行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※
※　　　　　　　　　　　　　　　　　　　　　　　※
※　　　　　　**視覺化密碼之研究及其應用**　　　　　　※
※　　　　　　　　　　　　　　　　　　　　　　　※
※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：　**個別型計畫**　　**□整合型計畫**
計畫編號：NSC　89－2213－E－009－016
執行期間：　88 **年**　8 **月**　1 **日至**　89 **年**　7 **月**　31 **日**

計畫主持人：陳玲慧　教授
共同主持人：

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

執行單位：

中　華　民　國　八十九　年　九　月　十一　日

行政院國家科學委員會專題研究計畫成果報告

視覺化密碼之研究及其應用

A Study on Visual Cryptography and Its Applications

計畫編號：NSC 89-2213-E-009-016

執行期限：88 年 8 月 1 日至 89 年 7 月 31 日

主持人：陳玲慧　　國立交通大學 資訊科學研究所

一、中文摘要

視覺化密碼是一種利用人類的視覺系統進行解碼的密碼技術。其主要目的為保護機密訊息，機密訊息可為文字、數字、符號或圖形，而且解碼的過程不需要電腦以及任何密碼知識的支援，非常簡單。它先將機密訊息轉換成數張不同的二元值黑白圖片，解碼時只要將數張或全部圖片對齊相疊，利用人類的視覺系統就可解出機密訊息。本計畫已提出一種視覺化密碼的方法，不但可保護秘密訊息，且儲存秘密訊息的容量較其他方法加倍。另外，本計畫亦提出兩種進行訊息驗證的方法。此方法是以上述視覺化密碼方法為基礎，用人類的視覺系統就可得知所得訊息有無受到非法篡改。最後，本計畫已提出一種進行身份識別的方法，此方法也是利用上述的視覺化密碼的方法為基礎，再利用人類視覺系統來確認使用者的身份。

關鍵詞：視覺化密碼、人類視覺系統、視覺驗證、視覺識別

Abstract

Visual cryptography is a technique that uses human visual system to decode the secret message, which can be text, number, symbol or image. It represents the secret message by several different binary images, and when parts or all of these binary images are aligned and stacked together, the secret message will be revealed by human visual system without using computers or any knowledge about cryptography. In this project, we proposed a visual cryptograph scheme. The size of the concealed data by the proposed scheme can be double that through the existing schemes. Moreover, we proposed two schemes for visual authentication based on the proposed visual cryptograph scheme. These two schemes can detect the alteration through human visual system if the received message is changed by an adversary. At last, we also proposed a method for visual identification. The scheme is also based on the proposed visual cryptography scheme, and we can prove the identity of the user through human visual system.

Keywords: Visual cryptography, human visual system, visual authentication, visual identification

二、緣由與目的

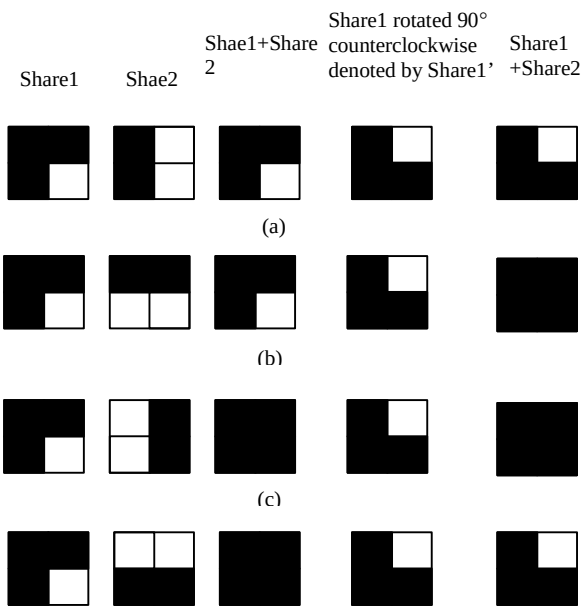
為了解決傳統密碼方法計算繁複以及需要大量的資料量的缺點，Naor 與 Shamir [6] 提出了一

個新的密碼方法，視覺化密碼 (Visual Cryptography)。它利用了人類的視覺系統來進行資訊加密以及解密的工作。完全不需要任何的計算及密碼學知識。這個方法最基本的模型是這樣的：機密訊息由 printed page of ciphertext 與 printed transparency 兩張影像所組成，而 printed transparency 相當於秘密金鑰。而這兩張影像中，單獨的一張均看不出任何的機密訊息。必須將兩張對齊重疊在一起，方可看出所隱藏的訊息。此模型稱為 2 out of 2 視覺秘密分享法。

然而，除了資訊的加密以外，訊息認證 Authentication[5]與身份確認 Identification[14]在目前的資料傳輸上也相當地重要。有關這兩項的相關協定，也在不同的假設下被廣泛地研究著。也因此，Naor 及 Pinkas[11] 基於視覺密碼的方式對於 authentication 及 identification 各提出了一個新的方法。這方法可以適用於任何的文字或影像。

