- Charming Eyes- 密碼&迷人的眼「神守護」 -

社團法人台灣 E 化資安分析管理協會 理事長
中央警察大學資訊密碼暨建構實驗室 (ICCL) 王旭正教授

電影或電視中，我們常可見到要進入管制區或要存取機密訊息時，都一定會有一套身分鑑定的程序，確認使用者的身分之後再來決定其權限。而在今日不管使用何種安全系統，第一步也都是身分鑑定，我們要去讓系統知道我是誰？我是否被允許登入系統？我擁有那些權利？系統一收到我們所輸入的訊息後，就可以知道我們是誰並且清楚我們是否有權執行那些指令或閱讀哪些檔案。就目前一般較為廣泛應用的系統而言，身分鑑定主要有以下三項: 你所記得的東西、你的特徵、或你所持有的東西。這些大致上可對應到「密碼」(Password)、「生物測定學」(Biometrics) 、及「信物」(Token)。

先談「密碼」吧, 身分鑑定的傳統方法是使用個人帳號與密碼，例如我們經常使用網頁進入 Email 的系統如圖一所示。

圖一

或者提款時所輸入的密碼，或者在網路上購物時所輸入的個人 ID 與密碼。密碼登入方式是使用

電腦系統中存有一個使用者代號及對應的密碼清單的資料庫。因此若在使用者輸入時有任一項不符的話就會被系統所拒絕，這是最簡單也最易被實作的方法。然而使用者代號及密碼並不如我們所想像中的來的可靠，因為以密碼作為身份鑑定是基於使用者會選擇諸如「E1Bk%Y!o9」等無意義的文數字組合作為密碼，而非「1369」、「TWNSB」、「MJIB」等有意義的數字或單位符號作為密碼能得以方便記憶。密碼是否為無意義的文數字組合與其長度等兩大元素是決定其是否有效的關鍵要點。例如: 一組長度四位數的密碼，可以在幾分鐘之內破解，但長度八位數以上的組合，就可能要花上一個月的時間的破解，因此，選擇不當的密碼，就易於被攻擊者所破解。同時對使用者而言，要能記憶多組不同的密碼也是一大挑戰, 也不經意造成管理上的負擔。

「生物測定學」或稱為生物統計學。係一種依據使用者獨有的生理或行為特徵為基礎所建立的資料做為識別與認證基準的方法。目前發展中的生物特徵辨識技術包括指紋、眼睛虹膜(Iris)、視網膜(Retina)、脫氧核醣核酸(DNA)、掌形(Hand Geometry)、聲紋、手寫簽字、鍵盤敲打頻率、臉型、脣型等。其中指紋辨識技術發展可說最早也較成熟，也是現階段較具代表性的技術。多年來，生物測定學在於身分鑑定上的技術越來越好。其優點在於使用者無須攜帶任何東西或是記憶密碼即可達到身分識別與認證的目的。另一優點則是生物特徵難以偽造，製作假指紋與視網膜是相當困難的。然而缺點在於一套完善的生物測定機器相當昂貴，且精確度標準不易測量，精確度提高系統辨識速度就會減慢;精確度降低，則安全度不夠, 同時使用生物特徵還要面對個資隱私問題的質疑。

第三種即是使用我們所持有的東西，來證明我們的身分，也就是「信物」的概念。例如電視、電影上常見在古代拿著朝廷的令牌或是尚方寶劍便可代表朝廷行使職權,這令牌或是尚方寶劍便就是信物的一種。目前最常見的就是利用智慧卡(Smart Card)，IC 卡(Integrated Circuits Card)來做爲信物。如此一來，使用者無須記憶複雜的密碼，遺失了一樣可以補發。但是使用此法的缺點一樣是要面臨信物會被竊取、仿冒或是被複製的問題。同時，攻擊者可以針對智慧卡或是 IC 卡來進行破解以取得系統重要的資訊。

在這三種方法中，現今的運用上多是以其中一至二種來進行身分鑑定。然而，卻還有一個問題難以解決，也就是「內賊」。內部不肖人員可以直接竊取系統資料庫的鑑定比對資訊，使得所屬單位損失慘重。因此要做爲一個好的安全的系統最好是讓雙方共享祕密資訊，而任一方所擁有的資訊無法讓他推斷出全部的資訊。在這一方面上，目前最具成效的應用之一可是視覺安全呢。

