植基於視覺密碼之遠端醫療安全系統建置

劉政廷　　魏國瑞　　李榮三
逢甲大學資工所　　逢甲大學資工所　　逢甲大學資工所
sky008451@gmail.com　weiray654@gmail.com　leejs@fcu.edu.tw

摘要

隨著網絡技術的蓬勃發展與資訊的電子化，電子病歷也逐漸地取代傳統病歷，而TMIS(Telecare medical information systems)即是用來確保電子病歷存取的的主要技術之一。病人與醫生可藉由遠端登入系統來查詢電子病歷，醫院與醫院之間也可以利用這樣的技術來即時分享病患的病歷，提升整體醫療訊息交換的效率。然而，公開的網路對病患隱私造成的威脅是不容小覷的，因此，建構一個高安全性與高隱密性的 TMIS 系統是近年醫療資訊領域重點發展之一。本研究提出一套輕量化的安全協定，供使用者匿名地和伺服器相互驗證，並且透過視覺密碼(Visual secret sharing) 疊合出一次性密碼，進一步保障使用者的資料安全，同時結合行動裝置提高整體架構之便利性。

關鍵詞：醫療照護系統、視覺密碼 、相互驗證、 一次性密碼

Abstract

The telecare medical information system (TMIS) is one of the major techniques used to guarantee the authorized access to the electronic health record. Patients and doctors could remote login the system to query corresponding records. Also, instinct hospitals could share essential information immediately once a consultation is required. In this article, we have adopted the visual secret sharing (VSS) technique to develop an efficient TMIS with privacy-preserving property. Specifically, an OTP is stacked out at the smartphone monitor to enhance the communication security.

Keywords: TMIS, VSS, mutual authentication, OTP

前言

現代網路蓬勃發展，許多事物與此結合而更加便利，在健康醫療越來越受重視的現況下，醫療與網路科技的結合逐漸成為未來發展的重點項目。此一理念中，醫生可查詢觀察病人的病情發展；相對地，病患也能知曉自身的病況，以便日後與醫生討論後續醫療方針。TMIS 在電子醫療領域中，是最常被討論與應用的，在 TMIS 架構中，病患的電子病歷個別存於醫院的資料庫，透過網路遠端登入，病人與醫生可在任何地點查看病歷。在此技術的幫助之下，對病患而言，由於可自行觀看服用的藥劑及相關醫療影像，讓病患能更加清楚了解自身的身體狀況。

TMIS 架構提供了病人與醫生查詢過往的病歷以及醫療影像的功能，但在目前的網路環境中，若這些電子病歷沒有做近一步的保護處理，網路上的惡意攻擊者便可輕易取得電子病歷，甚至竄改病歷上的資料而造成醫療疏失的發生。為了保障電子病歷的安全性及病患隱私，須將相關的安全協定加入 TMIS 架構中，透過加密資料庫中的電子病歷提高其安全性，並藉由雙向驗證的達成，使得伺服器端及用戶端可以確認彼此的合法性，以降低受到網路釣魚攻擊的可能性。

為了提升遠端登入 TMIS 的安全性[2,4,5,10]，2013 年 Xie 等人[10]提出一套保護使用者隱私的架構，該架構中使用者進行登入時，能匿名自身身分，避免攻擊者追蹤使用者。並且利用指數運算及對稱式加密來保障使用者和伺服器之間的通訊安全。然而，此篇架構中，使用者存的資料是透過智慧卡來存取，假使智慧卡遺失或被竊取，攻擊者可以透過離線密碼猜測攻擊獲得使用者的密碼。Lee 等人[5]於 2014 年提出另一套架構改善智慧卡參數的安全問題，使攻擊者在竊取智慧卡後仍無法猜測出帳號密碼。但該架構的註冊階段，使用者的帳號與密碼以明文方式儲存於伺服器端，當伺服器端遭破解或其內工作人員惡意竊取，使用者於其他網站的資料可能進一步遭竊。在 2015 年 Chaturvedi 等人[2]改善 Xie 等人架構上的缺失，不僅讓使用者能以匿名方式登入於伺服器中，智慧卡儲存的參數與驗證傳遞的訊息都有經過加解密來做保護，但提高安全性的同時，其時間運算量也大幅增加。

為了防範網路攻擊者惡意攻擊 TMIS 架構，

過去學者提出不同的安全協定，但多數的方法仍有一些安全性上的問題，可能造成電子病歷遭竊取或竄改。另一方面，部分學者們為了較高的安全性，使用非對稱式加解密和指數運算，增加了破解上的難度，但這些加密方式運算量較大，以現況而言，使用者多透過智慧卡或行動裝置進行登入。這些裝置進行上述的運算將耗費龐大的運算時間，行動裝置也過於耗電，伺服器端亦需要花費較多時間，伺服器可同時服務的使用者數量將會大幅降低，進而影響服務品質。

本篇研究提出一安全既有效率的新協定來增強 TMIS 架構的安全性，讓伺服器與使用者可以快速完成安全驗證並取得正確內容。考量過去學者提出方法的安全性疑慮，本篇架構除了可抵擋現今常見的攻擊手法之外，為了加強驗證的安全強度，本篇架構也利用視覺密碼疊合出一次性密碼，讓攻擊者無法監聽與竊取敏感資料。在運算效率方面，本方法僅需要輕量的安全加密運算。

