行動裝置上的視覺認證

Visual Authentication on Mobile Devices

徐熊健
銘傳大學
資訊工程學系
sjshyu@mail.mcu.edu.tw

黃昱霖
臺北市立教育大學
資訊科學系
shiningmosquito@gmail.com

莊竣傑
銘傳大學
資訊工程學系
hellion0724@gmail.com

賴阿福
臺北市立教育大學
資訊科學系
lai@tmue.edu.tw

***摘要*—視覺認證在 1997 年由 Naor and Pinkas 首先提出，他們點出使用視覺密碼機制在認證需求上弱點；進而以結合視覺密碼機制和運算加密技巧的機制來完成視覺認證。本論文提出一個簡單的雙機密視覺機密分享機制來實現視覺認證，無需額外的運算加密演算法。我們的機制擁有低科技與高可攜帶性的優點，使認證能透過視覺有效的完成。藉由應用我們的方法在一個使用先進手機裝置的簡易電子付款場景做驗證，展現我們的理念是可行的。**

***關鍵詞*—視覺認證、視覺密碼、雙機密視覺機密分享，認證，手機。**

***Abstract*-The notion of visual authentication was first devised by Naor and Pinkas in 1997. They addressed that a straightforward application of a naïve visual cryptographic scheme in the authentication requirement is vulnerable and proposed a scheme incorporating visual cryptography with an additional encryption algorithm to achieve visual authentication. We develop a simple visual two-secret sharing scheme, without any other encryption algorithm, to accomplish the same goal in this paper. Our approach possesses the advantages of low-technology and portable which enable the authentication to be validated in a visual sense. A simple scenario of utilizing our scheme in the authentication phrase of E-payment via modern mobile cell phones is designed to show the feasibility of our ideas.**

***Keywords*-Visual authentication, visual cryptography visual two-secret sharing, authentication, cell phone.**

一、簡介

視覺密碼的概念與理論是由Naor 與 Shamir 在1995年所提出 [6]。在編碼階段利用表一中黑點和白點的編碼基本模型，將機密影像的各個像素加密成兩組雜亂無序的分享區塊；解密時，僅需將這兩組分享區塊進行疊合，即可由我們的視覺系統判讀出原機密像素。

表一、Naor 和 Shamir 視覺密碼基本模型

Secret pixel	Share 1	Share 2	Superimposed
□	□■	□■	□■
	■□	■□	■□
■	□■	■□	■■
	■□	□■	■■

機密影像上各像素的編碼基本模型可表示成 2×2 的 M_0 和 M_1 基本矩陣如下，分別供白點和黑點使用：

$$M^0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \quad M^1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

每個白（黑）像素皆透過 M_0 (M_1) 做欄的隨機排列後，將其矩陣元素做為兩分享影像對應區塊的編碼像素值；俟所有像素如是編碼後，得到的兩分享影像即為雜亂無序的影像，以投影片列印後，分送給機密分享者。由於白（黑）編碼區塊疊合後，會得到一黑一白（二個皆黑）的兩個像素，人類視覺系統會分辨出此差異，遂可在投影片疊合的結果上，看出原機密影像的黑白區域，得知原來的機密訊息。

1997 年 Naor and Pinkas [5] 描述了直接採用視覺密碼機制於電子錢包 (electronic wallet) 應用時，會產生驗證時安全性上的漏洞；於是提出採用視覺密碼為基準，配合加密演算法的運算處理，透過分享影像疊合後的結果，以視覺判讀做為付款驗證，實現認證的需求，稱之為「視覺認證」 (visual authentication)。

