東海科學第二卷：43–53
89 年 7 月

應用視覺式秘密分享的安全線上交談軟體之製作

林祝興*　李正隆*　簡睿成*

摘　要

由於網際網路的蓬勃發展帶動了電子商務，創造了無限的商機，但是接連不斷的駭客攻擊事件卻暴露了網路的不安全性，使得各項資訊安全相關的研究受到相當的重視。本文將針對視覺式秘密分享(Visual Secret Sharing Scheme, VSSS)作一探討，並針對視覺式秘密分享應用於網路上的方法做檢討與改進，並將視覺式秘密分享應用於一安全的線上交談軟體之中，我們利用視覺式秘密分享來做此線上交談軟體的遠端認證，為了效益的考量，我們用 RSA[4][5]對使用者與伺服器間的認證作加密，並採用 RC6[6]演算法對使用者與使用者間所傳遞的訊息作加密。

關鍵詞：RSA，RC6，視覺式秘密分享，線上交談，遠端認證。

簡　介

在各種的加密的系統中都會面臨到一個相同的問題，就是金鑰的保存，通常金鑰有幾種被保存的方法，第一個方法是將金鑰存放在安全的地方，只有被允許的人可以取得金鑰，但如果發生什麼意外導致這把唯一的金鑰受到毀損，將會使資料無法再使用；第二個方法是記在腦海中，但要是記這個金鑰的人有一天忘記了，那這個金鑰是否就永遠消失了呢？第三種則是將金鑰複製多份存放在不同的地方，但是這樣一來金鑰被盜用的可能性就增加了。由於網路實際的需要，以及上述這些方法的不夠安全，因此在 1979 年，Shamir[1] 和 Blackly[2]提出了秘密分享這個概念。

秘密分享可以把一個秘密拆解成數個子秘密，當需要取得秘密的時候，則必須擁有一定數量的子秘密才能解出秘密，當子秘密的數量低於一個門檻時，將無法輕易的解出秘

* 東海大學資訊科學系

密。而在現實世界中有許多祕密分享應用的實際例子，Time Magazine[3]就曾舉出過一個類似的例子，俄羅斯控制核子武器就是採用“two-out-of-three”的機制，也就是一個(2,3) Threshold Secret Sharing Scheme，他們將啟動核子武器的鑰匙分為三份，一份給總統、一份給國防部長，最後一份給參謀總長，當這三個人中的兩人同意提供他們所擁有的鑰匙來啟動核子武器時，方可啟動，若是只有一個人想啟動核子武器，是無法達成目的的。

而視覺式秘密分享就是因循此觀念發展出來的一個直覺且易懂的方法，它是將一張有意義的圖片拆解成數張無意義的子圖，當我們將達到門檻數量的子圖作疊合時，便可以運用人眼的視覺特性直接解讀。

而在視覺式秘密分享的應用方面也有學者提出在網際網路上應用的方法[7][9]，其主要應用就是作為網路上的遠端認證。在本文中，我們針對視覺式秘密分享的應用方法進行討論，並加以改善，此外也提出了一種安全的線上交談方法，它就是利用視覺式秘密分享的概念來做使用者的身分驗證。另外，我們也將所提出的方法，以軟體實際來實作。

本文在第貳節中將會介紹視覺式秘密分享技術及其應用，第參節則詳述我們針對視覺式秘密分享在網際網路應用上所做的改良，第肆節則是將我們所設計的交談軟體的安全架構做一介紹，最後做一結論。

視覺式秘密分享(Visual Secret Sharing Scheme)及其應用

一、 視覺式秘密分享的概念：

Shamir 和 Noar[8]兩位學者在 EUROCRYPT ’94 的會議中提出了視覺式秘密分享的技術，以下便針對視覺式秘密分享做一簡單介紹。

假設一張 binary 的黑白影像，要將它做(k,n) Threshold 的視覺式祕密分享處理，首先將原影像中的每一個像素(pixel)S 擴充為 m 個子像素(subpixel)，並以 S’來表示，m 為一完全平方數，這些子像素亦是非黑即白的緊鄰在一起。我們將這張影像分成 n 張投影片，將來若是將這些投影片重疊在一起，並以 Boolean 值表示子像素，黑點為 true，白點為 false，重疊等於是將每個單位 S’的 m 個子像素做 or 運算，只要投影片中有一張 S’的某個子像素為黑，重疊後該子像素即為黑。

