

視覺密碼門鎖系統

Door Lock System Using Visual Cryptography

專題組員: 王景誠、盧冠翰、黃冠穎、鐘皓暄、陳麒升

專題編號: PRJ-NTPUCSIE-111-008

執行期間: 2022 年 08 月 至 2023 年 06 月

一、摘要

我們從以視覺密碼為核心設計出了一個新的演算法，名為視覺密碼門鎖系統演算法，這個演算法可以依據門鎖 Secret 影像、門鎖 Share 影像以及使用者名稱大量產生使用者 Share 影像也就是鑰匙，之後依此演算法實作出了包含伺服器、門鎖、使用者以及管理者的 APP 的系統架構。

我們設計的門鎖系統由於開鎖過程的雙向掃描以及黑名單功能，而有著難以竊錄鑰匙、自動尋找鑰匙、識別使用者身份、開鎖過程不需網路以及降低鑰匙遺失的成本等優點。在解決傳統門鎖系統的安全和便利性方面取得了重要突破。

二、簡介

(一) 研究動機

本研究的動機源於使用者在日常生活中面臨的門鎖系統相關問題，以及現有鑰匙解決方案的不足之處。首先，使用者需要攜帶多把鑰匙，這給他們帶來了不便。不僅如此，尋找特定門鎖的鑰匙也不方便，造成了時間和精力的浪費。其次，傳統門鎖系統無法確認使用者的身份，無法區分合法開鎖

者和非法入侵者，存在一定的安全風險。此外，更換門鎖時需要花費高昂的成本，這對於使用者來說是一個額外的負擔。另外，鑰匙的使用也存在一些缺點，例如鑰匙遺失後不易被發現，這可能導致潛在的安全風險。此外，鑰匙容易被複製，使得冒用和盜用的風險增加。因此，現有的門鎖系統和鑰匙解決方案無法完全滿足使用者的需求，需要開發一種新的解決方案來提高便利性和安全性。本研究旨在利用視覺密碼技術，開發一個能夠辨識使用者身份的門鎖系統，以解決上述問題，提升使用者體驗，同時提供更高的安全性。

(二) 研究目標

本研究的目標是解決傳統門鎖系統和鑰匙使用中的問題，並提供更便利和安全的解決方案。對於使用者而言，我們的目標是開發一個裝置，使他們能夠將所有鑰匙集中存儲，並實現自動尋找對應鑰匙的功能，從而提高便利性。對於門鎖而言，我們致力於開發一種能夠識別用戶身份的門鎖系統，確保只有合法用戶可以進行開鎖操作，同時降低更換門鎖的成本。此外，我們希望減少鑰匙遺失的機會，提供即時發現和警示功能，並提高鑰匙複製的

難度，增加防止未授權複製的安全性。同時，我們也將開發能夠即時防範盜用和冒用者的鑰匙系統。總之，本研究旨在利用視覺密碼技術，實現這些目標，從而改進傳統門鎖系統和鑰匙的使用體驗，提供更為便利和安全的解決方案。

三、專題進行方式

(一) 視覺密碼演算法

本系統以視覺密碼[1]的概念來實作，視覺密碼是可以直接透過肉眼進行解碼的加密方式，將一定張數影像疊合後可以顯示出秘密訊息。

1. n 取 k 分享模型

在模型中一個分享者把秘密分成 n 張影像，影像稱為 share，而使用者湊齊 k 張 share 以上時就能得到秘密訊息；若只疊合 $k-1$ 張 share，將無法顯示秘密訊息。

本系統使用的模型為 2 取 2 的秘密分享模型。

2. 原始視覺密碼

將秘密訊息轉換為兩張 share，每張 share 表面上看起來只是雜訊，但將這些 share 重新疊回去後，就可顯示出被隱藏起來的秘密訊息(Figure 3.1)。

