視覺安全式使用者登入系統鑑定機制[&]

Authentication Systems on the Basis of Visual-based Recognitions

王旭正[*]　嚴志宏　林宜萱　陳宏和

Shiuh-Jeng Wang, Chi-Hong Yen, I-Shan Lin, and Hong-Hern Chen

中央警察大學資訊管理學系

Department of Information Management
Central Police University
*sjwang@mail.cpu.edu.tw

摘　要

本論文應用視覺密碼學於遠端通行鑑定系統的應用，提出一個能對遠端使用者的身份做認證的方法，建立一套安全度高，強調個人身份識別，又易於伺服端管理的機制。而這個方法必須利用到智慧卡當作媒介，當使用者要登入系統時，將個人之智慧卡插入終端機，再根據視覺辨識結果鍵入隨機值及密碼。此時智慧卡針對使用者的輸入訊息，利用 Hash 函數的運算，再傳回給系統做驗算。假若相符即能登入系統，反之無法登入系統。另外，我們並利用時戳的技巧，使它能防範重送攻擊。

關鍵字：智慧卡，識別，視覺密碼學

Abstract

In this paper, we propose a system that fulfills the user log-in authentication on the basis of visual cryptography. In our systems, not only can the identity of user authenticate via the server, but also the connected server comes to the flexible management in system operations. The smart card considered in our systems is a key-medium to operate our authentication scheme. Whenever the user requests to log-in the systems, the smart card is then inserted to the card reader prior to the recognition of user identity. Meanwhile, the random key and password generated by the visual cryptography are shown in the systems to seek the double check via user's eyes vision system. Once the correct messages which match up the previous random codes are given, the smart card is then launched the hash computation for the output of digest. With right digest comparison between the generated one by smart card and the pre-stored digest in the systems, the legal user is then authenticated. But reject those who are illegal users with the wrong digest comparisons. In addition to the visual-based authentication, the replay attacks usually existed in network systems are also deterred via the incorporation of key-timestamp in the system operations.

Keyword: Smart card, identification, visual cryptography

[&] This work was supported in part by National Science Council, R.O.C. under Grant No. NSC 95-2221-E-015-002-MY2
[*] Correspondence author: sjwang@mail.cpu.edu.tw

1. Introduction

隨著網際網路的快速發展，使用者可以利用網路的連線使用遠端伺服器的服務與資源，或與其他遠端使用者互通訊息，藉此可推動了許多重要的網路應用，例如電子文件交換、電子商務等活動。在這樣一個開放的網路環境中，所有的資訊都是在共通的網路上傳輸，任何人都可以輕易的取得資料，便利知識的流通與汲取。但相對地，網路上的使用者亦可能利用這些資源取用便利性成為惡意的攻擊者，對使用者的個人權益及隱私等造成莫大的傷害。因此如資料的加解密(Encryption and decryption)、資料來源鑑定(Authentication)和使用者身分識別(Identification)，就成為安全機制中最重要的議題。如何藉由一些機制有效地，正確地的實行使用權限的管控，確定訊息的接收者或發送者的身份，將是研究重點。

一個好的認證系統，必須擁有機密、鑑定、完整與不可否認性[14]，等特性：

一、機密性：在可公開資訊當中，攻擊者無法合理的推測出使用者秘密資訊。

二、鑑定性：系統中心有良好的註冊認証機制，可提供使用者鑑定其合法性。

三、完整性：確定資訊是否經過第三者增加、修改或刪除，以確保資料的完整性。

四、不可否認性：所有傳遞的參數配合所推導的結果皆為唯一值，使得訊息簽署者無法否認其簽署資訊的內容。

傳統的使用者鑑定機制是當使用者利用網路從遠端登入(Login)電腦系統時，系要求使用者輸入名稱(User name)及密碼(Password)，再透過數位簽章技術來作加解密的驗證程序。傳統數位簽章技術所使用的演算法是架構在指數運算上，不但金鑰管理不易且在爾後在進行交易時，所耗費在簽章及驗證的時間也是相當可觀的。近來有所謂的生物驗証系統，其方式大部份是取用使用者身上的自然特徵當作驗証身份的依據，例如每個人手指的指紋[6]、視網模的紋路[7]，或是人的脣型[4]，等。這些特徵都具有代表個人身份的意義，皆可做為驗証個人身份的條件。但在驗証過程中，其所需器材設備成本昂貴，無法普及到一般民眾身上。且又有侵犯隱私權上的困擾，更重要的是一旦發生遺失或被竊取的情況，這些特徵將有無法撤銷的限制性障礙。

