改良分享影像於視覺化密碼之研究

沈友硯、陳文儉,吳昭明

E-mail: 9606935@mail.dyu.edu.tw

摘 要

視覺化密碼（Visual Cryptography）在1994 年由M.Naor 與 A.Shamir 所提出，是一種將機密影像（Secret Image）加密，得出 兩張或數張的分享影像（Share Image），再利用人類的視覺系統進 行解碼的密碼學技術。機密影像可為文字、數字、符號或圖片等， 而且在解密的過程中，是不需要任何密碼學的知識及複雜的計算。 傳統的視覺化密碼，所產生出的每張分享影像的尺寸（Size）都是 一樣大的，傳送的資料量（Data quantity）及儲存空間（Storage space） 就等於兩張或數張分享影像的大小。 本研究以M.Naor 和A.Shamir （1994）所提的方法為基礎並 將L.H.Chen 和C.C.Wu （1998）所提出加大機密影像容量的方法 與觀念做進一步改變。首先，機密影像經過視覺化密碼加密後，產 生出兩張分享影像，其中一張的大小與傳統方法相同，是整張的； 而另一張則是之前那張分享影像的1/4。在解碼時，只要將1/4 張 的分享影像重疊在整張分享影像的四個角落，即可分別解出機密影 像的1/4。此一方法除了可以保護機密影像之外，其中一張分享影 像尺寸只有原先的1/4，相較於傳統視覺化密碼產生兩張整張的分 享影像，本研究所產生出來的分享影像只需要1.25 張，故傳送資 料量及儲存空間比傳統視覺化密碼還要更少。此外，還可將一個或 兩個以上的機密影像藏入同一組分享影像中。

關鍵詞 : 視覺化密碼，機密影像，分享影像

目錄

參考文獻

[1] N. Naor and A. Shamir,“ Visual cryptography, advances in cryptography ”, Eurocrypt ’ 94, Lecture Note in Computer Science Springer-Verlag, Perugia, Italy, pp.1-12, 1994.

[2] Ateniese, G., C. Blundo, A. De Santis, and D. R. Stinson,“ Extended Schemes for Visual Cryptography ”, Theoretical Computer Science, 1996.

[3] L.H. Chen, C.C. Wu,“ A Study on Visual Cryptography ”, Master thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[4] C.S. Tsai, C.C. Chang, and T.S. Chen,“ Sharing multiple secrets in digital images ”, Journal of Systems and Software, Vol. 64, pp. 163-170, 2002.

[5] H.C. Wu, C.C. Chang,“ Sharing visual multi-secrets using circle shares ”, Computer Standards & Interfaces, Vol. 28, 2005, pp. 123-135, 2005.

[6] A. Houmansadr, S. Ghaemmaghami.“ A Novel Video Watermarking Method Using Visual Cryptography ”, Engineering of Intelligent Systems, 2006 IEEE International Conference on Publication Date: 22-23 April 2006. pp. 1-5, 2006.

[7] Hyoung Joong Kim, Yongsoo Choi, ”A New Visual Cryptography Using Natural Images“ , Circuits and Systems, ISCAS 2005. IEEE International Symposium on 23-26 May 2005 pp. 5537-5540, Vol. 6. 2005.

[8] D.j. Wang, L.G. Jiang, G.R. Feng,“ Novel blind non-additive robust watermarking using 1-D chaotic map ”, Acoustics, Speech, and Signal Processing, 2004. Proceedings. （ICASSP '04）. IEEE International Conference on Publication Date: 17-21 May 2004 Volume: 3, pp. iii- 417-20 vol.3, 2004.

[9] Wong P., Memon N.,“ Secret and public key image watermarking schemes for image authentication and ownership verification ”, IEEE Transactions on Image Processing, 2001, pp. 1593-1601, 2001.

[10] Chang, C. C., Chuang, J. C. and Lin, P. Y.,“ Sharing a Secret Two-Tone Image in Two Gray-Level Images ”, Proceedings of The First International Workshop on Security in Networks and Distributed Systems, pp. 300-304, Jul. 2005.

[11] Hou, Y. C., Chang, Chao-Yuan, and Tu, S. F. （2001.07），“ Visual Cryptography for Color Images Based on Halftone Technology ”, Proceedings of SCI 2001/ISAS 2001, Vol. XIII, Orlando, Florida. pp. 441-445, 2001.
[12] C. C. Lin, W. H. Tsai, “ Visual cryptography for gray-level images by dithering techniques ”, Pattern Recognition Letters Vol. 24, pp. 349-358, 2003.
[13] W.-Q. Yan, D. Jin, and M. S. Kankanhalli, “ Visual cryptography for print and scan applications ”, Circuits and Systems, 2004. ISCAS '04. Proceedings of the 2004 International Symposium, vol. 5, pp. 572-575, 2004.