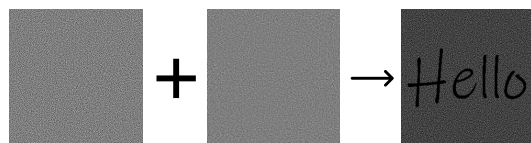


Figure 3.1

我們將秘密訊息中之一個 pixel 拆分成 2×2 的 subpixel，在秘密訊息中的 pixel 有兩種可能：一是會顯示出訊息的深色區塊(如 Figure 3.1 的「Hello」字樣)、二是不顯示訊息的淺色區塊(「Hello」外的區域)。根據混色法(dithering)，當 subpixel 中黑色比例比

白色多時，人眼看起來就會偏暗色。因此運用在 2×2 的 subpixel，深色區塊使用 4 個黑色、0 個白色，淺色區塊使用 3 個黑色、1 個白色。在 share 的 2×2 subpixel 中，一律使用 2 個黑色、2 個白色的組合(2 黑 2 白可排出六種組合)，由於黑色和白色的比例皆為 50%，所以 share 整體看起來像是一塊黑白雜訊。

3. 具偽裝之視覺密碼

傳統的視覺密碼在 Share 的表面只是一些雜訊，每個人拿到 Share 皆很類似，無法輕易分別，所以 Naor 與 Shamir 將原始的視覺密碼做出改良，Share 上不再只是雜訊，而可以包含偽裝訊息，如 Figure 3.2。偽裝功能的視覺密碼中，當 Share 經過疊合後，表面上的訊息會完全消失，最後會顯示隱藏在 Share 裡的 Secret (Figure 3.2)。



Figure 3.2

與傳統的視覺密碼一樣，對於每個 pixel 拆分成 2×2 的 subpixel，但是具偽裝功能的視覺密碼想在 Share 表面上包含訊息，所以如果想表示此像素為白色，該 subpixel 中任意 2 格為黑，2 格為白色；如果想表示此像素為黑色，該 subpixel 中任意 3 格為黑，1 格為白色，利用視覺差與 subpixel 中不同密度的黑白分佈，肉眼可以輕鬆在 Share 上看到訊息。

經過疊合後的 Share 與傳統的視覺密碼相同，深色區塊為 4 個黑色、0 個白色，淺色區塊使用 3 個黑色、1 個白色。

在 k 取 n 的秘密分享模型中，假

設 k 與 n 皆為 2，Figure 3.3 基於改進後的視覺密碼整理出其可能發生的情形，其中 subpixel 型態有很多種，本使用其中一種可能的型態當作範例：

Share1與Share2顏色組合	Share1與Share2 subpixel型態組合	Secret 顏色	疊合後的結果
0白2黑		黑	
1白1黑			
2白0黑			
0白2黑		白	
1白1黑			
2白0黑			

Figure 3.3

4. 門鎖系統演算法

具偽裝功能的視覺密碼中 Share 在選擇使用哪一個 subpixel 型態時無先後順序之分，換句話說可以先隨機選擇 Share1 的 subpixel，也可以先隨機選擇 Share2 的 subpixel，兩種方法都是可行的，因此兩張產生出來的 Share 具有相似的自由度。

我們將具偽裝功能視覺密碼演算法套用到門鎖系統，我們先隨機選擇門鎖 Share 中的 subpixel，再配合門鎖 Share 產生出使用者 Share 的 subpixel，兩者順序無法對調，所以產生出來的結果中，門鎖 Share 內的 subpixel 會比使用者 Share 具比較高的自由度。

在門鎖系統演算法的 k 取 n 秘密分享模型中，我們的 k 與 n 皆為 2，也就是將秘密訊息分成兩份 share，必須要同時擁有這兩個 share，疊起來才能得到秘密。將 secret 分成兩份 share，一份交給門鎖、一份交給使用者，門鎖 share 和使用者 share 表面上皆含有資訊(稱作門鎖 cover 與使用者 cover)。流程上會先新增門鎖再新增該門鎖的使

用者，新增門鎖時，會先產生門鎖唯一的 share 和 secret；新增使用者時，一律根據這個門鎖 share 和門鎖 secret 來產生使用者 share。當有一個門鎖、多位使用者以及要新增一位使用者時，可畫出 Figure 3.4：