以下舉一 2 out of 2 Scheme 的例子：

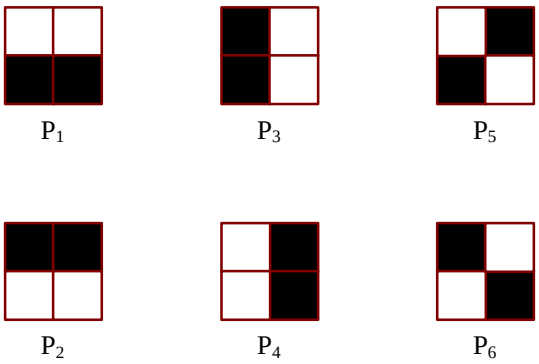

圖 1: 六種可能的像素組合

如上圖所示，一個 2 out of 2 Scheme，將原始影像資料分散於兩張圖中，我們以四個子像素的集合來表示原始圖的一個像素，當原始圖像素為黑時，我們可以拆成(P_1 & P_2)或(P_3 & P_4)或(P_5 & P_6)的組合，若是原始圖像素為白者，可任選兩者重疊後有三個子像素為黑者即可。舉例如下圖：

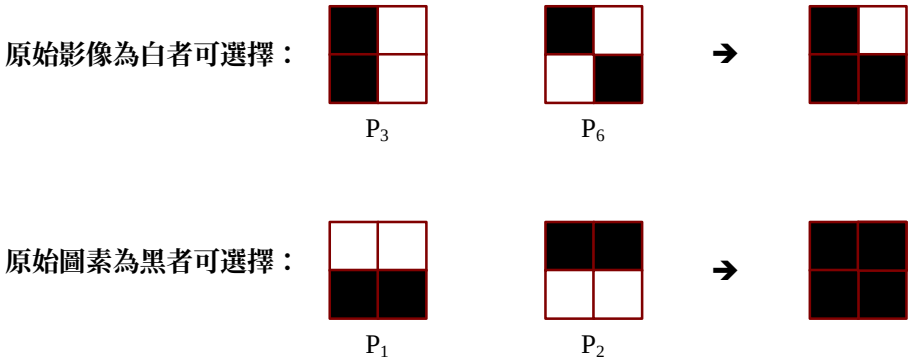

圖 2：黑點與白點的表示方法

就上例來說，當達到所謂的門檻(Threshold)，也就是 2 張投影片時，如果原始影像中 S 為黑色的像素，則所對應的單位 S'的 m 個子像素有 4 個為黑色，我們定義其 Hamming Weight = 4；相對的，其餘應為白色的像素其 Hamming Weight = 3，如此人類眼睛視覺的特性會把 Hamming Weight = 4 和 Hamming Weight ＝3 的單位區分出來。

假設要達成一個 k out of n 的視覺式祕密分享，首先要訂出所要用的編碼書(codebook)來，利用兩個 n × m 的 Boolean 陣列 C_0、C_1 來表示，每一列都代表一個子像素的集合，如前文所舉的例子，利用四個子像素來表示原來的一個圖素，那麼 m 就是 4，因此每一列都代表了一種子像素的黑白排列情形，黑點為 true，白點為 false，當某個原始的圖素為白時，就從 C_0 中找一列來代表此像素，若是原始像素為黑者，就由 C_1 中選一列來代表，如此使得當投影片數量小於門檻(Threshold) k 時，其 Hamming Weight 每一點皆為相同，只有等於門檻(Threshold) k 時才會顯現出各點不同的差異，舉例來說，若是一個 3 out of 3 的 Scheme 就可以如下表示：

$$C_0 = \begin{pmatrix} 0011 \\ 0101 \\ 0110 \end{pmatrix} \qquad C_1 = \begin{pmatrix} 1100 \\ 1010 \\ 1001 \end{pmatrix}$$

