Cryptology ePrint Archive: Report 2011/340

Encrypting More Information in Visual Cryptography Scheme

Feng Liu, Peng Li, ChuanKun Wu

Abstract: The visual cryptography scheme (VCS) is a scheme which encodes a secret image into several shares, and only qualified sets of shares can recover the secret image visually, other sets of shares cannot get any information about the content of the secret image. From the point of view of encrypting (carrying) the secret information, the traditional VCS is not an efficient method. The amount of the information that a VCS encrypts depends on the amount of secret pixels. And because of the restrictions of the human eyes and the pixel expansion and the alignment problem of the VCS, a VCS perhaps can only be used to encrypt a small secret image. VCS requires a random number generator to guide the generation of the shares. As we will show in this paper, the random input of VCS can ba seen as a subchannel which helps carrying more secret information. We propose a general method to increase the amount of secret information that a threshold VCS can encrypt by treating the pseudo-random inputs of the VCS as a subchannel, i.e. the Encrypting More Information Visual Cryptography Scheme (EMIVCS). We also study the bandwidth of the proposed EMIVCS. The disadvantage of the proposed scheme is that, the decoding process is computer aided. However, compared with other computer aided VCS, the proposed scheme is more efficient.

Available formats: PDF | BibTeX Citation

Version: 20110627:075208 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]