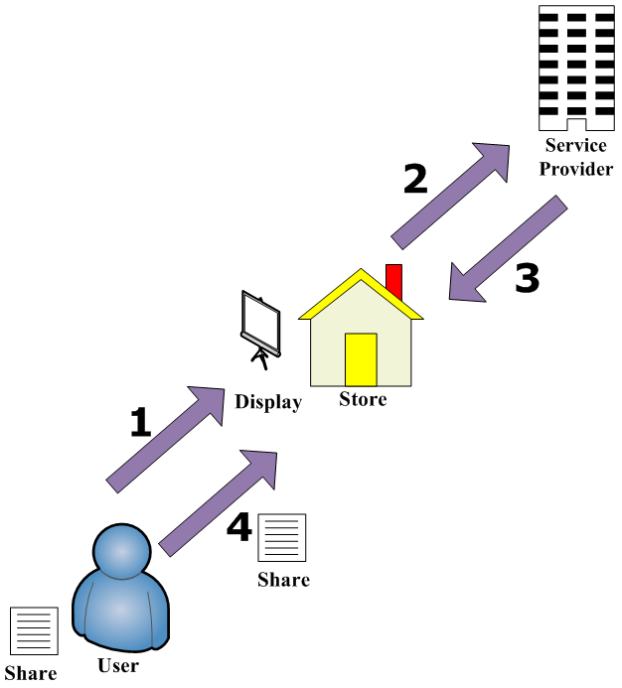
Naor and Pinkas 提到的視覺認證電子錢包交易流程是在 POS (point of sales) 連線系統下完成，如圖一所示。在電子錢包服務啟用後，每一使用者會持有其智慧卡 (smartcard) 與唯一的雜亂分享影像 S_2，系統業者則可自智慧卡資訊，查訊得此 S_2；這些資訊建立於使用者與系統業者之間，商家無法得知。其交流程如下：

步驟 1：使用者選購物品後持智慧卡至櫃台結帳；

步驟 2：商家依使用者購物總金額 M 與其智慧卡，透過 POS 向系統業者請款；

步驟 3：系統業者依智慧卡資訊得知 S_2，將 M 和 S_2 編碼出另一分享影像 S_1，傳送到商家的 POS 螢幕上顯示；

步驟 4：使用者持 S_2 和商家 POS 螢幕上的 S_1 疊合，驗證消費金額 M 是否正確；若正確，則輸入智慧卡密碼，同意商家該次請款。



圖一、電子錢包交易流程圖 [5]

會產生安全性漏洞的地方在於步驟 2 及 3，商家可能更改請款金額（由 M 改為 M'），將 M' 和 S_2 送至系統業者；俟取得 S_1' 時，依前述的基本視覺密碼機制，由(M', S_1', S_2)，解得 S_2; 再用 M 與 S_2，編出 S_1；將 S_1 呈現在 POS 螢幕上，欺騙使用者；因為使用者會用其 S_2 與螢幕的 S_1 疊合看到 M，而同意商家的請款；但商家請款的金額實為 M'！使用者著實受騙也。

他們採用的解決方法是配合加密演算法的運算處理，而商家無法得知此運算函式，只有業者與使用者知道，這些運算是透過人類即可計算，不需再額外使用電腦計算。分享影像疊合後的結果已不再是購物總金額，而是運算後的結果。由於商家無法得知整個運算的流程，所以也無法利用分享影像之間的關聯性來欺騙使用者。

但是我們認為這「人為的計算」，仍然是一種額外的負擔；而且對老幼使用者、或無法全然避免的計算錯誤等因素，依然不方便、不完

善。

由於視覺密碼技術在解密階段不需軟硬體設備，僅需透過人眼即可解密；是個簡易、低成本、可攜性高的機制。後來有幾位學者也利用視覺密碼,在其它環境中做不同的驗證應用，例如 Hegde 等人提出了一個透過視覺密碼做銀行簽名驗證的機制 [2]；然而他們仍需電腦做簽名實例與簽名範本的比對。Rao 等人利用視覺密碼技術應用在指紋驗證系統中[7]；其中需要額外的加密計算。

在本篇論文中，我們提出一個雙機密視覺機密分享機制 (visual two-secret sharing scheme) 來實現視覺驗證。此機制無需再引用額外的加密演算法；而且擁有理想的安全性，即擁有其中一張分享影像，要猜出兩個機密的機率，與盲目猜的機率是一樣的。本文其餘內容架構如下：第二節介紹一些已被提出的雙機密視覺機密分享機制；第三節描述我們所提出的雙機密視覺機密分享機制；第四節是電子錢包在手機上交易的場景中，以此機制實作視覺驗證的實驗結果；最後第五節是結論與未來發展方向。