由上例可以發現，若三張投影片皆由 C_0 中選擇，則四個子像素中只會有三個為黑，但若是三張中有任一張由 C_1 中選擇，那麼三張疊合時該點四個子像素皆為黑，因此就造成了人眼視覺上的區別了。

二、 視覺式祕密分享的應用：

Noar 和 Pikas 兩位學者在 CRYPTO ’97 會議中提出了視覺式祕密分享的相關應用[7]，在 1998 年，葉育斌先生在論文中也提出了有關視覺式祕密分享在網際網路上應用的方法[9]，而其主要應用就是在於網路上的遠端認證，它是利用 2 out of 2 Scheme 來達成。以下就以一個伺服器與使用者間的登入過程作為一個例子：

步驟 1：首先使用者向伺服器註冊，伺服器會利用視覺式祕密分享的方法產生一張圖像，我們稱之為母圖，然後將此圖儲存下來，再複製一份並透過安全的管道送給使用者。

步驟 2：當使用者要登入伺服器時先輸入帳號並傳給伺服器，當伺服器收到該帳號後，確認該帳號是否存在伺服器的資料庫中，如果沒有則傳回一拒絕登入的訊息，如果有就產生一 5 位數的亂數，再從資料庫中找出屬於該使用者的視覺式祕密分享的母圖，此時伺服器會根據母圖和亂數利用視覺式祕密分享的演算法產生一張子圖，再將子圖傳給使用者。

步驟 3：使用者收到子圖後與母圖做疊合即可透過肉眼就看到 5 位數的密碼，將

此密碼傳回給伺服器。

步驟 4：伺服器根據傳送回來的密碼的正確與否來決定是否提供服務給使用者。

視覺式秘密分享在網際網路應用上的改良

由上一節所介紹的視覺式秘密分享再網際網路上的應用可以看出來，使用者登入一個遠端的系統時並不需要去記憶任何密碼，因為每次登入的密碼都是由伺服器所產生的亂數，這樣雖然提高了密碼的安全性，但是隨著登入次數的增加，產生的子圖越來越多，母圖被破解的機會也相對提高，因此，Noar 和 Pinkas 在論文中[7]提出了一個 Many-times Method，但是這個方法有次數上的限制，而且所使用的母圖面積也隨著要使用的次數而增大，因此本文中提出了另一個改良的方法。

我們所提出的方法基本概念就是讓母圖每次被使用過就會更新成一張與之前完全不同的圖，做法如下：

在伺服器產生母圖的同時也產生一把金鑰，然後將金鑰和母圖一起傳給使用者，之後母圖每被使用一次後就利用金鑰做更新，接著再利用虛擬亂數產生器(Pseudo-Random-Number Generator, PRNG)並以金鑰作為種子，產生新的金鑰，而如何用金鑰將母圖更新的詳細過程如下所述。

我們的遠端認證是利用 2 out of 2 Scheme，其中母圖的大小為 r ×c 個像素(pixel)，而每一個像素有 4 個子像素(subpixel)，每一個像素都是圖 1 其中的一個，我們以下面的矩陣來表示：

P_1=[0011] P_2=[1100] P_3=[1010] P_4=[0101] P_5=[0110] P_6=[1001]

而我們所產生的金鑰長度為(4 ×c) bits，也就是和母圖每一列的長度一樣，利用這把金鑰與母圖的第一列做 XOR，接著將金鑰做一排列(Key Permutation)，再與下一列做 XOR，金鑰再度經過排列後與下一列做 XOR，以此規則處理到最後一列，其過程如圖 3 所示；由於母圖與金鑰做 XOR 後的像素並不一定會落在 P_1 ~P_6 之中，可能是 0111 或 1101 等，因此我們將第一個出現不屬於 P_1 ~P_6 中的像素以 P_1 代替，第二個不屬於 P_1 ~P_6 中的像素以 P_2 代替，以此類推，因此第 50 個出現不屬於 P_1 ~P_6 中的像素以 P_2 代替。