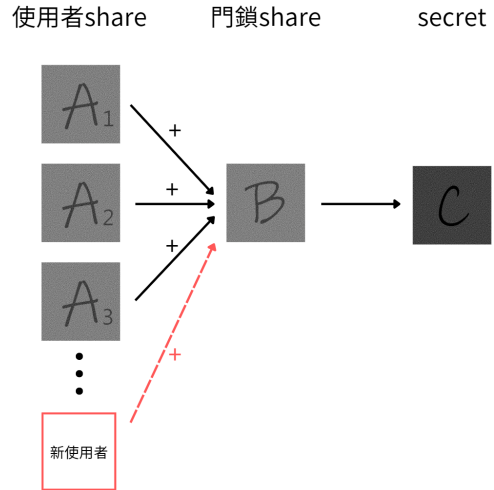


Figure 3.4

以下為我們新增不同 share 之說明：

4.1 新增門鎖 Share：

Share 表面上可呈現訊息，將要呈現的訊息 cover 每一個 Pixel 拆分成 2×2 的 subpixel，如果想表示此像素為白色，該 subpixel 中任意 2 格為黑，2 格為白色，因此該 subpixel 可以選擇 6 種 (C_2^4) 中任意 1 種型態；如果想表示此像素為黑色，該 subpixel 中任意 3 格為黑，1 格為白色，因此該 subpixel 可以選擇 4 種 (C_3^4) 中任意 1 種型態。

4.2 新增使用者 Share：

使用者的 Share 需要配合門鎖的 Share，以及 Secret 為黑或白來產生出對應的 subpixel，並且使用者 Share 表面上也可呈現訊息，因此會有 8 種可能，我們將其中 4 種可能發生的所有情形整理成下表。因為使用者的 subpixel 受限於被指定的門鎖的 subpixel 與 Secret，使用者能選擇的

subpixel 型態不如門鎖 subpixel 選擇的多，因此門鎖的 Share 會比使用者 Share 中的 subpixel 具較高的自由度，我們畫出 Figure 3.5 來說明。

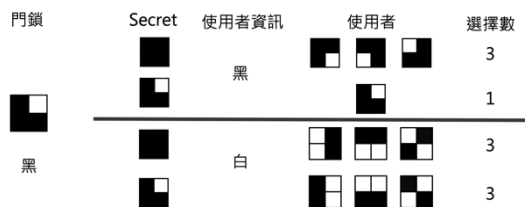


Figure 3.5

本門鎖系統是應用門鎖系統演算法。

(二) 系統架構

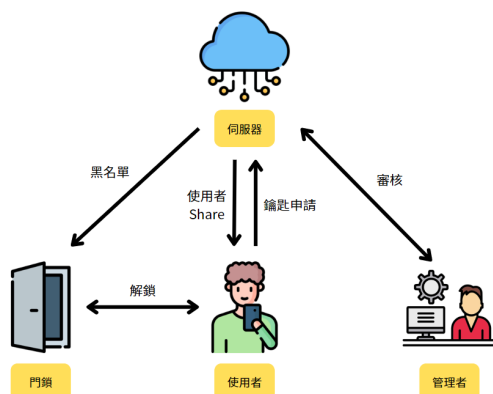


Figure 3.6

本系統含有四支程式：門鎖、使用者、伺服器與管理者。每一個門鎖存有唯一一份門鎖 Share 與 Secret，使用者可存有多份使用者 Share 用來解鎖每一道門。

使用者若想要新增解鎖其他門的鑰匙必須要向伺服器傳送鑰匙申請，伺服器會將此申請送交給管理者進行審核，審核通過後伺服器產生一份使用者 Share 傳給使用者，使用者程式將此使用者 Share 存在裝置中。後續即可不需連網來解鎖門鎖。

此外，門鎖會和伺服器連線，以新增黑名單資訊。

1. 鑰匙性質設計

一位使用者可以存有多份使用者 Share 用來解鎖不同門鎖，如下 Figure 3.7。

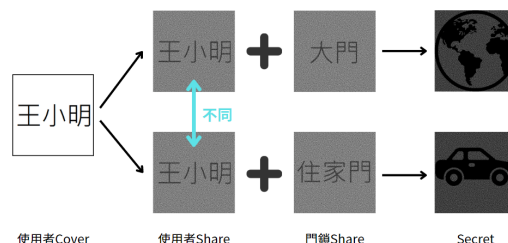


Figure 3.7

使用者「王小明」擁有解鎖「大門」和「住家門」的使用者 Share，目的在於使用者 Share 需疊合門鎖的門鎖 Share 產生 Secret。而每份使用者 Share 表面上含有資訊，稱為使用者 Cover，在本系統中是用來辨別使用者的依據。