基於上述方法的缺點，我們運用資訊安全的研究領域中有一類迥異於傳統密碼技術的加解密機制，我們稱其為資訊隱藏(Information Hiding)技術。資訊隱藏技術的主要精神是將機密的資訊藏入另一個具有意義但較不敏感的資料中，使人類的感官神經(視覺、聽覺)無法直接察覺到該機密資料的存在，進而除了得以確保通訊的安全之外，並可進一步地加強該機密資料之保護。我們運用資訊隱藏中的視覺密碼學的理論，來達到不需作複雜的運算，僅需結合人類視覺行為與電腦輔助運算之識別機制，並可達到高安全性。

本文引用 2002 年，由 Chang 和 Chuang[3]所提出的在智慧財產權應用的視覺秘密分享方法。其主要的精神在不修改原圖的基礎下產生所要分享秘密資訊的子圖影像 (Share)，再透過子圖影像 (Share)的互相疊合，運用視覺的判斷以獲得我們所需的秘密資訊。我們另外結合文獻[11]的作法，使得萃取和重建重要機密資訊時，不需要使用原先的掩護圖作為基底，而可直接對有重要機密資訊的偽裝圖做萃取的工作。藉此，我們提出視覺密碼學於遠端通行鑑定系統(Remote Password Authentication System, RPAS)的應用，我們的方法能對遠端使用者的身份做認證，改進以往金鑰密碼系統、生物驗証系統兩者所潛在的缺點。

我們所提出的方法，其基本的作法由認証中心利用 Torus Automorphisms 函式產生一張子圖影像，並核發合法使用者一張智慧卡，作為將來進入鑑定系統的依據。Torus Automorphisms 係由 Voyatzis and Pitas 於 1996 年[9,10]所提出的一種平面兩維轉換。其核心在於利用一 2×2 常數元素矩陣的乘積來進行運算。

而在離散二維空間中，Torus Automorphisms 可以視為是一種排列函數(Permutation function)，其轉換函數如下[9,13]：

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix}^{n} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \bmod N \quad (1)$$

意即 2×2 的矩陣先自乘 n 次後再乘上原座標值 (x_i, y_i)，再取除以 N 的所除餘數，即得新的座標值 (x_{i+1}, y_{i+1})。而 n 會有一個週期數為 R，其與參數 k、N 及 (x_i, y_i) 有關。根據[9,10]的分析，當 N 質數時，R 通常會等於 $N-1$ 或 $N+1$，至於其他的條件下，R 就會呈現不規則變化。

再參照文獻[9,10]中，上述的轉換亦可以下列方

式表示：

$$A_N(k):\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix}\begin{pmatrix} x_i \\ y_i \end{pmatrix}\bmod N \qquad (2)$$

其中A代表矩陣，k為一可控制的參數，N則為所控制的餘數值，且此函數$A_N(k)$有一週期時間T。而所謂的週期時間，意即若運算次數達T次時，座標值(x_i, y_i)就會回到原來的位置。透過Torus Automorphisms函式，讓一張原圖利用不同的參數組合就能非常快速產生不同的子圖影像，在此特質下，若引用至我們的環境，則各個伺服主機所要保留的僅是一張或是再多一些的原圖，不必隨著使用者數目的增加，而增加所使用影像圖或相關使用參數在儲存管理的困難度。

在視覺密碼學裡，若沒有兩張子圖影像的疊合，很難從單獨一張子圖影像獲得任何機密資訊的安全性。但經過偽裝的子圖影像僅為二元影像圖其隱藏效果有限，如果直接放置於網路上傳，其子圖影像的外表易遭到非法者質疑，增加被攻擊、破壞的風險。因此我們取而代之將子圖影像隱藏入正常的圖片中，這樣一來，所有網路傳輸的資料都是可是自然可見的明文，不易造成非法者的懷疑，而且透過一張圖片來隱藏有意義的子圖影像，就算能取出此子圖影像，缺少另一張子圖影像也是無濟於事，很難得到任何相關資訊，因此達到雙重保障的功能，此理念即我們研究的安全性基礎。

在本篇論文的編排方面，我們於第二節中對於本文相關的技術與比較文獻做描述。第三節則細部說明我們提出的視覺密碼於伺服認証機制上之應用模式。第四節則為我們的安全度分析與相關討論，最後的第五節為我們之結論。

2. Survey

2.1 Naor 和 Shamir 的文獻簡介

Naor and Shamir[5] 在 1994 年提出了一門新的學問，稱之為視覺密碼學(Visual cryptography)，其主要特色在於還原機密影像時不需要任何的計算，而是直接以人類的視覺系統即可將機密訊息辨識出來，此想法完全不若傳統的密碼技術，因為在傳統的技術中，於解密過程中須靠大量且複雜的計算才可解出真正的訊息。

