Novel Non-expanded Visual Cryptography Scheme with Block Encoding

Yi-Jing Huang[1, *], Chih-Chiang Lee[2], Hsien-Chu Wu[3], Jun-Dong Chang[4], Chwei-Shyong Tsai[1],
and Ya-Ting Tsao[3]

[1] Department of Information Management,

National Chung Hsing University,

Taichung 402, Taiwan

`yjhang1221@gmail.com;tsaics@nchu.edu.tw`

[2] Information and Communication Research Laboratories,

Industrial Technology Research Institute,

Chutung Hsinchu 310, Taiwan

`ccianglee@itri.org.tw`

[3] Graduate School of Computer Science and Information Technology,

National Taichung Institute of Technology,

Taichung 404, Taiwan

`wuhc@ntit.edu.tw, winds2012@gmail.com`

[4] Department of Computer Science and Information Engeineering,

National Chung Hsing University,

Taichung 402, Taiwan

`phd9607@cs.nchu.edu.tw`

Abstract. In the traditional visual cryptography, secret pixels are expanded to cause the size of the recovered image is larger than the original one. Although many researches successfully solve expansion problem, the quality of the recovered image is not better. In order to improve quality of reconstruction, this paper proposes a novel non- expansion scheme. The principle of the proposed scheme is to divide the secret image into a number of blocks in the first place and then each block generates a number of combinations of share blocks by using same color pixels. After generating combinations of share blocks, two pixels with a corresponding position are executed by the "OR" operation when stacking two share images. In spite of solving the expansion problem and increasing the clearly visible of the recovered image, the result of the proposed scheme tends towards dark. In order to increase contrast of the recovered image, the second scheme is proposed by modifying original secret blocks before dividing the secret image into blocks, and then the further processes are in common as the first scheme. From the experimental results, the image quality of the second scheme is clearer than the first scheme.

Keywords: Visual cryptography, non expanded, block encoding

References

[1] M. Naor and A. Shamir, "Visual Cryptography," *Advances in Cryptology: Eurocrypt'94, Lecture Notes In Computer Science, Springer Verlag,* Germany, Vol. 950, pp. 1-12, 1995.

[2] 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.

[3] D. R. Stinson, "Decomposition Constructions for Secret-sharing Schemes," *IEEE Transactions on Information Theory*, Vol. 40, No. 1, pp. 118-125, 1994.

＊Correspondence author

[4] O. Kafri and E. Keren, "Encryption of Pictures and Shapes by Random Grids," *Optics Letters*, Vol. 12, No. 6, pp. 377-379, 1987.

[5] C.H. Lin, "Visual Cryptography for Color Image with Image Size Invariable Shares," MS Thesis, National Central University, Taiwan, 2002.

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

[7] Y.F. Chen, Y.K. Chan, C.C Huang, M.H. 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.

[8] 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.

[9] R.W. Floyd and L. Steinberg, "An Adaptive Algorithm for Spatial Grayscale," in *Proceedings of the Society for Information Display*, Vol. 17, No. 2, pp. 75-77, 1976.