王小明的每一份使用者 Share 需配合不同門鎖的門鎖 Share 疊出 Secret，因此 Figure 3.7 中用來解鎖大門的使用者 Share 和用來解鎖住家門的使用者 Share 是不一樣的，不可混用。

若王小明想要再新增一個解鎖「側門」的鑰匙，系統只需要配合王小明的使用者 Cover 和側門的門鎖 Share 來產生使用者 Share，如此一來王小明也可解鎖側門。此過程中側門的門鎖 Share、Secret 以及其他原先可解鎖側門的使用者手上的使用者 Share 皆不會受到影響，可參考 Figure 3.4。

(三) 系統流程設計

1. 開鎖流程

開鎖流程牽涉到使用者以及門鎖兩個角色，我們將開鎖設計為雙向掃描的方式，所以分為兩大步驟：使用者掃描門鎖和門鎖掃描使用者。

1.1 使用者掃描門鎖

Figure 3.8 為第一步驟的流程圖，

使用者掃描後會獲得兩個資訊，一為門的代號用來自動尋找使用者的對應鑰匙，二為一個具時效性的亂數種子 Seed 與 Seed 做 XOR 加密，用來保護使用者的 Share，進而提高複製鑰匙的難度，最後使用者會獲得 XORed 使用者 Share。

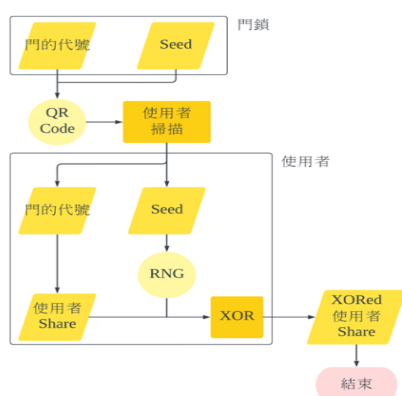


Figure 3.8

1.2 門鎖掃描使用者

Figure 3.9 為第二步驟的流程圖，門鎖掃描後會獲得一個 XORed 的使用者 Share，我們會利用亂數種子進行解密獲得使用者 Share。首先，我們會先判斷該使用者 Share 是否為黑名單，若不為黑名單則將使用者 Share 與門鎖 Share 進行疊合，若疊合影像為秘密影像，那就開鎖成功，反之則開鎖失敗。