在安全性方面，當破密者運用 Know-plaintext attack，蒐集了大量的子圖，並且知道

其中所隱藏的訊息時，仍然很難將母圖解出，因為我們運用虛擬亂數產生器(PRNG)所產生的金鑰使得每一次所使用的母圖都完全不同，因此每一個母圖都只能透過一組子圖和其中隱藏的訊息來破解；此外，在我們變換母圖的過程中將可能出現的 16 種像素對應到 P_1 ~P_6 等六個像素，所以當破密者破解得出連續兩組母圖時也無法得出正確的金鑰，這樣一來破解的難度自然也就相當的高。

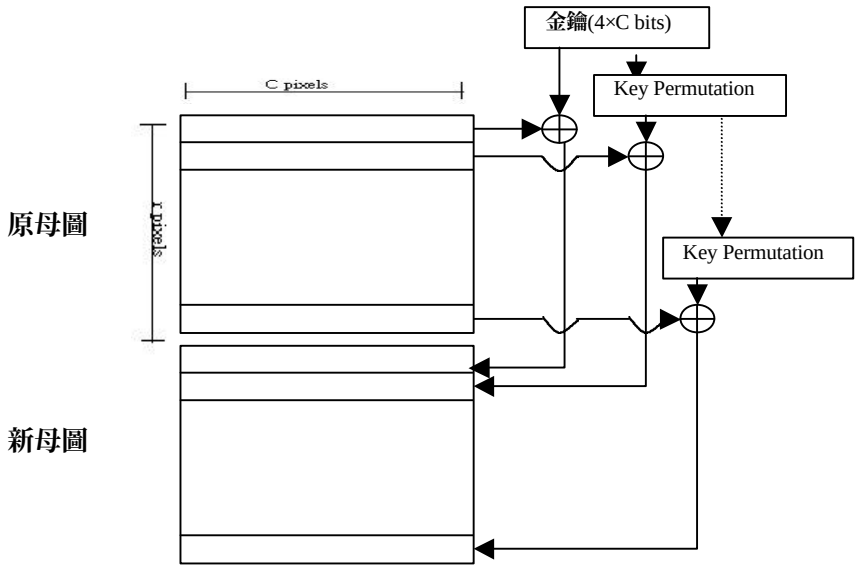

圖 3：利用金鑰將母圖改變

安全線上交談軟體之架構

利用第二和第三節所提供的方法，我們發展一套安全線上交談軟體系統。而其架構主要分為四個部分，註冊、登入、尋找與新增好友、傳送訊息等。為了簡便說明起見，我們僅示範一部份程式畫面如圖 8 所示，假設該次所登入密碼為 075364。我們的系統使用 RSA[4][5]公開金鑰加密演算法加密使用者與伺服器之間所傳送的資料，並以 RC6[6]私密金鑰加密演算法加密各個使用者間所傳送的訊息。以下就 4 個子系統，分別說明其運作步驟。

一、 註冊：(概念如圖 4、使用 RSA 加密演算法)

步驟 1：使用者傳送一註冊訊息至伺服器。

步驟 2：伺服器回傳一把伺服器的公開金鑰給使用者。

步驟 3：使用者使用伺服器的公開金鑰加密註冊的資料，連同使用者本身的公開金鑰傳送至伺服器。

步驟 4：伺服器將註冊資料解密，並確認資料的完整性後允許使用者的註冊後在資料庫建立使用者的資料。

步驟 5：伺服器利用視覺式秘密分享產生一張母圖和一把用來更新母圖的金鑰，並儲存在伺服器端，然後複製一份母圖和金鑰並使用使用者註冊時所傳來的公開金鑰加密後傳回給使用者。

步驟 6：使用者將收到的資料予以解密得到圖像與金鑰，並將之儲存下來。

二、 登入：(概念如圖 5)

