Abstract

Visual cryptography is a new secure technology that distributes a secret image by separating it into a number of shares using different visual cryptography schemes (VCS). Early VCS schemes mainly focused on black-and-white secret images. Using a black & white VCS normally degrade the image quality and also suffered from a major drawback of pixel expansion, which means that the size of each secret share is several times larger than that of the original image. The black & white VCS were extended to the colour VCS. The main problem with the colour VCS is larger pixel expansion when number of colours increases. So in order to avoid these drawbacks a scheme called Black&White-Colour Visual Cryptography Scheme (B&W-C VCS) is used here. This scheme exploits the colour model to split a b & w image into coloured shares using a smaller pixel expansion and improved contrast. For any of
the VCS, the main issue to be considered is authentication, i.e., there are no means by which one can ensure that the secret recovered is genuine. It would be advantageous to check the fidelity of the shares before they are used to reconstruct the secret. For this purpose, this paper proposes a watermark method to authenticate coloured shares thereby ensuring a successful secret recovery. Unlike other watermarking techniques, the pattern is not directly embedded into the share, but an authentication matrix is generated which checks the authenticity of the shares before they are used for secret recovery.

Referen
ences

- Mahmoud A Hassan and Mohammed A Khalili, "Self Watermarking based on
Visual Cryptography; Proceedings of World Academy of Science, Engineering and Technology 8:159-162, October 2005.


Index Terms

Computer Science

Security

Keywords

Secret Sharing

Visual Cryptography

Threshold Schemes

B&w Secret Images

Color Shares

watermarking