然而，由 Naor 與 Shamir 所提出的視覺化密碼方法於每一次加密時僅僅只能隱藏一張圖形或文字，所加密的資料量相當地少。所以，在本計畫中我們已提出一個基於 2 out of 2 的視覺密碼方法所建構出來的系統。這個方法可以比 Naor 及 Shamir 的方法多隱藏一倍的資訊。之後，我們也定義 visual authentication 的模型及基於我們所提出的視覺密碼方法所發展出來的兩種 authentication 方法。

三、結果與討論



在這一個段落中，我們將介紹利用我們所發展出來新的視覺化密碼的方法所做的實驗結果，以及將我們的視覺化密碼方法應用到視覺驗證的一

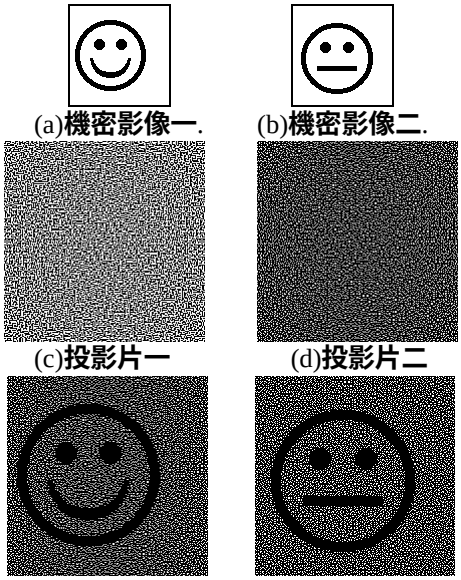
(f)將旋轉後的
(c)重疊之後
結果

些實驗結果。

圖一是我們所提出的方法，利用三點與兩點黑點的變化，我們可以將 share 旋轉，以增加所隱藏的資料量。

圖一、我們所提出的 2 out of 2 視覺化密碼

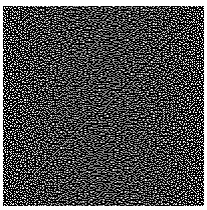
首先是利用我們方法的實驗結果。圖二(a)與(b)是兩張尺寸大小為 100×100 個像素的機密影像。而圖二(c)與(d)則是利用我們所提出之視覺化密碼方法所建構出來之影像。將圖二(c)與(d)對其重疊之後，我們便可以得到圖二(e)之影像。接著，我們將圖二(c)逆時鐘旋轉九十度角並且將其對齊後重疊在圖二(d)上面，我們便可以得到圖二(f)之影像。



圖二、基於我們所提出方法的實驗結果

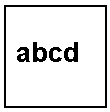
接著，我們將展示利用我們所提出之視覺化密碼方法應用於驗證的實驗結果。首先會介紹可用一次(one-time method)的視覺驗證方法，接著介紹可用多次(many-times method)的視覺驗證方法。

為了作視覺驗證，首先接收者與通知者事先都要擁有相同的一張投影片 P，如圖三所示。

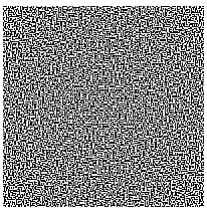


圖三　投影片 P

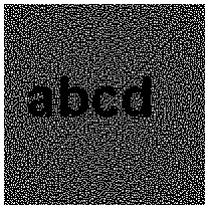
現在我們所要傳遞的訊息為 abcd(如圖四(a)所示)。現在則利用我們所提出的方法以及投影片 P 將機密訊息藏入之後，產生投影片 C(圖四(b))。而當接收者收到投影片 C 時，將兩張重疊後可以先看到機密訊息 abcd(圖四(c))，之後再將 C 做逆時針旋轉九十度後再重疊(圖四(d))。如果出現全黑的圖形，表示機密訊息並沒有遭受竄改，若否，表示機密訊息有遭受竄改的可能。



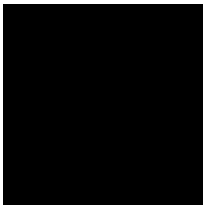
(a)　機密訊息"abcd."



(b)　投影片 C



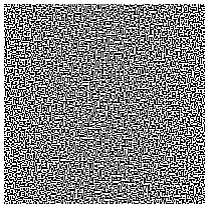
(c)　重疊投影片 C 與 P 之結果



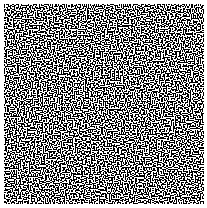
(d)　旋轉投影片 C 後與 P 重疊之結果

圖四、可用一次(one-time)視覺驗證的實例

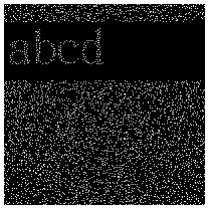
以下接著介紹另外一個多次視覺驗證方法(many-times method)的實驗結果。首先，將欲隱藏的機密訊息縮小成 30 ×100 的大小，藉著改變隱藏資訊位置的不同，我們可以將先前一次驗證的方法的安全性提高。圖五(a)及(b)兩張投影片分別將資訊隱藏於不同的位置，藉由和投影片 P 重疊便可以得到機密資訊(圖五(c) 與 (e))；之後再分別將之逆時鐘旋轉九十度後再次重疊，藉由檢查先前出現訊息的位置是否為全黑來作為資訊是否遭到竄改的根據(圖五(d) 與 (f))。若是該區域並非全黑的區域，則該機密資訊有遭到竄改的嫌疑。