我們簡單描述[5]的視覺密碼學，並且列出疊合的結果於圖 1 所示。[5]的方法只適合使用於 2 元影像。其作法首先選用一張大小為 *MxN* 的機密影像圖，接著將之分解成 Share-1 與 Share-2 兩張大小為 *2Mx2N* 的投影片。其產生機密影像的作法，是以疊合兩張 Shares 時所呈現的影像在某點像素若是黑色，則先以 1/2 機率方式決定其中一 Share 影像在相對應位置的樣式，再以另一 Share 該位置使用互補的樣式，故可使兩張 Shares 在製作完成後，相疊在一起時得以呈現全黑的像素；而當需白點像素時，也以 1/2 機率取一點樣式，使兩張子圖影像在相對應位置是相同的樣式，故在兩張 Shares 相疊時，在相對應位置上，呈現出的是一個黑色全色素和一個白色半白點樣式，經人類視覺對比效果視為白色。

使用[5]的方法具有相當程度的安全性，若想從某張 Share 來分析明文是非常困難的。但其缺點在於每一張 Share，看起來都是雜亂的黑白點，毫無任何意義，因此容易引起非法者的注意。因此文獻[1]又提出了一種新的方法以改良 Naor and Shamir 的缺點，其視覺密碼定義如圖 1 所示。

2.2 Chang 和 Hwang 的文獻簡介

Chang and Hwang[1]在 1998 年加強[5]的方法，其中對於 Share 的產生是利用 3x3 像素擴張法，使得其中一張 Share 改進為有意義的影像，此有意義的 Share 可進一步地提高其偽裝功能。以下為此方法之說明：

1. 產生一張不具意義的 Share-1, 其產生由許多 3x3 區塊所組成，每一個區塊包含 6 黑 3 白的像素值，其中黑點的位置是隨機的。
2. 將機密影像(Secret image)擴成 3x3 的區塊，其中若原本像素值如為黑色，則擴成 8 黑 1 白；像素值如為白色，則擴成 7 黑 2 白。
3. 產生一張有意義 share-2
   分成兩個步驟，首先將一張偽裝影像(Camouflaged image)，擴成 3x3 的區塊，原本像素值如為黑色，則擴成 5 黑 4 白；像素值如為白色，則擴成 2 黑 7 白，其大小和 Share-1 同等。再來搭配 Share-1 和步驟 2 裡的擴充影像，整調成偽裝影像裡黑點和白點的位置，因此形成最後的 Share-2。

事實上 Chang and Hwang[1]方法的安全性，相較於[5]是有過之無不及。況且其產生的 Share 為有意義之圖像，更具豐富的變化性。它

不但承襲視覺密碼學(Visual cryptography)還原機密影像時不需要任何輔助設備的特色,而且更適合用於驗證收發資料兩端的合法性。因為只需一張 Share-1，配合各式各樣的偽裝影像，就可產生不同偽裝後的 Share-2。下圖 2 在[1]中為一個黑白區塊定義的例子，圖 3 為[1]的流程示意圖。

影像	白色	黑色
Share1	(6，3)	(6，3)
Share2	(2，7)	(5，4)
疊合	(7，2)	(8，1)

圖 2：黑白區塊產生之定義

2.3 Chang 和 Chuang 的文獻簡介

在 2002 年時，Chang and Chuang[3] 又提出了一種對於智慧財產權應用的視覺秘密分享方法。這種方法在不修改原圖的基礎下產生具順序性 Share-1，因此運用的領域與彈性也就更為廣泛。基本上, [3]的方法結合了兩種技術，分別是 Torus automorphisms[9,10] 和應用 Visual cryptography[1]，其中之 Torus automorphisms 主要用來將原圖打散成一張不規則的圖形，再透過適當排列的演算法將產生 Share-1,再利用[1]將機密影像藏於 Share-1 和 Share-2 之中。因[3]的方法的最主要特點是在藏機密影像的過程，不修改原圖，僅調整了 Share-2 中像素的位置。它可大致分為四個步驟：

1. 首先使用 Torus automorphisms [9,10]技術將一張灰階的原圖打散形成一張混亂的 image O', 其係用公式如(1)。
2. 從混亂的 image O' 中選取一個 size 為 $3N' \times 3M'$ 的部分影像圖 I。
3. 將 I 分成許多 3x3 的區塊，選取每一個區塊中 t 個最小的像素值圖並標以黑色，其它剩下的 $9-t$ 則標以白色，此時即可將原灰階圖轉為黑白點圖，也正式產生第一張 share，稱為 Share-1。
4. 再利用先前所提於[1]方法裡的技術來產生第二張 share，稱為 Share-2。