2. 文獻探討

本方法採用視覺秘密分享 Visual secret sharing(VSS)[6-9]疊合出一次性密碼 OTP[1,3]，圖 2-1 為 VSS 的簡單架構。視覺秘密分享概念最早是由 Naor 及 Shamir[7]於 1979 年所提出，透過資料隱藏將秘密藏於兩張僅有黑白兩色交錯的影像中，解密的方式僅需將其中一張影像疊合於另一張上，即可用肉眼看出藏於兩影像的密碼，若僅取得其中一張影像則無法從其中獲得密碼資訊。在此架構中，秘密影像被拆分為 S_1, S_2 兩黑白影像，若要使秘密影像顯示為白色區塊，則 S_1, S_2 須同為白色區塊，反之若要讓秘密影像為黑色區塊，S_1 和 S_2 則為互補色(一黑一白)或兩者皆為黑色。藉由表 2-1 的規則，便可根據秘密影像產生出藏入秘密的 S_1, S_2 兩分享圖。

表 2-1 VSS 規則表

S_1	S_2	S_1VS_2
□	□	□
■	□	■
□	■	■
■	■	■

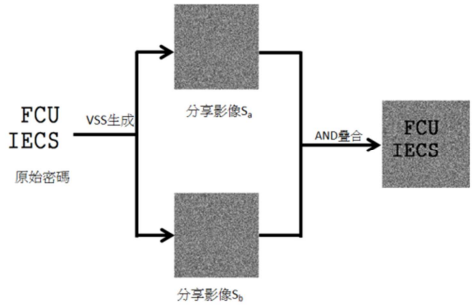


圖 2-1 一般 VSS 架構

3.主要架構

本篇架構共分為四個部份；註冊階段、登入與驗證階段、密碼更換階段與 VSS 建立流程。前三個階段所使用到的進階 VSS 技術都詳列在 VSS 建立流程裡面，下表 3-1 為本方法所用符號表。

表 3-1 符號表

符號	說明
s	說明
ID_{LR}, ID_{LR2}	伺服器端的私密金鑰
$time_1$, $time_2$, $time_3$	使用者註冊於伺服器的假名
base/share image	時戳
V,V'	視覺秘密分享基底圖/分享圖
$h(\ )$	伺服器驗證使用者之參數
$E_x()/D_x()$	Hash 函數
- - →	對稱式加解密，金鑰為 x
⟶	安全通訊通道

3.1 註冊階段

使用者欲使用 TMIS 架構，需先進行註冊讓伺服器端記錄使用者資料，於註冊階段完成後，行動裝置儲存部份參數，供登入及相互驗證使用。圖 3-1 為註冊階段流程圖。

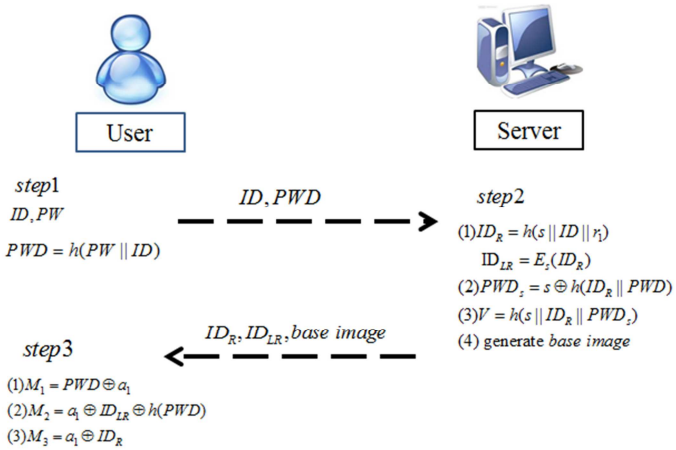


圖 3-1 註冊階段流程

步驟 1.使用者自行決定帳號 ID 以及密碼 PW，並計算 $PWD=h(PW||ID)$，將 PWD, ID 透過安全通道傳至伺服器端。

步驟 2.伺服器端收到使用者的請求及參數後，利用私密金鑰 s 和隨機亂數 r_1 建立下列參數：$ID_R=h(s||ID||r_1)$, $ID_{LR}=E_s(ID_R)$, $PWD_s=s\oplus h(ID_R||PWD)$, $V=h(s||ID_R||PWD_s)$，最後隨機產生 VSS 之基底圖。伺服器端將 ID_R, ID_{LR} 和基底圖透過安全通道回傳至使用者，並且將 V, PWD_s, ID_{LR} 和基底圖存於資料庫。

步驟 3.使用者收到 ID_R, ID_{LR} 和基底圖後，計算 $M_1=PWD\oplus a_1$, $M_2=a_1\oplus ID_{LR}\oplus h(PWD)$, $M_3=a_1\oplus ID_R$ 並將這些結果與基底圖存於智慧型裝置即完成註冊階段的流程。

3.2 登入與驗證階段

使用者想取得電子病歷資料時，需登入伺服器驗證使用者身分，使用者方可做查詢及下載資料的動作，圖 3-2 為登入與驗證流程圖。

步驟 1.使用者輸入 ID 和 PW，行動裝置根據此分別與 M_1, M_2, M_3 運算取得亂數 a_1, ID_R 與 ID_{LR}。

步驟 2.使用者產生亂數 c_1 及時戳 $time_1$，計算 $A_1=h(ID_R)\oplus c_1\oplus time_1$, $A_2=h(c_1)\oplus PWD$，之後將 $time_1$, ID_{LR}, A_1 與 A_2 透過網路傳至伺服器端。