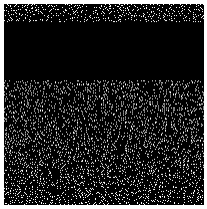
(a)　投影片 C1



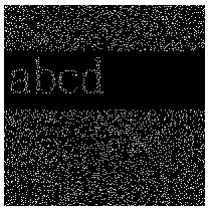
(b)　投影片 C2



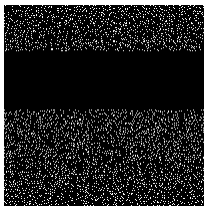
(c)　重疊投影片 C1 與 P 之結果



(d)　旋轉投影片 C1 後與 P 重疊之結果



(e)　重疊投影片 C2 與 P 之結果



(f)　旋轉投影片 C2 後與 P 重疊之結果

圖五、可用多次(many-times)之視覺驗證之實例

在優缺點的討論上面，我們所提出的方法比先前 Naor 與 Shamir 所提出的方法可以隱藏多一倍的資料量，不過在對比上面的效果並不算很好。另外基於我們的方法所建構出來的視覺驗證方法在驗證的過程上不需要大量的計算，只需要經由人類視覺系統便可以以輕易地達到視覺驗證的目的。

四、計畫成果自評

這一個計畫於執行期間的進度與工作目標與當初所提出的計畫內容大致吻合，不論是視覺編碼

以及解碼器及其餘相關的覺驗證與覺識別的編碼解碼器都相繼完成。於資訊驗證相關的應用領域有：可將機密訊息加密、確認資訊所有權及安全性。於資訊識別相關的應用領域有：銀行郵局的密碼識別系統、門禁出入系統、及相關使用者身分確認之應用。學術價值上可供碩博士發表論文之用。

五、參考文獻

[1] NBS FIPS PUB 46, "Data Encryption Standard," National Bureau of Standards, U.S. Department of Commerce, Jan. 1977.

[2] R. M. Davis, "The Data Encryption Standard in Perspective", Computer Security and the Data Encryption Standard, National Bureau of Standards Special Publication, Feb, 1978.

[3] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, Vol. 21, No. 2, pp. 120-126, Feb. 1978

[4] X. Lai and J. Massey, "A proposal for a new block encryption standard", Proceeding of EUROCRYPT' 90, pp. 389-404.

[5] G. Simmons, "A survey of information authentication", in Contemporary Cryptography-The Science of Information Integrity, IEEE Press, pp. 379-419, 1991.

[6] M. Naor and A. Shamir, "Visual Cryptography", Advances in Cryptology: Eurocrypt'94, Lecture Notes in Computer Science Vol. 950, pp.1-12, 1995.

[7] Dr. Stinson, "An Introduction to Visual cryptography", presented at Public Key Solutions '97, http://bibd.unl.edu/~stinson/VCS-PKS.ps.

[8] G. Ateniese, C. Blundo, A. De Santis and Dr. Stinson, "Visual cryptography for general access structures, Information and Computation Vol. 129, pp. 86-106, 1996.

[9] C. Blundo, A De Santis and Dr. Stinson, "On the contrast in visual cryptography schemes", ftp://theory.lcs.mit.edu/pub/tcryptol/96-13.ps.

[10] M. Naor and A. Shamir, "Visual cryptography II: improving the contrast via the cover base", ftp://theory.lcs.mit.edu/pub/tcryptol/96-07.ps.

[11] M. Naor and B. Pinkas, "Visual Authentication and Identification", Advances in Cryptology, CRYPTO' 97, Lecture Notes in Computer Science, Vol. 1294, pp. 322-336, 1997

[12] G. R. Blakley, "Safeguarding cryptographic keys", Proceedings of the National Computer Conference, American Federation of Information Processing Societies Proceedings, Vol. 48, pp. 313-317, 1979

[13] A. Shamir, "How to share a secret", Communications of the ACM, Vol. 22, pp. 612-613, 1979.

[14] R. Rivest, Class notes of lecture 9 in Computer and Network Security, http://www.theory.lcs.mit.edu/~rosario/6.915/lecture9.ps

[15] K. Kobara and H. Imai, "Limiting the Visible Space Visual Secret Sharing Schemes and Their Application to Human Identification", Advances in Cryptology, ASIACRYPT' 96, Lecture Notes in Computer Science, Vol. 1163, pp. 185-195, 1996.