我們以圖 4 說明[3]的方法如下：

3. 視覺安全式使用者登入系統鑑定機制

目前常見的兩類鑑定系統為:金鑰密碼系統[2,12]與生物驗証系統[4,6,7]。在金鑰密碼系統中，若以數位簽章進行數位身份認証，在處理秘密資料上將依不同的認証協定而有不同的應對形式。並進一步，若未能有較為理想的資訊安全管理策略，若有部分資料遺漏，其所造成之影響勢必是無法想像的。更由於一般數位簽章技術所使用的演算法是架構在指數運算上,計算量高且金鑰管理不易,此方法使得在簽章運算及驗證的時間是相當可觀的。另外的生物驗証系統則利用人類特徵聲音、指紋、脣形、視網模等進行身份辨識,但所需器材設備成本昂貴,造成在系統建置之初,必須投資大筆的經費購買硬體設備,且精確度高低不易決定,太高則影響辨視效率,太低則安全性不足。因此本篇我們運用資訊隱藏中的視覺密碼學的理論,來達到不需作複雜的運算,僅需結合人類視覺行為與電腦輔助運算之識別機制,並可達到高安全性。以下我們介紹我們的機制：

我們的遠端使用者視覺識別系統,需輔以智慧卡的使用，其中智慧卡內嵌結構上具有抗偽造、竄改的記憶功能。我們的方法分成三個階段進行：起始階段，註冊階段及驗證階段。

- 起始階段：CA 先驗證伺服主機之合法性。
- 註冊階段：在取得伺服主機服務使用權之前，使用者必須先向 CA 註冊。
- 驗證階段:伺服主機對於收到的登入需求訊息進行驗證，來決定是否核發給此使用者登錄系統的權利。

以下我們將分別針對這三個階段,詳細說明我們的方法。並事先定義一些相關的符號，以方便說明本研究中相關參數處理的過程,及安全技術的應用。

- **相關單位符號定義：**

1、 CA(Certificate Authority)：公開金鑰認證當局，負責簽發公開金鑰憑證，並為具公信力的可信賴仲裁者。

2、 Server（簡稱S）：伺服主機，提供資源的使用，在本系統中假設有n個伺服主機，S_i，$i=1$、2、…、n。

3、 M_i：合法主機的識別資料。
4、 r_i：亂數產生器產生的隨機數。
5、 $E(\bullet)$：表示加密所使用之密碼演算法，在我們的方法中，可用 3-DES 系統實現此演算法。
6、 K_i：CA所賦予各個合法主機的秘密金鑰，可視為秘密識別代碼。
7、 User(簡稱 U)：使用者，並使用智慧卡作為遠端登入系統伺服主機的工具。
8、 $H(\bullet)$：One-way Hash 函數，可達到訊息的完整性與不可否認性，本文中的 $H(\bullet)$ 可以 MD5 來實現。
9、 PID：為一使用者帳號。CA 若接受使用者 U 的註冊，則賦予 U 一個唯一的 PID，並嵌入智慧卡中，作為 U 登入伺服主機時使用。

[起始階段]

步驟一： 各個伺服主機S_i，向CA提出加入整個系統組織的要求，並提供相關資料(含身份登記所在區域及網路分配區域等)，進一步待CA審核。

步驟二： CA逐一驗證各個伺服主機S_i之合法性，依所提供資料檢視是否符合系統建置需求。如果同意建置伺服主機，則賦予各個合法$S_1, S_2..., S_n$不同的識別資料$M_1, M_2..., M_n$，CA並依序為各個S_i，$i=1$、2、…、n，產生隨機碼$r_1, r_2..., r_n$。

步驟三： CA計算 $K_1=E(r_1, M_1)$
$K_2=E(r_2, M_2)$
•
•
•
$K_n=E(r_n\ M_n\ )$。
之後將$K_1, K_2..., K_n$配交由各伺服主機$S_1, S_2..., S_n$使用，並秘密保存於伺服主機內。

■

[註冊階段]

步驟一： 使用者U自選一個密碼(Password)，稱PW，並經秘密管道交給CA，以為註冊程序。

步驟二： CA若接受U的註冊，則賦予U一個帳號PID。CA進一步從影像資料庫之中選出一張灰階圖，令為O_{CA}，並依[3]的方式設定相關參數i, k, N，藉此產生一張二元像素值的子圖影像，令為Share-1，其中i, k, N為Torus Automorphisms函數產生時設定的參數。