步驟 3.當伺服器端收到使用者的驗證請求訊息後，首先檢查時戳 $time_1$ 的時效性，判斷該訊息是否過期或重送。接著以驗證參數 ID_{LR} 作為索引，從資料庫中取得對應的相關參數，利用私密金鑰 s 與 ID_{LR} 解密並取得 ID_R'，以 ID_R' 與 A_1 計算出 c_1'，並進一步於 A_2 中取得 PWD'。透過 V 驗證 PWD' 與 ID_R' 之正確性，並進一步取出該用戶的基底圖。

步驟 4.伺服器端驗證使用者所傳參數後，選定亂數 d_1、時戳 $time_2$ 以及一次性密碼 OTP，利用使用者傳遞的參數建立 $R_1=h(time_1||time_2)\oplus c_1$, $R_2=h(c_1||ID_R)\oplus d_1$，並以 OTP 作為秘密影像，利用視覺密碼的技術，根據使用者之基底圖產生分享圖。接著運算 $R_3= h(c_1)\oplus ID_{R2}$, $R_4= h(c_1||d_1)\oplus ID_{LR2}$。計算出 R_1, R_2, R_3 及 R_4 後，伺服器將其傳至使用者。

步驟 5.使用者收到伺服器端的參數後，利用 $time_1$, $time_2$ 和驗證參數 R_1 計算出 c_1'，檢查是否與亂數 c_1 相同以驗證伺服器端。接著，透過 c_1, ID_R 與 R_2 取得的亂數 d_1。