二、雙機密視覺機密分享機制的相關研究

Wu 和 Chen 倆人在 1998 年提出了一個利用視覺密碼分享兩個機密的方法 [1]。他們把兩機密影像 P_1 與 P_2 編碼成兩張正方形分享影像 A 與 B，P_1 可藉由 A 和 B 疊合而看到；而 P_2 則可經由 A 旋轉 90（180 或 270）度後，疊上 B 而看到。

Wu-Chen 方法在旋轉角度上有限制。此限制在 2005 年由 Wu 和 Chang，以圓形分享影像的編碼方式獲得解決[9]—即機密影像會編碼成兩張圓形的分享影像。而 Ulutas 等人於 2008 年亦指出 [8]：Wu-Chen 方法在分享機密影像 A 上的雜亂程度 (randomness) 較低。Hsu 等人則提出了使用圓柱分享影像的概念，實現雙機密視覺機密分享 [4]。

雖然上述所提出的方法，可以實現雙機密的視覺機密分享；然而 Wu-Chen 和 Wu-Chang 的方法編碼後的分享影像 A 與 B,會有深淺上的差異（A 深而 B 淺）；而 Wu-Chang 的圓形分享影像和 Hsu 等人的圓柱分享影像，則有製作不易（與方形、矩形者比較）、起始位置不可得、旋轉角度難精準…等問題，在行動裝置（如 PDA 或手機）上，不容易實作；未能達到簡易、低成本的期望。

Hou [3] 在 2003 年提出了透過 CMY 減色模型,將機密影像分 CMY 三色、分別執行半色調、利用基本視覺密碼模型（表一）、分別編碼再合成 CMY 三分色，而完成彩色視覺密碼機制之實作。我們在下節所提出的黑白雙機密視覺機密分享機制，即可以其此技巧，擴展成彩色雙機密視覺機密分享機制。

三、雙機密視覺機密分享機制

考慮兩張機密影像 P_1 與 P_2，在此我們設計簡易實用的雙機密視覺機密分享機制，使 P_1 和 P_2 可編碼出分享影像 S_1 和 S_2 ，使得 $S_1 \otimes S_2$ 可看出 P_1 ，而 $S_1 \otimes \text{flip}(S_2)$ 可看出 P_2；其中 $\otimes$ 表示疊合的動作，而 flip(S) 代表將分享影像 S 做水平翻轉的動作。

首先我們對 P_1 利用表一的基本編碼模型，編碼成兩張分享影像 A_1 與 A_2,再將 P_2 依同法，編碼成 B_1 與 B_2。然後將 A_1 與 B_1 結合成為 S_1，將 A_2 與 flip(B_2) 結合成為 S_2；而結合的必要條件則是 $S_1 \otimes S_2$ 要看出 P_1 且 $S_1 \otimes \text{flip}(S_2)$ 要看出 P_2。Algorithm 1 先行描述此想法。

Algorithm 1 Encrypting two secret images into two shares.

Input：Two $h \times w$ binary images P_1 and P_2 where $P_k[i, j] \in \{0, 1\}$ (white or black), $1 \le i \le h$, $1 \le j \le w$ and $k \in \{1, 2\}$

Output：Shares S_1 and S_2 such that $S_1 \otimes S_2$ reveals P_1, while $S_1 \otimes \text{flip}(S_2)$ reveals P_2 to our eyes

1. for ($1 \le i \le h$, $1 \le j \le w$) do

1.1 { if ($P_1[i, j]$==0) N = permutation(M^0)
else N = permutation(M^1)
// permutation(M) permutes M columnwise

1.2 $A_1[i, j] = N[1]$ // $N[1]$ is row 1 of N

1.3 $A_2[i, j] = N[2]$ // $N[2]$ is row 2 of N

1.4 if ($P_2[i, j]$==0) N = permutation(M^0)
else N = permutation(M^1)

1.5 $B_1[i, j] = N[1]$

1.6 $B_2[i, j] = N[2]$
}

2. B_2 = flip(B_2) // flip(B_2) flips B_2 horizontally

3. (S_1, S_2) = *merge*(A_1, A_2, B_1, B_2)