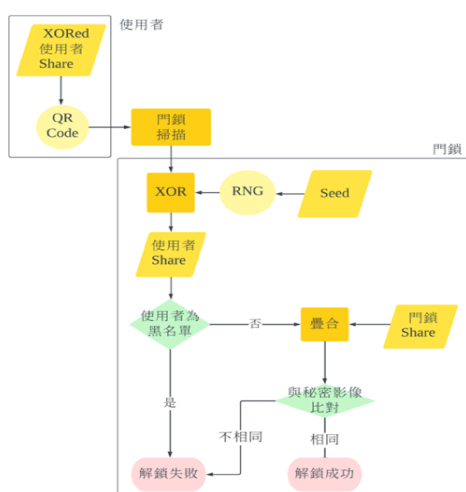


Figure 3.9

2. 加入黑名單流程

加入黑名單會牽涉到三個角色，使用者、門鎖以及管理者。

當使用者的手機遺失，使用者可向管理者通報，接著管理者會將該使用者的鑰匙加入到對應門鎖的黑名單內，進而達到即時防範盜用者的效果。

四、主要成果與評估

(一) 管理者

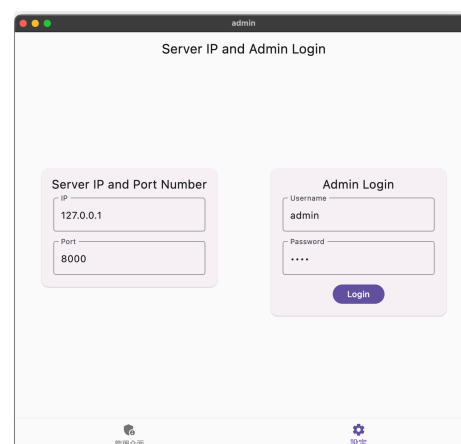


Figure 4.1 管理者介面：伺服器 IP、管理者登

 $\wedge$

Figure 4.1 開始打開管理者程式要先打開右下角的設定輸入伺服器 IP 以及 Port 還有管理者帳號密碼，完畢後即可開始打開管理介面。

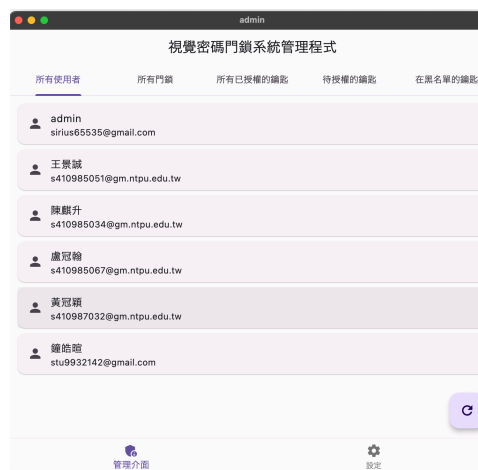


Figure 4.2 管理者介面：所有使用者



Figure 4.3 管理者介面：使用者詳細資料

管理介面(Figure 4.2)上方有五個欄位，點選之後可以切換不同的列表，看到伺服器裡的資料。「所有使用者」能夠看到所有使用者，而點選使用者則可以看到使用者的詳細資訊：使用者以及他擁有的鑰匙 Figure 4.2。「所有門鎖」能夠看到所有門鎖，而點選門鎖則可以看到門鎖的詳細資訊：門鎖以及跟他有關的鑰匙。「所有已授權的鑰匙」能夠看到所有已授權的鑰匙，此時的鑰匙有一個按鈕可以把該鑰匙加入黑名單。「待授權的鑰匙」能夠看到所有待授權的鑰匙，此時的鑰匙可以兩個按鈕來選擇是否授權該鑰匙。「在黑名單的鑰匙」能夠看到所有在黑名單的鑰匙，此時的鑰匙會有紅字明顯提示該鑰匙在黑名單中。所有的鑰匙都可以點選看到鑰匙的詳細資訊：鑰匙以及它的擁有者還有對應的門鎖，三種狀態的鑰匙在 Figure 4.3 看到。

(二) 使用者

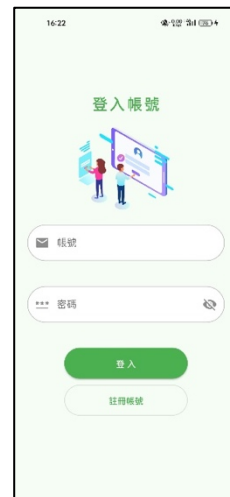


Figure 4.4 使用者介面：登入畫面

首先使用者要進行登入(Figure 4.4)，若是新使用者擇要先註冊帳號。成功後會進到 APP 首頁(Figure 4.5)。



Figure 4.5 使用者介面：首頁

點擊「申請鑰匙」，可以向管理者申請鑰匙，輸入門鎖名稱和申請原因(Figure 4.6 左)，並傳送申請，等待後續管理者審核。審核成功後，在「鑰匙清單」可看到該鑰匙已新增到裝置中(Figure 4.6 右)。

