Safeguarding Visual Information using (*t*, *n*) Verifiable Secret Shares

Chin-Chen Chang[1,2,*], Chia-Chen Lin[3], and Huynh Ngoc Tu[1]

[1] Department of Information Engineering and Computer Science,
Feng Chia University,
Taichung 407, Taiwan
ngoctu84vn@gmail.com

[2] Department of Computer Science and Information Engineering,
National Chung Cheng University,
Chiayi 621, Taiwan
ccc@cs.ccu.edu.tw

[3] Department of Computer Science and Information Management,
Providence University,
Taichung 43301, Taiwan
mhlin3@pu.edu.tw

Received 11 January 2011; Revised 15 April 2011; Accepted 15 June 2011

Abstract. In this paper, we propose a new (t, n) threshold visual secret sharing scheme which is suitable for grayscale images and for color images. The proposed scheme achieves the following objectives. First, it satisfies the four general criteria of visual secret sharing systems: security, accuracy, shadow size and computation cost. Second, it ensures the reliability of verification procedures compared with existing verifiable secret sharing schemes. Moreover, the scheme can reconstruct the secret image exactly. Finally, the computational complexity of our proposed scheme is much less than required with other previous schemes. Therefore, our proposed scheme is suitable for real-time applications.

Keywords: Visual secret sharing, visual cryptography

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] G.R. Blakley, "Safeguarding Cryptographic Keys," in *Proceedings of the National Computer Conference, American Federation of Information Processing Societies*, pp. 313-317, 1979.

[3] George Blakley, http://en.wikipedia.org/wiki/George_Blakley

[4] M. Naor and A. Shamir, "Visual Cryptography," *Lecture Notes in Computer Science*, Vol. 950, pp. 1-12, 1995.

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

[6] C.C. Thien and J.C. Lin, "Secret Image Sharing," *Computers and Graphics*, Vol. 26, pp. 765-770, 2002.

[7] R.Z. Wang and C.H. Su, "Secret Image Sharing with Smaller Shadow Images," *Pattern Recognition Letters*, Vol. 27, No. 6, pp. 551-555, 2006.

[8] Y.S. Wu, C.C. Thien, J.C. Lin, "Sharing and Hiding Secret Images with Size Constraint," *Pattern Recognition*, Vol. 37, No. 7, pp. 1377-1385, 2004.

*Correspondence author

[9] Y.F. Chen, Y.K. Chan, C.C. Huang, C.C. Tsai, Y.P. Chu, "A Multiple-Level Visual Secret-Sharing Scheme without Image Size Expansion," *Information Sciences*, Vol. 177, No. 21, pp. 4696-4710, 2007.

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

[11] D.T. 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. 19, pp. 3247-3254, 2009.

[12] Y.Y. Lin and R.Z. Wang, "Scalable Secret Image Sharing with Smaller Images," *IEEE Signal Processing Letters*, Vol. 17, No. 3, pp. 316-319, 2010.

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

[14] S. Cimato, R. D. Prisco, A. D. Santis, "Probabilistic Visual Cryptography Schemes," *The Computer Journal*, Vol. 49, No. 1, pp. 97-107, 2006.

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

[16] R. D. Prisco and A. D. Santis, "Cheating Immune (2, *n*)-Threshold Visual Secret Sharing," in *Proceedings of Security and Cryptography for Networks*, Vol. 4116, pp. 216-228, 2006.

[17] 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.

[18] C.C. Chang, Y.P. Hsieh, C.H. Lin, "Sharing Secrets in Stego Images with Authentication," *Pattern Recognition*, Vol. 41, No. 10, pp. 3130-3137, 2008.

[19] C.N. Yang, T.S. Chen, K.H. Yu, C.C. Wang, "Improvements of Image Sharing with Steganography and Authentication," *Journal of Systems and Software*, Vol. 80, No. 7, pp.1070-1076, 2007.

[20] R. Zhao, J.J. Zhao, F. Dai, F.Q. Zhao, "A New Image Secret Sharing Scheme to Identify Cheaters," *Computer Standards and Interfaces*, Vol. 31, No.1, pp. 252-257, 2009.

[21] C.C. Chang, C.C Lin, T.H.N. Le, H.B. Le, "Sharing a Verifiable Secret Image Using Two Shadows," *Pattern Recognition*, Vol. 42, No. 11, pp. 3097-3114, 2009.

[22] Shiozaki, "Digital Half-Toning by Error Diffusion with Perturbation," *Electronics Letters*, Vol. 32, No. 18, pp. 1655-1656, 1996.

[23] K.L. Chung and S.T. Wu, "Inverse Halftoning Algorithm Using Edge-Based Lookup Table Approach," *IEEE Transactions on Image Processing*, Vol. 14, No. 10, pp. 1583-1589, 2005.

[24] G. Voyatzis and I. Pitas, "Applications of Toral Automorphisms in Image Watermarking," in *Proceedings of the IEEE International Conference on Image Processing*, Lausanne, Switzerland, Vol. 2, pp. 237-240, 1996.

[25] G. Matthew, K. Bruce, Z. George: "Visualizing Toral Automorphisms," *The Mathematical Intelligencer*, Vol. 15, No. 1, pp.63-66, 2003.

[26] H.S. Kwoka and W.K.S. Tang, "A Fast Image Encryption System Based on Chaotic Maps with Finite Precision Representation," *Chaos, Solitons and Fractals*, Vol. 32, No. 4, pp. 1518-1529, 2007.