4. Output(S_1, S_2)

其中 permutation(M) 表示將矩陣 M 做欄的隨機排列後所得的矩陣；$N[k]$ 表示矩陣 N 的第 i 列（含二個編碼值）。Algorithm 1 中的步驟 1.1-1.3 將 P_1 利用表一的基本編碼模型，編碼成 A_1 與 A_2，1.4-1.6 則將 P_2，編碼成 B_1 與 B_2。機密影像 P_1 與 P_2 在編碼時，是各自獨立編碼，其間沒有任何的相關性。

現在我們敘述結合的方法（步驟 3 的 *merge*(A_1, A_2, B_1, B_2)。基本上 A_1 與 B_1 結合成為 S_1 時，我們把 A_1 和 B_1 的各列依序交叉擺置在 S_1 的各列中，而 S_2 的產生亦然。下列程序皆為可行的結合方法：

merge$_1$(A_1, A_2, B_1, B_2)

1. for ($1 \le i \le h$) do
{ $S_1[2i-1] = A_1[i]$
// S 的列 $2i-1$ 設為 A_1 的列 i
$S_1[2i] = B_1[i]$
$S_2[2i-1] = A_2[i]$
$S_1[2i] = B_2[i]$
}

2. return(S_1, S_2)

merge$_2$(A_1, A_2, B_1, B_2)

1. for ($1 \le i \le h$) do
{ if ($q > 1/2$) // $q \in [0, 1]$, a random number
{ $S_1[2i-1] = A_1[i]$
$S_1[2i] = B_1[i]$
$S_2[2i-1] = A_2[i]$
$S_2[2i] = B_2[i]$
}
else
{ $S_1[2i-1] = B_1[i]$
$S_1[2i] = A_1[i]$
$S_2[2i-1] = B_2[i]$
$S_2[2i] = A_2[i]$
}
}

2. return (S_1, S_2)

merge$_3$(A_1, A_2, B_1, B_2)

1. for ($1 \le i \le h$) do
{ if ($q > 1/2$)
{ $S_1[2i-1] = A_1[i]$
$S_1[2i] = B_1[i]$
}
else
{ $S_1[2i-1] = B_1[i]$
$S_1[2i] = A_1[i]$
}
if ($q > 1/2$)

{ $S_2[2i-1] = A_2[i]$
$S_2[2i] = B_2[i]$
}
else
{ $S_2[2i-1] = B_2[i]$
$S_2[2i] = A_2[i]$
}
}

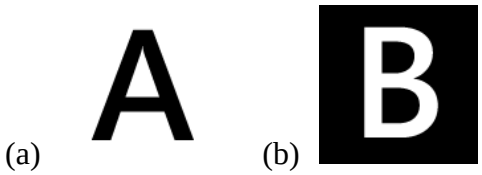
2. return(S_1, S_2)

merge$_1$ 此程序固定放置A_1的各列依序在S_1的奇數列，而B_1的各列依序在S_1 的偶數列；S_2依同法，放了 A_2 和 B_2 （實為 flip(B_2)，見 Algorithm 1 步驟 2） 的各列，完成分享影像之合併。那麼 $S_1 \otimes S_2$ 在奇數列處（即為 $A_1 \otimes A_2$），自然得見 P_1；而 $S_1 \otimes$flip(S_2)在偶數列處（即為 $B_1 \otimes$flip(flip(B_2)) = $B_1 \otimes B_2$），可看見 P_2 也。