步驟 6.使用者將收到的分享圖與基底圖疊合得出 OTP，建立驗證訊息 h(OTP)傳至伺服器端。伺服器收到參數後驗證 OTP 之正確性，以驗證使用者合法性。

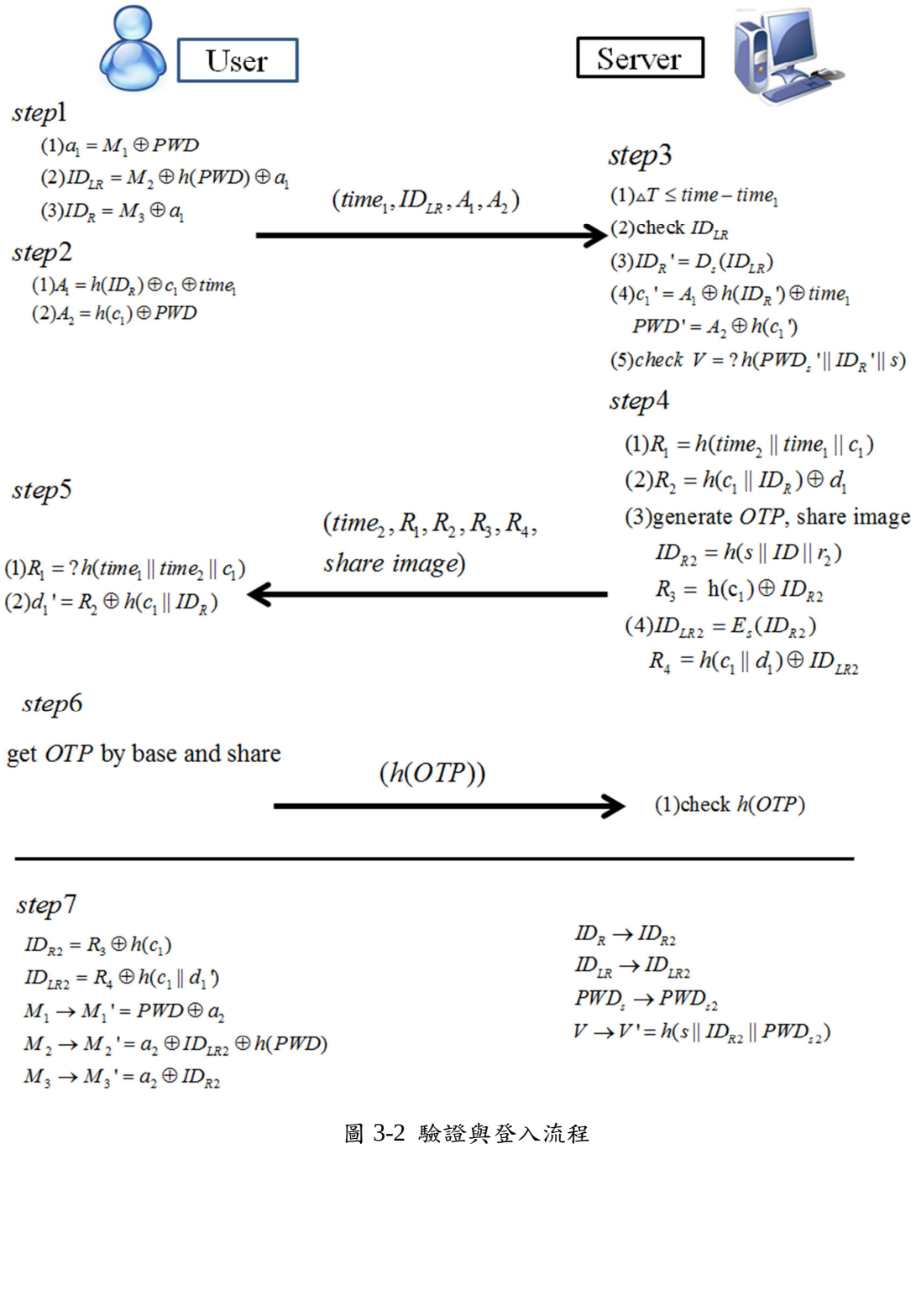

User
Server
step1
(1)$a_1 = M_1 \oplus PWD$
(2)$ID_{LR} = M_2 \oplus h(PWD) \oplus a_1$
(3)$ID_R = M_3 \oplus a_1$
step2
(1)$A_1 = h(ID_R) \oplus c_1 \oplus time_1$
(2)$A_2 = h(c_1) \oplus PWD$
$(time_1, ID_{LR}, A_1, A_2)$
step3
(1)$\Delta T \le time - time_1$
(2)check ID_{LR}
(3)$ID_R' = D_s(ID_{LR})$
(4)$c_1' = A_1 \oplus h(ID_R') \oplus time_1$
$PWD' = A_2 \oplus h(c_1')$
(5)check $V = ?\, h(PWD_s' \| ID_R' \| s)$
step4
(1)$R_1 = h(time_2 \| time_1 \| c_1)$
(2)$R_2 = h(c_1 \| ID_R) \oplus d_1$
(3)generate OTP, share image
$ID_{R2} = h(s \| ID \| r_2)$
$R_3 = h(c_1) \oplus ID_{R2}$
(4)$ID_{LR2} = E_s(ID_{R2})$
$R_4 = h(c_1 \| d_1) \oplus ID_{LR2}$
step5
$(time_2, R_1, R_2, R_3, R_4,$ share image)
(1)$R_1 = ?\, h(time_1 \| time_2 \| c_1)$
(2)$d_1' = R_2 \oplus h(c_1 \| ID_R)$
step6
get OTP by base and share
$(h(OTP))$
(1)check $h(OTP)$
step7
$ID_{R2} = R_3 \oplus h(c_1)$
$ID_{LR2} = R_4 \oplus h(c_1 \| d_1')$
$M_1 \rightarrow M_1' = PWD \oplus a_2$
$M_2 \rightarrow M_2' = a_2 \oplus ID_{LR2} \oplus h(PWD)$
$M_3 \rightarrow M_3' = a_2 \oplus ID_{R2}$
$ID_R \rightarrow ID_{R2}$
$ID_{LR} \rightarrow ID_{LR2}$
$PWD_s \rightarrow PWD_{s2}$
$V \rightarrow V' = h(s \| ID_{R2} \| PWD_{s2})$

圖 3-2 驗證與登入流程

步驟 7.完成登入驗證後，使用者與伺服器將會更新參數供下次驗證使用，於使 用者端，由 R_3, R_4 中取得新參數 ID_{R2}, ID_{LR2}: $ID_{R2}=R_3\oplus h(c_1)$, $ID_{LR2}=R_4\oplus h(c_1\|d_1)$，並將原本存於裝置中的 M_1, M_2, M_3 更新為 $M_1'=PWD\oplus a_2$, $M_2'=a_2\oplus ID_{LR2}\oplus h(PWD)$, $M_3'=a_2\oplus ID_{R2}$，其中 a_2 為新的隨機亂數。而在伺服器端，將原資料庫中的舊參數 ID_R, ID_{LR}, PWD_s, V 更新至 $ID_{R2}=h(s\|ID\|r_2)$, $ID_{LR2}=E_s(ID_{R2})$, $PWD_{s2}=s\oplus h(ID_{R2}\|PWD)$, $V_2=h(s\|ID_{R2}\|PWD_s)$。

3.3 密碼更換

使用者可透過密碼更換流程來更新密碼，將行動裝置上與資料庫的參數更新方可完成密碼更換流程，圖 3-3 為密碼更換流程。

步驟 1.使用者輸入 ID 和 PW 於裝置中，並利用參數 M_1, M_2, M_3 得出 ID_{LR}, ID_R。

步驟 2.使用者產生新密碼 PW_{new} 及亂數 d_1、時戳 $time_3$，依序計算出 $PWD_{new}=h(ID\|PW_{new})$, $P_1=h(ID_R)\oplus c_1\oplus time_3$, $P_2=h(c_1)\oplus PWD_{new}$，最後將更新密碼請求 $time_3$, ID_{LR}, P_1 與 P_2 傳至伺服器端。

步驟 3.當伺服器端收到使用者的更換密碼請求訊息後，透過時戳 $time_3$ 判定時效，若訊息符合有效時間內才進行下一步處理。伺服器以參數 ID_{LR} 作為索引，從資料庫中取得使用者資料，將 PWD_s 與 V 更新為 $PWD_{s\_new}=s\oplus h(ID_R\|PWD)$, $V_{new}=h(s\|ID_R\|PWD_{s\_new})$。

步驟 4.使用者將裝置內的參數更新：$M_1=PWD_{new}\oplus a_1$, $M_2=a_1\oplus ID_{LR}\oplus h(PWD_{new})$, $M_3=a_1\oplus ID_R$。