步驟三： CA嵌入PID，Share-1 和$K_1, K_2, \ldots\ldots K_n$至智慧卡中，並發智慧卡給U。

步驟四： CA將U在步驟二內影像資料庫所選用之O_{CA}與相關參數i，k，N及U的PW與PID傳至各參與的伺服主機S_i ，$i=1$、2、…、n。

■

[驗證階段]

步驟一： U將智慧卡插入終端機，由智慧卡中提出PID給S_i，向S_i提出登入需求。

步驟二： S_i檢查U輸入之PID是否為正確之格式，並比對是否與S_i 所登記之PID相同。若是，則隨即透過U的設定參數i, k，N，運用Torus Automorphisms函數，將內存之O_{CA}轉成(Share-1)'。

步驟三： S_i 由內建的影像資料庫中，隨機找一張二元標記影像，令為$O_{Si-logo}$，及目的在於影像偽裝使用。並隨機產生一個亂數值，令為Nounce，與時戳，令為T。接著合併$Nounce$與T，製成一張與(Share-1)'同大小之二元像素值影像。再將(Share-1)'應用[1]的方法配合$O_{Si-logo}$產生另一張二元像素值的子圖影像，令為Share-2。

步驟四： S_i 再從影像資料庫中隨機取出一張灰階圖，令為O_{si}。。將Share-2 應用資料隱藏之文字嵌入方法，例如[11]，嵌入於O_{si}中，令此已嵌入資料的影像圖，稱為O_{si}'。

步驟五： S_i計算$H(Nounce, K_i)$，其中K_i為起始階段時，已內建於S_i 之中。另S_i將O_{si}'及$H(Nounce, K_i)$回傳給U。

步驟六： U經由網路收到的O_{si}'，再以[11]之方法，將所隱藏入之二進位碼萃取出，並還原成Share-2。

步驟七： U收到$H(Nounce, K_i)$與Share-2 之後，

將Share-1 和Share-2 疊合，可產生 *(Nounce)'*及*T'*，並判斷T' 與現階段系統時間，是否在可接受時差範圍內後。若在系統時間誤差內，進一步比對*H((Nounce)', K_i)* 是否等於S_i 所回傳的 *H(Nounce, K_i)*，以確認伺服主機S_i 合法性。其中前者*H(•)*之*(Nounce)'*為視覺辨認出之隨機值，至於K_i則已事先內存於智慧卡。若比對成功，則視S_i為合法伺服主機，否則主機為非登記之主機，使用者得退出登入。

步驟八： U進行*H((Nounce)', PW, K_i)*運算，其中*(Nounce)'* 為兩張二元子影像Share-1 與Share-2 之疊合，後以視覺辨認出之隨機值，K_i 為內存於U智慧卡內之秘密參數，*PW*及*(Nounce)'* 為登入之輸入值。接著U將*H(•)*運算結果再傳送給S_i。

步驟九： S_i收到*H(Nounce', PW, K_i)*後，以S_i內存的*Nounce*，*PW*，K_i進行*H(•)*，並比對是否等於來自U的*H(•)*。如果是則表示U為合法使用者， S_i將允許U登入系統，使用伺服主機資源。否則，拒絕使用者U登入。

■

我們將本文機制的完整流程圖附錄於文後的Appendix A。

【範例】

假設在起始階段S_I已經通過CA的驗証，成為合法的伺服主機。CA並發給S_I一個驗證代碼“8088”。

假設在註冊階段U_I 自選Password=“68115388”，並通過CA的驗証，成為合法的使用者。CA並配給U_I一個PID=“freezewind”。CA再從影像資料庫之中選出一張O_{CA}，如圖5所示。接著運用Torus automorphisms函數將O_{CA}打散成一張混亂的影像，如圖6所示，其中相關參數設定為*i=10 , k=3 , N=191*，藉函數轉換將其轉為子影像圖Share-1，如圖7所示。

使用者登入伺服主機的相互合法性的驗証步驟如下：

步驟一： U_I將智慧卡插入終端機，依卡內存的參數PID=“freezewind”，向S_I提出登入請求。

步驟二: S_I檢查U_I提供之“freezewind”是否為正確之格式，與是否等於S_I所登記之PID相同。若是，則隨即透過U的設定參數*i=10 , k=3 , N=191*，運用Torus automorphisms將內存之O_{CA}轉成(Share-1)' ，如圖7所示。

步驟三： S_I由內建的影像資料庫中，隨機找一張$O_{Si-logo}$ ，如圖8所示。並隨機產生一個亂數值Nounce=“Fz52L96A”與產生現行系統時間T=“2006/01/15-17:02:48”，合併*Nounce*與*T*，製成一張與(Share-1)'同大小之二元像素值影像，再將(Share-1)'應用[1]的方法配合$O_{Si-logo}$產生另一張二元像素值的子圖影像，Share-2，如圖9所示。