我們亦可打亂分享影像放入 S_1 與 S_2 時的列位置，*merge*$_2$ 和 *merge*$_3$ 即為兩種不同的打亂的作法。

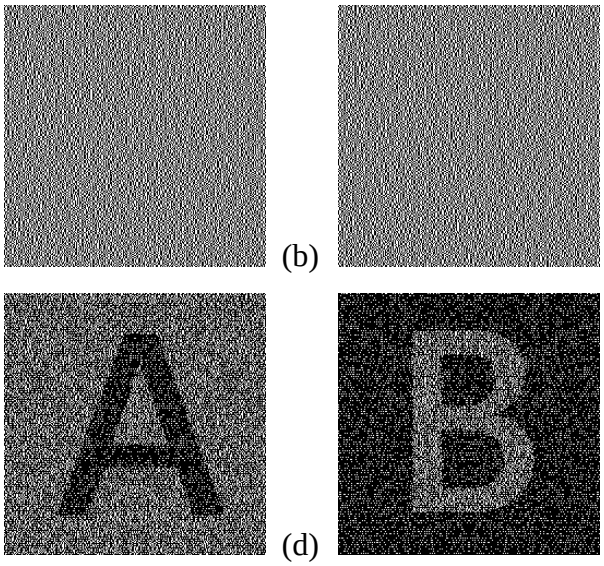
在疊合分享影像 S_1 和 S_2、以及 S_1 和 flip(S_2) 時，由於水平翻轉時奇數列相疊的關係，不會影響偶數列的疊合關係，所以機密之間的關係依然獨立，仍然保持了 Naor and Shamir 機制的安全性。即使擁有了其中一個分享影像 S_1（或 S_2），要猜到 S_2（或 S_1）、甚至於 P_1 或 P_2 的盲目猜測機率，皆與沒有 S_1（或 S_2）的盲目猜測機率是一樣的，因此我們所提出的雙機密視覺機密分享機制具有理想的安全性。

為驗證 Algorithm 1 的可行性，我們撰寫電腦程式以實驗求證。圖二陳列測試用的機密影像 P_1 與 P_2，圖三至圖五展示了 Algorithm 1 針對 P_1 與 P_2，採用不同 *merge* 程序的實驗結果。圖三 (a) 和 (b) 為採用 *merge*$_1$ 程序結合後的分享影像 S_1 和分享影像 S_2；(c) 為 S_1 疊合 S_2 後的結果；(d) 為 S_1 疊合水平翻轉後 S_2 的結果。圖四和圖五則分別為採用 *merge*$_2$ 和 *merge*$_3$ 程序結合後的對應結果。



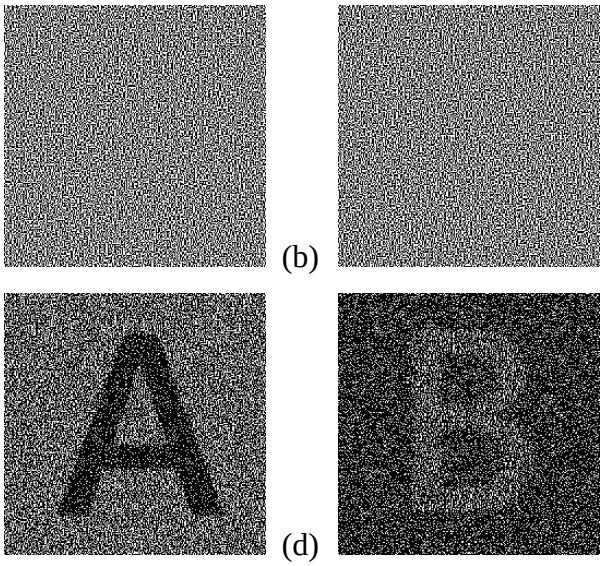
(a) (b)

圖二、黑白機密影像：(a) P_1, (b) P_2.



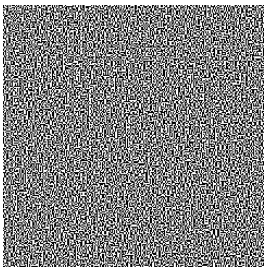
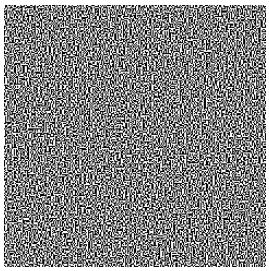
(a) (b) (c) (d)

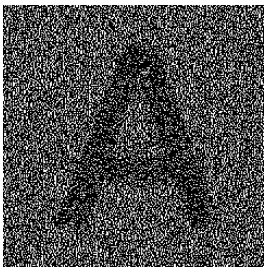
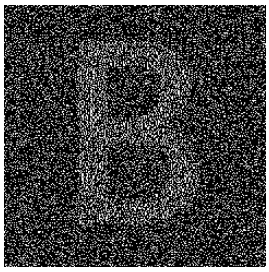
圖三、Algorithm 1 採用 *merge*$_1$ 程序的測試結果：(a) S_1, (b) S_2, (c) $S_1 \otimes S_2$, (d) $S_1 \otimes$ flip(S_2).