視覺安全主要是依據人類視覺系統對於影像色差的反應,而賦與影像意義爲基礎。例如在進行健康檢查時，檢測色盲所用的卡片，便是以人眼視覺的反應來判斷在多個不同色彩的雜點所包含的訊息。視覺安全解決了傳統密碼學在解密過程中需要大量複雜的計算過程，在安全性上，同樣可以確保竊取資料者無法從這些個別的分享影像(或稱爲子圖)中，察覺出機密影像的輪廓。使用視覺安全的方法的優點就在於可使得電腦系統與使用者雙方所持有的資訊都是無意義的圖形，唯有在正確的組合之下，才會顯現出有意義的訊息。而這樣的方式就會使得有意進行攻擊或入侵者必須同時取得雙方的資訊方可成功, 藉此得以降低入侵行為的成功率，因此便能有效提高系統的安全程度。

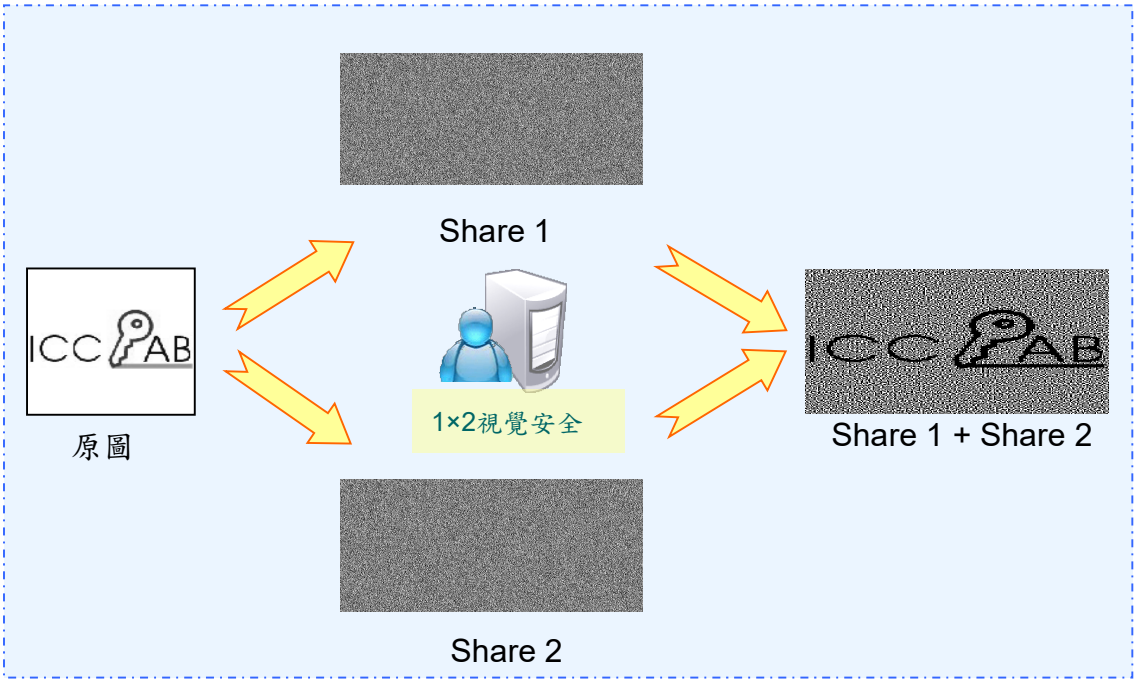
視覺安全， 亦可稱為視覺密碼。視覺安全是將一張擁有秘密訊息的影像，經由一些方法，分解出數張秘密分享圖(Shares)。若獨自擁有一張秘密分享圖是解讀不出來其秘密資訊的內容，而是需要部分或者是全部的秘密分享圖疊合在一起，才可以看出其所要表達的秘密資訊。而這種方法不需要複雜或大量的數學計算，也可以不需要電腦的輔助來完成解讀，只要藉由人類的視覺系統即可直接解讀出機密訊息。