步驟四： S_I再從影像資料庫中隨機取出一張灰階圖，O_{si}，如圖10所示。將Share-2轉成二進位碼的型式，並以[11]資料隱藏之文字嵌入方法，將Share-2隱藏入所選擇的灰階圖中，O_{si}，如圖11所示。

步驟五： S_I以MD5計算*H(Nounce, K_i)*=“312D6029980E9416C7C6AD10F6109E40”，將O_{si}'及“312D6029980E9416C7C6AD10F6109E40”回傳給U。

步驟六： U_I經由網路收到的O_{si}'，利用[11]之方法，將所隱藏入之二進位碼萃取出，並還原成Share-2。

步驟七： U_I收到 *H(Nounce, K_i)*後，利用解得的Share-2，將Share-1 和Share-2 疊合，如圖12所示，可產生(Nounce)'=“Fz52L96A”與T'=“2006/01/15-17:02:48”，若確定時戳與現階段系統時間，在可接受時差內後，進一步比對*H((Nounce)', K_i)* 是否等於 S_i 所回傳的“312D6029980E9416C7C6AD10F6109E40”，以鑑定主機合法性。若比對失敗，則U_I登將被拒絕登入。

步驟八： U_I確認主機為合法後，接著運算 *H((Nounce)', PW, K_i)*=“AF5BBDB790113DDC07908547E5927201”，並將結果再傳送給S_I。

步驟九： S_1收到$H((Nounce)', PW, K_i)$後，計算$H(Nounce, PW, K_i)$是否等於U_1所傳過來的“AF5BBDB790113DDC07908547E5927201”。如果是則S_i將允許U_1登入系統，使用伺服主機資源。否則，拒絕U_1登入。若U_1連續三次登入失敗，即封鎖U_1所持有智慧卡的權限。

圖 5：O_{CA}：其為CA從影像資料庫之中選出之灰階圖

圖 6： 混亂影像，由O_{CA}經Torus automorphisms函數轉換而來。

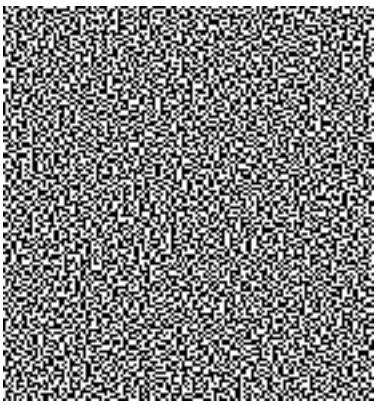


圖 7： Share-1，為經參數設定轉換而來混亂影像

圖 8： $O_{Si-logo}$，可用來偽裝*Nounce*及*T*之二元標記影像來

圖 9： O_{Si}表原灰階圖，目地乃進行偽裝Share-2 之用

圖１０： 0_{si}’ 表將Share-2 嵌入0_{si}後的偽裝圖

圖 11： Share-2：另一張二元像素值的子圖影像

圖 12：Share-1+Share-2 表疊合兩張二子圖影像，可得 *Nounce* 及 *T*

4. 安全性分析與討論

本篇使用[1]及[11]的方法，而達到雙重掩飾的效果。為了避免攻擊者的非法不當截取，本文應用[1]的方法，首先將隨機碼隱藏入我們所傳輸的Share之中，其中此Share是透過另一張有意義的$0_{Si-logo}$偽裝而來的，再將此Share透過[11]的資訊隱藏技巧。如此一來，完全用明文的型式傳輸秘密訊息，一般攻擊者看到一張圖片，並不會加以懷疑，而不會有較劇烈的攻擊行為。如此的方式，不僅具欺騙攻擊者之效果，也達到了資訊安全的目的。但若攻擊者試圖解出其中的秘密訊息，將會遭遇到以下的兩個基本問題。

(1) 如何將隱藏在圖片中每一像素的二進位碼，即Share-2，萃取出，而且如何判斷一個像素中到底隱藏入多少個二進位碼？

藉由[11]的研究中，其資訊隱藏方式為空間域(Spatial domain)形式，並根據每一像素的像素值與門檻值相比較去判斷欲在每一個像素中，取代多少個二進位碼。在所選用的門檻值及預先選定之兩個模組數，有多重選擇變化性，使得讀得所隱藏的像素位置困難度提升，更由於每一像素值不同，取代的位元個數也不盡相同，如此的安排相對減少攻擊者解讀出我們所嵌入秘密訊息，Share-2，的可能性。