(a) (b) (c) (d)

圖四、Algorithm 1 採用 *merge*$_2$ 程序的測試結果：(a) S_1, (b) S_2, (c) $S_1 \otimes S_2$, (d) $S_1 \otimes$ flip(S_2).

(a)  (b) 

(c)  (d) 

圖五、Algorithm 1 採用 $merge_3$ 程序的測試結果：(a) S_1, (b) S_2, (c) $S_1 \otimes S_2$, (d) $S_1 \otimes$ flip(S_2).

由圖三至圖五的實驗結果，可發現經由 $merge_1$ 和 $merge_2$ 程序結合出的分享影像，在疊合後，影像辨識度較 $merge_3$ 者高。由於 $merge_1$ 採固定的奇偶列別擺放 A_1 和 B_1（A_2 和 B_2）在 S_1 (S_2) 中，容易遭受猜測，為了讓使用者能清楚辨識疊合結果，且又有較高的安全性，所以在下一節的實驗中，我們皆以 $merge_2$ 做為 Algorithm 1 中的結合運算。

四、以雙機密視覺分享機制實現視覺驗證

在本節中我們以 Naor and Pinkas 所提出的電子錢包交易流程（如圖一）為實驗場景，我們以所提的雙機密視覺機密分享機制實現視覺驗證；其中交易行為可在行動裝置（如手機）上完成。在此的實驗平台為以解析度 240×320 畫素，搭配 Windows Mobile 6.1 作業系統的手機。

首先使用者在申請電子錢包服務時，除了系統業者所給的智慧卡、雜亂分享影像 S_2 外，再自行設定一識別影像，謂之 I。消費時的驗證過程，除如節一描述之步驟 1 和 2 外，步驟 3 和 4 則更新為：

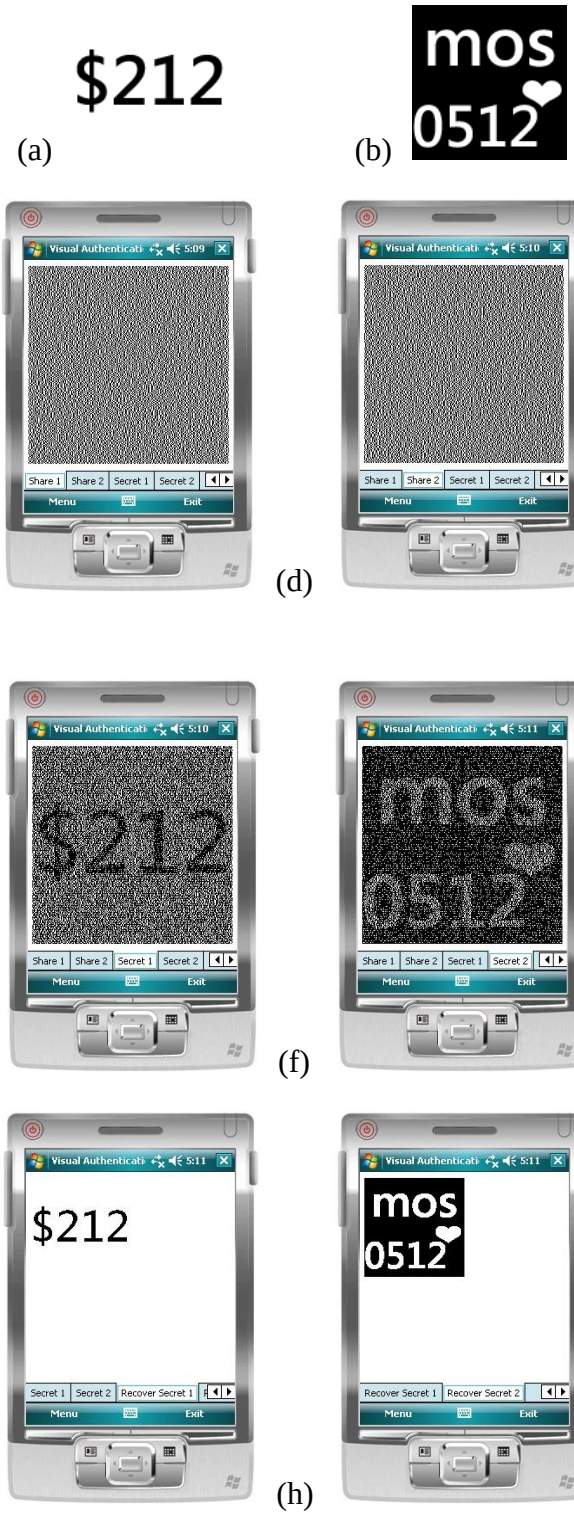
步驟 3：系統業者依智慧卡資訊得知 S_2；依所提的雙機密視覺機密分享機制，將 M 與 I（雙機密）和 S_2 編碼出另一分享影像 S_1，傳送到商家的 POS 螢幕上顯示。