步驟 1：使用者將帳號傳送至伺服器。

步驟 2：伺服器收到使用者帳號後搜尋資料庫看看是否有該使用者的註冊資料，如果沒有，則傳送一"使用者帳號錯誤"之訊息給使用者，如果找到，則先亂數產生一組 6 位數字，再從伺服器的資料庫中找到屬於該使用者的視覺式秘密分享的圖像，再依之前產生之數字與此圖像產生與該圖像相對應之子圖，再將此圖傳送給使用者。

步驟 3：使用者收到該圖之後與自己的圖像重疊，可以看到一組 6 位數的密碼，再將此密碼連同帳號一起傳送到伺服器。

步驟 4：伺服器收到帳號與密碼後再加以對照，若符合則允許該使用者登入使用各項資源，若不符，則回傳一錯誤訊息，再從步驟 1 開始。

步驟 5：使用者成功登入伺服器後，雙方都使用更新母圖的金鑰將母圖予以更新，並將此金鑰作為虛擬亂數產生器(PRNG)的種子，產生新的金鑰。

三、 尋找與新增好友：(概念如圖 6)

步驟 1：使用者 A 傳送欲尋找之好友的相關資料給伺服器。

步驟 2：伺服器依照傳送過來的資料在資料庫中搜尋與資料相符的使用者 B，然後將搜尋的結果回傳給使用者 A。

步驟 3：使用者 A 收到搜尋結果後會將結果列出，使用者可以點選其中一個要求與其成為好友，此時使用者會送出一個要求成為好友的訊息給被另一

方，如果同意的話則由伺服器使用 RC6[6]的演算法產生交談金鑰並分別傳送給使用者 A 和使用者 B，A 和 B 收到金鑰後將金鑰保存於電腦中，並將對方加入自己的好友名單中，以後兩方便可以使用該金鑰秘密通訊。

四、 傳送訊息：(概念如圖 7)

