臺灣二００八年國際科學展覽會

科　　別：電腦科學

作 品 名 稱：不能說的秘密---網路釣魚防治技術

學校 / 作者：臺中市私立衛道高級中學　　蔡昕潔
　　臺中市私立衛道高級中學　　蔡昕霓

作者簡介

我的名字叫做蔡昕潔。

從小,我就對電腦充滿了好奇心，玩電腦時，總會有一種說不出的快樂，尤其是在當你發現了一個新功能後，那感覺總是深深吸引著我！

很開心有機會參加這次的科學展覽，讓我能更進一步踏入電腦的殿堂，並學習和應用到許多在課堂上所學到的知識，獲得了很多快樂與成就。要謝謝老師不辭辛勞的指導，以及同學一路上的幫忙，才能將這份作品成功地展現！

作者簡介

我是蔡昕霓。

或許是因爲環境的關係，在很小的時候就有機會開始接觸電腦，且從此就愛上它了！它吸引人之處不只是可以連接網路，上網了解全世界的資訊，或者進入部落格的世界，它還可以利用程式設計出對我們有幫助的系統，促進生活及工作上的便利。因此一直以來自己很渴望能學習電腦有關的知識，且希望能學以致用。期待藉由參加本次科學展覽的機會，來充實自己。

摘要

在數位化的今日，由於網際網路的技術蓬勃發展，網際網路變得更容易使用及具高度的親和性，使得網際網路的使用逐年成長。隨著越來越多人依賴網路進行交易，也衍生了層出不窮的網路詐騙問題。其中，網路釣魚就是一項著名的詐騙技術：詐騙者透過僞裝成知名企業的網站，藉此騙取使用者的個人私密資料。在本研究中，我們提出了一套植基於彩色視覺密碼學原理的網站驗證機制，使用者可以透過此機制，直接利用人類視覺的方式來驗證所連上的網站是否有問題，並在此機制之下，設計出另一套管理使用者密碼的方式，進而方便使用者不必費心的去記憶密碼。

關鍵詞：視覺密碼學、網路釣魚

Abstract

Recently, as networks technology flourishes, Internet becomes easier and friendlier to use, and makes the usage of Internet grow up year after year. With more and more people relying on online transactions, it leads to endless network fraud issues. Among them, phishing is a well-known fraud technology to disguise the famous business website to get user's private information by cheating. Therefore, in this study, an effective scheme based on color visual cryptography is proposed to test and verify the website. Through the proposed mechanism, users can check whether there is a problem website by using human vision directly. Furthermore, the proposed scheme also provides another way to manage user's password effectively.

Keywords：Visual cryptograph, phishing

壹、 研究動機及目的

近十年來，網際網路的使用日漸普及，上網的人口自 1998 年的 301 萬人激增至 999 萬人，上網的普及率更達到 44%[1]。除了瀏覽資訊及收發電子郵件之外，越來越多的網路使用者透過網際網路進行線上購物、網路拍賣…等等應用。同時，利用網際網路的即時性及便利性，線上轉帳及信用卡交易也是眾多人使用的熱門功能。但是上述的服務大部份都需要使用者藉由輸入帳號及密碼的方式，登入至提供服務的網站後，再使用所提供的服務。伴隨而來的就是網路使用者會面臨到網路詐騙問題[3-4]，詐騙者通常會利用垃圾郵件或是僞裝網站的方式，進而取得使用者的個人資料，像是登入網站用的帳號、密碼、信用卡號、通訊相關資料等，令網路的使用存在許多風險。

針對上述的現象，若是能夠在使用者登入網站時，利用一套機制先行對網站進行驗證，並且網站在通過驗證的同時，即可讓使用者進行登入的動作。在此，我們引用了一套在密碼學界發展成熟的技術-視覺密碼學，作爲本研究的核心技術。透過此項技術，希望不僅可以達到網站驗證的目的，更能夠幫助使用者記憶密碼，讓使用者能在茫茫網海中用有效且安全的方式管理自己的密碼，並提供在網際網路的使用上多一層的保護降低被“駭”的風險。