步驟 4：使用者持 S_2 和商家 POS 螢幕上的 S_1 疊合，驗證消費金額 M 是否正確；再水平翻轉 S_2 疊合 S_1，驗證自我識別影像 I 是否正確；若兩者皆正確，則輸入智慧卡的密碼，同意商家該次請款。

圖六為在手機平台實現利用黑白視覺密碼模型完成電子錢包購物驗證的實驗結果。假設使用者購物的總金額為 \$212 (M)（如圖六 (a)），使用者的識別影像為 I 且分享影像為 S_2（如 (b) 和 (c) 顯示在使用者的手機上）；使用者上網（或電話）購物後，商家傳送智慧卡資訊和購物金額給系統業者；後者據之編碼出分享影像 S_1（如(d)）傳送至使用者手機螢幕上。注意：在此傳送媒介是公用網路，非 POS 系統；但商家皆有竊聽竄改的可能。使用者做驗證：透過 S_1 和 S_2 疊合，看到 M （\$212 如 (e)），接著透過 S_2 水平翻轉後疊合 S_1，得到自我識別影像 I（如 (f)），藉此確認 S_1 未曾遭到竄改！若 M 與 I 皆無誤，使用者同意商家此次請款。

由於商家無法得知使用者識別影像為 I，所以只更改 M，無法獲得足以欺騙使用者的 S_1 也。使用者可看到 M，但看不到 I，使用者可知商家有詐，應撤回商家請款權。

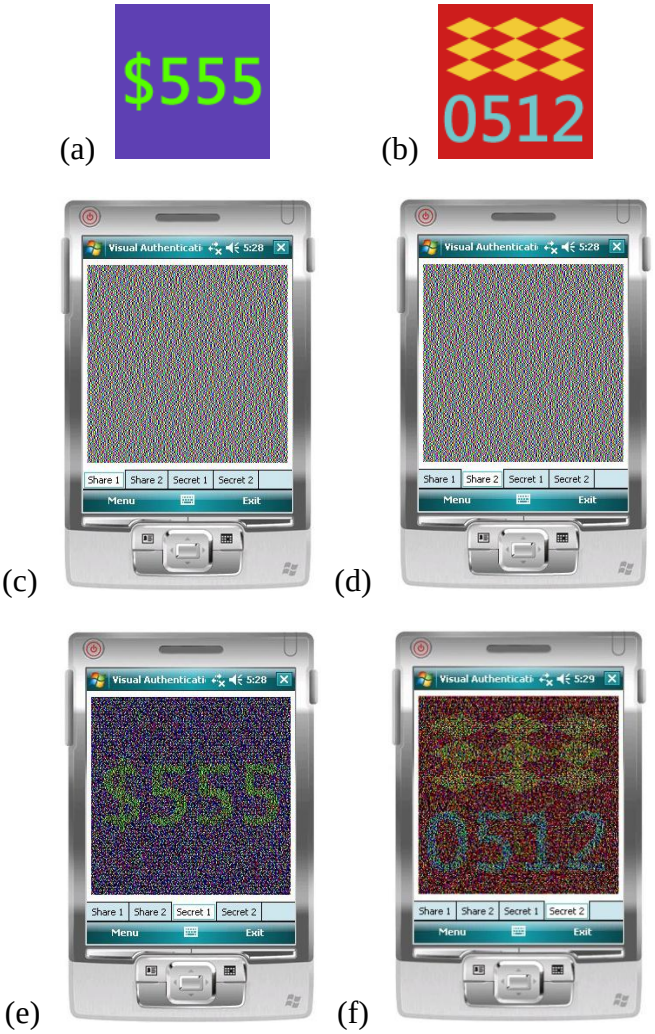
利用手機設備擁有的簡易運算功能，我們能將兩張分享影像利用 XOR 的運算進行疊合，使還原的結果與機密影像完全一樣。圖六 (g) 為 M 在手機螢幕上完美還原的結果，而 (h) 為 I 完美還原的結果。