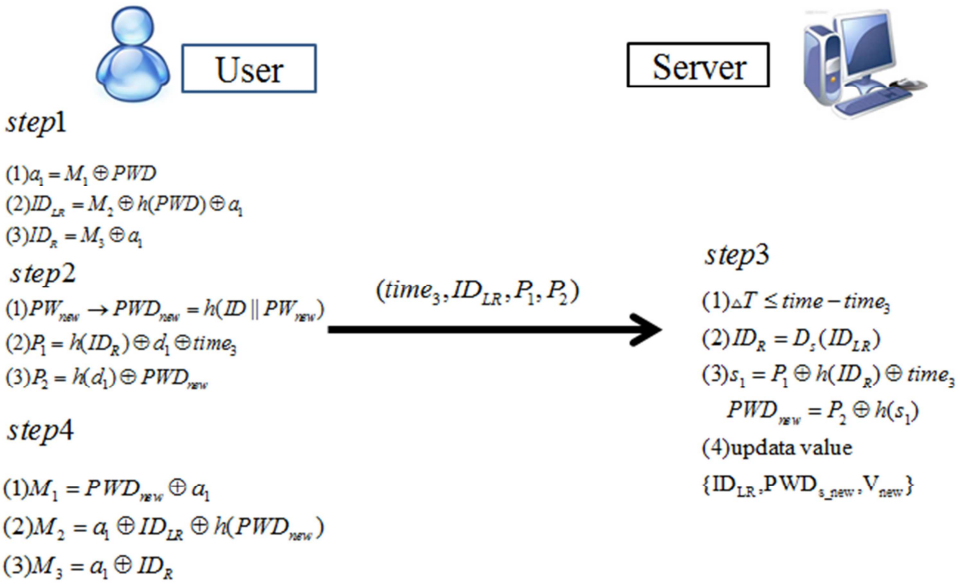


圖 3-3 密碼更換流程

3.4 VSS 建立流程

本文所設計架構是採用像素不擴張的多秘密之視覺秘密分享，為了讓使用者容易旋轉出正確角度，本文所設計的影像形狀為正六角形。此外，為了讓使用者容易識別密碼，本架構所設計的視覺秘密分享是透過彩色來顯示密碼，不同角度所疊合出的密碼顏色也會不相同，本篇架構將一次性密碼拆分成三組子密碼，分別以紅色(R),綠色(G),藍色(B)顯示。

3.4.1 基底圖建立流程

步驟 1.建立一張 512*512 的空白影像，選定空白影像的中心作為正六角形中心，透過 sin, cos 來求得六角形六個頂點的 x, y 座標，公式如下：

X: (半徑r) $* cos\left(\frac{2\pi}{n}\right)$ + (中心座標x值)

Y: (半徑 r)* $sin\left(\frac{2\pi}{n}\right)$ + (中心座標y值)

步驟 2.將六個頂點相互連線可得到一正六角形之外框，如圖 3-4 所示，接著，利用隨機網格產生彩色像素值，完成基底圖的建置，如圖 3-5 所示。

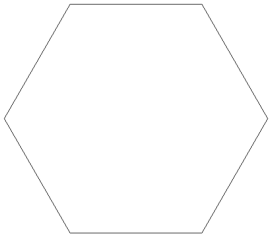


圖 3-4 六角形外框

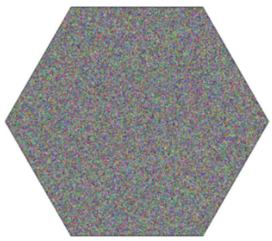


圖 3-5 亂數彩色六角形

3.4.2 分享圖建立流程

步驟 1.伺服器以亂數產生一組 OTP 並分成三組小密碼，繪製成三張秘密影像，假設一組 OTP 為 0487888，拆解至三張秘密影像如圖 3-6~3-8 所示。

步驟 2.分別決定三組秘密的顯示顏色及角度，其中顏色分別為紅、綠、藍，角度為 0°~300° 間 60° 的任意倍數。

步驟 3.根據基底圖和秘密圖藏入第一層秘密，依序判定每個像素值，若密碼為白色(255)，則分享圖亂數給予像素值，反之若密碼為黑色(0)，取得基底圖對應位置的 R_b 值，設定分享圖的 R 為 $255 \oplus R_b$，重覆此流成直至第一張秘密影響處理完畢。

步驟 4.將基底圖(圖 3-9)順時旋轉至選定角度，利用第二部份秘密圖(圖 3-7)重複步驟 3，不同之處為處理頻道為 RGB 中之 G。之後，再將基底圖順時旋轉至另一角度，重複步驟 3 以處理 RGB 中之 B。完成後即得到分享圖，如圖 3-10。