貳、 研究過程及方法

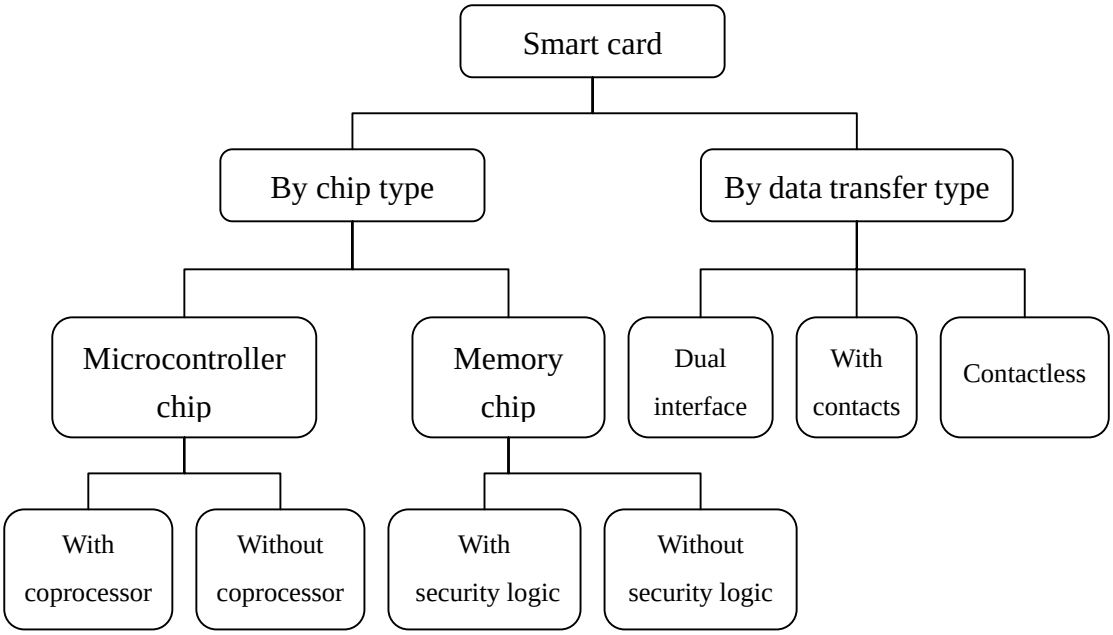
首先，我們將對網路詐騙中的網路釣魚技術作明確的定義，並且針對使用者儲存密碼的媒介-IC 智慧卡進行簡單的介紹，接下來將針對核心技術---視覺密碼學的加密及解密方式分別進行說明，最後，整合上述議題，提出本研究的主要架構。

一、 網路釣魚(Phishing)

網路釣魚主要是詐騙者利用發送垃圾郵件的方式來騙取網路使用的個人相關資料[3-4]。和一般垃圾郵件所不同之處在於，網路釣魚發送的垃圾郵件內容多半是以知名的企業網站名義，並以「定期更新密碼」、「帳號被鎖定，請上網解除」、「更新使用者個人資料」等訊息並且隨後附上連結網址，請使用者連上網站。然而，若利用該網址連上網站，則會出現一個和原企業網站相仿的僞裝網站，若使用者將自己的帳號及密碼登入該網站，則相關的資料就會落入至詐騙者的手中，令使用者防不勝防。

二、 IC 智慧卡(Smart Card)

IC 智慧卡也就是俗稱的晶片卡，通常在晶片當中包含了微處理器、記憶體及 IO 介面，以提供資料的計算、儲存及存取的功能[2]。而 IC 智慧卡的特色在於提供資料存取的安全控管，若是具有微處理器的卡，更可在卡中進行資料的加密及解密，提高資料的安全性。目前國內常見的全民健康保險卡、晶片金融卡、悠遊卡（EasyCard）、台中 e 卡通等都是屬於 IC 智慧卡的一種。IC 智慧卡的分類可如圖一所示[7]。若依照晶片類型，可分爲具微處理器及只有記憶體二類；若依照資料的傳輸方式，可分爲混合式、接觸式及非接觸式三類。除了上述的應用之外，更可根據需求，選擇不同類型的 IC 智慧卡並將所需應用程式燒錄其中以達不用層面的應用。



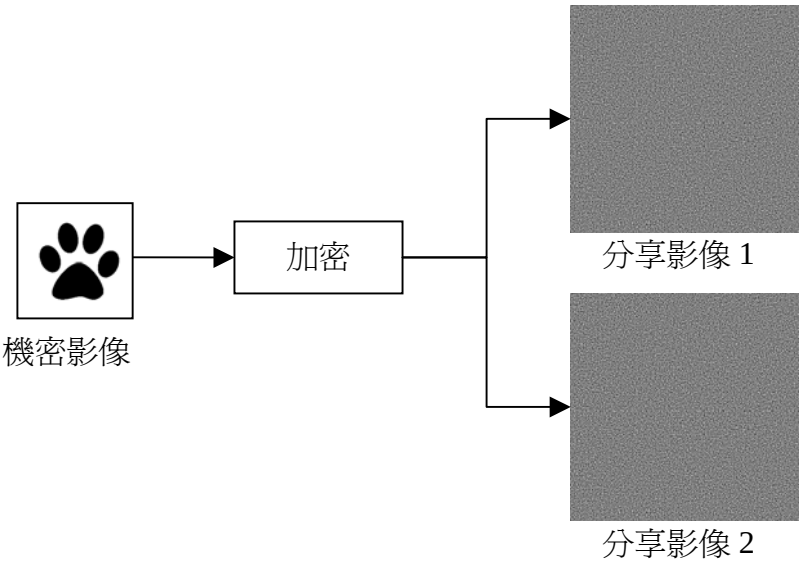
圖一 IC 智慧卡分類

三、 視覺密碼學(Visual Cryptography)