步驟 1：使用者在資料庫中找出要傳送訊息對象所使用的交談金鑰，並將要傳送的訊息用此金鑰加密在傳送出去。

步驟 2：使用者收到加密的訊息後，從資料庫找出與傳訊者之交談金鑰將訊息解

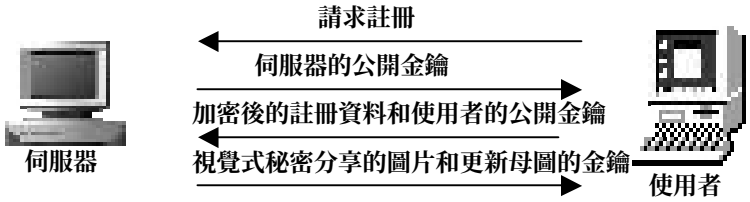

圖 4：註冊

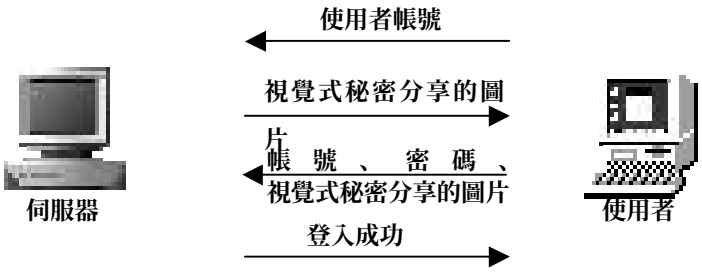

圖 5：登入

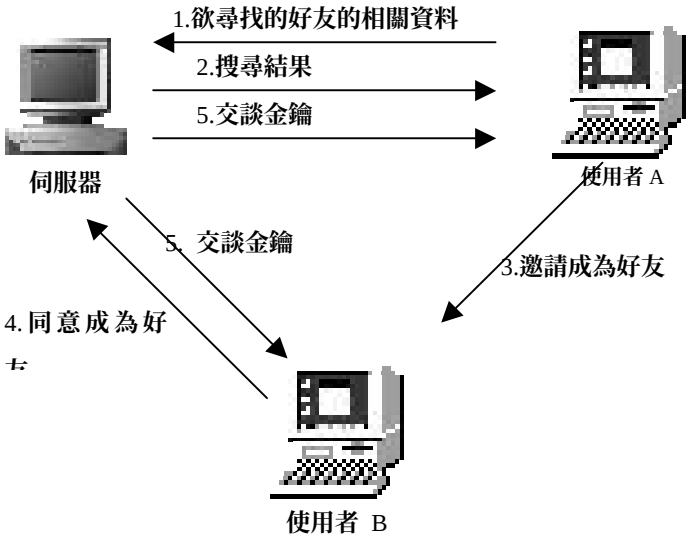

圖 6：新增好友

密。

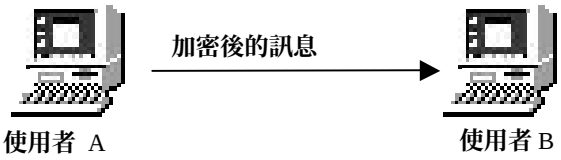

圖 7：傳送訊息

圖 8：程式主畫面

結　論

透過視覺式秘密分享的技術來做遠端認證的最大特點就是使用者只需要用眼睛來做解密的動作，而且使用者並不需要擔心密碼會在網路上傳送的過程中被竊取，因為每次登入所使用的密碼都不同，而本文中我們所提出的方法讓每次使用的圖都完全不同，更加提高了密碼的安全性，但是還有一點是我們要考慮的，就是伺服器的負擔，因為當每個使用者登入時，伺服器就要產生一張視覺式秘密分享的圖像，因此我們要盡可能的在不影響安全性的前提下減少所要產生圖像的大小。

*本論文已投稿第一屆管理學域學術研討會

參考文獻

[1] Shamir, A. (1979) "How to Share a Secret," *Communication of the ACM* 22, pp. 612-613.

[2] Blackly, G.R. (1979) "Safeguarding Cryptographic Keys," *AFIPS Conference Proceedings* 48, pp. 313-317.

[3] *Time Magazine*, May 4, 1992, p. 13.

[4] Rivest, R.L., Shamir, A., and Adleman, L.M (1978) "A Method for Obtaining Digital Signatures and Public-Key Cryptosystem," *Communications of the ACM* 21(2), pp.120-126.

[5] Rivest, R.L., Shamir, A. and Adleman, L.M. (1979) "On Digital Signatures and Public Key Cryptosystems," MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212.

[6] Rivest, R., Robshaw, M.J.B., Sidney, R., and Yin, Y.L. "The RC6 Block Cipher," http://theory.lcs.mit.edu/~rivest/rc6.pdf

[7] Naor, M., and Pinkas, B. (1997) "Visual Authentication and Identification," *Advanced in Cryptology-Crypto '97*, pp. 322-336.

[8] Naor, M., and Shamir, A. (1995) "Visual Cryptography," *Advances in Cryptology-EUROCRYPT '94*, Lecture Notes in Computer Science, Springer-Verlag, pp. 1-12.

[9] 葉育斌 (1998) 視覺式秘密分享在網路安全上之應用與實現。成功大學資訊工程研究所碩士論文。

[10] 黃仁俊 (1998) 機密共享技術之設計與應用。中正大學資訊工程研究所博士論文。

Secure Chat Software Based on Visual Secret Sharing

C. H. Lin* C. L. Lee * R. C. Jien*

Abstract

The rapid growth of the Internet brings infinite possibility of the electronic business. But the increasingly frequent attacking events reveal the Internet was insecure. Therefore, people pay much attention to various researches of information security. In this paper, we will discuss the algorithm of Visual Secret Sharing Scheme (VSSS). We will then probe and improve the application of Visual Secret Sharing Scheme in the Internet, and we apply VSSS in the authentication of a secure chat software. For the consideration of the efficiency, we use RSA in the authentication protocol and use RC6 in the communication between users.

Keywords: RSA, RC6, Visual Secret Sharing, conversation on line, remote authentication.

* Department of Computer and Information Sciences, Tunghai University, Taichung 407, TAIWAN.

Email: chlin@mail.thu.edu.tw