視覺安全是在西元 1994 年中所提出的概念，當加密時將原始機密分散成多張分享影像；解密時再結合所有分散的分享影像即可解讀原始機密的作法。而這種方式並不需要用到任何密碼學的專業知識。視覺安全具有視覺化、操作簡易、高度保密等優點使得密碼學得以邁向另一個不同的層面，但在作法上會產生一些仍需克服的缺點，例如影像容量的增加、影像對比的下降及影像的清晰度等問題。我們接著來聊聊基礎視覺安全、等比例擴展視覺安全，並介紹視覺安全之

有趣資安生活應用。

A. 基礎視覺安全

在傳統視覺密碼中，為了達到秘密分享的目的，機密影像中的每一個像素(Pixel)都會被擴張成若干個子像素(Sub-pixel)，此作用稱為像素擴張(Pixel-expansion)，在原始提出的基本觀念裡是將祕密影像(Secret Image)中每一像素擴張成1 × 2的區塊，若原祕密影像圖的像素值是白色，所分解出的分享圖疊合起來會是一黑一白的像素區塊；若原祕密影像圖的像素值是黑色，所分解出來的分享圖疊合則要是二個黑點像素區塊。藉由這種方式，所分解出來的分享圖個別而言會是無意義的影像，但疊合起來的結果，以人類的視覺系統觀察，卻可還原成原來的祕密影像，如圖二所示。在基本觀念裡所分解出來的分享圖個別而言會是無意義的影像，但疊合起來的結果，以人類的視覺系統而言，卻可還原成原來的祕密影像，而其所呈現的效果將使秘密影像有拉長的視覺效果，形成不等比例之擴張。



圖二 視覺安全基本概念

視覺安全最初的設計是在黑白的二元影像上，主要是將擁有秘密資訊的機密影像分解成2張分享影像。(0)表示白色、(1)表示黑色，如果機密影像的像素點為白色，可分為兩張分享影像。將原機密影像每個像素點擴張為兩倍成為分享影像，也就是分享圖1為兩倍像素點(1，0)或(0，1)，分享圖2為兩倍像素點(1，0) 或(0，1)。若點為黑色的話，分享圖1為(1，0) 或(0，1)，分享圖2為兩倍像素點(0，1) 或(0，1)。依序將整張機密影像分解成兩張分享圖，其表現出的方法就如如圖三所示。

