Tradeoff between Share Size and Security in Visual Cryptography for Mobile Devices

Shyong-Jian Shyu* and Jia-Ru Tsai

Department of Computer and Information Engineering,
Ming Chung University,
Guei Shan, Taoyuan 33348, Taiwan, R. O. C.
sjsyu@mail.mcu.edu.tw

Received 5 January 2011; 15 February 2011; Accepted 25 March 2011

Abstract. Visual cryptography proposed by Naor and Shamir in 1995 encrypts a secret among several shares and decrypts the secret by observing the stacked shares using human visual system. This simple yet powerful mechanism for sharing images can be effectively applied on the mobile devices due to the popularity, portability and simple computation ability. When transferring the shares via local networks, especially among mobile devices using Bluetooth, a share with a smaller size is preferred in order to reduce the cost of transmission and the threat of being intercepted. Based on a random elementary block, we propose two simple algorithms to shorten the size of one share and examine the resultant degradation in the security. The tradeoff between them enriches the applications of visual cryptography in mobile devices.

Keywords: Visual cryptography, visual secret sharing scheme, share size, security analysis, mobile device

References

[1] M. Naor and A. Shamir, "Visual Cryptography", in *Proceedings of Workshop on the Theory and Application of Cryptographic Techniques*, Italy, Perugia, Vol. 950, pp.1-12, 1995.

[2] Y.C. Hou, "Visual Cryptography for Color Images," *Pattern Recognition*, Vol. 36, No. 7, pp. 1619-1629, 2003.

[3] D. Jin, W.Q. Yan, M.S. Kankanhalli, "Progressive Color Visual Cryptography," *Journal of Electronic Imaging*, Vol. 14, No. 3, pp. 033019, 2005.

[4] S.J. Shyu, "Efficient Visual Secret Sharing Scheme for Color Images," *Pattern Recognition*, Vol. 39, pp. 866-880, 2006.

[5] H. Yamamoto, Y. Hayasaki, N. Nishida, "Securing Information Display by Use of Visual Cryptography," *Optics Letters,* Vol. 28, pp. 1564–1566, 2003.

[6] H. Yamamoto, Y. Hayasaki, N. Nishida, "Secure Information Display by Use of Multiple Decoding Masks," in *Proceedings of* SPIE 5600, pp. 192-199, 2004.

[7] S. Droste, "New Results on Visual Cryptography," in *Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, Vol. 1109, pp. 401-415, 1996.

[8] G. Ateniese, C. Blundo, A. De Santis, D. R. Stinson, "Visual Cryptography for General Access Structures," *Information and Computation*, Vol. 129, No. 2, pp. 86-106, 1996.

[9] W.P. Fang and J.C. Lin, "Progressive Viewing and Sharing of Sensitive Images," *Pattern Recognition Image Analysis*, Vol. 16, No. 4, pp. 632-636, 2006.

[10] R.Z. Wang, "Region Incrementing Visual Cryptography," *IEEE Signal Processing Letters*, Vol. 16, pp. 659-662, 2009.

[11] S.J. Shyu, Y.L. Huang, C.C. Chuang, A.F Lai, "Visual Authentication on Mobile Devices", in *Proceedings of the 2009 National Computer Symposium*, pp. 346-353, 2009.

[12] C. Hegde, S. Manu, P. D. Shenoy, K. R. Venugopal, L. M. Patnaik, "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications", in *Proceedings of the IEEE 16th International Conference on Advanced Computing and Communications*, pp. 65-72, 2008.

* Correspondence author

[13] M. Naor and B. Pinkas, “Visual Authentication and Identification”, in *Proceedings of the 17th Annual International Cryptology Conference Santa Barbara, California*, Vol. 1294, pp. 322–336, USA, California, 1997.