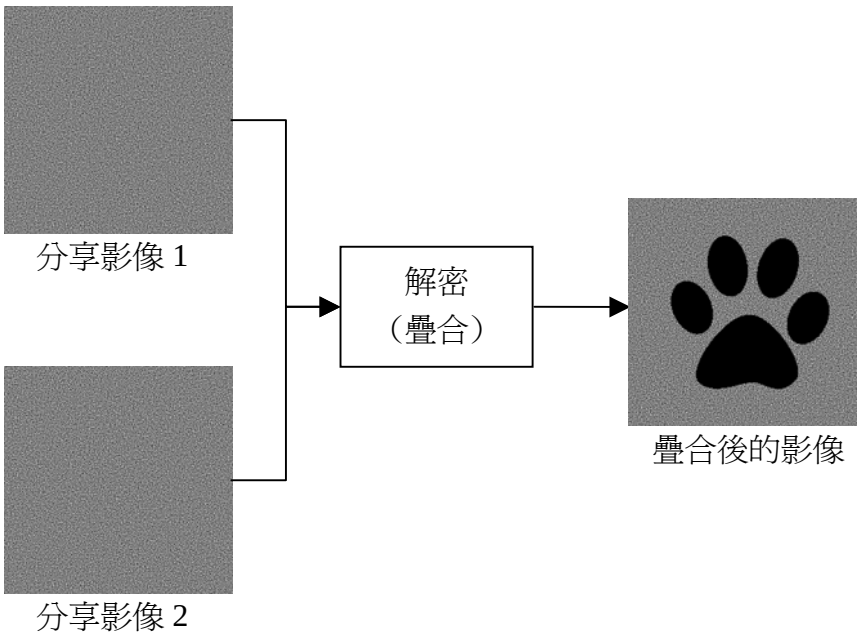
Naor 與 Shamir 二位學者於 1994 年提出了第一個視覺機密分享技術(visual secret sharing)，也稱之爲視覺密碼學(visual cryptography)[6]。此技術是建構在(*k*, *n*)門檻式的視覺機密分享技術，最大的特色在於機密的訊息在解密的過程中不需複雜的運算，只需利用人眼視覺系統即可解密。其方法主要的概念在於將一張機密影像(secret image)利用加密流程產生 *n* 張的分享影像(share image)，在解密的過程中只需將 *k* 張分享影像疊合(其中 $k \leq n$)，即可還原機密影像。若是分享影像疊合的張數小於 *k* 張時，則無法還原機密影像。而其另一個特色在於加密後所提供的高安全性，因爲很難從任一張分享影像中推算出機密影像的資訊爲何，此技術兼具高安全性及低計算複雜度的特色。

首先，以(2,2)門檻視覺機密分享技術來說明 Naor 及 Shamir 二位學者的方法。其加密及解密的流程如圖二所示。假設有一張 $N_1 \times N_2$ 的二元機密影像，其中該影像的每一個像素在加密過程中皆會被擴張成一個由 2x2 像素所構成的區塊，每一區塊皆會由 2 個白色像素及 2 個黑色像素所組成，其黑白像素組合如圖三所示。每一個像素根據其顏色皆會產生二個區塊，分別屬於分享影像 1 及分享影像 2。當要呈現白色像素時，則二區塊疊合後會產生 2 黑 2 白的效果，如圖四(a)；若要呈現黑色像素，則二區塊疊合後會產生全黑的效果，如圖四(b)。藉由圖三的不同組合及圖四的定義，即可設計出一個編碼表，如表一。接下來，只需針對機密影

像中的每一個像素，對照其顏色並且從中任意挑選一欄作爲分享影像 1 及分享影像 2 的區塊，即可產生二張分享影像。由於每一個像素皆會及擴大 2x2 倍，所以一張 $N_1 \times N_2$ 的二元機密影像會被加密成爲二張 $2N_1 \times 2N_2$ 的分享影像。另外，因爲分享影像的每一區塊皆是由 2 黑 2 白所組成，所以無法從中發現原機密影像的像素是黑色或是白色，因此可確保其安全性。

