，魔高一丈，從沒停過。

使用網路首重資訊安全，經由企業架構視圖，可以快速而且清楚明瞭，資訊安全相關的利害關係人以及資訊安全的問題所在，進而建構安全的網路使用環境。

參考文獻

[1] 何姿燕，「以貝式分類法為基礎之即時手寫簽名辨識系統」，新竹教育大學資訊科學研究所碩士論文，2010 年。

[2] 林銀議、賀嘉律及陳緯達，「類神經網路在手寫數字辨識之研究」，國立中央大學通訊工程研究所碩士論文，2004年。

[3] 李偉誌、葉經緯及王進賢，「加速度計於手寫簽名辨識之應用」，國立中正大學電機工程研究所碩士論文，2008年。

[4] 莊尚仁、高健智，「使用類神經網路於手寫簽名辨識與預測標準普爾500指數」，國立高雄海洋科技大學電訊工程所碩士論文，2012年。

[5] 羅德章、陳震武、鄭宇祈等三人，「類神經網路之視窗化程式開發於颱風降雨量預測」，國立高雄海洋科技大學海事資訊科技研究所，碩士論文，民102年。

[6] 陳松安、陳詠隆，「結合小波分析及倒傳遞類神經網路預報潮位」，國防大學理工學院環境資訊及工程學系空間科學碩士班碩士論文，民100年。

[7] 李中彥、蘇偉庭，「以類神經網路分析財報預測台灣上市公司股價之變動」，中國文化大學商學院資訊管理研究所碩士論文，民

100年。
[8] 沈淵源、李永霖 ， 「電子彩券系統之研究」， 東海大學應用數學系碩士論文， 民101年。
[9] 薛夙珍、温晴芳，「電子書租借應用之研究」，朝陽科技大學資訊管理系碩士論文，民100年。
[10] 葉怡成，「類神經網路模式應用與實作」，儒林圖書，2009 年。
[11] R. Kumara, J.D. Sharma, B. Chanda, "Writer-independent off-line signature verification using surroundedness feature," *Pattern Recognition Letters*, 33, pp. 301–308, 2012.
[12] K. Bence, C. Hassan, "A study on the consistency and significance of local features in off-line signature verification," *Pattern Recognition Letters*, 34, pp. 247–255, 2013.
[13] The Open Group, *ArchiMate 2.1: A Pocket Guide*, 2013.
[14] The Open Group, *TOGAF Version 9: The Open Group Architecture Framework (TOGAF)*, 2009.