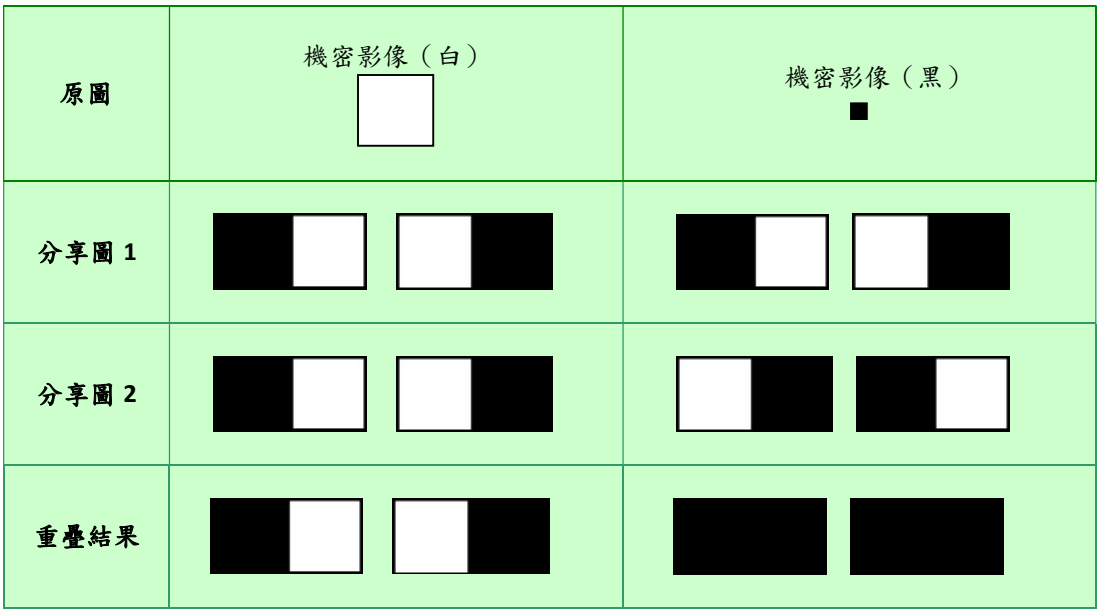


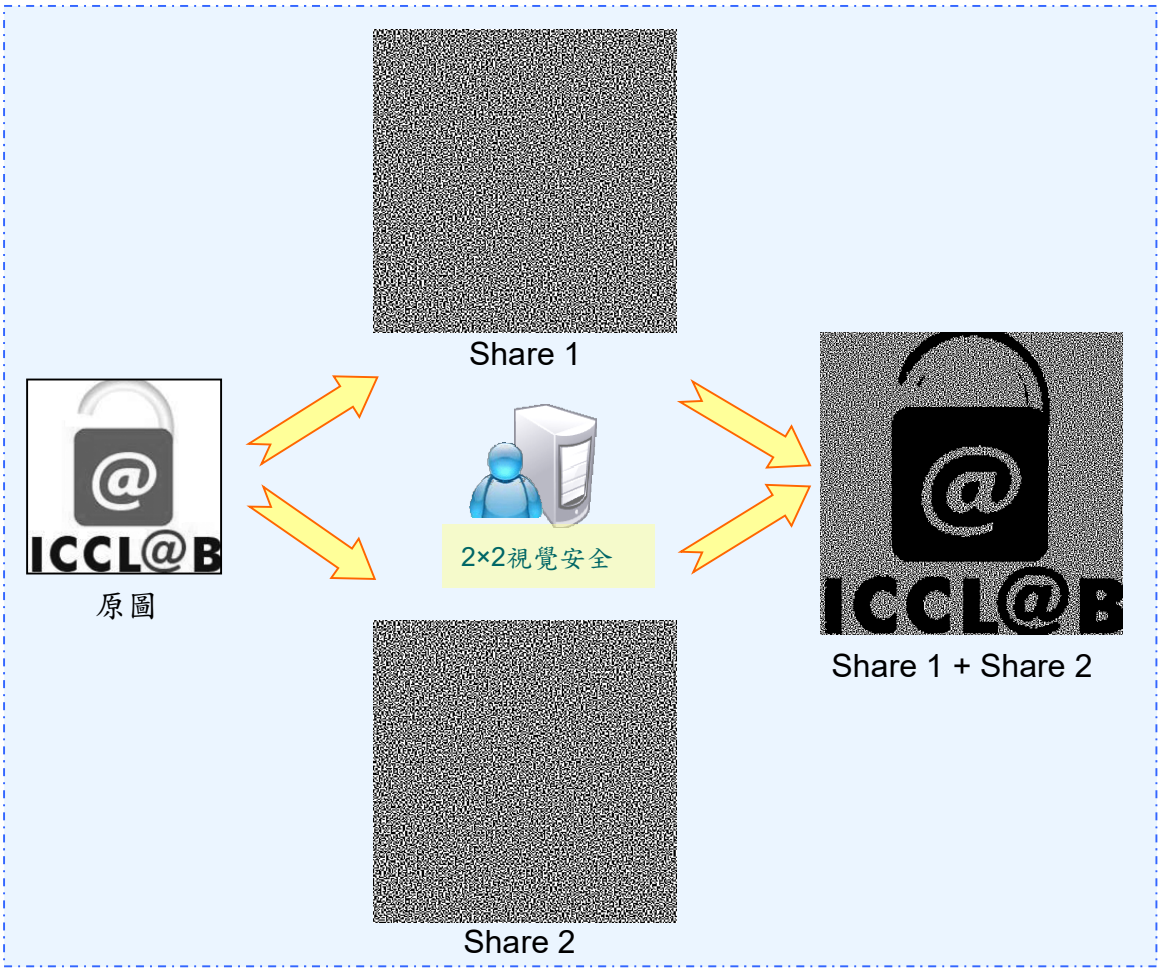
圖 三 1×2 視覺安全

視覺安全其原理在於人類的視覺系統在辨識影像時，是以一像素與周圍像素所產生的對比效果。而人類視覺系統無法清楚的辨識出每一個像素值，只能感覺得出來一塊區域所呈現的效果。所以在此方法中，黑色以全黑來表示，而白色以一黑一白來表示。整體看起來，它就和黑色產生對比，因此人類的視覺系統就會將一黑一白認定為白色。