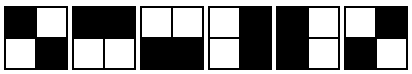


(a) 加密流程

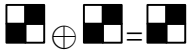


(b) 解密流程

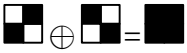
圖二 加密及解密流程



圖三 各區塊組合圖



(a) 白色像素疊合後的結果



(b) 黑色像素疊合後的結果

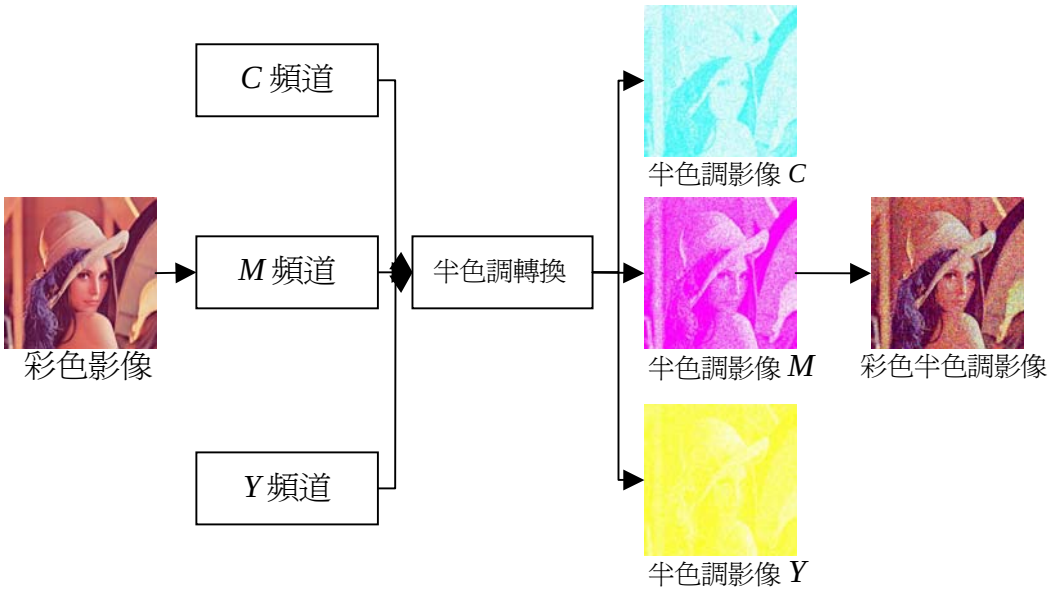
圖四 像素疊合示意圖

表一 編碼表

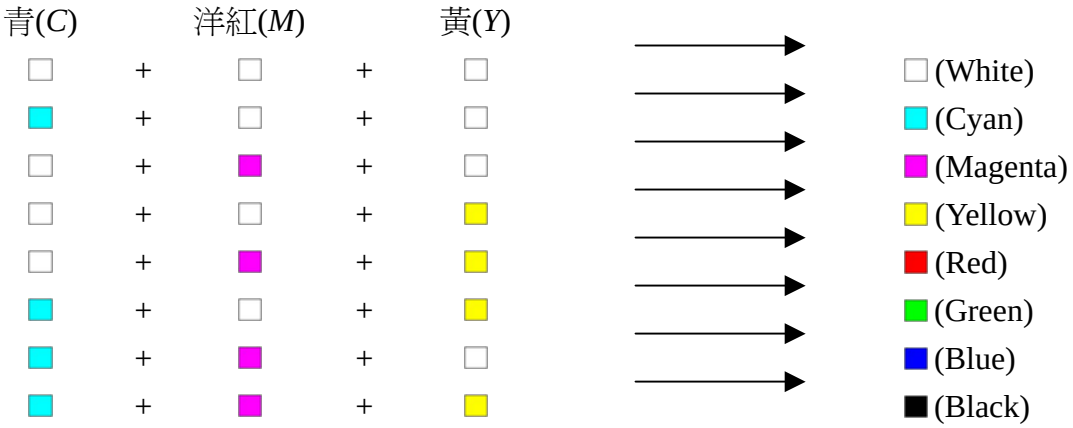
機密像素	□						■					
分享影像 1												
分享影像 2												
疊合後結果												

四、 彩色視覺機密分享技術[8]