圖六、黑白機密影像驗證結果：(a) M, (b) I, (c) S_2, (d) S_1, (e) $S_1 \otimes S_2$, (f) $S_1 \otimes$ flip(S_2), (g) M, (h) I.

圖七為利用 Hou 提出的彩色視覺密碼機制

[3] 完成彩色視覺驗證的實驗結果；其中 (a) 為使用者購物總金額 M ($555)，(b) 使用者的識別影像為 I，(c) 為使用者分享影像 S_2；(d) 是系統業者根據 M 和 S_2 編碼出的分享影像 S_1，顯示在使用者手機螢幕上。使用者做驗證：透過 S_1 和 S_2 疊合，看到 M （$555 如 (e)），接著透過 S_2 水平翻轉後疊合 S_1，得到自我識別影像 I（如 (f)），藉此確認 S_1 未曾遭到竄改！



圖七、彩色機密影像驗證結果：(a) M, (b) I, (c) S_2, (d) S_1, (e) $S_1 \otimes S_2$, (f) $S_1 \otimes$ flip(S_2).

五、結論與未來發展

透過視覺密碼原理以及所提出的雙機密視覺機密分享機制，的確可以做到視覺驗證。這裏的雙機密視覺機密分享機制，雖然簡易，卻有理想的安全性。

在未來我們會利用視覺驗證的機制應用在更多的電子化服務，例如：電子投票、網路購物...等，以簡易、低成本、高可攜性的方式達到安全的電子化服務。

六、致謝

此研究在國科會計畫（編號 NSC 97-2213-E-130-022-MY3）的支助下完成，特此致謝。

七、參考文獻

[1] L.-H. Chen and C.-C. Wu, “A Study on Visual Cryptography”, Master Thesis, National Chiao Tung University, Taiwan, ROC, 1998.

[2] C. Hegde, S. Manu, P. D. Shenoy, K. R. Venugopal and L. M. Patnaik, “Secure Authentication using Image Processing and Visual Cryptography for Banking Applications”, Proceedings of the IEEE 16th International Conference on Advanced Computing and Communications, pp.65-72, 2008.

[3] Y.-C. Hou, “Visual cryptography for color images", Pattern Recognition, vol.36, pp.1619–1629, 2003.

[4] H.-C. Hsu, T.-S. Chen and Y.-H. Lin, “The ring shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing”, in: Proceedings of the 2004 IEEE International Conference on Networking, Sensing& Control, pp. 996–1001, 2004.

[5] M. Naor, B. Pinkas, “Visual authentication and identification”, in: B.S. Kaliski Jr. (Ed.), Advances in Cryptology: CRYPTO'97, Lecture .Notes in Computer Science, vol. 1294, pp.322–336, 1997.

[6] M. Naor and A. Shamir, “Visual cryptography”, in: A. De Santis (Ed.), Advances in Cryptology: Eurpocrypt’94, Lecture Notes in Computer Science, vol. 950, pp. 1-12, 1995.

[7] Y.V.S. Rao, Y. Sukonkina, C. Bhagwati and U.K. Singh, “Fingerprint based authentication application using visual cryptography”, Proceeding of the IEEE Region 10 Conference on TENCON, pp.1-5, 2008.

[8] M. Ulutas, R. Yazlcl, V.V. Nabiyev and G. Ulutas, “(2, 2)-Secret Sharing scheme with improved share randomness”, Proceedings of the IEEE 23th International Symposium on Computer and Information Sciences, pp.1-5, 2008.

[9] H.-C. Wu and C.-C. Chang, “Sharing visual multi-secrets using circle shares”, Comput. Stand. Interfaces, vol.134 (28), pp.123-135, 2005.