B. 等比例視覺安全

繼 1 × 2 視覺安全概念之後，因為 1 × 2 視覺安全此方法所產生的分享圖長是原圖的兩倍，當分享圖疊合之後，得到的機密影像寬不變，長卻是原圖的兩倍，造成機密影像變形。因此，接下來陸續發展出了等比例擴展的視覺安全技術，等比例擴展的視覺安全大致上可分為 2 × 2 擴展與 3 × 3 擴展，我們以 2 × 2 擴展視覺安全方法為例一窺究竟。

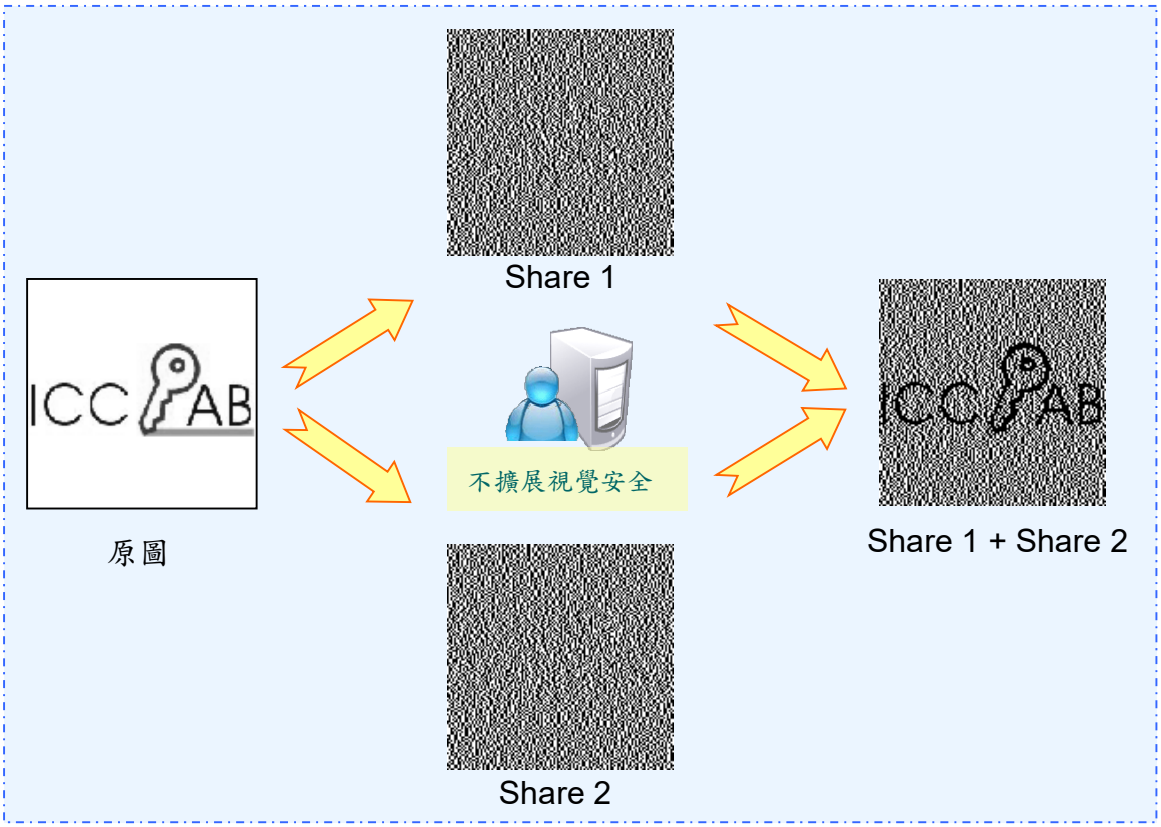
為使得原祕密影像之分享圖在疊合之後能保有原秘密影像之型態，在實際操作上，得將祕密影像中每一像素擴張成 2 × 2 的區塊，如圖四所示。若原圖的像素值是白色，所分解出的分享圖疊合起來會是二黑二白的區塊；反之，若原圖的像素值是黑色，所分解出來的子圖疊合則要是四黑零白的區塊，2 × 2 視覺安全像素擴張法範例如圖五所示。藉由這種方式，所分解出來的子圖個別而言會是無意義的影像，但疊合起來的結果，以人類的視覺系統而言，仍可還原成原來的祕密影像，並且不會造成變形。除此外, 視覺安全的演進亦有不擴張像素的視覺安全機制，如圖六所示。