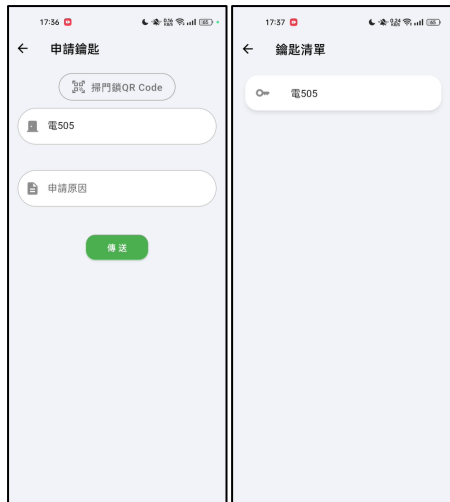


Figure 4.6 使用者介面：

(左)申請鑰匙 (右)鑰匙清單

要開門時，在首頁點擊「掃 QR Code」掃描門鎖螢幕上的 QR Code，若裝置中存有解鎖該門鎖的使用者 Share，會顯示出 QR Code (Figure 4.7) 供門鎖掃描。



Figure 4.7 使用者介面：開鎖 QR Code

(三) 門鎖

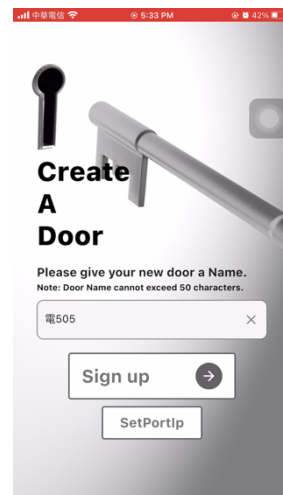


Figure 4.8

首先進入到門鎖的註冊頁面，如 Figure 4.8，可以先幫門鎖取名，門鎖名可當作代號用幫助來使用者找出對應鑰匙。

註冊成功後，會進入掃描頁面，下方 Figure 4.9 的 QR Code 為使用者掃描門鎖提到的門的代號以及亂數種子。如果開鎖成功，畫面上方紅色會轉成綠色並顯示 Pass! 如 Figure 4.9 右圖的畫面，代表開鎖成功。

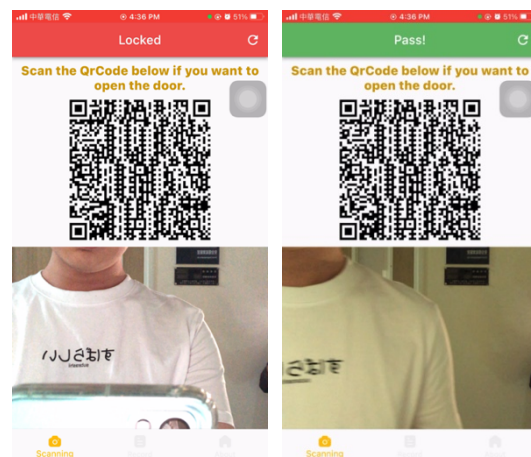


Figure 4.9

下方 Figure 4.10 紀錄開鎖時間與開鎖的使用者，因為我們可以根據使用者 Share 上辨別使用者。

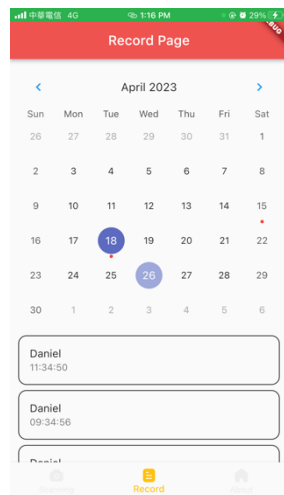


Figure 4.10

五、 結語與展望

過去傳統門鎖有許多的缺點，我們透過手機 app 結合光學鏡頭和 QR Code 的方式來防止盜用和側錄，並透過視覺密碼演算法作為我們紀錄祕密的方式，並在使用者 Share 上加入時效性亂碼的機制來防止有心人士的盜用。

六、 銘謝

感謝教授一路上對我們的建議，透過教授的循循善誘下我們改善了很多，也感謝實驗室學長對我們的鼎力相助，在期末的追趕下協助我們減輕了我們很多壓力

七、 參考文獻

- [1] Moni Naor, and Adi Shamir."Visual cryptography.", 1995
- [2] Jena, Debasish, and Sanjay Kumar Jena. "A novel visual cryptography scheme." 2009 International Conference on Advanced Computer Control. IEEE,