Share Authentication based Cheating Prevention in Naor-Shamir's Visual Cryptography

Yu-Chi Chen[1,*] , Gwoboa Horng[1], and Du-Shiau Tsai[2]

[1] Department of Computer Science and Engineering,
National Chung Hsing University,
Taichung 40227, Taiwan, ROC
{s9756034, gbhorng}@cs.nchu.edu.tw

[2] Department of Information and Networking Technology,
Hsiuping Institute of Technology,
Taichung 41280, Taiwan, ROC
dstsai@hit.edu.tw

Received 12 January 2011; 10 February 2011; Accepted 21 March 2011

Abstract. Visual cryptography (VC), first proposed by Naor and Shamir, is a variant of secret sharing with many applications, such as providing secure services in communications. In 2006, Horng et al. showed that VC is vulnerable to cheating attacks. They also presented two approaches to prevent cheating, namely share authentication and blind authentication. In this paper, we review some share authentication based cheating prevention schemes and propose a new one for Noar-Shamir's (*2*, *n*)-VC.

Keywords: Secret sharing, visual cryptography, cheating, cheating prevention, share authentication

References

[1] M. Naor and A. Shamir, "Visual Cryptography," in *Proceedings of Advances in Cryptology-EUROCRYPT 94*, LNCS 950, pp. 1-12, 1994.

[2] A. Shamir, "How to Share a Secret," *Communications of the ACM*, Vol. 22, No. 11, pp. 612-613, 1979.

[3] 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.

[4] C. Blundo, A. D. Santis, M. Naor, "Visual Cryptography for Grey Level Images," *Information Processing Letters*, Vol. 75, No.6, pp. 255-259, 2000.

[5] C. Blundo, P. D'Arco, A. De Santis, D. R. Stinson, "Contrast Optimal Threshold Visual Cryptography Schemes," *SIAM Journal on Discrete Mathematics*, Vol. 16, No. 2, pp. 224-261, 2003.

[6] C.C. Chang and J.C. Chuang, "An Image Intellectual Property Protection Scheme for Gray-level Image Using Visual Secret Sharing Strategy," *Pattern Recognition Letters*, Vol. 23, No. 8, pp. 931-941, 2002.

[7] C.C. Chang, C.C. Lin, T.H.N. Le, H.B. Le, "Self-Verifying Visual Secret Sharing Using Error Diffusion and Interpolation Techniques," *IEEE Transactions on Information Forensics and Security*, Vol. 4, No. 4, pp. 790-801, 2009.

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

[9] C.C. Lin and W.H. Tsai, "Visual Cryptography for Gray-level Images by Dithering Techniques," *Pattern Recognition Letters*, Vol. 24, No. 1-3, pp. 349-358, 2003.

*Correspondence author

[10] F. Liu, C. Wu, X. Lin, "Cheating Immune Visual Cryptography Scheme," *IET Information Security*, Vol. 5, No. 1, pp. 51-59, 2011.

[11] M. Naor and B. Pinkas, "Visual Authentication and Identification," in *Proceedings of Advances in Cryptology-CRYPTO 97*, LNCS 1294, pp. 322-336, 1997.

[12] V. Rijmen and B. Preneel, "Efficient Color Visual Encryption for Shared Colors of Benetton," in *Proceedings of Eurocrypto'96, Rump Session, Berlin*, 1996.

[13] C.C. Wang, S.C. Tai, C.S. Yu, "Repeating Image Watermarking Technique by the Visual Cryptography," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E83-A, No. 8, pp. 1589-1598, 2000.

[14] M. Tompa and H. Woll, "How to Share a Secret with Cheaters," *Journal of Cryptology*, Vol. 1, No. 3, pp. 133-138, 1989.

[15] G. Horng, T.H. Chen, D.S. Tsai, "Cheating in Visual Cryptography," *Designs, Codes and Cryptography*, Vol. 38, No. 2, pp. 219-236, 2006.

[16] T. Rabin, "Robust Sharing of Secrets when the Dealer is Honest or Cheating," *Journal of the ACM*, Vol. 41, No. 6, pp. 1089-1109, 1994.

[17] R. De Prisco and A. De Santis, "Cheating Immune Threshold Visual Secret Sharing," *The Computer Journal*, Vol. 53, No. 9, pp. 1485-1496, 2010.

[18] C.M. Hu and W.G. Tzeng, "Cheating Prevention in Visual Cryptography," *IEEE Transactions on Image Processing*, Vol. 16, No. 1, pp. 36-45, 2007.

[19] D.S. Tsai, T.H. Chen, G. Horng, "A Cheating Prevention Scheme for Binary Visual Cryptography with Homogeneous Secret Images," *Pattern Recognition*, Vol. 40, No. 8, pp. 2356-2366, 2007.

[20] S. Cimato and C.N. Yang, *Visual Cryptography and Secret Image Sharing*, CRC press, 2011.