圖四 2x2 視覺安全

影像	機密影像（白）	機密影像（黑）
分享圖1		
分享圖2		
疊合結果		

圖五 2 x 2像素擴張



圖六 不擴展視覺安全

經歷概念之旅後, 我們來看看視覺安全應用於資安生活的身份鑑定,「一張圖勝萬言字」如圖七到圖十一。

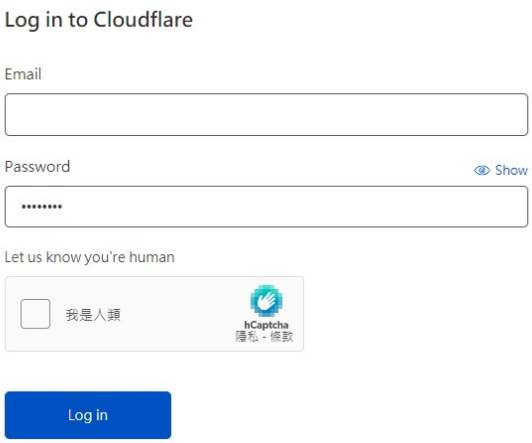
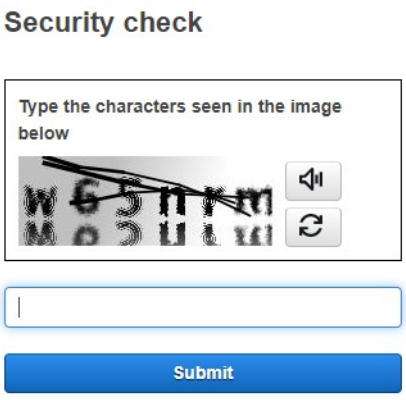