步驟 5.使用者收到分享圖以及疊合角度的資訊後，按照角度疊合可依序得到對應密碼，如圖 3-11~3-13 所示。

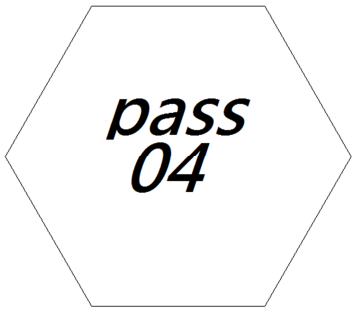


圖 3-6 第一層密碼

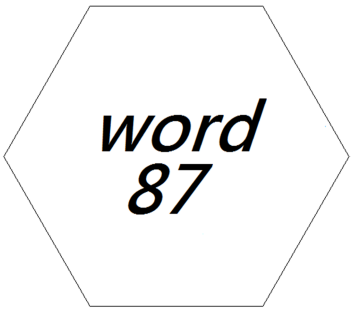


圖 3-7 第二層密碼

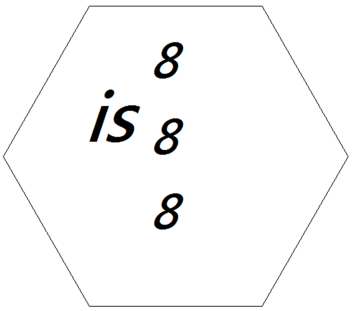


圖 3-8 第三層密碼

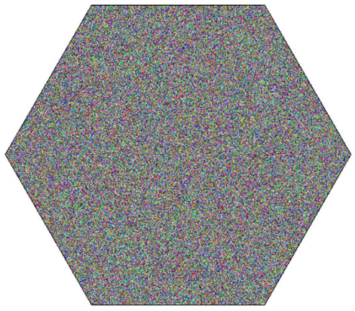


圖 3-9 基底圖

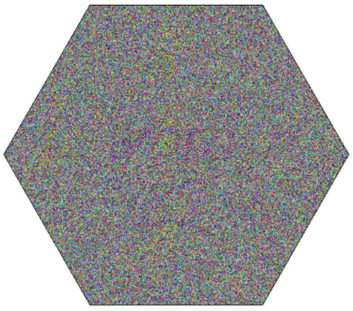


圖 3-10 分享圖

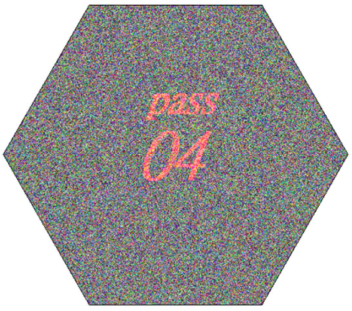


圖 3-11 第一層密碼疊合結果

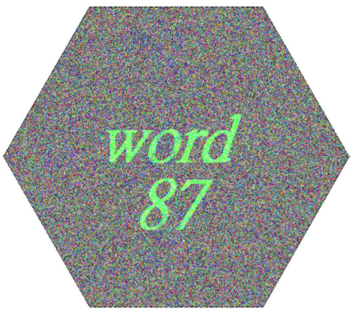


圖 3-12 第二層密碼疊合結果

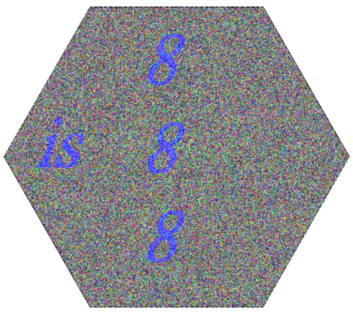


圖 3-13 第三層密碼疊合結果

4.安全分析

在此章節中，將提出一些常見的攻擊模式，並探討此篇架構如何抵禦以達到所需的安全性。

4.1 使用者匿名性與不可追蹤

匿名特性在於無法讓第三者由驗證過程來知曉使用者帳號，保障使用者的隱私。在驗證過程中，使用者的重要身分 ID_R 已透過伺服器的私密金鑰 s 加密為 ID_{LR}，在之後的驗證參數中，若攻擊者想獲得 ID_R 需破解 hash 及猜出其中的隨機亂數。因此，攻擊者無法透過攔截驗證參數來獲得使用者相關資訊。

4.2 二次驗證

藉由視覺秘密分享理念，讓使用者透過 OTP 來完成和伺服器二次驗證。使用者可能因 *ID* 與 *PW* 過於簡單而遭攻擊者猜出，進而仿冒使用者使用服務。在本篇架構上我們加入視覺秘密分享，唯有正確的基底圖與正確角度才可解密成功，一般情境下，攻擊者無法輕易取得使用者的基底圖，無法輕易猜測出一次性密碼。

4.3 重送攻擊

重送攻擊手法是攻擊者藉由重新發送使用者的驗證請求給伺服器，以此來假冒合法使用者取得資料，在本篇架構上我們使用時戳驗證請求的時效性來預防重送攻擊。伺服器收到驗證請求後，透過時戳來鑑定訊息的時效性。假設攻擊者攔截訊息($time_1$, ID_{LR}, A_1, A_2)並將時戳更換至最新時戳 $time_1'$，並將新的請求($time_1'$, ID_{LR}, A_1, A_2)發至伺服器端，伺服器端雖然會判定訊息符合有效時效，但在驗證過程中會發現 $A_1=h(ID_R)\oplus c_1 \oplus time_1$ 與時戳 $time_1'$ 不符合，伺服器端將不做後續的驗證。