(2)若能由影像中猜出秘密訊息的Share-2，但無Share-1如何反向推出真正的隨機碼？

若要以Share-2影像推算出隨機碼或

Share-1影像，依Naor and Shamir[5]分析結果，是不可能達成。就算非法者偽冒進行重送攻擊(Replay attack)，因本系統的處理具金鑰系統的One-time-pad性質，且配合時戳的設計，是可達到防範重送攻擊的效果。

本文應用[1]的 Torus automorphisms 技術，讓伺服主機能對設定參數 i，k，N 作動態的掌握，減少儲存大量影像的管理問題。又在離散二維空間中，因 Torus automorphisms，可以視為是一種排列函數，其具備有一些安全特質，例如無需原圖、設定秘密參數、不固定基準座標，故要猜出秘密的 Share-1 是非常困難的。另外若使用者不慎遺失智慧卡，亦由於非法擁有者無法輸入正確密碼，亦使得偽冒的非法者無法成功。倘使採用暴力法攻擊，在連續三次登入失敗後，立即封鎖此卡的權限，亦使得非法者的入侵機會降低。

在伺服主機方面，由於CA配發不同的識別資料K_i給不同的伺服主機，使得伺服主機具唯一性。因此伺服主機不能偽冒成其他的伺服主機。又在每一次使用者登入的過程中，互相傳遞的訊息$H(\bullet)$都包含有K_i，可視為交互驗證的基本鑑定資料，一旦U與S雙方有爭議，亦可透過CA將K_i解密產生M_i。利用M_i在伺服主機及智慧卡在CA的登入記錄進行比對，以達成不可否認性(Non-repudiation)。

5. Conclusions

本文以智慧卡為使用者嵌入的工具，運用視覺密碼學的技術與資訊隱藏的技巧，提出一個能對遠端使用者身份做確認的系統。有別於目前市面上常見的兩類鑑別系統，我們解密時不須靠電腦作複雜計算，較佳於一般的金鑰密碼系統[2,12]在處理時間及管理上所面臨的問題。而我們所提的環境，並不需精密昂貴的儀器，此部份在生物驗証系統[4,6,7]的比較下，由於較低成本的建置，當然應較為一般使用者登入系統所接受。另外，我們在資料的傳輸過程中，是用雙重掩飾的效果加以保護，並植基於破解視覺密碼的低機率困難度上，因此有較佳的安全保障。最後在應用方面，本文提供一個安全度高，強調個人身份識別，又易於伺服端管理的機制，可作為解決現在日益嚴重的金融卡盜刷問題的另一個有效參考管道。

References

[1] C.C. Chang and R. J. Hwang, "A simple picture hiding scheme," *Computer Processing of Oriental Languages*, vol. 12, no. 2, 1998, pp. 237-248.

[2] C.C. Chang and S. J. Hwang, "Using smart cards to authentication remote Passwords," *Computer Mathematics with Applications*, vol.26, no.7, 1993, pp.19-27.

[3] C.C. Chang and J.C Chuang, "An image intellectual property protection scheme for gray-level images using visual secret sharing strategy," *Pattern Recognition Letters*, Vol.23, 2002, pp.931-941.

[4] E.Gomez, C.M. Travieso, and J.C. Ferrer , "Biometric identification system by lip shape Briceno," *Proceedings of 36th Annual 2002 International Carnahan Conference*, 2002, pp. 39 -42.

[5] M. Naor and A. Shamir, "Visual cryptography," in Eurocrypt'94, *Lecture Notes in Computer Science*, Springer-Verlag, Perugia, Italy, 1994, pp. 1-12.

[6] R. Sanchez-Reilla, C. Sanchez-Avila,and L.Mengibar-Pozo, "Microprocessor smart cards with fingerprint user authentication," in *Proceedings of the 36th Annual 2002 International Carnahan Conference*, 2002, pp. 46 -49.

[7] R. Sanchez-Reillo, C.Sanchez-Avila, "Multiscale analysis for iris biometrics," *Proceedings of 36th Annual 2002 International Carnahan Conference*, 2002, pp. 35 -38.

[8] M. J. Tsai, K. Y. Yu and Y. Z. Chen, "Joint wavelet and spatial transformation for digital watermarking," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, February 2000

[9] G. Voyatzis and I. Pitas, "Chaotic mixing of digital image and applications to watermarking," *Proceedings of European Conference on Multimedia Applications, Services and Techniques (ECMAST '96)*, vol. 2, May 1996, pp. 687-695.

[10] G. Voyatzis and I. Pitas, "Embedding robust watermarks by chaotic Mixing," *Proceedings of 13th International Conference on Digital Signal Processing (DSP '97)*, vol. 1, 1997, pp. 213-216.