針對機密影像爲彩色影像時，侯永昌教授提出了利用像素擴張的彩色視覺機密分享技術[8]。此方法會利用半色調技術將具有16,777,216色階的彩色影像轉換成由8色階的彩色半色調影像。其流程如圖五所示，首先會將彩色機密影像分解成爲青、洋紅及黃色三個頻道的影像，再分別針對各頻道的影像進行半色調轉換，最後將三個頻道的半色調影像利用減色模式原理合併爲一張彩色半色調影像，合併後的彩色色調影像根據減色模式的原理，將會由白色、青色、洋紅色、黃色、紅色、綠色、藍色及黑色八種顏色所組成。圖六爲三個頻道的半色調影像合併時所產生的各種顏色組合。由於合併後的彩色半色調影像在視覺的呈現上和原彩色影像相似，因此，此方法會利用此彩色半色調影像進行加密的處理。



圖五 彩色影像半色調轉換



圖六 色彩混合

以下將說明侯永昌教授所提出的彩色視覺機密分享的其中一個方法，此方法將一張尺寸爲$N_1 \times N_2$的彩色半色調機密影像，如圖七(a)。透過表二的編碼表產生二張尺寸爲$2N_1 \times 2N_2$的分享影像，分別爲分享影像1及分享影像2，如圖七(b)及圖七(c)。透過二張分享影像的疊合，即可還原彩色機密影像，如圖七(d)。此方法中，每一個機密影像的像素皆會擴張爲由2×2像素組成的區塊，而區塊中皆由青色、洋紅色、黃色及白色四個顏色像素所組成，藉由分享影像1及分享影像2中區塊內顏色像素的排列，可疊合近似於機密影像像素的其中一種顏色，其顏色的定義如表二所示。

假設彩色半色調機密影像某一位置像素顏色爲洋紅色，對照表二，即可在表中第4列中找出屬於分享影像1及分享影像2的區塊，分別爲 及 。之後藉由分享影像1及分享影像2區塊的疊合，即可重建區塊 。

表二 編碼表

機密像素	分享影像 1	分享影像 2	還原後的機密影像
(White)			
(Cyan)			
(Magenta)			
(Yellow)			
(Red)			
(Green)			
(Blue)			
(Black)			

(a) 彩色半色調機密影像

(b) 分享影像 1

(c) 分享影像 2

(d) 還原後的機密影像

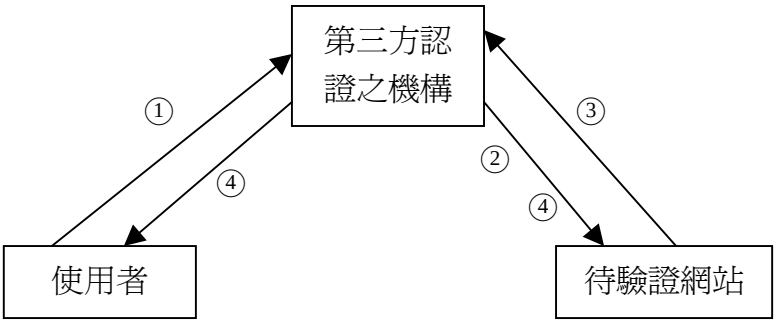
圖七 彩色視覺機密分享技術的一個例子

五、 研究方法

本研究的方法主要可分爲二大主要架構，第一個架構是使用者建立/變更密碼，此部份主要是使用者透過由第三方認證的機構[5]利用視覺密碼學的技術將使用者的密碼加密爲二組分享影像，並將一組分享影像交給使用者，另一組交給待驗證網站管理。若是使用者需變更密碼的話，一樣是需要透過此機構來變更密碼。第二個架構則是網站驗證，此部份主要是透過二組分享影像的疊合，若能成功解密，則表示此網站通過驗證。本研究的目的是希望能夠透過此機制來有效預防網路釣魚的情況發生，萬一使用者不小心點選垃圾郵件中的網址，在此機制的運作之下，也能夠避免帳號及密碼被騙取。另外，由第一個架構所產生使用者所屬的分享影像，可將其資料儲存於 IC 智慧卡中，藉此提高可攜性及安全性，並且降低資料毀損的風險。

1. 使用者建立/變更密碼

在進行使用者建立密碼階段，有一項假設必須一定要成立，也就是使用者已事先在待驗證網站建立了自己的帳號及密碼，並且待驗證網站會在使用者建立完成資料後，告知使用者第三方認證之機構的資訊。有了上述的假設之後，接下來就可根據圖八的流程，建立屬於使用者的視覺密碼了！



圖八 使用者建立/變更密碼流程圖

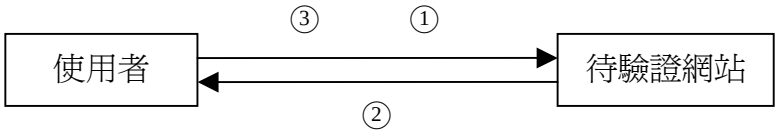
首先，使用者利用待驗證網站所提供的資訊至第三方認證之機構中，該機構可以是網站或是其它實體的單位。使用者必須提供自己的帳號、IC 智慧卡的識別碼及密碼供第三方認證之機構參考(步驟 1)。接下來，第三方認證之機構會通知待驗證網站，並請該網站提供有關使用者的相關資料進行核對(步驟 2、3)。核對無誤後，第三方認證之機構會將使用者的密碼，