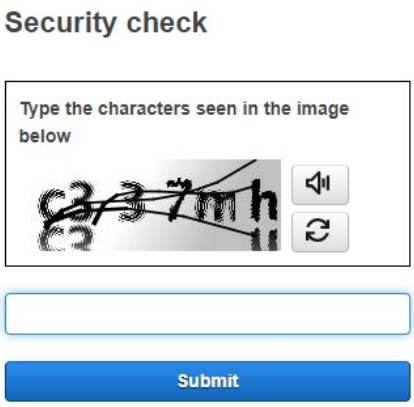
圖 七

圖 八

圖九



圖十

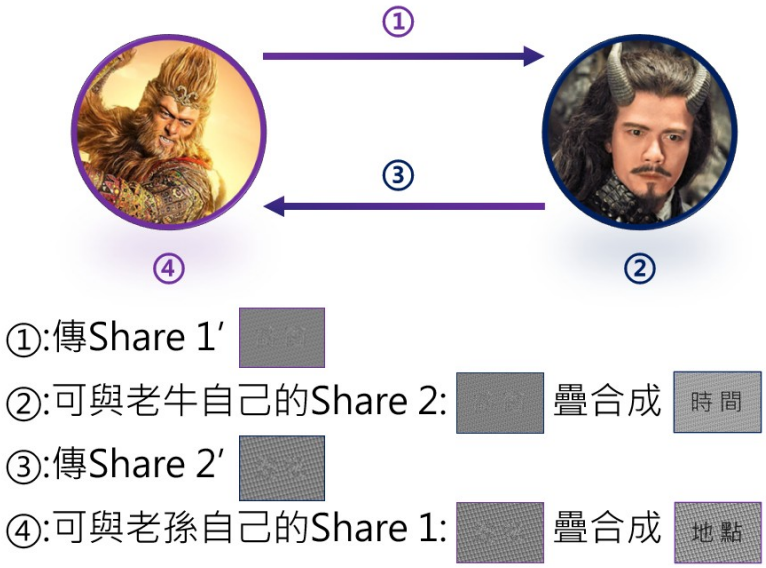


圖十一

是否你已看出一些端倪了呢？ 從圖九到圖十一中不再輸入記憶中的資料, 而是眼睛要開始說話了, 要開「眼/演」了, 要你重視它的存在價值了。 先請看看你是不是人類？ 若你說是, 那麼繼續問你, 你看到什麼, 看到卡車嗎? 看到飛機嗎? 這可不能胡亂比畫勾選的, 一旦眼睛看錯了, 錯把兩輪機車看成卡車, 錯把河海輪船看成飛機。 視力測驗不再只是眼科醫生的專利, 在資安生活裡, 也來問問你, 猜猜這幸運文數字究竟是「w65nrm」, 還是「c337mh」。 智力測驗不再是 IQ 計算,

而是眼睛視力判斷, …, 呵呵, 你猜到了嗎？胡亂瞎猜裡, 系統可是不隨便買單的, “reject”是無情地「翻你白眼」擋你於門外的, 要你再來一次。 幾次後, 還會警告你, 再亂玩, 會被停權而「拒絕再玩」的, 讓你不得不收斂些呀。哈哈, 是否能想見視覺安全在我們資安科技裡竟也開始軋上一腳, 還是重要關鍵呢。

我們再以我們的好朋友孫悟空與牛魔王這搭檔唱雙簧來做些概念說明視覺安全的玩味與驚奇。老孫與老牛這兩位好友, 事先都先分享彼此的「Shares」, 也就說老孫有自己的黑白亂碼「Share 1」, 也有老牛的黑白亂碼 「Share 2」; 相對地, 老牛有自己的黑白亂碼「Share 2」, 也有老孫的黑白亂碼「Share 1」。若老孫欲與老牛設定 “碰面時間” 為「Nov. 16, 2021」, 即用 內含「Nov. 16, 2021」的影像內容 , 並依據老牛的 Share 2 產生 Share 1’ , 再送給老牛。老牛收到後用自己的 Share 2 經由 Share 1’ 與 Share 2 疊和後, 眼睛會看影像內容為「Nov. 16, 2021」, 得以分享秘密訊息。 相對地, 老牛傳 “神秘地點” 給老孫也是一樣的概念呢。 過程裡別人霧煞煞的看到傳送亂碼的 Share 1’ 或 Shaire 2’ , 而且每次的時間與地點內含不同, 所傳送的 Share 1’ 或 Shaire 2’ 也跟著變變變呢。然這倆哥們可是心照不宣彼此完全解密的, 每次開心自在地辦 私人 home party (轟趴)呢。



Charming Eyes 一旦融入我們的資安生活, 文學殿堂的靈魂之窗也得昇華為科技資安神守護, 多了項頭銜讓我們安心放心享受資安生活。這是多變豐富，有趣、耐人尋味、各種驚訝形容詞下的多媒體，資訊時代。你該也從沒想過原來我們的 Eyes 除了「放電」也會「計算」，在眨眼間「計算」(解密）出正確的訊息，看到什麼，寫出什麼，判讀出什麼, 輸入系統裡, 呵呵瞬間 decode it。

資安生活的時代，我們透過電腦、手機也節省了我們許多繁瑣的工作程序，想當然，電腦、手機也儲存了個資、帳號、密碼、個是生活理財的重要資訊在其中。這些都是為了減輕我們記憶負擔，科技裡竟也成為我們最是重視的好朋友，「不離不棄」，二十四小時守著手機、等著「他」/「她」，堪稱情人等級的待遇。呵，好友一旦變臉，遭到入侵，帳號密碼盜用下那麼瞬間所有秘密將全部曝光。 是否也喚起我們內心最深層的思維，還是天然的最好, 我們與生俱來身體，形體裡自然而迷人的 Eyes 是最好的朋友，永遠貼身近隨著你，永遠不會被「盜用」(入侵)，也將是最值得信賴的守護神。視覺安全在資訊科技裡可真是讓我們看到科技再發達，終究還是回到我們人類身上的眼「神守護」，才得最是「資安」的「自」在與「資安」的「安」心, 原來資安裡已有著科技蘊涵「人」、「機」、「心」相互融入合一的精髓了。