[11] S.J. Wang and K.S. Yang, "A scheme of high capacity embedding on image data using

Modulo Mechanism," *Proceedings of The Second International Workshop on Information Security Applications (WISA),* Korea, Sept., 2001, pp. 299-309.

[12] T.C. Wu, "Remote login authentication scheme based on a geometric approach," *Computer Communications* Vol.18, No.12, 1995, pp.959-963.

[13] 張真誠、黃國峰、陳同孝，*電子影像技術*，台北市：松崗，2001 年 2 月，頁 271-273。

[14] 賴溪松、韓亮、張真誠, *進代密碼學及其應用*，台北市：松崗，2001，頁 3-6。

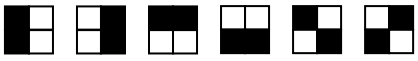
影像	機密影像（白）	機密影像（黑）
Share1		
Share2		
疊合結果		

圖 1：在[5]裡疊合可能產生的結果

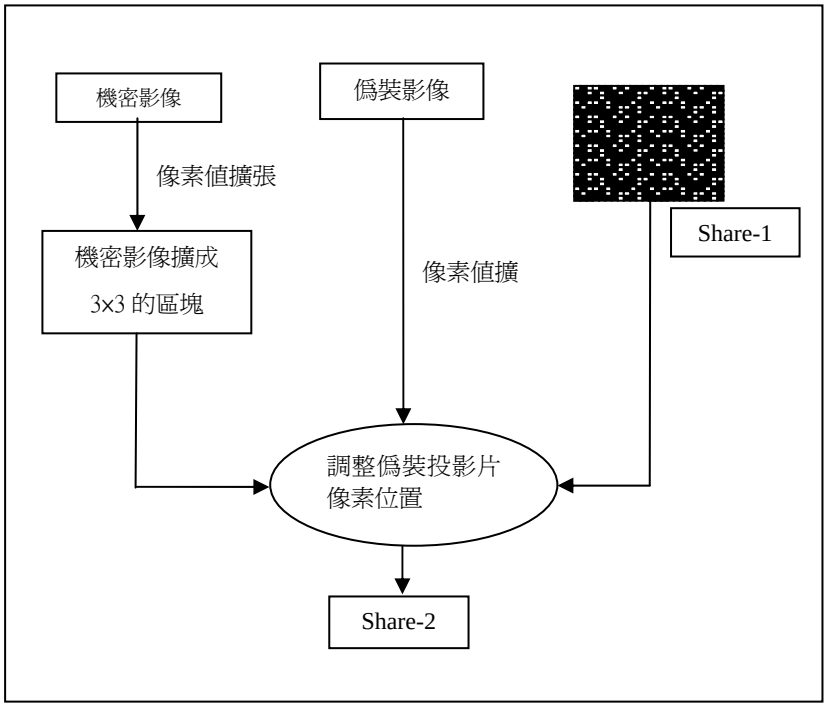


圖 3：Chang and Hwang 方法[1]的流程示意圖

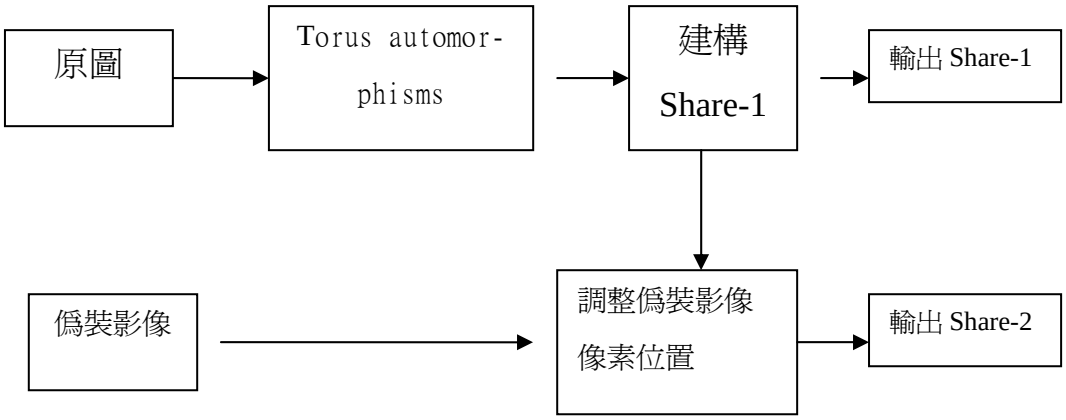


圖 4：Chang 和 Chuang 方法[3]流程示意圖

Appendix A

使用者登入系統鑑定機制流程圖