4.4 竊取裝置攻擊

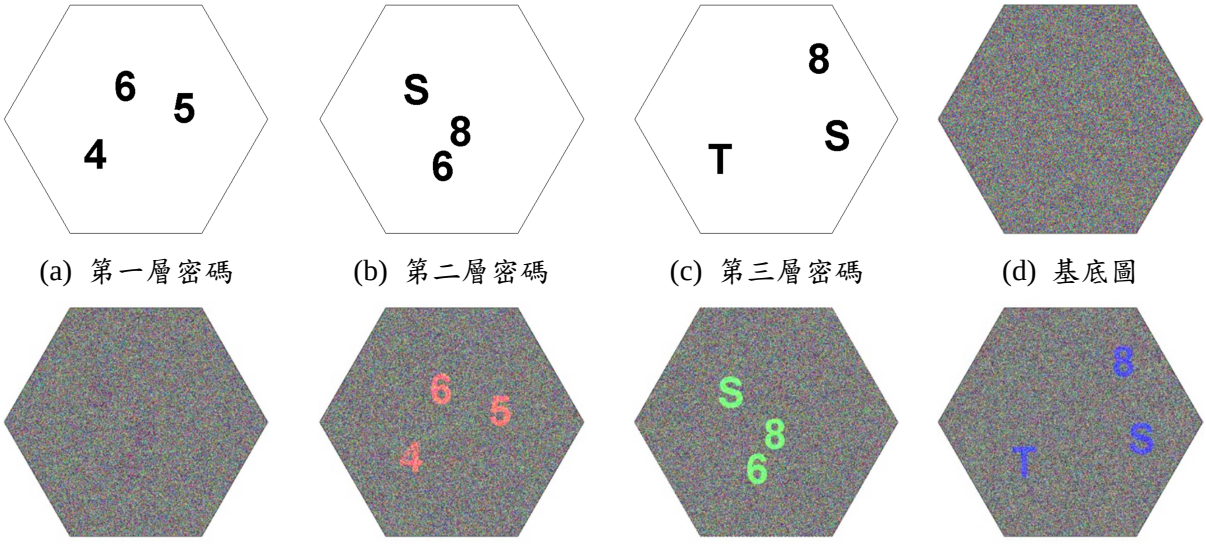
攻擊者藉由竊取使用者的裝置來取得內部參數，假冒合法使用者進行登入或是由內部參數來取得使用者的 *ID*, *PW*。在此篇架構中使用者裝置儲存的參數分別為 $M_1 = PWD\oplus a_1$, $M_2 = a_1\oplus ID_{LR}\oplus h(PWD)$, $M_3 = a_1\oplus ID_R$，均無法運算取得使用者的 *ID*, *PW*，此外，每當使用者完成一次驗證 M_1, M_2, M_3 都會進行更新至新的參數 M_1', M_2', M_3'，如此一來，竊取 *ID* 和 *PW* 會變得更加困難。

4.5 中間人攻擊

攻擊者於使用者和伺服器之間，攔截訊息或拆解訊息來取得使用者機密資料。但在本篇架構的參數，是透過對稱式加密以及 hash 函數來保護資訊，故攻擊者若沒有金鑰 s 或使用者的 *ID*, *PW* 則無法取得機密資料。相對地，若攻擊者若想偽造登入訊息，在沒有獲得金鑰 s 條件下，攻擊者無法建立出符合規格的登入請求訊息。

4.7 離線密碼猜測

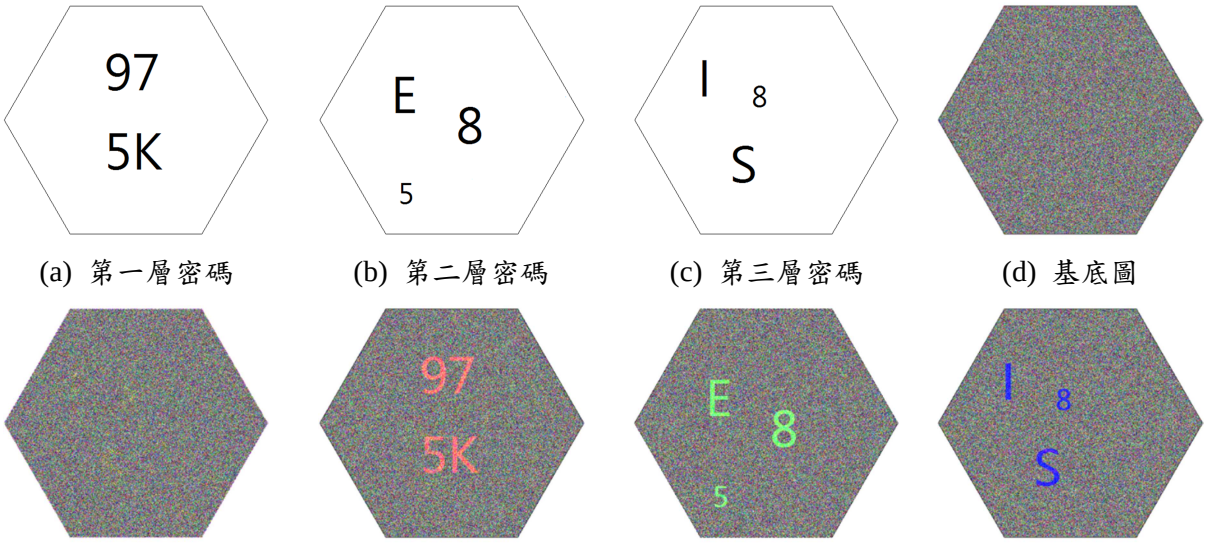
攻擊者偷取裝置中的參數以及攔截驗證請求，猜測使用者的 *ID*, *PW*。於此篇架構中，使用者裝置儲存的參數為 $M_1 = PWD\oplus a_1$, $M_2=a_1\oplus ID_{LR}\oplus h(PWD)$, $M_3=a_1\oplus ID_R$，攻擊者



(a) 第一層密碼 (b) 第二層密碼 (c) 第三層密碼 (d) 基底圖

(e) 分享圖 (f) 疊合結果(60°) (g) 疊合結果(180°) (h)疊合結果(300°)