利用視覺密碼學技術加密成爲二組分享影像，一組交給使用者，另一組及 IC 智慧卡的識別碼交給待驗證網站(步驟 4)。屬於使用者的分享影像會直接存入至 IC 智慧卡中；而屬於待驗證網站的分享影像則存入該網站所屬的資料庫當中。如此，即完成了建立密碼的動作。

若是使用者需要變更密碼的話，只要至第三方認證之機構中將自己的帳號、IC 智慧卡的識別碼、IC 智慧卡中的分享影像及要變更密碼提供給第三方認證之機構參考(步驟 1)。由於已知分享影像及變更密碼，所以第三認證之機構可利用使用者的分享影像作爲基底配合新密碼來產生另一組分享影像，再將此影像傳送至待驗證網站中儲存(步驟 2)，利用已知的分享影像來產生另一組分享影像，將可以有效的節省資料寫入 IC 智慧卡的時間。

2. 網站驗證

在完成使用者建立/變更密碼後，使用者就可以利用自己的帳號、密碼及手中的 IC 智慧卡進行網站驗證的動作了。網站驗證主要有三個步驟，其流程如圖九所示。



圖九 網站驗證流程圖

首先，使用者連上待驗證網站並提供 IC 智慧卡的識別碼及分享影像(步驟 1)，待驗證網站接收到使用者的資訊後，可透過識別碼找到另一組分享影像，並且將二組分享影像的疊合結果回傳至使用者(步驟 2)。此時使用者接收到驗證網站所傳回的疊合結果後，即可以視覺的方式驗證該網站是否爲通過驗證，此時，使用者就可放心的輸入自己的帳號及密碼進行登入的動作(步驟 3)。若是網站無法通過驗證，則代表該網站可能爲釣魚網站，使用者不能輕易的輸入自己的登入帳號及密碼。

附帶一提，在密碼上的應用，使用者可在建立密碼階段自行決定要使用和登入用的密碼相同或是其它密碼(驗證密碼)，使用登入密碼的好處在於，使用者不用特別的記憶該組密碼，因爲密碼會在分享影像疊合後解密傳回，所以只需要在驗證成功後，連同登入帳號一同輸入即可；而使用驗證密碼的好處在於，提供了多一層的安全性，驗證密碼用於驗證而登入密碼則用於登入網站。

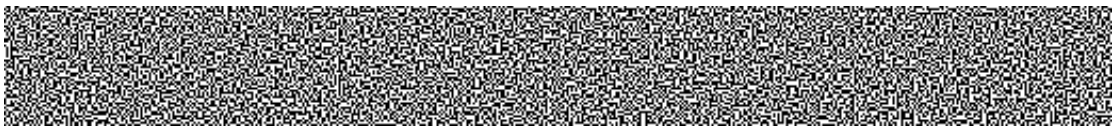
參、 研究結果與討論

研究結果部份，我們將以模擬實驗的方式來達到網站驗證的目的，實驗中，定義使用者的帳號爲 user，密碼爲 ntsec2008；待驗證網站的網址爲 http://www.yahooooo.com.tw；第三方認證之機構則以網站的方式呈現，其網址爲 http://www.tpa.com.tw。在模擬的實驗中，會進行僞裝網站攻擊，讓使用者連上僞裝網站並且對該網站進行驗證的動作，僞裝網站的網址爲 http://www.yahooooooo.com.tw，其中，網址內的一個英文字母 o 由 5 個被改爲 6 個藉此讓使用者無法查覺。在 IC 智慧卡部份，我們將利用 USB 介面的隨身碟模擬使用者 IC 智慧卡並以長度爲 512bits 的隨機字串作爲 IC 智慧卡的識別碼。而在分享影像大小，我們設爲 520×56 像素。以下將用三個部份來說明我們的模擬實驗。

一、使用者建立/修改密碼

此部份主要是要讓使用者可透過待驗證網站所提供的第三方認證之機構的網址建立使用者自己的密碼，圖十爲使用者建立密碼可看到的頁面，一開始網站會讀入 IC 智慧卡的識別碼並顯示於頁面中(在此爲隨身碟中的隨機字串)，並且要求使用者輸入帳號及密碼來建立分享影像。在送出資料後，該網站會產生四張分享影像，如圖十一。圖十一(a)及(b)爲使用者所屬的分享影像，會存入於使用者的 IC 智慧卡(在此爲隨身碟)，圖十一(c)(d)爲待驗證網站所屬的分享影像，會傳回待驗證網站進行管理。

