An Efficient Authentication Mechanism for (2, 2)-Visual Cryptography Scheme

Yi-Hui Chen*

Department of Applied Informatics and Multimedia,
Asia University,
Taichung 413, Taiwan, ROC
chenyh@asia.edu.tw

Received 15 May 2011; Revised 15 July 2011; Accepted 25 September 2011

Abstract. Visual cryptography (VC) is often used in secret communications between two different sides. The benefit of visual cryptography is that the decryption procedure is without any computations. In the past schemes, they focused on the quality of decoded images and the problem of pixel expansion, but rarely concerned on the authentication issue. The authentication mechanism can be used to verify whether the decrypted image is valid. This paper proposed two authentication mechanisms, namely Scheme-1 and Scheme-2, for (2, 2)-visual secret sharing (VSS) with pixel expansion and that with no pixel expansion, respectively. The experiments provide the positive data to confirm the feasibility of the proposed schemes.

Keywords: Visual cryptography, visual secret sharing, authentication

References

[1] A. Shamir, "How to Share A Secret," *Communications of the Association for Computing Machinery*, Vol. 22, No. 11, pp. 612-613. 1979.

[2] M. Naor and A. Shamir, "Visual Cryptography," in *Proceedings of Eurocrypto'94*, Springer-Verlag, Berlin, pp. 1-12, 1995.

[3] C. Blundo, A. De Satis, M. Naor, "Visual Cryptography for Grey Level Images," *Information Processing Letters*, Vol. 75, No. 3, pp. 255-259, 2000.

[4] M. Iwamoto and H. Yamamoto, "The Optimal N-out-of-n Visual Secret Sharing Scheme for Grey-scale Images," *IEICE Transactions on Fundamentals of Electronics*, Vol. E85-A, No. 10, pp. 2238-2247, 2002.

[5] I. Muecke, "Greyscale and Color Visual Cryptography," *master's thesis*, *department of computer science*, *Dalhouse University*, 1999.

[6] R. Ito, H. Kuwakado, H. Tanaka, "Image Size Invariant Visual Cryptography," *IEICE Transactions on Fundamentals of Electronics*, Vol. E82-A, NO. 10, pp. 2172-2177, 1999.

[7] C.N. Yang, "New Visual Secret Sharing Schemes Using Probabilistic Method," *Pattern Recognition Letters*, Vol. 25, No. 4, pp. 481-494, 2004.

[8] C.S. Hsu, S.F. Tu, Y.C. Hou, "An Optimization Model for Visual Cryptography Schemes with Unexpanded Shares," in *Proceedings of Foundations of Intelligent Systems, 16th International Symposium*, Springer-Verlag, Berlin, pp. 58-67, 2006.

[9] C.N. Yang and T.S. Chen, "Visual Secret Sharing Scheme: Prioritizing the Secret Pixels with Different Pixel Expansions to Enhance the Image Contrast," *Optical Engineering*, Vol. 46, No. 9, pp. 097005-1-097005-19, 2007.

*Correspondence author

[10] D.S. Wang, L. Zhang, N. Ma, X. Li, "Two Secret Sharing Schemes Based on Boolean Operations," *Pattern Recognition*, Vol. 40, No. 5, pp. 2776-2785, 2007.

[11] C.C. Chang, C.C. Lin, T. H. N. Le, H. B. Le, "A New Probabilistic Visual Secret Sharing Scheme for Color Images," in *Proceedings of Fourth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, Harbin, China, pp. 1305-1308, 2008.

[12] C.C. Chang, C.C. Lin, T. H. N. Le, H. B. Le, "A Probabilistic Visual Secret Sharing Scheme for Gray-scale Images with Voting Strategy," *International Journal of Intelligent Information Technology Application*, Vol. 1, No. 1, pp. 1-9, 2008.

[13] M. Ulutas, V. V. Nabiyev, G. Ulutas, "A PVSS Scheme Based on Boolean Operations with Improved Contrast," *International Conference on Network and Service Security*, Paris, pp. 1-5, 2009.

[14] Y.F. Chen, Y.K. Chan, C.C. Huang, "A Multiple-level Visual Secret-sharing Scheme Without Image Size Expansion," *Information Sciences*, Vol. 117, No. 6, pp. 4696-4710, 2007.

[15] D.S. Tsai, G. Horng, T.H. Chen, Y.T. Huang, "A Novel Secret Image Sharing Scheme for True Color Images with Size Constraint," *Information Sciences*, Vol. 179, No. 1, pp. 866-880, 2009.