圖 5-1 VSS(隨機產生密碼)實驗結果



(a) 第一層密碼 (b) 第二層密碼 (c) 第三層密碼 (d) 基底圖

(e) 分享圖 (f) 疊合結果(60°) (g) 疊合結果(180°) (h) 疊合結果(300°)

圖 5-2 VSS(自定義產生密碼)實驗結果

若想藉由猜測來取得正確的 *ID* 與 *PW*，需額外猜測出正確 a_1。若攻擊者嘗試從驗證請求參數 $A_1=h(ID_R)\oplus c_1\oplus time_1$, $A_2=h(c_1)\oplus PWD$ 中獲取資訊，以 A_2 訊息而言，攻擊者需額外猜測出正確 c_1, *ID*, *PW*，因此攻擊者無法以離線方式猜測出使用者的 *ID*, *PW*。

▪5.實驗數據與效能分析

此章節展示本篇架構的整體驗證過程的運算時間花費以及視覺密碼圖的成果圖。

5.1 效能分析

本篇架構分成註冊階段、相互驗證階段及密碼更換階段，表 5-1 展示了各階段運算花費時間，其中 T_h 代表運算一次 hash 所需花費時間、T_x 代表運算一次 Xor 所需花費時間和 T_E 是運算一次對稱式加解密所需花費時間。

表 5-1 效能分析

	使用者	伺服器
註冊階段	$2T_h+4T_x$	$3T_h+T_x+T_E$
相互驗證階段	$8T_h+15T_x$	$9T_h+8T_x+T_E$
密碼更換階段	$6T_h+11T_x$	$2T_h+3T_x+T_E$
總共	$16T_h+30T_x$	$14T_h+12T_x+3T_E$

透過表 5-1 可以發現整體運算多使用 hash 函數以及邏輯運算 Xor 來完成，相較其他加密運算時間較低，因次本篇設計的架構對於使用者和伺服器端皆可達到較高的效能。

5.2 視覺密碼結果圖

以下將介紹視覺密碼的成果圖，圖 5-1 展示亂數產生密碼的模型，其完整密碼為 654S868ST，每層密碼讀取方式由上至下順時針，圖 5-1.a~5-1.c 分別為第一、二、三層密碼，圖 5-1.f~5-1.h 分別為基底圖旋轉 60°, 120°和 180°與分享圖疊合結果。圖 5-2 為手繪產生密碼的模型，圖 5-2.a~5-2.c 展示密碼 975KE8518S 分成三層子密碼圖，並分別以 60°, 180°和 300°藏於分享中，圖 5-2.f~5-2.h 為疊合成果圖。

6. 結論與未來展望

於本篇研究中我們提出一套新的安全協定可應用於 TMIS 的架構，並利用視覺密碼來來建立溝通金鑰。在主要的驗證架構中以 hash 函數以及 XOR 運算來達到安全驗證，不僅減輕手機端運算成本，也讓伺服器可以負荷更多使用者，相較於過去的架構，我們的方法減少許多驗證時間花費。

在未來研究中，除了正確驗證使用者身分，也期盼能做到事後追蹤，當使用者下載電子病歷或是醫療影像時，若將影像散播出去後，我們希望可進一步追蹤散播者以便後續處理

7.參考文獻

[1]Aloul, F., Zahidi, S. and Hajj, W. E., “Two factor authentication using mobile phones,” ***International Conference on Computer Systems and Applications***, pp. 641-644, 2009.

[2]Chaturvedi, A., Mishra, D. and Mukhopadhyay, S., “An enhanced dynamic ID-based authentication scheme for telecare medical information systems,” ***Journal of King Saud University Computer and Information Sciences***, pp. 1-9, 2015.

[3]Eldefrawy, M. H., Alghathbr, K. and Khan, M. K., “OTP-Based Two-Factor Authentication Using Mobile Phones,” ***8th International Conference on Information Technology: New Generations(ITNG)***, pp. 327-331, 2011.

[4]Kim, K. W. and Lee, J. D., “On the Security of Two Remote User Authentication Schemes for Telecare Medical Information Systems,” ***Journal of Medical Systems***, Vol. 38, pp.1-11, 2014.

[5]Lee, Y. C., Hsieh, Y. C., Lee., P. J. and You, P. S., “Improvement of the ElGamal based remote authentication scheme using smart cards,” ***Journal of Applied Research and Technology***, Vol. 12, pp. 1063-1072, 2014.

[6] Lin, C. H., Chen, T. H., Wu, Y. T., Tsao, K. H. and Lin, K. H, “Multi-factor cheating prevention in visual secret sharing by hybrid codebooks,” ***Journal of Visual Communication and Image Representation***, Vol. 25, pp.1543-1557,2014.

[7]Naor, M. and Shamir, A., “Visual cryptography,” ***Advances in Cryptology EUROCRYPT***, Vol. 950, pp. 1-12, 1995.

[8]Shyu, S. J., Huaug, S. Y., Lee, Y. K., Wang, R. Z. and Chen, K., “Sharing multiple secrets in visual cryptography,” ***Displays***, Vol. 39, pp. 80-92, 2015.

[9]Wu, X. and Sun, W., “Extended Capabilities for XOR-Based Visual Cryptography,” ***IEEE Transactions on Information Forensics and Security***, Vol. 9, pp. 1592-1605, 2014.

[10]Xie, Q., Zhang, J. and Dong, N., “Robust anonymous authentication scheme for telecare medical information systems,” ***Journal of Medical Systems***, Vol. 37, pp. 1-8, 2013.