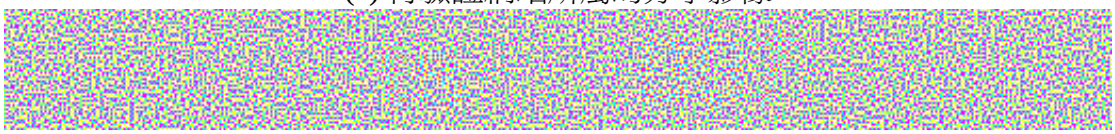
圖十 建立密碼頁面



(a) 使用者所屬的分享影像

(b) 使用者所屬的分享影像

(c) 待驗證網站所屬的分享影像



(d) 待驗證網站所屬的分享影像

圖十一 第三方認證之機構所產生的分享影像

圖十二爲使用者修改密碼時可看到的頁面，其流程和建立密碼大同小異，一開始網站會讀入 IC 智慧卡的識別碼並顯示於頁面中(在此爲隨身碟中的隨機字串)，接下來要求使用者載入自己的分享影像(在此爲隨身碟中的分享影像)並且輸入帳號及密碼。在送出資料後，該網站會根據使用者所載入的分享影像來產生另一組分享影像，並且會將這組新的分享影像傳回待驗證網站進行管理。

圖十二 修改密碼頁面

二、網站驗證

此部份主要是要讓使用者連上待驗證網站後，可載入自己的分享影像，來驗證網站，圖十三所示。在圖十三(a)中，使用者首先必須從 IC 智慧卡中載入分享影像(在此爲隨身碟中的分享影像)。待載入完成後，待驗證網站會從利用使用者的 IC 智慧卡識別碼(在此爲隨身碟中的隨機字串)從網站資料庫中找出對應的一組分享影像，並且將使用者載入的分享影像和網站資料庫中分享影像進行解密的計算，並將結果顯示如圖十三(b)之頁面。若是解密的結果爲使用者所設立的密碼，則代表該網站通過驗證，使用者可放心輸入自己的帳號及密碼進行登入的動作。

(a) 載入分享影像頁面

(b) 驗證結果頁面

圖十三 網站驗證頁面

三、僞裝網站攻擊

此部份主要是模擬要讓使用者連上僞裝網站後可利用本研究所提出的機制進行驗證。圖十四(a)爲僞裝網站所建構的分享影像頁面，主要流程和網站驗證部份相同，唯一不同的是，在圖十四(b)中，可以發現驗證結果所呈現的內容並非使用者當初所建立的密碼，如此就可知道此網站無法通過使用者的驗證，是一個僞裝的網站，使用者大可不必輸入自己的帳號及密碼，以避免資料洩漏危機。

(a) 僞裝網站的載入分享影像頁面

(b) 僞裝網站的驗證結果頁面

圖十四 僞裝網站驗證頁面

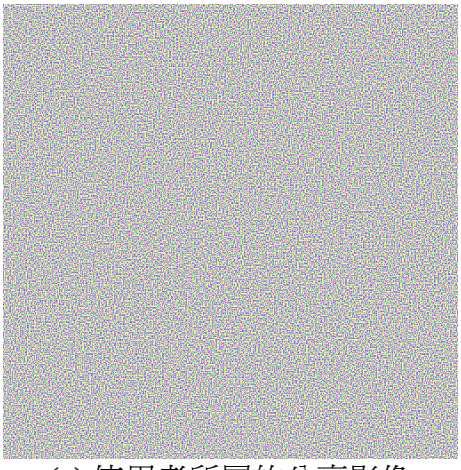
四、延伸應用

彩色視覺密碼學的分享影像除了可作爲彩色密碼的驗證之外，我們也可利用彩色視覺密碼學可呈現多種色彩的特性，單獨進行應用。在此我們使用一張 256x256 像素的彩色影像來表示使用者的身份，如圖十五(a)。圖十五(b)爲經過半色調處理的彩色影像，圖十六(a)爲使用者所屬的分享影像，圖十六(b)爲待驗證網站所屬的分享影像。其主要流程和網站驗證部份相似，使用者在連上待驗證網站後，可載入自己的分享影像，利用自己的身分作爲密碼對網站進行驗證，圖十七所示。在圖十七(a)中，使用者首先必須從 IC 智慧卡中載入分享影像(在此爲隨身碟中的分享影像)。待載入完成後，待驗證網站會從利用使用者的 IC 智慧卡識別碼(在此爲隨身碟中的隨機字串)從網站資料庫中找出對應的一組分享影像，並且將使用者載入的分享影像和網站資料庫中分享影像進行解密的計算，並將結果顯示如圖十七(b)之頁面。若確定是自己的身份無誤，則代表該網站通過驗證，由於待驗證網站存有使用者的相關資訊，所以使用者可直接進行登入。

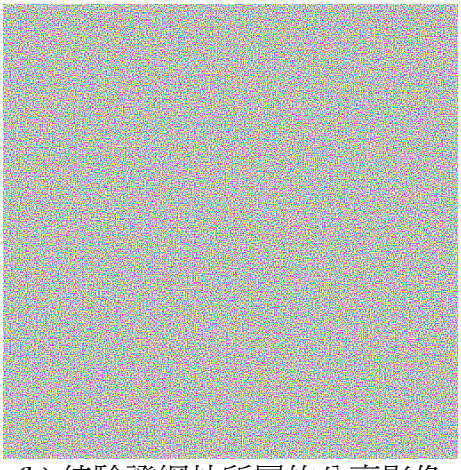
(a) 代表使用者身份的彩色影像

(b) 將使用者身份影像進行半色調轉換後的結果

圖十五 使用者身份影像

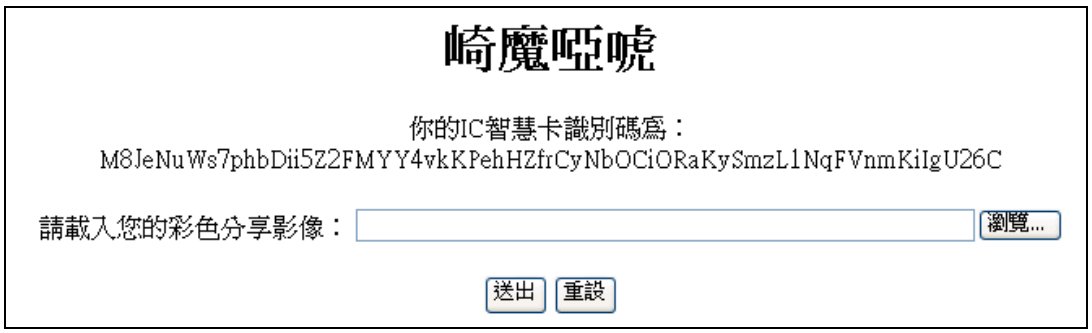


(a) 使用者所屬的分享影像



(b) 待驗證網站所屬的分享影像

圖十六 彩色分享影像



(a) 載入分享影像頁面

(b) 驗證結果頁面

圖十七 利用身份進行網站驗證頁面

肆、 結論與應用

本研究提出了一套植基於視覺密碼學的網站驗證機制，用於防範網路釣魚對使用者所帶來個人資料的損失。透過我們的方法，使用者可以輕易的以人類視覺的方式驗證所連上的網站是否爲僞裝網站。此外，本研究所附帶的另一個好處在於可以有效的幫助使用者進行密碼的管理，使用者只需透過自己的 IC 智慧卡連上驗證正確的網站，即可以視覺的方式得知自己的密碼，而不用特別費心去記憶當初自己所設立的密碼爲何。本研究所提出的網站驗證機制，特別適合用於金融機構的相關網站，此類機構通常需要進行大量的網路金融交易，因此在網站的驗證上，更是需要多一道防線來幫助使用網路的客戶，以免因爲連至有問題的網站而造成重要資料被竊取。

伍、參考文獻

[1] http://www.find.org.tw/find/home.aspx?page=many&id=180

[2] http://aca4.saihs.edu.tw/pps/download/9402jour.pdf

[3] http://taiwan.cnet.com/enterprise/features/0,2000062876,20090588-4,00.htm

[4] http://taiwan.cnet.com/enterprise/technology/0,2000062852,20087713,00.htm

[5] http://blog.roodo.com/orz0121/archives/329976.html

[6] M. Naor and A. Shamir, “Visual Cryptography, Advances in Cryptography: Eurpocrypt'94,” *Lecture Notes in Computer Science*, Springer, Berlin, Vol. 950, 1995, pp. 1-12.

[7] W. Rankl and W. Effing, “Smart Card Handbook,” Second Edition, Feb. 2001, also available at http://www.wired.com/news/technology/0,1282,12459,00.html.

[8] Y. C. Hou, “Visual Cryptography for Color Images,” *Pattern Recognition*, Vol. 36, No. 7, 2003, pp. 1619-1629.

評語

主題不具創新性。給予以下之建議：

- 所提之方法與一般「私鑰演算法」之差異處爲何？
- 所提演算法應可做複雜度（運算）的評估。
- 如何證明所提之演算法的安全性強度。